Ausgewählte Chancen und Herausforderungen der digitalen Transformation für die Produktentwicklung und Unternehmens-organisation im Finanzdienstleistungssektor

Von der Wirtschaftswissenschaftlichen Fakultät der
Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des akademischen Grades

Doktorin der Wirtschaftswissenschaften
– Doctor rerum politicarum –

Dr. rer. pol.

genehmigte Dissertation

von

Master of Science Theresa Eden
geboren am 02. April 1995 in Bremen

2023

Referent: Prof. Dr. Johann-Matthias Graf von der Schulenburg

Korreferent: Prof. Dr. Michael H. Breitner

Tag der Promotion: 21.07.2023

Zusammenfassung

Vor dem Hintergrund der digitalen Transformation sind Finanzdienstleistungsunternehmen auf unterschiedlichen Ebenen zahlreichen Chancen sowie Herausforderungen ausgesetzt. Während der Einsatz neuer Technologien die Optimierung bestehender Geschäftsprozesse sowie das Angebot digitalisierter Finanzdienstleistungen ermöglicht, geht dies zugleich mit veränderten Arbeitsbedingungen innerhalb der Unternehmensorganisation einher. Darüber hinaus sind Finanzdienstleister dazu angehalten die sich ändernden Kundenerwartungen bei den bisherigen Geschäftsaktivitäten sowie bei der Produktentwicklung zu berücksichtigen.

Das Ziel der vorliegenden kumulativen Dissertation ist es, bestehende Forschungsdesiderate hinsichtlich der Auswirkungen der digitalen Transformation auf den Finanzdienstleistungssektor, differenziert nach der Kunden- und Produktperspektive sowie der internen Unternehmensperspektive, vertiefend zu analysieren. Das Technology-Organization-Environment (TOE)-Framework von DePietro et al. (1990) wird dabei als theoretischer Rahmen zur Einordnung und Strukturierung der Forschungsmodule verwendet.

Die Ergebnisse der acht Module zeigen, dass die Kundenbedürfnisse und –erwartungen im Finanzdienstleistungssektor verstärkt von der digitalen Transformation beeinflusst werden. Dies zeigt sich in der Beratungstätigkeit bspw. durch das Angebot neuer Kundenkanäle sowie der aus dem steigenden Wettbewerbsdruck resultierenden erhöhten Preistransparenz. Im Rahmen der Produktentwicklung sind zudem u. a. ESG-Risiken und Silent Cyber-Risiken zu beachten. Aus der Analyse der Auswirkungen der digitalen Transformation auf die Unternehmensorganisation geht hervor, dass über den Einsatz digitaler Innovationen innerhalb des Backoffice die Realisation von Effizienzgewinnen sowie das Entgegenwirken eines Personalmangels möglich ist. Darüber hinaus wird in den Modulen der Einfluss des Faktors Mensch auf die Cyber-Sicherheit hervorgehoben. Während dieser einerseits als „schwächstes Glied“ und potenzielles Angriffsziel im Sicherheitskonstrukt der Unternehmen dargestellt wird, ist andererseits das Potenzial der Beschäftigten zur Frühwarnung zu berücksichtigen.

Schlagwörter:
Digitale Transformation, Finanzdienstleistungssektor, Kundenerwartungen, Produktentwicklung, Unternehmensorganisation, TOE-Framework, Qualitative Forschung

Abstract

In the context of digital transformation, financial services companies face numerous opportunities and challenges at various levels. While the use of new technologies makes it possible to optimize existing business processes and offer digitalized financial services, it is also accompanied by changes in working conditions within the company's organization. In addition, financial services companies need to consider changing customer expectations in their current business activities and product development.

This cumulative dissertation aims to analyze existing research gaps regarding the effects of the digital transformation. The contributions are differentiated into the customer and product perspective as well as the internal company perspective. The Technology-Organization-Environment (TOE) framework of DePietro et al. (1990) is used as a theoretical framework to classify and structure the research modules.

The results of the eight modules show that the digital transformation increasingly influences customer requirements and expectations in the financial services sector. This can, for example, be seen in advisory services offering new customer channels and the increased price transparency with the resulting intensified competitive pressure. In the context of product development, ESG risks and silent cyber risks, among others, must also be addressed. The analysis of the impact of digital transformation on the company organization shows that the use of digital innovations within the back office facilitates efficiency gains and can alleviate staff shortages. In addition, the modules highlight the influence of the human factor on cyber security. While on the one hand, the human factor is presented as the "weakest link" and a potential target for attacks on the security system of companies, on the other hand, the potential of employees for early warning should be considered.

Keywords:
Digital Transformation, Financial Services Sector, Customer Expectations, Product Development, Company Organization, TOE Framework, Qualitative Research

Inhaltsverzeichnis

1 Einleitung und Einordnung der Beiträge

1.1 Motivation und Fragestellungen

Finanzdienstleistungsunternehmen[1] sind im Rahmen ihrer Geschäftstätigkeiten zahlreichen Herausforderungen ausgesetzt. Die Auswirkungen der digitalen Transformation werden dabei bereits seit einigen Jahren aus wissenschaftlicher sowie praxisorientierter Perspektive erforscht (Cziesla, 2014; Bohnert et al., 2019). Auf technologischer, organisationaler und individueller Ebene führt die digitale Transformation innerhalb des Finanzdienstleistungssektors zu unterschiedlichen Chancen sowie auch Herausforderungen (Werth et al., 2020). Der Einsatz neuer Technologien bietet in diesem Zusammenhang die Möglichkeit, bereits bestehende Geschäftsprozesse zu optimieren und digitalisierte Finanzdienstleistungen zur Verfügung zu stellen (Karagiannaki et al., 2017; Keller, 2018), woraus innerhalb des organisationalen Kontextes weiterhin veränderte Arbeitsbedingungen und Anforderungen an die Beschäftigten resultieren (Berghaus und Back, 2016; Groen et al., 2018). Insbesondere aufgrund der sich ändernden Kundenbedürfnisse sind Finanzdienstleistungsunternehmen dazu angehalten, ihre bisherigen Strategien und Geschäftsaktivitäten zu überdenken (Eickhoff et al., 2017). Zum Erwerb von Finanzdienstleistungsprodukten sowie zur Kommunikation mit den Unternehmen wird seitens der Kunden dahingehend verstärkt auf technologiebasierte Ressourcen und Informationsquellen zurückgegriffen (Cziesla, 2014; Leimeister et al., 2014; Niemand et al., 2020). Inwieweit sich dabei technologische Innovationen auf die Beratungstätigkeit im Finanzdienstleistungssektor oder auf das Backoffice von Versicherungsunternehmen auswirken, findet in der Forschung bisher kaum Beachtung. Zudem führt der Wettbewerbsdruck und die zunehmende Regulierung zu einer Steigerung der Komplexität primärer Geschäftstätigkeiten im Finanzdienstleistungssektor (Werth et al., 2020). Hinsichtlich des Regulierungsdrucks stellen bspw. die Vorgaben der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) die Versicherungswirtschaft vor die Herausforderung einer gesetzeskonformen Umsetzung. In der wissenschaftlichen Literatur sind dazu erste Ansätze zur theoretischen Betrachtung vorhanden (Streitz, 2019; Dreher, 2019), wohingegen eine ganzheitliche Analyse der VAIT im Hinblick auf den aktuellen Umsetzungsstand fehlt.

[1] Als Finanzdienstleistungsunternehmen werden in der vorliegenden kumulativen Dissertation Banken und Versicherungen verstanden.

Die aus der wachsenden digitalen Vernetzung hervorgehenden Cyber-Risiken stellen eine weitere Schwierigkeit für die Unternehmen dar. Insgesamt gehören Cyber-Risiken weltweit zu den bedeutendsten Geschäftsrisiken im 21. Jahrhundert (Allianz Global Corporate & Specialty, 2023). Ergänzend zum klassischen Cyber-Risikomanagement bieten Frühwarnsysteme das Potenzial aus Cyber-Angriffen resultierende Schäden zu reduzieren oder bestenfalls zu verhindern (Marotta und McShane, 2018). Während die Relevanz von Risikomanagement-Frameworks für die Informationssicherheit (Disterer, 2015; Petrenko, 2018) sowie die Implementierung von Frühwarnindikatoren für das Management von Vorfällen innerhalb der Informationssicherheit (Bernsmed und Tøndel, 2013) bereits in der Wissenschaft analysiert wurden, sind Frühwarnindikatoren im Bereich der Cyber-Sicherheit bislang wenig erforscht. Darüber hinaus stellt der Faktor Mensch im Rahmen der Cyber-Sicherheit als potenzielles Angriffsziel eine zusätzliche Dimension dar (Von Solms und Van Niekerk, 2013) und sollte innerhalb der Frühwarnung zum bestmöglichen Schutz ebenfalls berücksichtigt werden. Da kein vollständiger Schutz vor Cyber-Angriffen zu erreichen ist, sind Cyber-Versicherungen zum Risikotransfer und zur umfassenden Absicherung der Schadenauswirkungen sinnvoll (Tonn et al., 2019). In diesem Zusammenhang stehen Versicherungsunternehmen jedoch vor der Herausforderung, dass neben Cyber-Versicherungen auch traditionelle Policen aufgrund des fehlenden expliziten Ausschlusses oder unklar formulierter Versicherungsbedingungen Cyber-Schäden unbewusst einbeziehen und somit sogenannte Silent Cyber-Risiken für die Versicherer entstehen (Bank of England Prudential Regulation Authority, 2017; European Insurance and Occupational Pensions Authority, 2022). Wrede et al. (2020) liefern dahingehend bereits einen ersten Überblick zum Umgang mit Silent Cyber-Deckungen in deutschen Versicherungsunternehmen, aber das Pricing und Underwriting von Silent Cyber-Risiken wird in der Forschung bisher nicht analysiert.

Das Ziel der vorliegenden kumulativen Dissertation ist es, u. a. die aufgezeigten Forschungsdesiderate hinsichtlich der Auswirkungen der digitalen Transformation auf die Finanzdienstleistungsbranche, differenziert nach der Kunden- und Produktperspektive sowie der internen Unternehmensperspektive, vertiefend zu analysieren und einen holistischen Überblick zu geben. Zur Strukturierung dessen wird das Technology-Organization-Environment (TOE)-Framework von DePietro et al. (1990) verwendet,

da sowohl die „Technologie“ und „Organisation“ als auch die „Umwelt“ als Einflussfaktoren für die Auswirkungen der digitalen Transformation auf die genannten Perspektiven zu identifizieren sind. Auf der Grundlage von acht Modulen werden folgende zwei Forschungsfragen beantwortet:

Kunden- und Produktperspektive

1. *Welchen Einfluss hat die digitale Transformation auf die Kundenerwartungen und die Produktentwicklung in deutschen Finanzdienstleistungsunternehmen?*

Interne Unternehmensperspektive

2. *Welche Chancen und Herausforderungen resultieren aus der digitalen Transformation für die Unternehmensorganisation?*

1.2 Theoretischer Rahmen

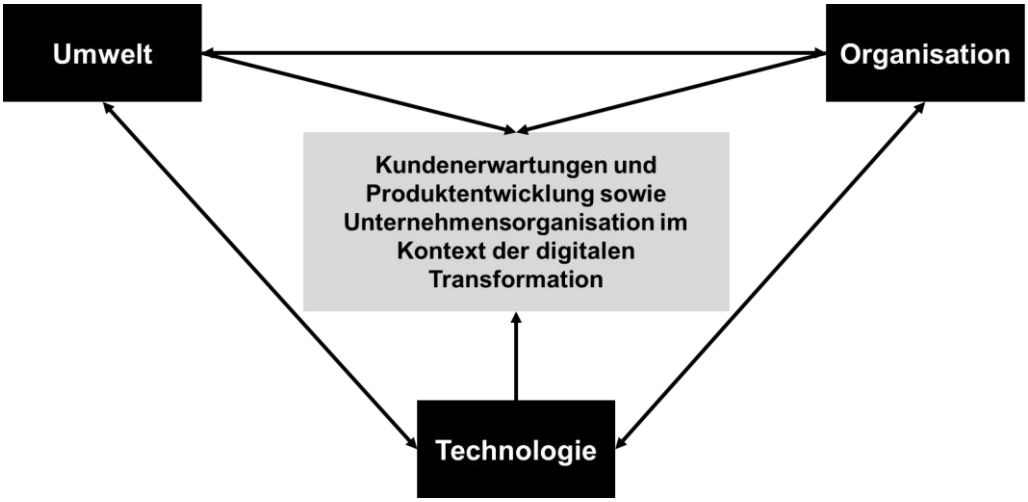
Zur Strukturierung der vorliegenden kumulativen Dissertation dient das TOE-Framework von DePietro et al. (1990) als theoretischer Bezugsrahmen. DePietro et al. (1990) identifizieren die drei Bereiche „Technologie“, „Organisation“ und „Umwelt“ als Einflussfaktoren für die „Entscheidungsfindung bei technologischen Innovationen“ (original: „Technological Innovation Decision Making“). Genannte Faktoren beeinflussen nicht nur die Entscheidungsfindung als solche, sondern stehen zudem selbst in wechselseitigen Wirkungsbeziehungen (DePietro et al., 1990). In der wissenschaftlichen Literatur geben Zhu et al. (2004), Baker (2012) und Chiu et al. (2017) einen Überblick über Studien, die das TOE-Framework für unterschiedliche Kontexte bezüglich variierender Rahmenbedingungen, Anwendungsbereiche und Faktoren anwenden. Die Autoren zeigen, dass unter den drei Bereichen verschiedene Faktoren subsumiert werden können, welche sich in den Studien und je nach Art der Innovation, der Branche und dem kulturellen Hintergrund unterscheiden (Baker, 2012).

Der technologische Kontext beschreibt alle dem Unternehmen zur Verfügung stehenden internen und externen Technologien. Weiterhin umfasst die Technologie neue Hardware und sich ändernde Prozesse. Beispielhafte Faktoren sind interne Informationstechnologie (IT)-Fähigkeiten (hinsichtlich Personal und Ausstattung), relative Vorteile der Technologie (Li et al., 2010), erkannter Nutzen (Iacovou et al., 1995; Chau und Tam, 1997), wahrgenommene Barrieren und wahrgenommene Bedeutung der Einhaltung von Normen sowie Interoperabilität und Interkonnektivität (Chau und Tam,

1997). Ferner werden auch die Technologiekomplexität bzw. Technologiekompatibilität (Borgman, 2013), das Technologierisiko und die Anpassungsfähigkeit an Aufgaben (Rosli et al., 2012) zu den technologischen Faktoren gezählt. Der organisationale Kontext beinhaltet im Rahmen der Eigenschaften und Fähigkeiten eines Unternehmens bspw. die Zufriedenheit mit den bestehenden Systemen, die Komplexität der IT-Infrastruktur (Chau und Tam, 1997), unternehmensinterne Kommunikationsprozesse, die Unterstützung durch das Top-Management (Baker, 2012), die technische Kompetenz der Mitarbeiter (Eden et al., 2022) und finanzielle Ressourcen (Zhu et al., 2004). Der Umweltkontext beschreibt die Rahmenbedingungen außerhalb des Unternehmens, wie z. B. Einflüsse des Marktes. Mögliche Umweltfaktoren sind bspw. Marktunsicherheit (Chau und Tam, 1997) oder allgemeinere Unsicherheit (Li et al., 2010), regulatorisches Umfeld (Zhu et al., 2004; Baker 2012), Wettbewerbsintensität (Zhu et al., 2004), allgemeiner externer Druck (Iacovou et al., 1995) und das Fehlen oder Vorhandensein fachkundiger Mitarbeiter oder Technologiedienstleister (Baker, 2012). Insgesamt beeinflussen sich die drei Bereiche des TOE-Frameworks gegenseitig. Sie sind aber vor allem entscheidend für den Prozess sowie die Ergebnisse der Einführung und Übernahme neuer Technologien (DePietro et al., 1990).

Wenngleich das TOE-Framework im Grundsatz der Analyse von Entscheidungen zur Einführung technologischer Innovationen dient, wird die Theorie in der Literatur gleichermaßen für die Untersuchung der Phase nach der Implementierung (Zhu et al., 2004; Zhu und Kraemer, 2005; Zhu et al., 2006), wie z. B. hinsichtlich geschäftlicher Auswirkungen sowie der Bewertung der Implementierungsentscheidung (Zhu et al., 2004; Baker, 2012), angewendet. Eden et al. (2022) zeigen in Anlehnung daran, dass die technologische Innovation als abhängige Komponente des TOE-Frameworks angepasst und zur Strukturierung der Analyse der Auswirkung dieser verwendet werden kann. Dementsprechend wird das TOE-Framework in der vorliegenden Dissertation zur Strukturierung der einzelnen Module hinsichtlich der Einflüsse der digitalen Transformation auf die Kundenerwartungen und Produktentwicklung sowie Unternehmensorganisation im Finanzdienstleistungssektor herangezogen. Wie in Abbildung 1 dargestellt, wurde dafür die abhängige Variable im Vergleich zum ursprünglichen TOE-Framework („Entscheidungsfindung bei technologischen Innovationen“) nach DePietro et al. (1990) angepasst.

Abbildung 1: Adaptiertes TOE-Framework

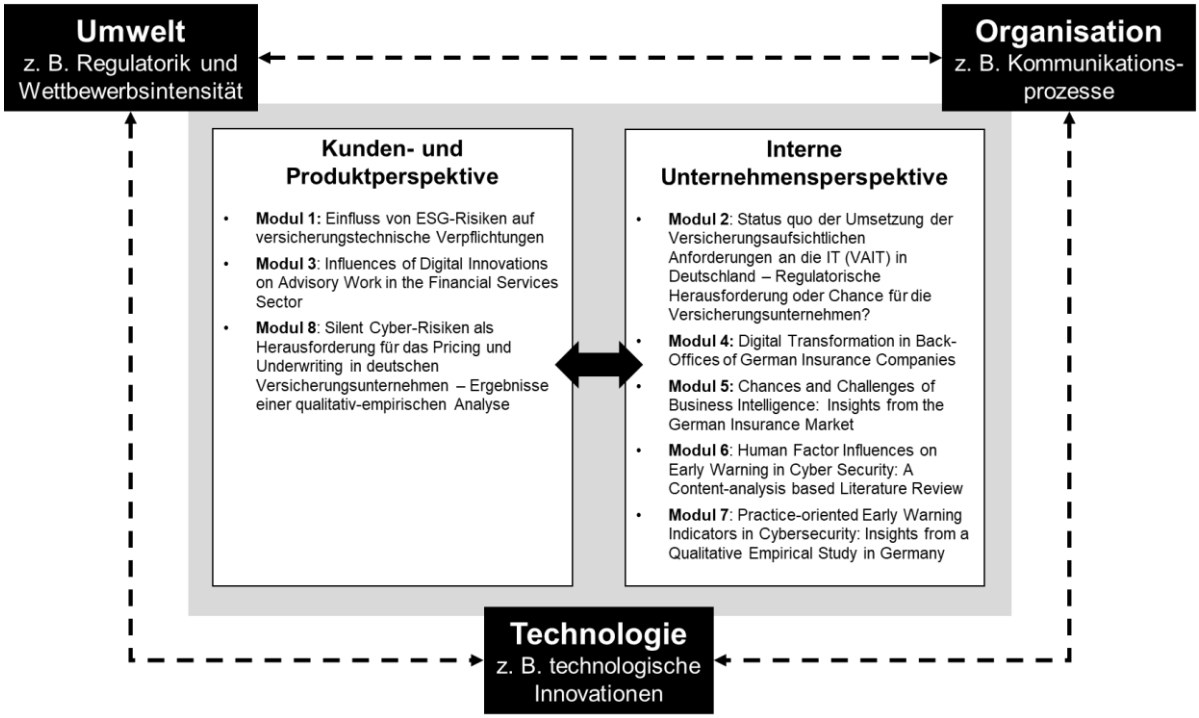


Quelle: Eigene Darstellung in Anlehnung an DePietro et al. (1990).

1.3 Beitrag und Einordnung der Publikationen

Die vorliegende kumulative Dissertation gliedert sich in insgesamt acht Module. Diese acht Module bilden die Auswirkungen der digitalen Transformation auf die Kunden- und Produktperspektive (Modul 1, 3 und 8) sowie die internen Unternehmensperspektive (Modul 2, 4 bis 7) ab, die wiederum von der Technologie, der Organisation sowie der Umwelt beeinflusst werden. Eine Übersicht dessen zeigt Abbildung 2.

Abbildung 2: Einordnung der Module in das TOE-Framework



Quelle: Eigene Darstellung in Anlehnung an DePietro et al. (1990).

In Modul 1 werden die Einflüsse von ESG-Risiken auf versicherungstechnische Verpflichtungen in der Versicherungsbranche untersucht sowie die Herausforderungen der Versicherbarkeit genannter Risiken aus der Praxisperspektive identifiziert. Das Thema Nachhaltigkeit ist für Versicherungsunternehmen zunehmend von Relevanz, woraus sowohl Risiken als auch Chancen resultieren können. Nachhaltigkeit wird in diesem Zusammenhang oftmals entlang der ESG-Kriterien evaluiert, wobei „E“ Environment (Umwelt), „S“ Social (Sozial/Gesellschaft) und „G“ Governance (Unternehmensführung) repräsentieren. ESG-Risiken lassen sich für Versicherungsunternehmen wiederum bspw. in Haftungs-, Reputations-, physische und transitorische Risiken untergliedern. Zur Analyse der Forschungsfrage wurden sowohl eine Online-Umfrage (n=116) als auch eine qualitative Studie in Form von Experteninterviews (n=6) durchgeführt. Die Ergebnisse zeigen, dass insbesondere Umweltrisiken die Versicherungstechnik beeinflussen. Als Grund dafür ist anzuführen, dass im Vergleich zu anderen Nachhaltigkeitsaspekten der Klimawandel in der Regulatorik sowie Öffentlichkeit vermehrt Aufmerksamkeit erhält. Zudem stehen Haftungs-, Reputations-, physische und transitorische Risiken mit dem Klimawandel im Zusammenhang und beeinflussen infolgedessen eine Vielzahl von Versicherungsprodukten. Darüber hinaus konnte gezeigt werden, dass ESG-Risiken insbesondere aufgrund der Versicherbarkeitskriterien der Schätzbarkeit sowie Unabhängigkeit als Herausforderung für die Versicherungsunternehmen angesehen werden. Die Schadenhäufigkeit wurde hingegen als unkritisch evaluiert. Neben den genannten Kriterien der Versicherbarkeit werden zudem physische Risiken infolge ihrer hohen Eintrittswahrscheinlichkeit und transitorische Risiken hinsichtlich ihrer Ungewissheit in den Studienergebnissen als erhebliche Schwierigkeit angesehen. Während Haftungsrisiken in der kurzen Frist als unkritisch bewertet werden, zeigen Klimaklagen, dass sich dies in der längerfristigen Perspektive ändern könnte. Zusammenfassend ist davon auszugehen, dass ESG-Risiken langfristig einen Einfluss auf die Versicherungstechnik haben werden und somit bei der Konzeption von Versicherungsprodukten zu berücksichtigen sind.

Neben den aus ESG-Risiken resultierenden Herausforderungen, welche ebenfalls in der Regulatorik Beachtung finden, sind Versicherungsunternehmen dazu angehalten die Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) zu erfüllen. Der aktuelle Umsetzungsstand sowie die Chancen und Herausforderungen der VAIT werden in Modul 2 vertiefend untersucht. Insgesamt wurden 13 Interviews (n=13) mit

Experten aus dem Versicherungssektor sowie aus Beratungs- und Wirtschafsprüfungsunternehmen durchgeführt und mit der Datenanalysesoftware MAXQDA unter Anwendung der qualitativen Inhaltsanalyse nach Kuckartz (2018) ausgewertet. Aus der Interviewstudie geht hervor, dass innerhalb der Versicherungsunternehmen ein heterogener Umsetzungsstand hinsichtlich der VAIT vorliegt. Grundsätzlich unterliegen die Versicherer nach Meinung der Experten infolge des hohen Umsetzungsaufwandes und der daraus hervorgehenden prozessualen und strukturellen Veränderungen erheblichen Schwierigkeiten. Darüber hinaus besteht bei denjenigen Unternehmen, die bisher keiner Vorprüfung oder Prüfung durch die Bundesanstalt für Finanzdienstleistungsaufsicht unterzogen wurden, die Unsicherheit dahingehend, inwieweit eine gesetzeskonforme Umsetzung der Anforderungen bereits erfolgt ist. Als Chancen werden hingegen die Erhöhung der Informationssicherheit sowie Effizienzgewinne hervorgehoben. Zusammenfassend liefert das Modul 2 einen ersten Überblick zum Umsetzungsstand sowie zu aktuellen versicherungsaufsichtlichen Prüfungsschwerpunkten der VAIT in der Fassung vom 20.03.2019 (Rundschreiben 10/2018).

Im Rahmen der Kunden- und Produktperspektive nimmt der Einfluss digitaler Innovationen auf die Beratungstätigkeit im Finanzdienstleistungssektor einen wesentlichen Stellenwert ein. Das Modul 3 zeigt dabei anhand von zwei Fallstudien die Herausforderungen sowie die Auswirkungen der digitalen Transformation auf die Kundenberatung im Finanzdienstleistungssektor. Insbesondere die sich verändernden Kundenbedürfnisse und der zunehmende Wettbewerbsdruck führen dazu, dass Finanzdienstleister ihre Strategien überdenken und anpassen sollten. Zur Beantwortung der Forschungsfrage hinsichtlich des Einflusses digitaler Innovationen auf die Beratungstätigkeit und den daraus abzuleitenden Implikationen, wurden je eine Fallstudie im Versicherungssektor (InsurCo) und im Bankensektor (BankCo) durchgeführt. In beiden Fällen ist vorhergehend eine neue Technologie im Beratungsprozess implementiert worden. Die Erhebung der Daten erfolgte anhand halbstrukturierter Interviews mit verschiedenen Stakeholdern innerhalb der zwei Transformationsprojekte. Insgesamt wurden sieben (n=7, InsurCo) und zehn (n=10, BankCo) Interviews geführt und mit der Datenanalysesoftware MAXQDA unter Einsatz der Grounded Theory nach Glaser und Strauß (1999) ausgewertet. Als Analyseframework ist ergänzend das TOE-Framework verwendet worden. Die Interviews haben gezeigt, dass in dem Ver-

sicherungsunternehmen ein Beratungs- und Kundenportal eingeführt wurde. Das Unternehmen aus dem Bankensektor hat den Beratungsprozess über die bisherigen Kundenkanäle hingegen mit der Möglichkeit der Videoberatung erweitert. Im technologischen Kontext des Frameworks wurden zur Unterstützung der Beratungsdienstleistungen in beiden untersuchten Fällen neuartige Technologien implementiert, wobei die gewählten Innovationen auf der Übernahme oder der Anpassung bereits bestehender Technologien beruhen. Insgesamt haben diese Technologien grundsätzlich zu Arbeitsveränderungen geführt, die im Vorfeld solcher Implementierungen zu berücksichtigen sind. Die Akzeptanz derartige Veränderungen variierte zwischen InsurCo und BankCo, was im organisationalen Kontext auf die divergente Unternehmensstruktur und –kultur zurückzuführen ist. Darüber hinaus muss auf die regulatorischen Anforderungen sowie die Kundenerwartungen und den Wettbewerbsdruck innerhalb der Umweltkomponente schnell reagiert werden können. Zusammenfassend liefert das Modul 3 sowohl Empfehlungen für Praktiker in Form von 13 Einflussfaktoren, die zur Orientierung bei der Implementierung technologischer Innovationen genutzt werden können als auch theoretische Implikationen für die Beratungstätigkeit entlang des TOE-Frameworks.

Neben den Auswirkungen digitaler Innovationen auf das Frontoffice von Finanzdienstleistungsunternehmen (Modul 3) untersucht das Modul 4 im Kontext der internen Unternehmensperspektive den Einfluss der digitalen Transformation auf das Backoffice von Versicherungsunternehmen. Als Backoffice-Tätigkeiten werden dabei im Wesentlichen das Underwriting sowie die Vertragsverwaltung verstanden. Auch im Rahmen des Backoffice ergeben sich Impulse für die digitale Transformation aus den sich stetig ändernden Kundenanforderungen sowie dem daraus hervorgehenden Wettbewerbsdruck, während regulatorische Anforderungen die Umsetzung dessen oftmals erschweren. In diesem Kontext ergibt sich folgende Forschungsfrage: „Wie wirken sich Projekte zur digitalen Transformation und Modernisierung der Backoffices von Versicherungsunternehmen auf die unternehmensinternen Stakeholder aus und was sind die daraus resultierenden Implikationen?“. Zur Beantwortung der Forschungsfrage wurde die Implementierung neuer Technologien im Backoffice deutscher Versicherungsunternehmen anhand technischer, organisationaler und persönlicher Veränderungen über halbstrukturierte Interviews untersucht. Innerhalb einer multiplen Fallstudie (n=4) konnten zwei Fokusgruppeninterviews mit jeweils zwei Experten (n=2,

Fall 1) sowie weitere 23 Interviews (n=7, Fall 2; n=10, Fall 3; n=6, Fall 4) erhoben werden. Die Analyse der vollständig transkribierten Interviews erfolgte unter Einsatz der Datenanalysesoftware MAXQDA nach der Grounded Theory (Glaser und Strauss, 1999). Zur Strukturierung der Ergebnisse wurde, wie im Modul 3, das TOE-Framework verwendet. Aus den Ergebnissen der qualitativen Studie geht hervor, dass im Rahmen der Fallstudien verschiedene Komponenten der Backoffice-Funktionen digitalisiert bzw. automatisiert wurden. Während sich Fall 1 auf die Preisgestaltung der Verträge fokussiert, wird ferner die Abwicklung der papierbasierten vertragsbezogenen Kommunikation (Fall 2), die Speicherung von Vertragsinformationen (Fall 3) und die automatische Abwicklung einer Vertragskündigung (Fall 4) betrachtet. Hierbei zeigt sich, dass Backoffice-Systeme auf der Technologieebene, wenn möglich, mit Standardsoftware aktualisiert werden. Modernste Technologien werden hingegen umfangreich getestet und mit Vorsicht implementiert. Derartige Umstrukturierungen gehen mit erheblichen Veränderungen einher, welche auf organisationaler Ebene jedoch idealerweise mit einer vertrauensvollen Unternehmenskultur, guter interner Kommunikation sowie umfangreich geschulten Mitarbeitern zu bewältigen sind. Über die Automatisierung von Routinetätigkeiten sollen Effizienzgewinne realisiert und einem Personalmangel entgegengewirkt werden. Ferner zeigt sich in den Fallstudien, dass ergänzend zu den regulatorischen Anforderungen auch der Wettbewerbsdruck erhebliche Auswirkungen hat, was sich u. a. durch die erhöhte Preistransparenz und den Fachkräftemangel in Versicherungsunternehmen zeigt. Zusammenfassend können im Modul 4 zwölf Einflussfaktoren und entsprechende praktische Implikationen für die Auswirkungen der digitalen Transformation auf das Backoffice innerhalb der TOE-Komponenten abgeleitet werden.

Neuartige Analyseverfahren und Visualisierungen bieten neben den bereits aufgeführten digitalen Innovationen für Versicherungsunternehmen ebenfalls die Möglichkeit innerhalb der Unternehmensorganisation neue Geschäftsprozesse zu etablieren, bestehende Geschäftsprozesse zu optimieren und darüber hinaus Kunden zu gewinnen. Eine verbesserte Datenaufbereitung kann dabei über die Nutzung von Business Intelligence (BI) Systemen unterstützt werden. Im organisationalen Kontext bildet BI die Koordinierung und Verwaltung derjenigen Prozesse ab, die sicherstellen, dass Daten aus internen und externen Informationsquellen integriert und analysiert werden. Der technologische Aspekt von BI bezieht sich auf das Identifizieren, Sammeln,

Strukturieren und Abrufen von Informationen aus verschiedenen Datenquellen. Das Modul 5 analysiert die derzeitigen Einsatzpotenziale von BI in Versicherungsunternehmen und evaluiert darüber hinaus die mit der Implementierung und Nutzung resultierenden Chancen und Herausforderungen. Es wurden acht Experten (n=8) aus dem Versicherungssektor in Deutschland befragt und die Auswertung der Interviews erfolgte mit der Datenanalysesoftware MAXQDA auf Grundlage der qualitativen Inhaltsanalyse nach Kuckartz (2018). Die Ergebnisse zeigen, dass Einigkeit unter den Experten dahingehend besteht, dass der Einsatz von BI im internen und externen Reporting die wichtigste Funktion abbildet und einen Vorteil gegenüber den bisherigen Systemen generiert. Für Versicherungsunternehmen stehen in diesem Zusammenhang insbesondere die Analysen von Vertriebspartnern und –kanälen sowie Marktprognosen im Vordergrund. Auch eine optimierte Entscheidungsfindung sowie die damit einhergehende erhöhte Plausibilität und Fundiertheit wurde in der qualitativen Studie hervorgehoben. Die Potenziale von BI werden derzeit in Versicherungsunternehmen jedoch nicht vollumfänglich ausgeschöpft, was nach Meinung der Experten u. a. auf die aus den Datenschutzrichtlinien hervorgehenden Herausforderungen zurückzuführen ist. Zusammenfassend konnten aus den zentralen Erkenntnissen der qualitativen Studie neun Implikationen abgeleitet werden. Das Modul 5 unterstützt den Entscheidungsprozess von Praktikern dahingehend, ob und in welchem Umfang BI in Versicherungsunternehmen implementiert werden sollte.

Infolge der in den Unternehmen voranschreitenden Digitalisierung ist ein signifikanter Anstieg der Häufigkeit, Komplexität und Reichweite von Cyber-Angriffen zu beobachten, wodurch die Relevanz der Cyber-Sicherheit stetig zunimmt. In diesem Kontext nimmt der Faktor Mensch innerhalb der Unternehmensorganisation einen wesentlichen Einfluss auf die Cyber-Sicherheit, da dieser das „schwächste Glied“ im Sicherheitskonstrukt der Unternehmen abbildet und damit ein potenzielles Ziel für Angreifer darstellt. Zur Verringerung des aus Cyber-Angriffen resultierenden Schadensausmaßes wird der Einfluss des Faktors Mensch auf eine potenzielle Frühwarnung in der Cyber-Sicherheit im Modul 6 anhand einer inhaltsbasierten Literaturrecherche erforscht. Das Ziel der Analyse ist es, die vorhandene Literatur des ausgewählten Themengebietes zu evaluieren, diskutieren und zusammenzufassen, um dadurch neue konzeptionelle Rahmen und Perspektiven zu schaffen. In Anlehnung an das Prozessmodell zur Inhaltsanalyse von Seuring und Gold (2012) wurden in der Studie folgende

vier Phasen angewendet: Materialsammlung, deskriptive Analyse, Auswahl und Definition der Kategorien und Bewertung des Materials. Innerhalb der Materialsammlung konnten bei der Suche in den ausgewählten Datenbanken 13.998 Artikel (n=13.998) generiert werden. Für die weitere Analyse wurden nach Anwendung der definierten Ein- und Ausschlusskriterien 67 Artikel (n=67) einbezogen. Aus den Ergebnissen der inhaltsbasierten Literaturanalyse geht hervor, dass neben der Technologie, den organisationalen Faktoren, der Infrastruktur sowie rechtlichen und regulatorischen Bestimmungen der Faktor Mensch einen wesentlichen Einfluss auf die Cyber-Sicherheit der Unternehmen einnimmt. Der kritischste Einflussfaktor ist dabei das komplexe Zusammenspiel der menschlichen und technischen Faktoren. Hinsichtlich einer potenziellen Frühwarnung kann die Auswertung von Awareness-Trainings, welche die Sensibilität für Auffälligkeiten von Cyber-Angriffen erhöhen, als möglicher Frühwarnindikator dienen. Insbesondere die Durchführung von Mitarbeiterumfragen und der Vergleich von Veränderungen der Ergebnisse im Zeitverlauf können dafür herangezogen und als Präventionsmaßnahme verwendet werden. Bei der Erfolgsmessung von Awareness-Trainings zeigt sich, inwieweit Mitarbeiter potenzielle Bedrohungen erkennen. Unzureichende Ergebnisse der Erfolgsmessung können eine Frühwarnung dafür sein, dass die Mitarbeiter nicht ausreichend sensibilisiert sind und eine erhöhte Gefahr für das Unternehmen darstellen.

Zur Validierung der aus der inhaltsbasierten Literaturrecherche resultierenden Ergebnisse wurde im Modul 7 eine qualitative Studie in Form von Experteninterviews durchgeführt. Über die Erweiterung der Ergebnisse mittels der qualitativen Interviewstudie können praxisorientierte Erfahrungen hinsichtlich Frühwarnindikatoren im Bereich der Cyber-Sicherheit einbezogen werden. In diesem Zusammenhang ist die folgende Forschungsfrage Gegenstand des Moduls 7: „Wie ist der Status quo der Frühwarnung im Bereich der Cyber-Sicherheit/Informationssicherheit und welche Aspekte sollten in die Konzeption möglicher praxisorientierter Frühwarnindikatoren einfließen?“. Im Rahmen der qualitativen Studie wurden 25 Experten (n=25) aus verschiedenen Unternehmensbereichen befragt. Die Auswertung der Experteninterviews erfolgte mittels der qualitativen Inhaltsanalyse nach Kuckartz (2018). Aus der Analyse der Experteninterviews geht hervor, dass Frühwarnsysteme einerseits technisch umzusetzen sind, aber andererseits ebenso der Faktor Mensch zu berücksichtigen ist. Zudem

wird in diesem Kontext das Potenzial des Informationsaustausches zur gegenwärtigen Bedrohungslage herausgestellt. Wie bereits aus der Literaturrecherche in Modul 6 hervorgegangen ist, zeigt die qualitative Studie gleichermaßen, dass die mitarbeiterbezogene Komponente den Erfolg von Sicherheitsmaßnahmen innerhalb der Unternehmensorganisation maßgeblich beeinflusst. Der Faktor Mensch sollte infolgedessen neben technischen Aspekten sowie dem aktuellen Stand der IT-Hygiene in potenzielle Frühwarnindikatoren integriert werden. Der Fokus der von den befragten Experten konstruierten Frühwarnindikatoren liegt nicht auf der Frühwarnung vor Cyber-Angriffen, sondern auf der Betrachtung von Schwachstellen innerhalb der IT-Hygiene und der unzureichenden Sensibilisierung der Mitarbeiter, welche die Angreifbarkeit eines Unternehmens erhöhen. Infolge der Umsetzung und Überwachung von technischen und organisationalen Schutzmaßnahmen sowie der Sensibilisierung der Beschäftigten sollte es, nach Meinung der Experten, den Angreifern bestmöglich erschwert werden, sich einen finanziellen Vorteil auf Kosten eines Unternehmens zu verschaffen.

Da jedoch kein vollständiger Schutz vor Cyber-Angriffen zu erreichen ist, erlangt die Cyber-Versicherung eine zunehmende Bedeutung. Während Cyber-Versicherungen die aus Cyber-Angriffen entstehenden Risiken größtenteils explizit einschließen, resultiert für Versicherungsunternehmen ein bedeutendes Haftungspotenzial bei Silent Cyber-Risiken, welche infolge unklar formulierter Versicherungsbedingungen und der daraus hervorgehenden impliziten Mitversicherung von Cyber-Risiken in traditionellen Policen entstehen. Im Kontext der Einflüsse der digitalen Transformation auf die Kunden- und Produktperspektive werden in Modul 8 die Herausforderungen von Silent Cyber-Risiken für das Pricing und Underwriting in deutschen Versicherungsunternehmen eruiert. Konkret erfolgt die Analyse des Status quos der Wahrnehmung von Silent Cyber-Risiken, der Gefährdungspotenziale und der Maßnahmen im Umgang mit Silent Cyber-Risiken bezüglich des Underwritings sowie Pricings und der Einschätzung zukünftiger Entwicklungen. Zur Beantwortung der Forschungsfragen wurden 24 Fachexperten (n=24) aus der deutschen Versicherungswirtschaft befragt. Die Auswertung der Ergebnisse mittels der Datenanalysesoftware MAXQDA unter Anwendung der qualitativen Inhaltsanalyse nach Kuckartz (2018) zeigt, dass Silent Cyber-Risiken in den Versicherungsunternehmen unterschiedlich priorisiert und eva-

luiert werden, wodurch im Rahmen des Silent Cyber-Risikomanagements ein heterogener Umsetzungsstand vorherrscht. Darüber hinaus heben die Experten die Quantifizierungsschwierigkeiten sowie geringe Datenbestände bzgl. der Risiken hervor, was ein präzises Pricing und Underwriting erschwert. Bezugnehmend auf die zukünftige Entwicklung im Umgang mit Silent Cyber-Risiken zeigen die Ergebnisse in Modul 8, dass zum einen die affirmative Einbeziehung der Cyber-Risiken in die traditionellen Sparten und zum anderen ein Ausschluss der Risiken aus den konventionellen Versicherungsverträgen denkbar ist.

Zusammenfassend zeigt die Tabelle 1 eine Übersicht der acht Module hinsichtlich der jeweiligen Journal Ratings sowie des aktuellen Publikationsstatus. Anschließend erfolgt auf Grundlage der aus den Modulen gewonnenen Ergebnisse und Erkenntnisse die Beantwortung der eingangs formulierten Forschungsfragen.

Tabelle 1: Modulübersicht der kumulativen Dissertation

Modul Nr.	Titel	Journal (VHB-JOURQUAL 3 Rating)	Status
1	Einfluss von ESG-Risiken auf versicherungstechnische Verpflichtungen	BFuP – Betriebswirtschaftliche Forschung und Praxis (VHB C)	Publiziert
2	Status quo der Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in Deutschland – Regulatorische Herausforderung oder Chance für die Versicherungsunternehmen?	Zeitschrift für die gesamte Versicherungswissenschaft (VHB C)	Eingereicht
3	Influences of Digital Innovations on Advisory Work in the Financial Services Sector	Die Unternehmung – Swiss Journal of Business Research and Practice (VHB C)	Publiziert

4	Digital Transformation in Back-Offices of German Insurance Companies	International Journal of Innovation and Technology Management (VHB C)	Revise und Resubmit (Minor Revision)
5	Chances and Challenges of Business Intelligence: Insights from the German Insurance Market	Zeitschrift für die gesamte Versicherungswissenschaft (VHB C)	Unter Begutachtung
6	Human Factor Influences on Early Warning in Cyber Security: A Content-analysis based Literature Review	Management Review Quarterly (VHB C)	Eingereicht
7	Practice-oriented Early Warning Indicators in Cybersecurity: Insights from a Qualitative Empirical Study in Germany	Journal of Information Technology (VHB A)	Eingereicht
8	Silent Cyber-Risiken als Herausforderung für das Pricing und Underwriting in deutschen Versicherungsunternehmen – Ergebnisse einer qualitativ-empirischen Analyse	Zeitschrift für die gesamte Versicherungswissenschaft (VHB C)	Unter Begutachtung

Quelle: Eigene Darstellung.

1. *Welchen Einfluss hat die digitale Transformation auf die Kundenerwartungen und die Produktentwicklung in deutschen Finanzdienstleistungsunternehmen?*

Im Hinblick auf die Beantwortung der ersten Forschungsfrage konnten die Module 1, 3 und 8 relevante Ergebnisse und Erkenntnisse liefern. Das Modul 1 zum „Einfluss von ESG-Risiken auf versicherungstechnische Verpflichtungen“ zeigt, dass Nachhaltigkeit und die daraus resultierenden Risiken in den Versicherungsunternehmen vermehrt Beachtung finden. Für die Kundenerwartungen und Produktentwicklung ergibt sich daraus, dass einerseits nachhaltige Versicherungsprodukte angeboten werden sollten

und andererseits ESG-Risiken und insbesondere Umweltrisiken bei der Produktentwicklung zu berücksichtigen sind. Darüber hinaus werden die Kundenbedürfnisse sowie –erwartungen im Rahmen der Beratungstätigkeit im Finanzdienstleistungssektor zunehmend von der digitalen Transformation beeinflusst. Aus Modul 3 geht hervor, dass die digitale Transformation grundsätzlich zum Angebot neuer Kundenkanäle, aber gleichzeitig auch zu Arbeitsveränderungen in der Beratung führt. Zum einen erfordert der Einsatz neuer Technologien in der Finanzberatung eine entsprechende Weiterbildung sowie Akzeptanz der Mitarbeiter. Zum anderen sind die generationenübergreifenden Kundenbedürfnisse bei dem Beratungsangebot unter Einsatz technologischer Innovationen zu beachten. Wenngleich die Relevanz der Cyber-Versicherung infolge der aus der digitalen Transformation resultierenden Cyber-Risiken steigt, nehmen Silent Cyber-Risiken ebenfalls Einfluss auf die Produktentwicklung in Versicherungsunternehmen. Das Modul 8 liefert einen Beitrag dazu, dass Silent Cyber-Risiken für das Pricing und Underwriting eine Herausforderung darstellen. Für die Produktentwicklung konnten dahingehend Trends aufgezeigt werden, dass Cyber-Risiken affirmativ in traditionelle Sparten einbezogen oder explizit bei konventionellen Versicherungsverträgen ausgeschlossen werden. Derzeit haben die Versicherungsunternehmen jedoch Quantifizierungsschwierigkeiten bzgl. der Silent Cyber-Risiken. Insgesamt zeigen die Module 1, 3 und 8, dass sowohl die Kundenerwartungen als auch die Produktentwicklung infolge dynamischer Veränderungen digitaler Innovationen beeinflusst werden und zur Bewältigung des steigenden Wettbewerbsdrucks stets Berücksichtigung finden sollten.

2. *Welche Chancen und Herausforderungen resultieren aus der digitalen Transformation für die Unternehmensorganisation?*

Das Modul 2 sowie die Module 4 bis 7 liefern einen Beitrag für die Beantwortung der zweiten Forschungsfrage. Aus dem Modul 2 geht hervor, dass für die Versicherungsunternehmen aus den regulatorischen Anforderungen der VAIT innerhalb der Unternehmensorganisation prozessuale und strukturelle Veränderungen resultieren. Insgesamt sind infolge der VAIT jedoch Effizienzgewinne sowie die Erhöhung der Informationssicherheit als Chancen hervorzuheben. Aufgrund der digitalen Transformation kommen den VAIT grundsätzlich eine erhöhte Bedeutsamkeit zu. Weitere Chancen und Herausforderungen für die Unternehmensorganisation zeigt das Modul 4 hin-

sichtlich der Auswirkungen der digitalen Transformation auf das Backoffice von Versicherungsunternehmen. Insgesamt stellt die Automatisierung von Routinetätigkeiten eine Maßnahme dar, welche die Realisation von Effizienzgewinnen ermöglicht sowie dem Personalmangel entgegenwirkt. Gleichzeitig ist der steigende Wettbewerbsdruck durch die aus der digitalen Transformation hervorgehende erhöhte Preistransparenz herauszustellen. Zudem wird der Einsatz von BI in Versicherungsunternehmen infolge der digitalen Transformation ermöglicht. In Modul 5 wird deutlich, dass die Einsatzmöglichkeiten jedoch nicht vollumfänglich ausgeschöpft werden. Als Herausforderung ist in diesem Zusammenhang anzuführen, dass die aus der digitalen Transformation resultierenden Potenziale nicht erkannt werden. Darüber hinaus erschweren Datenschutzaspekte die Implementierung derartiger Innovationen innerhalb der Unternehmensorganisation. Die Module 6 und 7 heben ferner den Einfluss des Faktors Mensch auf die Cyber-Sicherheit im Rahmen der Unternehmensorganisation hervor. Während dieser einerseits als „schwächstes Glied“ und potenzielles Angriffsziel im Sicherheitskonstrukt der Unternehmen dargestellt wird, ist andererseits das Potenzial zur Frühwarnung zu beachten. Insgesamt ist es in diesem Zusammenhang unerlässlich, die Mitarbeiter unter Einsatz von Awareness-Trainings hinsichtlich potenzieller Auffälligkeiten umfangreich zu schulen und zu sensibilisieren. Sofern dies ausreichend erzielt werden kann, besteht die Möglichkeit die eigenen Mitarbeiter als Sicherheitssensor zu etablieren. Die genannten Chancen und Herausforderungen der digitalen Transformation werden auch in Zukunft die Unternehmensorganisationen beeinflussen.

1.4 Kritische Würdigung und weiterer Forschungsbedarf

Die acht Module der vorliegenden kumulativen Dissertation zeigen, dass sich verschiedene technologische, organisationale und umweltbezogene Faktoren im Rahmen der Einflüsse der digitalen Transformation auf die Kunden- und Produktperspektive sowie die interne Unternehmensperspektive auswirken. Zur Gewinnung der Ergebnisse und Erkenntnisse wurden überwiegend qualitativ-empirische Forschungsansätze verwendet. Infolge des Mangels an kontextspezifischen Forschungserkenntnissen und des explorativen Charakters der eruierten Fragestellungen ist dieser Forschungsansatz unter anderem in Form von qualitativen Experteninterviews ausgewählt worden. Qualitative Forschung ermöglicht in diesem Zusammenhang eine systematische Auswer-

tung von praktischem Erfahrungswissen sowie die Analyse von Wirkungszusammenhängen. Neben genannten Vorteilen sowie der Generierung neuer Erkenntnisse sind zugleich Limitationen der gewählten Forschungsmethode zu verzeichnen. Einschränkungen ergeben sich hinsichtlich der Generalisierbarkeit und Repräsentativität der Ergebnisse aufgrund der vorliegenden Stichprobengrößen sowie subjektiven Einschätzungen der Befragungsteilnehmenden. Eine weitere Limitation der gewonnenen Ergebnisse bezieht sich auf die Erhebung in deutschen Finanzdienstleistungsunternehmen. Insgesamt ist die Übertragbarkeit der Forschungsergebnisse auf internationale Märkte infolgedessen eingeschränkt. Neben den qualitativen Experteninterviews wurde im Rahmen des qualitativ-empirischen Forschungsansatzes zudem eine inhaltsbasierte Literaturrecherche herangezogen. Die systematische Literaturanalyse ermöglicht es, die relevante Literatur des definierten Themengebietes zu analysieren und neue konzeptionelle Rahmen sowie Perspektiven zu schaffen. Als Limitation dieser Forschungsmethode ist anzuführen, dass aufgrund des konzipierten Suchstrings, der definierten Ein- und Ausschlusskriterien sowie den ausgewählten Datenbanken ggf. einschlägige Publikationen nicht einbezogen wurden. Infolgedessen kann die Verallgemeinerbarkeit der Ergebnisse eingeschränkt sein. Abschließend weist die zu den qualitativen Experteninterviews ergänzend verwendete Online-Umfrage in Modul 1 dahingehend Einschränkungen auf, dass nicht sichergestellt werden konnte, inwieweit die Fragen zutreffend interpretiert wurden, wodurch die Ergebnisse dieser Forschungsmethode ebenfalls bedingt generalisierbar sind.

Hinsichtlich der Einflüsse der digitalen Transformation auf die Kunden- und Produktperspektive konnten die Ergebnisse der vorliegenden kumulativen Dissertation zu den Auswirkungen der ESG-Risiken aufgrund der geringen Stichprobengröße nicht nach der Unternehmensgröße differenziert werden. Darüber hinaus wurde ausschließlich die Angebotsseite betrachtet. Die Erweiterung der Studie auf die Kunden- bzw. Nachfrageseite würde zukünftig umfassendere Ergebnisse bezüglich der Durchsetzbarkeit höherer Prämien liefern und weitere Differenzierungen ermöglichen. Auch die Erkenntnisse zu den Einflüssen digitaler Innovationen auf die Beratungstätigkeit im Finanzdienstleistungssektor sind nur eingeschränkt interpretierbar. Die Erhebung der Experteninterviews erfolgte ausschließlich in der Testphase der technologischen Innovationen. Infolgedessen konnten keine Aussagen zur Effektivität oder über den Langzeiterfolg der technologischen Lösungen getätigt werden und die Verallgemeinerbarkeit der

Ergebnisse ist aufgrund der spezifischen Unternehmenskontexte der Fallstudien nur teilweise gegeben. Zur Analyse der Effektivität derartiger Implementierungen wäre eine erneute Erhebung mit den bereits befragten Experten sinnvoll. Die Analyse der Erkenntnisse zu verschiedenen Erhebungszeitpunkten könnte Praktiker bei zukünftigen Implementierungsentscheidungen unterstützen. Im letzten Modul der Kunden- und Produktperspektive konnte bezüglich des Umgangs mit Silent Cyber-Risiken kein einheitlicher Umsetzungsstand in der Praxis identifiziert werden. Zudem werden derzeitige Quantifizierungsschwierigkeiten der Risiken von den befragten Experten herausgestellt. Auch hier erscheint es somit sinnvoll den Status quo zu einem späteren Zeitpunkt erneut zu erheben und den längerfristigen Umgang mit genannten Quantifizierungsschwierigkeiten im Pricing und Underwriting abzubilden.

Im Rahmen der internen Unternehmensperspektive wurden ausschließlich die Auswirkungen der VAIT in der Fassung vom 20.03.2019 (Rundschreiben 10/2018) analysiert. Zudem sind die VAIT spezifisch für den deutschen Versicherungsmarkt formulierte Anforderungen, wodurch eine Übertragbarkeit der Forschungsergebnisse auf internationale Märkte nicht gegeben ist. In Zukunft könnte eine Erhebung des Umsetzungsstandes des aktualisierten Rundschreibens in der Fassung vom 03.03.2022 die in dieser Dissertation gewonnenen Erkenntnisse erweitern. Überdies wäre zur Ermöglichung eines eingeschränkten internationalen Vergleichs die Analyse ähnlicher EU-weiter bzw. internationaler Regelwerke und Normen denkbar. Der am 16.01.2023 in Kraft getretene „Digital Operational Resilience Act“ (DORA) ist ein potenzielles Beispiel dafür. Darüber hinaus zeigt die Analyse der Auswirkungen der digitalen Transformation auf das Backoffice von Versicherungsunternehmen, dass sich die jeweilige Implementierung der technologischen Innovationen zum Erhebungszeitpunkt in einem unterschiedlichen Stadium befand und vorwiegend nicht abgeschlossen war. Infolgedessen konnte eine Evaluierung der Effektivität der implementierten technologischen Innovationen nicht einbezogen werden. Die Durchführung einer weiteren qualitativen Expertenbefragung mit denselben Teilnehmenden könnte ergänzende Erkenntnisse über die längerfristige Effektivität derartiger Innovationen liefern und zukünftige Implementierungen erleichtern. Bei der Analyse der Chancen und Herausforderungen der Einführung und Nutzung von BI ist gleichermaßen die Erhebung einer weiterführenden qualitativen Studie sowie die Erhöhung der Stichprobengröße und Ausweitung auf inter-

nationale Versicherungsmärkte zur Generierung holistischerer Erkenntnisse zu empfehlen. Ferner ist die Untersuchung des Einsatzes von BI in spezifischen Versicherungssparten sowie des Potenzials zur Kalkulation von Versicherungsprämien und zur Aufdeckung von Versicherungsbetrug sinnvoll. Im Rahmen der internen Unternehmensperspektive besteht infolge der zunehmenden Relevanz von Cyber-Angriffen weiterhin Forschungsbedarf im Bereich der Frühwarnung, da diese das Potenzial zur Reduzierung oder bestenfalls Verhinderung des resultierenden Schadens aufweist. Zudem ist die Ergänzung der im Modul 7 durchgeführten qualitativen Studie um die quantitative Analyse retrospektiver Daten von Unternehmenseigenschaften der durch Cyber-Angriffe geschädigter Unternehmen dahingehend sinnvoll, dass daraus potenziell erhöhte Angriffswahrscheinlichkeiten abgeleitet werden können, welche wiederum als Frühwarnindikator dienen würden. Diese Daten sollten zur bestmöglichen Qualität verwendbarer Informationen sowohl technischer und organisationaler als auch mitarbeiterbezogener Herkunft sein. Hinzukommend könnte der daraus generierte Datenbestand den Versicherungen die Risikobewertung der Unternehmen dahingehend erleichtern, dass die Einkalkulierung des bestehenden Restrisikos in die Prämie der Cyber-Versicherung über die Angriffswahrscheinlichkeiten präziser erfolgen kann. Die Erhebung derartiger Daten würde zugleich der in Modul 8 aufgekommenen Problematik hinsichtlich der Quantifizierungsschwierigkeiten und des erschwerten Pricings von Silent Cyber-Risiken unterstützen. Zusammenfassend bestehen in den betrachteten Themenfeldern vielfältige Anknüpfungspunkte für weiteren Forschungsbedarf.

2 Literaturverzeichnis

Allianz Global Corporate & Specialty SE (2023):
Allianz Risk Barometer: Identifying the Major Business Risks for 2023 – The Most Important Corporate Concerns for the Year Ahead, Ranked by 2,712 Risk Management Experts from a Record 94 Countries and Territories, URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf [Stand 16.03.2023].

Baker, J. (2012):
The Technology–Organisation–Environment Framework, in: Dwivedi, Y. K. / Wade, M. R. / Schneberger, S. L. (Hrsg.), Information Systems Theory, Springer, New York, Dordrecht, Heidelberg, London, S. 231–246.

Bank of England Prudential Regulation Authority (2017):
Cyber Insurance Underwriting Risk, URL: https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417 [Stand 15.03.2023].

Berghaus, S. / Back, A. (2016):
Stages in Digital Business Transformation: Results of an Empirical Maturity Study, in: 10th Mediterranean Conference on Information Systems (MCIS), Proceedings, S. 1–17.

Bernsmed, K. / Tøndel, I. A. (2013):
Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management, in: 7th International Conference on IT Security Incident Management and IT Forensics (IMF), Proceedings, S. 3–14.

Bohnert, A. / Fritzsche, A. / Gregor, S. (2019):
Digital Agendas in the Insurance Industry: The Importance of Comprehensive Approaches, in: The Geneva Papers on Risk and Insurance–Issues and Practice, 44, S. 1–19.

Borgman, H. P. / Bahli, B. / Heier, H. / Schewski, F. (2013):
Cloudrise: Exploring Cloud Computing Adoption and Governance with the TOE Framework, in: 46th Hawaii International Conference on System Sciences (HICSS), Proceedings, S. 4425–4435.

Chau, P. Y. / Tam, K. Y. (1997):
Factors Affecting the Adoption of Open Systems: An Exploratory Study, in: MIS Quarterly, 21 (1), S. 1–24.

Chiu, C. Y. / Chen, S. / Chen, C. L. (2017):
An Integrated Perspective of TOE Framework and Innovation Diffusion in Broadband Mobile Applications Adoption by Enterprises, in: International Journal of Management, Economics and Social Sciences, 6 (1), S. 14–39.

Cziesla, T. (2014):
A Literature Review on Digital Transformation in the Financial Service Industry, in: 27th Bled eConference, Proceedings, S. 25–36.

DePietro, R. / Wiarda, E. / Fleischer, M. (1990):
The Context for Change: Organization, Technology and Environment, in: Tornatzky, L. G. / Fleischer, M. (Hrsg.), The Processes of Technological Innovation, Lexington Books, Lexington, MA, Toronto, S. 151–175.

Disterer, G. (2015):
Frühwarnsysteme für das IT-Sicherheits- und Risikomanagement, in: HMD – Praxis der Wirtschaftsinformatik, 52 (5), S. 790–801.

Dreher, M. (2019):
Versicherungsaufsicht über IT und Governance, in: Versicherungsrecht, 70 (19), S. 1177–1191.

Eden, T. / Werth, O. / Rodríguez Cardona, D. / Schwarzbach, C. / Breitner, M. H. / Graf von der Schulenburg, J.-M. (2022):
Influences of Digital Innovations on Advisory Work in the Financial Services Sector, in: Die Unternehmung, 76 (1), S. 6–27.

Eickhoff, M. / Muntermann, J. / Weinrich, T. (2017):
What do FinTechs actually do? A Taxonomy of FinTech Business Models, in: 38th International Conference on Information Systems (ICIS), Proceedings, S. 1–19.

European Insurance and Occupational Pensions Authority (2022):
Supervisory Statement on Management of Non-Affirmative Cyber Exposures (2022), URL: https://www.eiopa.europa.eu/sites/default/files/publications/supervisory_statements/supervisory_statement_on_management_of_non-affirmative_cyber_exposures.pdf [Stand 15.03.2023].

Glaser, B. G. / Strauss, A. L. (1999):
Theoretical Sampling – The Discovery of Grounded Theory: Strategies for Qualitative Research, Routledge, London.

Groen, B. A. / Van Triest, S. P. / Coers, M. / Wtenweerde, N. (2018):
Managing Flexible Work Arrangements: Teleworking and Output Controls, in: European Management Journal, 36 (6), S. 727–735.

Iacovou, C. L. / Benbasat, I. / Dexter, A. S. (1995):
Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology, in: MIS Quarterly, 19 (4), S. 465–485.

Karagiannaki, A. / Vergados, G. / Fouskas, K. (2017):
The Impact of Digital Transformation in the Financial Services Industry: Insights from an Open Innovation Initiative in Fintech in Greece, in: 11th Mediterranean Conference of Information Systems (MCIS), Proceedings, S. 1–12.

Keller, B. (2018):
Big Data and Insurance: Implications for Innovation, Competition and Privacy, URL: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/research_brief_-_big_data_and_insurance.pdf [Stand 17.03.2023].

Kuckartz, U. (2018):
Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4. Aufl., Beltz Juventa, Weinheim, Basel.

Leimeister, J. M. / Österle, H. / Alter, S. (2014):
Digital Services for Consumers, in: Electronic Markets, 24, S. 255–258.

Li, D. / Lai, F. / Wang, J. (2010):
E-Business Assimilation in China's International Trade Firms: The Technology–Organisation–Environment Framework, in: Journal of Global Information Management, 18 (1), S. 39–65.

Marotta, A. / McShane, M. (2018):
Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach, in: Risk Management and Insurance Review, 21 (3), S. 435–452.

Niemand, T. / Rigtering, J. C. / Kallmünzer, A. / Kraus, S. / Maalaoui, A. (2021):
Digitalization in the Financial Industry: A Contingency Approach of Entrepreneurial Orientation and Strategic Vision on Digitalization, in: European Management Journal, 39 (3), S. 317–326.

Petrenko, S. (2018):
Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation, Springer, Cham.

Rosli, K. / Yeow, P. H. / Siew, E. G. (2012):
Factors Influencing Audit Technology Acceptance by Audit Firms: A New I-TOE Adoption Framework, in: Journal of Accounting and Auditing: Research & Practice, 2012, S. 1–11.

Seuring, S. / Gold, S. (2012):
Conducting Content Analysis Based Literature Reviews in Supply Chain Management. Supply Chain Management: An International Journal, 17(5), S. 544–555.

Streitz, S. H. (2019):
Von FAIT zu VAIT: Nur ein ausgetauschter Buchstabe oder grundlegend neue Anforderungen für Vorstand und IT-Steuerung?, in: Looschelders, D., Michael, L. (Hrsg.), Versicherungsaufsichtsrechtliche Anforderungen an die Informationstechnologie von Versicherungsunternehmen: VAIT, IT-Sicherheit, IT-Governance, Risikomanagement, Geschäftsleiterverantwortung, Verlag Versicherungswirtschaft, Karlsruhe, S. 39–61.

Tonn, G. / Kesan, J. P. / Zhang, L. / Czajkowski, J. (2019):
Cyber Risk and Insurance for Transportation Infrastructure, in: Transport Policy, 79, S. 103–114.

Von Solms, R. / Van Niekerk, J. (2013):
From Information Security to Cyber Security, in: Computers & Security, 38, S. 97–102.

Werth, O. / Schwarzbach, C. / Rodríguez Cardona, D. / Breitner, M. H. / Graf von der Schulenburg, J.-M. (2020):
Influencing Factors for the Digital Transformation in the Financial Services Sector, in: Zeitschrift für die gesamte Versicherungswissenschaft, 109, S. 155–179.

Wrede, D. / Stegen, T. / Graf von der Schulenburg, J.-M. (2020):
Affirmative and Silent Cyber Coverage in Traditional Insurance Policies: Qualitative Content Analysis of Selected Insurance Products from the German Insurance Market, in: The Geneva Papers on Risk and Insurance–Issues and Practice, 45 (4), S. 657–689.

Zhu, K. / Kraemer, K. L. / Dedrick, J. (2004):
Information Technology Payoff in E-Business Environments: An International Perspective on Value Creation of E-Business in the Financial Services Industry, in: Journal of Management Information Systems, 21 (1), S. 17–54.

Zhu, K. / Kraemer, K. L. (2005):
Post-Adoption Variations in Usage and Value of E-Business by Organisations: Cross-Country Evidence from the Retail Industry, in: Information Systems Research, 16 (1), S. 61–84.

Zhu, K. / Kraemer, K. L. / Xu, S. (2006):
The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-business, in: Management Science, 52 (10), S. 1557–1576.

3 Module der kumulativen Dissertation

3.1 Kunden- und Produktperspektive

1. Schwarzbach, C. / **Eden, T.** / Günther, D. / Rodriguez Gonzalez, M. / Graf von der Schulenburg, J.-M. (2022): Einfluss von ESG-Risiken auf versicherungstechnische Verpflichtungen, in: Betriebswirtschaftliche Forschung und Praxis (BFuP), 74 (6), S. 678–702.

3. **Eden, T.** / Werth, O. / Rodríguez Cardona, D. / Schwarzbach, C. / Breitner, M. H. / Graf von der Schulenburg, J.-M. (2022): Influences of Digital Innovations on Advisory Work in the Financial Services Sector, in: Die Unternehmung, 76 (1), S. 6–27.

8. **Eden, T.** / Wrede, D. / Meyer, N. M.: Silent Cyber-Risiken als Herausforderung für das Pricing und Underwriting in deutschen Versicherungsunternehmen – Ergebnisse einer qualitativ-empirischen Analyse, eingereicht bei: Zeitschrift für die gesamte Versicherungswissenschaft.

3.2 Interne Unternehmensperspektive

2. Wrede, D. / **Eden, T.** / Lohse, U.: Status quo der Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in Deutschland – Regulatorische Herausforderung oder Chance für die Versicherungsunternehmen?, eingereicht bei: Zeitschrift für die gesamte Versicherungswissenschaft.

4. Schwarzbach, C. / **Eden, T.** / Werth, O. / Lohse, U. / Breitner, M. H. / Graf von der Schulenburg, J.-M.: Digital Transformation in Back-Offices of German Insurance Companies, eingereicht bei: International Journal of Innovation and Technology Management.

5. **Eden, T.** / Werth, O. / Breitner, M. H.: Chances and Challenges of Business Intelligence: Insights from the German Insurance Market, eingereicht bei: Zeitschrift für die gesamte Versicherungswissenschaft.

6. **Eden, T.** / Wrede, D. / Graf von der Schulenburg, J.-M.: Human Factor Influences on Early Warning in Cyber Security: A Content-analysis based Literature Review, eingereicht bei Management Review Quarterly.

7. **Eden, T.** / Wrede, D. / Schwarzbach, C. / Basse, T.: Practice-oriented Early Warning Indicators in Cybersecurity: Insights from a Qualitative Empirical Study in Germany, eingereicht bei: Journal of Information Technology.

Modul 1

Einfluss von ESG-Risiken auf versicherungstechnische Verpflichtungen

Christoph Schwarzbach
Theresa Eden
Dennis Günther
Miguel Rodriguez Gonzalez
Johann-Matthias Graf von der Schulenburg

Betriebswirtschaftliche Forschung und Praxis (BFuP), 74 (6), S. 678–702
Verfügbar unter: https://datenbank.nwb.de/Dokument/1006469/

Modul 2

Status quo der Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in Deutschland – Regulatorische Herausforderung oder Chance für die Versicherungsunternehmen?

Dirk Wrede

Theresa Eden

Ute Lohse

Markus Wilkens

eingereicht bei:

Zeitschrift für die gesamte Versicherungswissenschaft

Status quo der Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in Deutschland – Regulatorische Herausforderung oder Chance für die Versicherungsunternehmen?

Dirk Wrede, Theresa Eden, Ute Lohse, Markus Wilkens

Dirk Wrede (korrespondierender Autor)
Wissenschaftlicher Mitarbeiter
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover
Deutschland
E-Mail: dw@ivbl.uni-hannover.de

Theresa Eden
Wissenschaftliche Mitarbeiterin
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover
Deutschland

Ute Lohse
Wissenschaftliche Mitarbeiterin
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover
Deutschland

Markus Wilkens
Gottfried Wilhelm Leibniz Universität Hannover
Welfengarten 1
D-30167 Hannover

Status quo der Umsetzung der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in Deutschland – Regulatorische Herausforderung oder Chance für die Versicherungsunternehmen?

Zusammenfassung

Vor dem Hintergrund der zunehmenden Digitalisierungstendenzen untersucht der vorliegende Beitrag einen seit Jahren anhaltenden Trend zur weiteren Verstärkung der Regulierung der Versicherungswirtschaft und der zunehmenden Komplexität des Regulierungsrahmens für Assekuranzen am Beispiel des derzeitigen Umsetzungsstands der Vorgaben der Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) in den Versicherungsunternehmen. Ergänzend hierzu wird ein Überblick über die aktuellen Prüfungsschwerpunkte und -tätigkeiten der Versicherungsaufsicht in der Praxis gegeben. Die Untersuchungsergebnisse zeigen, dass in der Unternehmenspraxis ein unterschiedlicher Umsetzungsstand in den einzelnen Unternehmen vorherrscht und in der Versicherungsbranche insgesamt erheblicher Nachholbedarf bezogen auf eine vollständige Implementierung der VAIT besteht. Ebenfalls resultiert aus der bislang eher geringen Anzahl an VAIT-Prüfungen und der fehlenden großflächigen Prüfungstätigkeit eine hohe unternehmensseitige Unsicherheit im Hinblick auf eine vollständige und anforderungskonforme Umsetzung der VAIT.

Abstract

In the context of increasing digitalization trends, this paper examines a continuing trend towards further tightening of insurance industry regulation and the increasing complexity of the regulatory framework for insurance companies, using the current implementation status of Supervisory Requirements for IT in Insurance Undertakings (VAIT) in insurance sector. In this regard, an overview of the current audit focus and activities of the insurance supervisory authority in practice is given. The results of the study show that the status of implementation varies between companies and the insurance industry in general has a lot of backlog to cover in terms of complete implementation of VAIT. The rather low number of VAIT audits and the lack of large-scale auditing activities also result in a high level of uncertainty among companies regarding the complete and compliant implementation of VAIT.

1 Ausgangssituation und Zielsetzung

Aktuell befinden sich große Teile des versicherungsspezifischen Regulierungsrahmens im Umbruch. Dabei betreffen die derzeitigen Reformen sowohl die Aufsicht über die Assekuranzen als auch den Vertrieb, die Informationsverarbeitung sowie die Versicherungsprodukte (Theis 2015). Dementsprechend unterliegt die Versicherungswirtschaft als eine stark regulierte Branche strengen gesetzlichen und regulatorischen Anforderungen (Beltratti und Corvino 2008; Handke 2012; Wrede 2021) und die Unternehmen sehen sich mit einem seit Jahren anwachsenden Regulierungsdruck wie auch der stetig zunehmenden Komplexität der neuen regulatorischen Anforderungen und den daraus resultierenden enormen Herausforderungen konfrontiert (Schiro 2006; Lehmann 2019). Aktuell herrscht in der Praxis ein anhaltender Trend zur weiteren Verstärkung der Regulierung der Versicherungswirtschaft vor (Köhne und Brömmelmeyer 2018; Gal 2020), sodass die Unternehmen eine Vielzahl versicherungsaufsichtsrechtlicher Offenlegungspflichten zu erfüllen haben (Dreher 2009). Folglich ist die zukünftige Leistungsfähigkeit der Versicherungsunternehmen maßgeblich von dem Gelingen einer sachgerechten Weiterentwicklung der Versicherungsregulierung abhängig (Theis 2015). Gleichzeitig werden durch die Umsetzung von regulatorischen und gesetzlichen Vorgaben, wie z. B. der EU-Versicherungsvertriebsrichtlinie (Insurance Distribution Directive, IDD), der EU-Datenschutz-Grundverordnung (EU-DSGVO), diversen Verbraucherschutzrichtlinien sowie der Bündelung der Anforderungen des europäischen Versicherungsaufsichtssystems Solvency II, aktuell eine Vielzahl von Ressourcen in den Versicherungsunternehmen gebunden. Dabei stellen die regulatorischen Herausforderungen nicht nur einen wichtigen Treiber für den Wandel etablierter Versicherer dar und bestimmen wesentlich deren Geschäfts- und Betriebsmodelle, sondern führen auch zu tiefgreifenden Veränderungen in den Unternehmen (Bierth et al. 2018).

Durch die Entwicklung der Versicherungs-IT zu einem strategischen Erfolgs- und Wettbewerbsfaktor für die Unternehmen (Olaisen 1990; Brady und Targett 1995; Channon 1998; Neirotti und Paolucci 2007; Cappiello 2018; Bohnert et al. 2019) sowie ihrer Bedeutung als Kernproduktionsfaktor für die Erzeugung wie auch Bereitstellung von Versicherungsleistungen (Stankat 2010) und als integralem Bestandteil assekuranzspezifischer Geschäftsmodelle (Puschmann 2017), ist diese in jüngster Zeit zunehmend in den Betrachtungsfokus der Versicherungsaufsicht gerückt. Traditionell besteht die IT-Landschaft von Versicherungen aus einer Vielzahl monolithischer Altsysteme, Mainframe-Rechnern und versicherungstechnischer Individualanwendungen (Smits et al. 1997; Petsch und Nissen 2009). Da die Geschäftstätigkeit von Assekuranzen im Wesentlichen auf der Gewinnung, Speicherung, Verarbeitung und Nutzung

von Informationen basiert (Bassellier et al. 2003; Berger 2003; Nicoletti 2016; Oletzky und Reinhardt 2022) und sich die betrieblichen Abläufe sowie Geschäftsprozesse nahezu vollständig auf informationsverarbeitende Systeme stützen (Ifinedo 2009), sind die Unternehmen hochgradig von der Datenverarbeitung, den eingesetzten IT- und Softwaresystemen (Taylor 2001) und einem funktionierenden IT-Betrieb abhängig (Manning et al. 1985; Harris und Katz 1991; Codington und Wilson 1994; Melliou und Wilson 1995; Francalanci und Galal 1998; Koch 2006; Aschenbrenner 2010; Goldstein et al. 2011). Infolgedessen verfügen Versicherer über eine hohe Eigenfertigungstiefe in den eingesetzten Informationsverarbeitungssystemen und nutzen für das Kerngeschäft überwiegend selbst entwickelte Individualanwendungen (KPMG AG Wirtschaftsprüfungsgesellschaft 2017; Naylor 2017). So ist es in den meisten Versicherungsunternehmen immer noch gängige Praxis, die geschäftskritischen Kern-Anwendungen, wie z. B. Partner-, Bestandsführungs- und Schadensysteme, entweder eigen oder individuell in Auftrag zu entwickeln (Gruhn et al. 2006), wodurch die IT-Kosten im Wesentlichen aus den Umstellungen, Erweiterungen und der Wartung der bestehenden IT-System- und Anwendungslandschaften aufgrund von sich ändernden Rahmenbedingungen resultieren (Buhl und Kundisch 2003; Christiaans und Steden 2018). Ebenso müssen die IT-Budgets für Investitionen vorrangig zur Umsetzung regulatorischer Anforderungen eingesetzt werden (Kappenberg und Drews 2014). Die Anwendungsarchitektur von Assekuranzen beruht wegen der historisch gewachsenen heterogenen IT-Infrastrukturen überwiegend noch auf dem Spartensystem des Versicherungsgeschäfts. Hierdurch herrscht in der Praxis größtenteils ein Aufbau und Betrieb der IT-Systeme und Anwendungen für jede einzelne Versicherungssparte vor (Moormann und Schmidt 2007). Darüber hinaus findet i. d. R. in den unterschiedlichen Assekuranzsparten anstatt des Einsatzes eines zentralen Versicherungskernsystems ein Parallelbetrieb verschiedener gleichartiger versicherungstechnischer Anwendungssysteme statt (Stankat 2010). Daraus entstehen vielfältige Redundanzen in der IT-Architektur, eine stark fragmentierte Datenhaltung (Uzquiano 2010; Braun et al. 2017) sowie die Bedienung der gleichen Geschäftsfunktionen durch mehrere Anwendungssysteme (Engelke 2010). In den versicherungseigenen Rechenzentren werden einerseits die Applikationsserver mit den geschäftskritischen Anwendungen, die verschiedenen Datenbanken wie auch die zentralen Systeme zur Kommunikation betrieben und andererseits erfolgt dort die Abwicklung sämtlicher Geschäftstransaktionen sowie die Speicherung der juristischen Daten (Moormann und Schmidt 2007). Dementsprechend gestaltet sich sowohl der Betrieb, die Wartung als auch die Anpassung der Altsysteme und der versicherungstechnischen Individualanwendungen als sehr kosten- und arbeitsintensiv (Basten et al. 2014; Roßmehl et al. 2017).

Im Bereich der IT verfügen Versicherer heutzutage vielfach immer noch über Systeme, Betriebsabläufe und Prozesse aus den 1980er-Jahren (Pisoni 2021), obwohl die Auswirkungen der zunehmenden Digitalisierungstendenzen in der Versicherungsbranche nahezu alle Bereiche der Wertschöpfungskette betreffen (Eling und Lehmann 2018; Schmidt 2018; Albrecher et al. 2019; Eckert und Osterrieder 2020; Werth et al. 2020; Eckert et al. 2021; Pauch und Bera 2022; Tsindeliani et al. 2022). Dabei ermöglichen die fortschreitende Digitalisierung und der Bedeutungswandel der IT den Versicherern nicht nur die Automatisierung bestehender Geschäftsprozesse (Braunwarth et al. 2010; Eling et al. 2022), sondern auch die Entwicklung neuartiger Produkte, Dienstleistungen und Geschäftsmodelle (Puschmann 2017; Lanfranchi und Grassi 2022). Aus der immer schneller voranschreitenden Digitalisierung in den Assekuranzen resultiert einerseits der Einsatz neuer Technologien in den Unternehmen und andererseits eine nachhaltige Erhöhung der Komplexität der Versicherungs-IT, wodurch die Implementierung neuer regulatorischer Vorschriften gefördert werden kann (Bonsón et al. 2010). In der Praxis haben sich Versicherungen inzwischen verstärkt zu Angriffszielen von Cyber-Kriminalität entwickelt (Lagazio et al. 2014; Bussmann et al. 2017, 2018; Cappiello 2020; Singh und Akhilesh 2020; Timofeyev und Dremova 2022) und sind in zunehmendem Maße der eminenten Gefährdung durch Cyberrisiken ausgesetzt (Eling 2018; Egan et al. 2019; European Insurance and Occupational Pensions Authority (EIOPA) 2019; Kaigorodova et al. 2020). Daher ist für die Versicherungsunternehmen die Implementierung und Etablierung eines umfassenden und effektiven IT-Risikomanagements unerlässlich (EIOPA 2019; Varga et al. 2021).

Die zunehmende Bedeutung der IT sowie die sich im stetigen Wandel befindende Cyber-Bedrohungslage für die im Finanzsektor beaufsichtigten Unternehmen hat in der jüngeren Vergangenheit dazu geführt, dass von den zuständigen Aufsichtsbehörden die Anforderungen an IT-relevante Sachverhalte zunehmend dokumentiert, angepasst und vielfach auch durch neue Vorgaben definiert wurden. In diesem Zusammenhang hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) auf Grundlage des bestehenden Versicherungsaufsichtsrechts auf nationaler Ebene erstmalig – im Gleichklang mit einem zuvor veröffentlichten korrespondierenden Rundschreiben für die Bankaussicht[1] – mit den Versicherungsaufsichtlichen Anforderungen an die IT (VAIT) im Rundschreiben 10/2018 (VA) vom 2. Juli 2018 ihre Erwartungen an

[1] Mit der Veröffentlichung der Bankaufsichtlichen Anforderungen an die IT (BAIT) im Rundschreiben 10/2017 (BA) vom 3. November 2017, die sich primär an die Geschäftsleitungen der Kreditinstitute richten, hat die BaFin erstmals die Erwartungshaltung der Bankenaufsicht hinsichtlich der sicheren Ausgestaltung der IT-Systeme einschließlich der zugehörigen Prozesse sowie die diesbezüglichen Anforderungen an die IT-Governance formuliert. Die BAIT konkretisieren die Anforderungen zum internen Kontrollsystem, die personelle und technisch-organisatorische Ausstattung der Bank sowie zum Notfallkonzept.

den sicheren und aktuellen Standards orientierten Einsatz der IT für Versicherungen in Deutschland konkretisiert. Durch die VAIT wird die Erwartungshaltung der Versicherungsaufsicht formuliert, wie Versicherungen ihre IT-Systeme und IT-Prozesse sicher auszugestalten haben. Hierbei werden Versicherer verpflichtet, einen bestimmten Rahmen für die technisch-organisatorische Ausstattung der Unternehmen – insbesondere für das Management der IT-Ressourcen und für das IT-Risikomanagement – einzuhalten. Seitens der BaFin erfolgte durch die Veröffentlichung einer aktualisierten Fassung des Rundschreibens 10/2018 (VA) am 20. März 2019 erstmals eine Novelle der VAIT. Dabei sind die Anforderungen gegenüber der Fassung vom 2. Juli 2018 wesentlich erweitert und präzisiert worden.[2]

Ungeachtet der oben dargestellten Entwicklungen wird die Betrachtung der IT als Herausforderung im regulatorischen Kontext in der Literatur zur Versicherungsregulatorik bisher unzureichend betrachtet. Vor diesem Hintergrund soll die vorliegende Untersuchung einen Beitrag zur Schließung dieser Forschungslücke leisten. Ziel ist es, einerseits einen Überblick über die neun Anforderungsbereiche der VAIT zu geben und andererseits relevante Erkenntnisse aus der Praxis zu dem aktuellen Umsetzungsstand, den Problemen und Herausforderungen einer anforderungskonformen Umsetzung der Regelungen der VAIT sowie der aktuellen Prüfungsschwerpunkte der bislang durchgeführten aufsichtsrechtlichen Prüfungen herauszuarbeiten. Dabei beziehen sich die Ausführungen in diesem Artikel auf die Veröffentlichung der BaFin vom 2. Juli 2018 mit den Ergänzungen vom 20. März 2019. Um die angeführte Zielsetzung zu erreichen, ist der vorliegende Beitrag wie folgt strukturiert: In Abschnitt 2 erfolgen kurze Ausführungen zur Einordnung der IT-Relevanz innerhalb der Versicherungsbranche sowie die Darlegung der neun verschiedenen Anforderungsbereiche der VAIT. Darauf aufbauend dient Abschnitt 3 der Beschreibung von Forschungsdesign sowie der Vorgehensweise bei der Datenerhebung und -auswertung. In Abschnitt 4 werden die Ergebnisse der analysierten Experteninterviews dargestellt. Eine entsprechende Diskussion der herausgearbeiteten Ergebnisse ist Gegenstand des Abschnitts 5 und in Abschnitt 6 befinden sich eine kurze Zusammenfassung der Ergebnisse und einige Schlussfolgerungen.

[2] Siehe zu der Ausgestaltung und den Änderungen der VAIT ausführlich das novellierte Rundschreiben 10/2018 (VA) in der Fassung vom 20. März 2019 (BaFin 2019).

2 Einordnung der IT-Relevanz innerhalb der Versicherungsbranche und Stand der VAIT-Anforderungen

Der Versicherungsmarkt in Deutschland ist in Zeiten von Krieg, Inflation und Energiekrise gekennzeichnet durch große systemische Bedrohungen. Der Klimawandel mit seinen Extremwetterereignissen stellt insbesondere die Schadenversicherung vor große Herausforderungen. Die notwendige Deckung dieser Risiken führt zu einem Wandel, ggf. auch zu einem Umbruch der Geschäftsmodelle der Versicherungsunternehmen. Denn die Lösung für eine Versicherbarkeit dieser Ereignisse führt einerseits zu einem Diskurs über „Umbrella-Policen“ bzw. konkreten Ausschlüssen in den Verträgen, andererseits nimmt gleichzeitig die Diskussion über Poollösungen der Industrieunternehmen mit oder ohne staatliche Unterstützung aufgrund der Zeichnungspolitik der Versicherer zu. Eine Unternehmenssteuerung im Sinne einer proaktiv-prognostizierenden Vorgehensweise mit technischer Unterstützung – dem Leitgedanken „from data to value“ folgend – könnte zum Erfolgsfaktor für die Versicherungsunternehmen in der Zukunft werden (Surminski 2023).

Die Versicherungswirtschaft steht unter enormen Regulierungsdruck: Nach der umfassenden Solvency II-Gesetzgebung folgt nun die Regulierung von Nachhaltigkeitsrisiken, eine noch wesentlich relevantere Herausforderung im Sinne der Komplexität und Dynamik der nationalen und internationalen Märkte. Daher ist eine risikoorientierte und effiziente Implementierung neuer regulatorischer Anforderungen und deren effektive Nutzung auch zur Optimierung der Unternehmensführung notwendig, d. h. von einer reinen Erfüllung aufsichtsrechtlicher Pflichten hin zu einer aktiven ganzheitlichen Unternehmenssteuerung (Linderkamp et al. 2023).

Unter Digitalisierung wird allgemein die Nutzung von Daten und algorithmischen Systemen für neue oder verbesserte Prozesse, Produkte oder Geschäftsmodelle sowie deren Vernetzung verstanden. Im Schrifttum werden zwar die Bedeutung der Digitalisierung (International Association of Insurance Supervisors (IAIS) 2018; Nicoletti 2021; Noordhoek 2021) und Cyber-Sicherheit (Kane und Goldstein 2017; Wilson et al. 2019; Zgraggen 2019; Didenko 2020; Kao 2020; Wojcik et al. 2022) als Herausforderungen für den regulatorischen Kontext im Versicherungsmarkt übereinstimmend hervorgehoben, jedoch liegen bisher insgesamt nur wenige Veröffentlichungen zur fokussierten Betrachtung der Ausgestaltung der IT-Regulatorik im Versicherungsumfeld vor. In diesem Zusammenhang behandeln Khosroshahi et al. (2014) die wichtigsten Herausforderungen und die allgemeinen Auswirkungen von Solvency II auf das

Enterprise Architecture Management von Versicherungsunternehmen und stellen aus Perspektive der IT verschiedene Strategien zur Umsetzung der Solvency II-Anforderungen vor. Demgegenüber analysieren Thalhofer und Beck (2016) die sich aus der Solvency II-Richtlinie ergebenden Auswirkungen auf das IT-Outsourcing bei Versicherungsunternehmen. Der Versicherungsaufsicht wird im Allgemeinen eine wichtige Rolle bei der Stärkung der Cyber-Resilienz von Assekuranzen zugesprochen (IAIS 2016). So diskutiert bspw. Bauer (2012) grundlegende Aspekte und Herausforderungen von IT-Risiken im Kontext der Regulierung von Banken und Versicherungen. Kashyap und Wetherilt (2019) skizzieren sechs unterschiedliche Prinzipien, die von den Aufsichtsbehörden bei der Regulierung von Cyberrisiken im Finanzsektor berücksichtigt werden. Von Aldasoro et al. (2022) wird betont, dass die Regulierung eine wichtige Rolle bei der Steigerung des IT-Sicherheitsniveaus in den Unternehmen des Finanzsektors spielen kann.

Die aktive Steuerung der IT-Risiken eines Versicherers stellt einen wichtigen Entwicklungsschritt im Rahmen der Unternehmensführung dar. Bisher finden die VAIT, veröffentlicht und unmittelbar in Kraft getreten Mitte 2018 durch die BaFin, im Schrifttum nur vereinzelt bei der Betrachtung anderer Forschungsthemen Erwähnung (z. B. Ammann 2020; Gennen 2021; Pohlmann et al. 2022). Erste Ansätze zur ausführlichen Betrachtung der VAIT aus theoretischer Sicht liefern Streitz (2019) und Dreher (2019). Während sich die Untersuchung von Streitz (2019) überwiegend auf einen vergleichenden Überblick von VAIT und BAIT beschränkt, analysiert Dreher (2019) die Struktur und Inhalte der VAIT sowie weitergehend ausgewählte Detailfragen dieser IT-aufsichtsrechtlichen Bestimmungen aus juristischer Perspektive.

Die Zielsetzung der VAIT ist es, vornehmlich für das Informationsrisiko- (IRM) und Informationssicherheitsmanagement (ISM) wie auch das Management der IT-Ressourcen einen für die Geschäftsführung der Unternehmen verständlichen und anpassungsfähigen Rahmen zu schaffen. Sie sollen darüber hinaus dazu beitragen, das IT-Risikobewusstsein in den Unternehmen und gegenüber deren IT-Dienstleistern zu erhöhen. Die im Jahr 2017 erlassenen BAIT dienten dabei als Grundlage der VAIT und wurden hinsichtlich versicherungsspezifischer Gegebenheiten angepasst (Thoma und Widemann 2018). Daraus ergeben sich komplexe Anforderungen an Organisation, Prozesse und Systeme der IT in den Unternehmen (Streitz 2019). Der Aufbau der VAIT (Rundschreiben 10/2018 (VA) in der Fassung vom 20. März 2019) gliedert sich in neun Themenbereiche bzw. Anforderungsfelder, die in Abbildung 1 dargestellt werden.

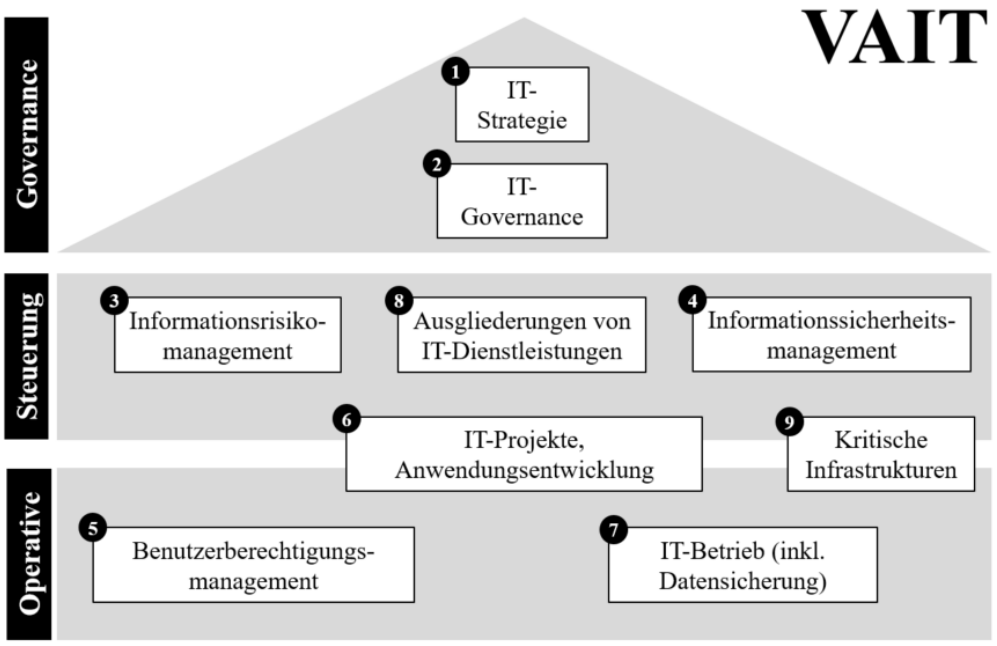


Abbildung 1: Anforderungsfelder der VAIT
Quelle: Eigene Darstellung (in Anlehnung an Gampe 2018)

Die neuen Kapitel „Operative Informationssicherheit“ und „IT-Notfallmanagement“ (Rundschreiben 10/2018 (VA) in der Fassung vom 3. März 2022), die den Fokus auf die Sicherheit von Informationen und IT-Systemen konkretisieren, finden in dem vorliegenden Beitrag keine Anwendung. Der Grund dafür ist, dass dieses Rundschreiben erst nach Durchführung der Studie veröffentlicht wurde und die Neueinführung für fundierte Erfahrungsberichte zu kurzfristig stattgefunden hat.

3 Methodik und Daten

Da die Studie ein breites Themenspektrum abdeckt und für viele der Fragestellungen kein systematisches wie auch aktuelles Datenmaterial vorliegt, woraus ein Mangel an kontextspezifischen Forschungserkenntnissen über den aktuellen Umsetzungsstand, die Probleme und Herausforderungen der anforderungskonformen Einführung bzw. Umsetzung der Regelungen der VAIT sowie die aktuellen Prüfungsschwerpunkte der bislang durchgeführten aufsichtsrechtlichen Prüfungen resultiert, wurde ein explorativer empirischer Forschungsansatz in Form einer qualitativen Expertenbefragung gewählt. Qualitative Verfahren eignen sich für explorative Fragestellungen aufgrund ihrer offenen und zugleich strukturierten Vorgehensweise (Mayring

2015). Ziel ist es, durch eine systematische Auswertung des erhobenen praxisbasierten Handlungs- und Erfahrungswissens der befragten Experten neue Erkenntnisse zu generieren (Schnell et al. 2011). Einen Überblick über das ausgearbeitete Forschungsdesign gibt Abbildung 2.

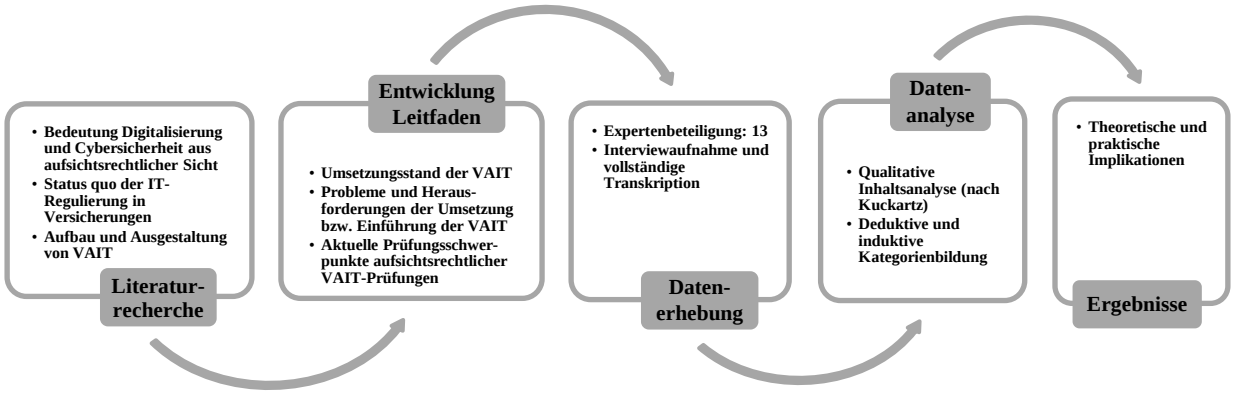


Abbildung 2: Bezugsrahmen und Elemente des Forschungsdesigns
Quelle: Eigene Darstellung

Als Befragungsform wurde die mündliche Befragung mittels semistrukturierter, leitfadengestützter Interviews gewählt, die sich insbesondere zur Ermittlung von Expertenwissen in der qualitativen Forschung etabliert hat (Schultze und Avital 2011). Dabei dienen Experteninterviews als eine ermittelnde und informatorische Interviewform um Wissensbestände zu erfahren (Lamnek 2005). Die Durchführung der Experteninterviews erfolgte mittels eines offenen Leitfadens (Myers und Newman 2007; Qu und Dumay 2011), der sämtliche relevanten thematischen Problembereiche als eigenständig formulierte Themenfelder beinhaltet (Modrow-Thiel 1993). Der Interviewleitfaden gliedert sich in sechs Teile und umfasst 22 übergeordnete Einzelfragen. Anfänglich dienten allgemeine Erläuterungen zum Forschungsvorhaben sowie die Erhebung von Angaben zur Person, beruflichen Tätigkeit und Position der befragten Experten der Schaffung einer angenehmen und vertrauensvollen Gesprächsatmosphäre und sollten den Einstieg in die Befragung erleichtern. Anschließend waren im ersten Teil einführende Fragen zur Organisation der IT-Sicherheit und aktuellen IT-Sicherheitslage in den jeweiligen Unternehmen enthalten. Der zweite Teil behandelt die Relevanz der VAIT sowie deren Auswirkungen auf die Organisationstrukturen und Prozesse in der IT. Fragen zu den wesentlichen Einzelanforderungen der VAIT und deren Umsetzungsstand in den Versicherungsunternehmen bilden den dritten Teil des Fragebogens. Der vierte Teil untersucht die Auswirkungen der VAIT auf den Ressourcenbedarf und die übergeordnete Unternehmensorganisation von Assekuranzen. Im fünften Teil wird bei den Fragen zu den praktischen Erfahrungen der Versicherer mit den Prü-

fungen zur Einhaltung der Anforderungen der VAIT durch die BaFin zwischen den Perspektiven der Unternehmen mit bereits abgeschlossenen und noch ausstehenden IT-Aufsichtsprüfungen differenziert. Der letzte Teil beinhaltet Fragen zur Einschätzung der zukünftigen Entwicklungen in der IT-Regulatorik. In Bezug auf die während der Experteninterviews gestellten Einzelfragen waren diese zum Teil vom jeweiligen Gesprächsverlauf und den Antworten der Befragten abhängig. Bei Bedarf umfassten die Einzelfragen teilweise weitergehende Unterfragen. Die explorative Untersuchung wurde mittels qualitativ-empirischer Experteninterviews von Mitte bis Ende 2020 durchgeführt. Hierfür wurden insgesamt 54 Versicherungsunternehmen und zehn weitere Institutionen (z. B. Interessenverbände oder Beratungs- und Wirtschaftsprüfungsunternehmen) kontaktiert, wovon elf Versicherungsunternehmen sowie zwei Beratungs- und Wirtschaftsprüfungsunternehmen an der Befragung teilnahmen. Dies entspricht bezogen auf alle kontaktierten Unternehmen einer Rücklaufquote der Befragung von 20,3%. Dabei fanden insgesamt 13 Experteninterviews statt, in denen unterschiedliche Fachexperten aus den Bereichen der unternehmensinternen Steuerung wie auch Überwachung der Versicherungs-IT, des IT-Risiko- und -Sicherheitsmanagements sowie der assekuranzspezifischen IT-Beratung, aufgrund ihres umfassenden praxisbasierten Handlungs- und Erfahrungswissens über den IT-bezogenen Regulierungsrahmen und den Umsetzungsstand der VAIT in der Praxis befragt wurden. Die Auswahl der Befragungsteilnehmer erfolgte nicht nach Repräsentativitätskriterien, weshalb keine Zufallsstichprobe gezogen wurde. Da qualitative Studien vorrangig das Ziel verfolgen, ein besseres Verständnis des Untersuchungsgegenstands zu generieren und Erkenntnisse, die über die untersuchten Fälle hinausreichen, zu erlangen (Hsieh und Shannon 2005; Eisenhardt und Graebner 2007; Kaczynski et al. 2014), orientierten sich die Kriterien der Stichprobenbildung an den aufgeworfenen Fragestellungen sowie den theoretisch-konzeptionellen Vorüberlegungen (Eisenhardt 1989; Yin 2003). Daher erfolgte die Kontaktierung der potentiellen Interviewpartner anhand der getroffenen Vorüberlegungen. Die Auswahl der zu befragenden Experten orientiert sich im Wesentlichen an den eingangs formulierten Forschungsfragen (Bogner et al. 2014). Der umfangreiche Wissensstand über den gewählten Forschungsgegenstand des befragten Personenkreises lässt sich im Wesentlichen auf entsprechendes Betriebs- oder Kontextwissen zu der Ausgestaltung der Versicherungs-IT als auch deren Sicherheits- und Risikomanagement wie auch der IT-regulatorischen Anforderungen an Versicherungen zurückführen. Ein Überblick über die Teilnehmerstruktur der Expertenbefragung wird in Tabelle 1 dargestellt.

Tabelle 1: Übersicht Teilnehmenden der Expertenbefragung

Interview	Experte	Unternehmensbranche	Position/Bereich
1	A	Erstversicherer	Zentralbereichsleiter IT
2	B	Erstversicherer	IT-Dokumentationsmanager
3	C	Erstversicherer	Fachreferent IT-Compliance
4	D	Erstversicherer	Vorstandsreferent IT
5	E	Erstversicherer	Hauptabteilungsleiter IT / Chief Information Security Officer (CISO)
6	G	Erstversicherer	Compliance-Officer / Informationssicherheitsbeauftragter (ISB)
7	H	Erstversicherer	Compliance-Officer
8	I	Erstversicherer	Leiter IT-Compliance
9	J	Erstversicherer	Teamleiter IT-Infrastrukturen / Informationssicherheitsbeauftragter (ISB)
10	K	Erstversicherer	Referatsleiter IT-Governance
11	L	Erstversicherer	Leiter IT
12	M	Wirtschaftsprüfung / Unternehmensberatung	Partner im Bereich Financial Services
13	N	Wirtschaftsprüfung / Unternehmensberatung	Senior Manager im Bereich Financial Services

Die Interviewdauer lag zwischen 50 und 70 Minuten, wobei die durchschnittliche Interviewdauer ungefähr 55 Minuten betrug. Die Gesprächsinhalte wurden vollumfänglich aufgezeichnet und im Anschluss vollständig transkribiert. Nach der Transkription aller Interviews fand eine abschließende inhaltliche Überprüfung der angefertigten Transkripte auf Vollständigkeit und Korrektheit statt (McLellan et al. 2003). Die Auswertung erfolgt gemäß dem Ablaufmodell der inhaltlich strukturierenden qualitativen Inhaltsanalyse nach Kuckartz (2018), das eine systematische und regelgeleitete Auswertung des Datenmaterials ermöglicht. Um den Kodierprozess zu erleichtern und systematisch zu gestalten, wurde die qualitative Datenanalysesoftware MAXQDA genutzt. Charakteristisch für die qualitative Inhaltsanalyse ist die Entwicklung eines auf der Forschungsfragestellung basierenden Kategoriensystems (Cavanagh 1997; Harwood und Garry 2003; Graneheim und Lundman 2004) und die Kodierung des Textmaterials mit dem ausdifferenzierten Kategoriensystem (Elo und Kyngäs 2008; Vaismoradi et al. 2013). Durch

eine Sichtung der Interviews wurde ein Kategoriensystem mit Ankerbeispielen entwickelt. Die Vorgehensweise der Datenanalyse zielte auf die Ziehung von Rückschlüssen zur Beantwortung der Forschungsfrage ab und das Kategoriensystem wurde deduktiv-induktiv entwickelt (Gläser und Laudel 2010; Mayring 2015), wobei mögliche Kategorien deduktiv aus den Fragen des Leitfadens abgeleitet und weitere Kategorien induktiv aus dem Material erschlossen wurden. Zu Beginn der Analyse wurde das gesamte Textmaterial mehrmals gelesen, um es dann in mehreren Iterationen mit Blick auf die in den Texten genannten inhaltlich relevanten Textsegmente zu kodieren. Dabei wurden die zu analysierenden Daten auf inhaltlich relevante Textsegmente überprüft. Die identifizierten Textelemente wurden markiert und mit „textnahen" Kodes versehen, die das Segment möglichst exakt umschreiben (Gioia et al. 2013). Gleichzeitig wurde aufbauend auf der deduktiv-induktiv Kategorienbildung in mehreren Iterationen am Material selbst ein vorläufiges Kodierschema entwickelt, in dem diejenigen Aspekte festgelegt waren, die für die Auswertung relevant erschienen und aus dem Material extrahieren werden sollten.

Um die Qualität der Kodierung zu gewährleisten, wurde eine doppelblinde Auswertung des Datenmaterials angewendet, wobei zwei Forscher die Entwicklung der Kodes unabhängig voneinander durchführen (Guest et al. 2006). Zusätzlich wurde zu den Kodes eine Beschreibung erstellt, die eine kurze Erläuterung der Bedeutung des Kodes und der intendierten Verwendung umfasste. So entstand im Verlauf der Kodierung ein finales Kodierschema, das eine Liste von primär deskriptiven Kodes enthielt und in einem zweiten Schritt strukturiert sowie in ein Kategoriensystem überführt wurde, das die induktiven und deduktiven Kategorien in eine hierarchische Ordnung (Hauptkategorien – Unterkategorien) brachte. Hierfür erfolgte eine Überprüfung der bestehenden deskriptiven Kodes auf ihren analytischen Gehalt. Durch die Zusammenfassung von bedeutungsähnlichen Kodes wurde die rein deskriptive Ebene verlassen und es entstanden analytische Kategorien, denen weitere Kodes als Unterkategorien zugeordnet wurden (Elo und Kyngäs 2008; Morse 2008; Graneheim et al. 2017). Das so entwickelte inhaltsanalytische Kategoriensystem stellte die Basis für die anschließende qualitative Auswertung dar. Das final konstruierte Kategoriensystem, auf dessen Grundlage das Textmaterial kodiert wurde, enthielt 17 Hauptkategorien, teilweise in weitere Unterkategorien differenziert, und umfasste insgesamt 55 Kategorien.

Zusätzlich erfolgte zur Sicherstellung einer eindeutigen Zuordnung des Textmaterials zu den Kategorien die Formulierung von Kodierregeln. Diese wurden getestet und falls erforderlich, basierend auf den Erkenntnissen der parallel von unterschiedlichen Personen durchgeführten

Datenanalyse und des regelmäßigen Vergleichs der Kodierungen, Präzisierungen bzw. Anpassungen der Kodierregeln vorgenommen (Downe-Wamboldt 1992; Cavanagh 1997; Burla et al. 2008).

4 Ausgewählte Ergebnisse der Studie

Die Darstellung der Ergebnisse erfolgt im nachfolgenden Abschnitt entsprechend der Empfehlungen von Yin (2003) auf weitgehend aggregierter Ebene.

4.1 Aufbauorganisation der Informationssicherheit

Allgemein beschränken sich die Versicherer nicht länger nur auf die Sicherstellung der IT-Sicherheit, d. h. den Schutz der IT-Infrastruktur. Spätestens infolge der Einführung der VAIT ist in den befragten Assekuranzen eine stärkere Berücksichtigung von Aspekten der Informationssicherheit und insbesondere die Einhaltung der Schutzziele der Informationssicherheit – d. h. der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und informationsverarbeitenden Systemen – erkennbar.

Die Ausgestaltung des organisatorischen Aufbaus der Informationssicherheit in Assekuranzen wird nach übereinstimmender Meinung der Experten im Wesentlichen durch die Unternehmensgröße bestimmt. Während in kleinen und mittelständischen Unternehmen eine Integration der Informationssicherheit in die IT-Organisation existiert, ist diese Unternehmensfunktion in großen Versicherungen ein eigenständiger und von der IT unabhängiger Teilbereich mit Schnittstellen zu dem Risikomanagement und der Unternehmens-Compliance, aber auch mit Abstimmungsprozessen zur oberen Managementebene. Als Rahmen hierfür kann ein übergreifendes Informationssicherheitsmanagementsystem dienen, mit der Funktion des ISB als eigenständigem Bindeglied zwischen sicherheits- bzw. risikorelevanten Organisationseinheiten sowie mit der Verantwortung sowohl für die Definition der prozessbestimmenden Richtlinien als auch die Sensibilisierung des Managements und der Mitarbeiter für sicherheitsrelevante Aspekte der IT. In einem kleinen Versicherer wurde die von einer Führungskraft wahrgenommene Aufgabe des ISB und Abteilungsleiters der IT auf eine von der IT ausgelagerte Stabsstelle der Informationssicherheit übertragen. Der im Rahmen der Implementierung der VAIT ernannte ISB ist für die organisatorische Umsetzung der Informationssicherheit über ein IT-Sicherheitskonzept im Unternehmen zuständig. In drei weiteren kleinen bis mittelständischen Versicherungsunternehmen hat im Zuge der Einführung der VAIT eine Auslagerung der Informationssicherheit in der Funktion des ISB aus dem Bereich der IT stattgefunden, während die operative

IT-Sicherheit weiterhin bspw. der Abteilung des IT-Betriebs zugeordnet war. Diese Zentralität der Informationssicherheit ermöglicht den befragten Unternehmen eine übergeordnete Überwachung durch interne Audits bei gleichzeitig kurzen Abstimmungswegen zum auf der Vorstandsebene angesiedelten Chief Information Officer oder Chief Digital Officer. Mit steigender Unternehmensgröße ist in Versicherungsunternehmen eine deutlich zunehmende zentrale Koordination der Informationssicherheit feststellbar, so steuert bspw. ein konzernweit zuständiger ISB die Informationssicherheit innerhalb einer separaten Abteilung über verschiedene IT-Security-Verantwortliche in den einzelnen IT-Service-Bereichen gemäß der Vorgaben der implementierten IT-Sicherheitsstandards.

Ferner stellen für die befragten Versicherer auch die Mitarbeiter ein zentrales Element der Informationssicherheit in den Unternehmen dar. Somit zählt für diese Befragtengruppe die Sensibilisierung der Mitarbeiter für die sicherheitsrelevanten Aspekte der IT und die Integration der Humanfaktoren in das Informationssicherheitskonzept zu den elementaren Aufgaben für den ganzheitlichen Schutz vor Cyber-Attacken. Mit der Implementierung der VAIT in den Unternehmen hat die Aufmerksamkeit für die verschiedenen Aspekte der Informationssicherheit auch in den höheren Managementebenen deutlich zu genommen.

4.2 Umsetzungsprozess der VAIT

4.2.1 Einflusspotenziale der VAIT auf die IT-Organisation, -Strukturen und -Prozesse

Bezogen auf den Umsetzungsprozess sind die befragten Experten überwiegend der Meinung, dass sich aus dem Inkrafttreten der VAIT im Jahr 2018 und den hieraus resultierenden regulatorischen Anforderungen an die Versicherungs-IT hochkomplexe und aktuell teilweise immer noch andauernden organisationale, strukturelle sowie prozessuale Anpassungsaktivitäten resultiert haben.

Dabei reicht der von der Umsetzung der VAIT ausgehende Einfluss in den Unternehmen von Anpassungen der IT-Strategien bis hin zu tiefgreifenden Änderungen der operativen Organisationsstrukturen, aus denen die Etablierung neuer Hierarchieebenen und Verantwortungsbereiche resultieren. Insbesondere bei den Bereichen Bestellung von ISB, Implementierung eines Benutzerberechtigungsmanagements (BBM), IT-bezogene Ausgliederungen, Individuelle Datenverarbeitung (IDV), IT-Projekte und Anwendungsentwicklung besteht aus Sicht der Befragten hoher Handlungsbedarf für die Versicherer. So ergeben sich bspw. aus der Neueinrichtung

von organisatorischen Funktionen und Informationswegen, der Etablierung neuer bzw. komplexerer Vergabe- und Rezertifizierungsprozesse im BBM, den verstärkten Kontroll- und Risikoanalyseaktivitäten bei IT-bezogenen Ausgliederungen, der Umstellung der Kapazitäts-, Ressourcen- und Budgetplanungsprozesse im Projekt- und Portfoliomanagement sowie der Entwicklung einheitlicher Vorgehensweisen oder gremienübergreifender Steuerungsmechanismen bei der Projektplanung und -durchführung wie auch der Übertragung von Anforderungen der Anwendungsentwicklung auf die IDV umfangreiche Auswirkungen bei den Versicherern. Zusätzlich haben sich auf den höheren Managementebenen durch die Anforderungsumsetzung eine Vielzahl zusätzlicher Berichtsprozesse und eine verstärkte Kontrolle der Quantifizierbarkeit von Informationssicherheitszielen etabliert. So rechnen die befragten Experten aufgrund der hohen Komplexität der VAIT bspw. bei Anwendungsentwicklungsentscheidungen in der Zukunft mit deutlichen Auswirkungen. Durch die Verteuerung der internen IT-Services und der Verlangsamung der Entwicklungsgeschwindigkeit können die VAIT durch angepasste Business-Case-Berechnungen Einfluss auf Make-or-Buy-Entscheidungen bei der Einführung neuer IT-Anwendungen haben.

4.2.2 Auslegung der Anforderungen der VAIT

Die Ergebnisse der Experteninterviews zeigen, dass bei den befragten Versicherern in der Auslegung der in den VAIT definierten Anforderungen umfangreiche Übereinstimmungen bestehen und nur vereinzelt Unterschiede in der Umsetzung existieren. So kommt es in den Unternehmen teilweise im Rahmen der Einführung der VAIT zu Anpassungen der langfristigen Geschäftsstrategien als Ordnungsrahmen für die Unternehmenssteuerung, bei denen etwaige Interdependenzen zu den *IT-Strategien* zu identifizieren und entsprechend zu berücksichtigen sind. Die IT-Strategie wird in enger Anlehnung an die Geschäftsstrategie meist auf IT-Managementebene ausgearbeitet. Dies umfasst neben dem IT-Vorstand auch die Bereichs- bzw. Abteilungsleiter der IT und in den meisten Fällen den ISB. Final beschlossen wird diese dann durch den Gesamtvorstand des Unternehmens. Der Prozess der Strategieentwicklung und -anpassung findet in den Unternehmen überwiegend innerhalb fester Gremien, Führungsrunden oder Strategieworkshops statt. Dort wirken neben dem IT-Management auch die relevanten Unternehmensbereiche, wie bspw. ISB, Datenschutz und Unternehmens-Compliance mit. Aus diesen Abstimmungsprozessen werden, nach der Prüfung und Überarbeitung der strategischen Inhalte, die Auswirkungen analysiert und ein Maßnahmenkatalog erstellt, der sich auf die operative Ebene zergliedert. Die Koordination der Umsetzung dieser Maßnahmen übernimmt teilweise eine separate Abteilung, z. B. die zentrale IT-Steuerung oder das strategische IT-Management.

Alternativ wird die Umsetzung über eine interne *IT-Governance*-Beratung, ein Demand- oder Anforderungsmanagement geregelt. Die Anpassung der IT-Strategie wird innerhalb der genannten Ausschüsse in den Unternehmen in unterschiedlichen zeitlichen Abständen durchgeführt. Der Zeithorizont reicht dabei von quartalsorientierter Überprüfung und Aktualisierung bis hin zu einer mehrjährigen festen Ausrichtung der Strategie. Durch die aus den Zeiten vor der Einführung der VAIT historisch gewachsenen Unternehmensstrukturen sind in den befragten Versicherungen teilweise nur in geringem Umfang standardisierte Prozesse der Strategieaktualisierung etabliert, sodass im Rahmen der Umsetzung neuer regulatorischer Anforderungen eine Adhoc-Umstellung der bestehenden Abläufe notwendig war.

Bezogen auf das Modul *IRM* wurden im Rahmen der Experteninterviews vornehmlich Informationen zu den wesentlichen Anforderungen für den Informationsverbund[3] und der damit einhergehenden Schutzbedarfsanalyse als bedeutende Elemente in diesem Bereich erhoben. Der Informationsverbund beinhaltet Prozesse, Daten, Anwendungssysteme und Infrastrukturkomponenten als Kernkomponenten und berücksichtigt zusätzlich die bestehenden Interdependenzen. Die Abbildung des Informationsverbundes erfolgt überwiegend in drei verschiedenen Systemen. In einer Configuration-Management-Databanken (CMDB) werden die Konfigurationselemente des IT-Betriebs (z. B. Infrastruktur, Netzwerkserver, Datenspeicher) zentral dokumentiert und zur Verwaltung bereitgestellt. Die Architekturmanagementwerkzeuge beinhalten neben einem Anwendungsregister auch die Anwendungskomponenten und die Anbindung der Systeme mit den Infrastrukturkomponenten. Auf übergeordneter Ebene liefern die Prozessmanagementwerkzeuge eine ganzheitliche Sicht auf die Geschäftsprozesse. Dabei sind diese Werkzeuge so miteinander zu verknüpfen, dass hierdurch die Ableitung eines vollständigen Informationsverbundes möglich ist. Während bei den befragten großen Versicherungen die Ableitung des Informationsverbundes auf diese Weise umgesetzt wird, findet sich in den kleinen und mittelständischen Versicherern häufig keine werkzeugbasierte Unterstützung bei der komponentenübergreifenden Abbildung des Informationsverbundes, sondern bspw. nur über die Prozesse und Schnittstellen aus den Übersichten des Business-Continuity-Managements (BCM) oder als Excel-basierte Übersichten.

Auch bei der Schutzbedarfsanalyse zeigen sich zwischen den befragten Unternehmen deutliche Unterschiede. Dabei wird das Vorgehen vorerst in einzelnen Richtlinien festgehalten bzw. ist

[3] Unter einem Informationsverbund wird die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Komponenten verstanden, der zur Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dient.

teils in der Informationssicherheitsleitlinie verankert und dient somit als Grundlage für die Zugriffs- bzw. Übertragungsbestimmungen wie auch die Ablage und Vernichtung von Informationen. Die Analyse der Schutzbedarfe kann einerseits über den ganzheitlichen werkzeugbasierten Ansatz über die Wesentlichkeit der Prozesse oder Daten vorgenommen werden. Dabei werden die Prozesse bzw. Daten nach dem Personenbezug, der Datenqualität, den Schutzzielen der Informationssicherheit und weiteren Kriterien nach der Wesentlichkeit klassifiziert. Anschließend wird der sich daraus ergebende Scorewert nach dem Maximalprinzip in die einzelnen Komponenten des Informationsverbundes vererbt. Andererseits kann die Vererbung der Schutzbedarfe bei einer Teilung des Informationsverbundes in die drei genannten Systeme durch Schnittstellen erfolgen. Hierbei ist aber vor allen auf durchgängige Konsistenz und Vollständigkeit von Interdependenzen zu achten. Auch im Startpunkt der Risikoanalyse unterscheiden sich einige Versicherer. Hierbei gehen diese entweder gemäß dem Top-Down-Prinzip über die Prozesse in die darunterliegenden Ebenen oder fokussieren sich auf die IT-Services und die darin enthaltenen Daten und spiegeln diese nach dem Bottom-Up-Ansatz auf die Prozesse. Demgegenüber kommen in kleineren Assekuranzen häufig Excel-basierten Individualanwendungen zur Abbildung des Informationsverbunds und der darin klassifizierten Schutzbedarfe zum Einsatz. Bei beiden in den befragten Unternehmen zur Schutzbedarfsanalyse eingesetzten Verfahren – der Bottom-Up-Methode oder den Excel-basierten Individualanwendungen – bestehen Risiken in der konsistenten und vollständigen Festlegung der Schutzbedarfe. Die Verwendung des Bottom-Up-Ansatzes kann die Notwendigkeit der Eskalation bereits festgelegter Schutzbedarfe induzieren, indem bei den IT-Systemen anfangs eine niedrigere Bewertung der Schutzbedarfe vorgenommen wurde als bei dem übergeordneten Prozess. Zudem können durch den Einsatz von Excel-basierten Individualanwendungen die bestehenden Abhängigkeiten von Systemen, Prozessen und anderen Komponenten nicht vollständig identifiziert bzw. nicht adäquat erfasst werden, woraus Inkonsistenzen in der Schutzbedarfsanalyse resultieren. Gleichzeitig ergibt sich durch die erstmalige Festlegung der Schutzbedarfe über alle Komponenten hinweg ein hoher Initialaufwand.

Unabhängig von der definierten Informationssicherheitsorganisation verbleibt die Gesamtverantwortung für die Informationssicherheit bei der Geschäftsleitung. Um die Planung und Durchsetzung des Informationssicherheitsprozesses angemessen fördern und koordinieren zu können, ist regelmäßig mindestens eine Person im Unternehmen – i. d. R. der ISB – zu benennen.

Vereinzelt existierte die Rolle des ISB in den befragten Unternehmen bereits vor den VAIT in der Informationssicherheitsorganisation. Überwiegend erfolgte die Schaffung der Position des ISB jedoch nach der erstmaligen Veröffentlichung des Rundschreibens zu den VAIT durch die BaFin im Jahr 2018. Grundsätzlich wird der ISB/CISO durch Beschluss der Geschäftsführung und i. d. R. intern bestellt. Organisatorisch verortet wird diese Unternehmensfunktion im Allgemeinen als separate Stabsstelle oder als eigenständige Einheit im IT-Bereich mit einer direkten Berichtslinie an die Geschäftsführung. Die wichtigsten in den VAIT bezogen auf die Rolle des ISB definierten Anforderungen zur Sicherstellung der Unabhängigkeit dieser Position gegenüber der operativen IT wird in den befragten Versicherungen unterschiedlich interpretiert und umgesetzt. Mit dem organisatorischen Lösungsansatz als eigene Stabsstelle ist der ISB offiziell prozessual und strukturell vollständig aus der IT gelöst. Der Verbleib des ISB im IT-Bereich muss über Kompetenzen und Aufgabendefinitionen legitimiert werden. Jedoch findet teilweise auch die Trennung vom operativen Geschäft durch die vollständige Auslagerung der IT-Dienstleistungen auf ein Tochterunternehmen oder durch die Separierung einer eigenständigen Abteilung für die Informationssicherheit im IT-Ressort statt. Dies hat zu Folge, dass der ISB keine administrativen Aufgaben innerhalb der IT wahrnehmen darf, sondern sein Aufgabenschwerpunkt überwiegend in der Koordination von Sicherheitsmaßnahmen liegt. Das Aufgabenspektrum umfasst die Erstellung von Richt- und Leitlinien, die Sensibilisierung der Mitarbeiter für die sicherheitsrelevanten Aspekte der IT durch regelmäßig stattfindende Sicherheitsaudits, die Steuerung technisch organisatorischer Sicherheitsmaßnahmen und die Erstellung der quartalsweisen Berichterstattung über die Informationssicherheitslage im Unternehmen.

Die Anforderungen des Moduls zum BBM führen in den befragten Versicherungsunternehmen zu umfangreichen Veränderungen im Bereich der privilegierten Benutzer und Rezertifizierungsprozesse. Aufgrund der unternehmensseitig bestehenden Unsicherheit hinsichtlich der zufriedenstellenden Umsetzung der neuartigen Regelungen der VAIT und des hohen Änderungsbedarfs in den bestehenden Strukturen sowie Prozessen ergeben sich bei einem Großteil der Befragtengruppe erhebliche Zweifel, ob durch die vorgenommenen Anpassungen in den Prozessen eine anforderungskonforme Implementierung erreicht wurde, da im Berechtigungsmanagement erhebliche Abhängigkeiten zu anderen Bereichen bestehen.

So schreiben die von den Unternehmen zu ermittelnden Schutzbedarfe den Umgang wie auch die Verwendung von Berechtigungen vor und sind daher im Voraus vollständig festzulegen, bevor die in Zusammenhang stehenden Berechtigungsprozesse finalisiert werden können. Für

jede Anwendung ist die Erstellung eines separaten Berechtigungsprozesses erforderlich, woraus ein deutlich erhöhter zeitlicher Aufwand resultiert. In zwei großen Mittelstandsunternehmen der Versicherungswirtschaft findet die Verwaltung der Berechtigungen in einem zentralen System statt, dessen Prozessabläufe und -strukturen im Rahmen der Umsetzung der VAIT diverse Anpassungen erforderten. Die Dokumentations- und Kontrollverfahren sind im Hinblick auf kritische Berechtigungen zu implementieren, um bspw. den Aufbau von Änderungshistorien zu ermöglichen. Hierzu wird bspw. ein Privileged-User-Management verwendet, in dem die Aktionen von Administratoren bzw. Benutzern mit speziellen Administrationsrechten aufgezeichnet und protokolliert werden. Aus technischer Perspektive gewinnen ebenfalls Aspekte, wie z. B. die Beschaffung zusätzlicher Speicherplatzkapazitäten zunehmend an Bedeutung. Die geforderten Rezertifizierungsprozesse sind überwiegend nur mit entsprechenden Systemeigenschaften umzusetzen. Optimalerweise sollten hierzu die Überprüfung konfliktärer Berechtigungen und regelmäßige Untersuchungen des bestehenden Berechtigungskonzeptes standardisiert in einem System umgesetzt werden. Jedoch gestaltet sich die Umsetzung solcher Anforderungen in den kleineren Versicherungsunternehmen deutlich schwieriger, da in dieser Befragtengruppe systemseitig hierfür auf einfache Lösungen zurückgegriffen wird. Darüber hinaus verfügen diese Unternehmen teilweise nicht über vollständige Übersichten zu allen existierenden Berechtigungen und potenziell kritischen Verbindungen. Hierdurch ist ein kontinuierlicher Überprüfungsprozess nur äußerst schwer abbildbar.

Im Bereich der *IT-Projekte* ergaben sich für die Mehrheit der Versicherer aus der Befragungsstichprobe keine wesentlichen Änderungsbedarfe. Teilweise haben die Unternehmen die Einführung der VAIT veranlasst einzelne mit IT-Projekten in Zusammenhang stehenden Prozesse zu überarbeiten. So sind in einer kleinen Assekuranz bei den Mechanismen zur Projektsteuerung Standardisierungen und Erweiterungen vorgenommen worden. Dabei fand die Etablierung von Maßnahmen zum Projektcontrolling, wie z. B. die Budgetplanung mittels Projektsteckbriefen, zur Optimierung des Ressourcen- und Kapazitätseinsatzes statt. Ebenfalls wurde die Projektportfolioplanung um ein IT-Management- und IT-Vorstandsboards in Zusammenarbeit mit einem Fachgremium für Projekte ergänzt. Eine befragte mittelständische Versicherung hat Anpassungen in der IT-Prozesswelt im Umfeld der IT-Projektorganisation durchgeführt. Nachdem bislang die einzelnen Projektleiter bei der Durchführung und Organisation der Projekte über hohe Entscheidungsspielräume verfügten, wurden mit den in den VAIT festgelegten Richtlinien unternehmensinterne Standards zu der Dokumentation und dem Berichtswesen von Projekten geschaffen, wodurch eine verbesserte Steuerung der Projekte und der damit im Zusammenhang stehenden Informationsrisiken ermöglicht wurde.

Bei der *Anwendungsentwicklung* wird durch die VAIT der Betrachtungsfokus schwerpunktmäßig auf die in den Versicherungen vorhandenen IDV gelegt. In den befragten Versicherungen umfasst diese Art von IT-Applikationen sowohl einfache Excel-basierte Individualanwendungen für die Urlaubs- und Abwesenheitsplanung als auch hochkomplexe Individualanwendungen zur versicherungsmathematischen Modellierung. Mit der Einführung der VAIT sind die Versicherungsunternehmen verpflichtet ein zentrales IDV-Register zu führen, das in enger Abstimmung mit den einzelnen Fachbereichen aufzustellen und regelmäßig zu aktualisieren ist. Hierüber wurde die Fachabteilungen in den befragten Unternehmen überwiegend im Rahmen von themenspezifischen Informationsveranstaltungen und Workshops informiert, um die Mitarbeiter für die Bedeutung der Thematik zu sensibilisieren und eine Bestandsaufnahme der gesamten IDV im Unternehmen zu initiieren. Insbesondere die Festlegung von Leitlinien zu den IDV-Anwendungen, die Konzeption und Durchführung von Schulungen und die Definition von Kriterien wurden in den Versicherungen als unterstützende Instrumente für die Fachabteilungen eingesetzt, um die Vollständigkeit des zu erstellenden IDV-Registers innerhalb ihres Verantwortungsbereichs sicherzustellen. In der Mehrheit der befragten Versicherer ist die Fertigstellung des IDV-Registers inzwischen abgeschlossen. Nur bei einer kleineren Assekuranz ist die Erstellung des IDV-Registers noch nicht vollständig beendet. Teilweise sehen die Experten aus den befragten Unternehmen noch betrieblichen Optimierungsbedarf vornehmlich bei der Erstellung und Aktualisierung dieses Registers. Mit steigendem Schutzbedarf wachsen auch die Anforderungen an die IDV von Versicherungen und nähern sich immer stärker den Vorgaben einer professionellen Anwendungsentwicklung an. Dadurch gewinnen Versionsverwaltungssysteme, Zugriffsschutzkonzepte und Releasemanagementprozesse zunehmend an Bedeutung, woraus sich für die betroffenen Fachabteilungen neue Herausforderungen ergeben. Für die Mehrheit der befragten Versicherer resultiert aus der Umsetzung der VAIT für die vorhandene IDV zwar ein deutlich gestiegener Arbeitsaufwand für die betroffenen Fachabteilungen, jedoch gehen sie auch überwiegend von einer Implementierung anforderungskonformer Lösungen in ihren Unternehmen aus. Die befragten Experten aus der Wirtschaftsprüfung und Unternehmensberatung kritisieren in diesem Zusammenhang jedoch den zu oberflächlichen Ansatz zur Definition von IDV. Die Befragungsergebnisse zeigen, dass in den Assekuranzen diesbezüglich aktuell zu kurzfristig ausgerichtete Steuerungsmechanismen implementiert sind, da selbst in wichtigen und teilweise rechnungslegungsrelevanten Unternehmensbereichen, wie z. B. dem Aktuariat, noch kein ausreichendes Bewusstsein für die Besonderheiten wie auch die Anforde-

rungen der IDV-Anwendungen existiert sowie der aus der Umsetzung der Anforderungen resultierende hohe Arbeitsaufwand für die Fachabteilung den Realisierungsprozess deutlich verlangsamt.

Ferner stellen die *Ausgliederungen und der sonstige Bezug von IT-Dienstleistungen* bzw. der *isolierte Bezug von Hard- und Software* ein wesentliches Betrachtungsfeld der VAIT dar. Die zugehörigen Prozesse werden in den Unternehmen der Befragungsstichprobe überwiegend durch einen zentralen Gesamteinkauf oder separaten IT-Einkauf in Abstimmung mit einem Dienstleister- oder Vertragsmanagement organisiert. Speziell der Bereich Ausgliederungen fällt bei den befragten Versicherern mehrheitlich in das Tätigkeitsfeld eines eigenständigen Ausgliederungsbeauftragten, der für diesen Aufgabenbereich in Zusammenarbeit mit anderen Schlüsselfunktionen, wie z. B. der Unternehmens-Compliance, die Verantwortung trägt. Diese sind für das Verfassen von Richt- bzw. Leitlinien zum Ausgliederungs- oder Beschaffungsprozess zuständig, die vom Anforderer vor und/oder während eines Outsourcings respektive der Beschaffung zu befolgen sind. So beinhaltet bspw. eine Ausgliederungsleitlinie i. d. R. eine Checkliste zur Feststellung der Art des Bezugs. Hierbei findet mittels eines Fragenkatalogs eine Abfrage bestimmter Kriterien zur Ermittlung der Art des Bezugs statt. In diesem Zusammenhang liegt ein sonstiger IT-Fremdbezug vor, sofern es sich um den Bezug von Hard- und Softwarekomponenten ohne Unterstützungsleistungen handelt. Kommen bei Wartungs- und Pflegeverträgen bspw. ergänzend Unterstützungsleistungen hinzu, dann stellt die Beschaffung eine sonstige IT-Dienstleistung dar. Damit eine Ausgliederung vorliegt, müssen besondere Faktoren zur Wesentlichkeit zutreffen, wie z. B. die Abgabe der Datenhoheit durch die Nutzung von Cloud-Computing (CC)-Diensten. Falls eine solche Ausgliederung besteht, ist diese dann verpflichtend der zuständigen Aufsichtsbehörde anzuzeigen. Handelt es sich nach der Checkliste um eine sonstige Dienstleistung mit IT-Bezug oder gar um eine Auslagerung, ist gemäß den Regelungen der VAIT zwingend eine Risikoanalyse des betroffenen Unternehmens durchzuführen. Diese wird ebenfalls mittels eines spezifischen Formblatts bzw. Fragenkatalogs durchgeführt, das vom Anforderer auszufüllen und zur finalen Prüfung sowie Gesamtrisikobewertung den Stellen des operationellen Risikomanagements, z. B. der Unternehmens-Compliance, Rechtsabteilung, dem ISB, der Datenschutzorganisation oder dem BCM vorzulegen ist. Von mehreren der befragten Unternehmen wird aufgrund der einschlägigen Erfahrungen aus vorangegangenen BAIT-Prüfungen aus dem Bankenumfeld auf die in der Praxis häufig auftretenden Schwierigkeiten der Klassifizierung von Auslagerungen hingewiesen, da es sich bspw. bereits bei der Entsorgung sensibler Daten durch externe Aktenvernichtungsanbieter aufgrund des hohen Schutzbedarfs um eine wesentliche Auslagerung handelt. Als Gründe für die Probleme bei

der Klassifizierung von Auslagerungen werden von diesen Versicherern einerseits fehlende Awareness für dieses Thema bei den Mitarbeitern und andererseits die in den Unternehmen vorherrschende mangelnde Wahrnehmung der Wichtigkeit des Klassifizierungsprozesses genannt. Hieraus resultieren aus Sicht der befragten Unternehmen u. a. aufgrund der gestiegenen regulatorischen Vorgaben der VAIT in diesem Bereich zunehmend zeitlich deutlich verlängerte Bestellvorgänge für die Versicherer.

Das im Rahmen der Überarbeitung der VAIT durch die BaFin ergänzte KRITIS-Modul ist nur für drei von elf Versicherern aus der Befragungsgruppe relevant. Zumeist ist die Thematik KRITIS den Versicherern jedoch nicht erst aufgrund der Novellierung der VAIT im Jahr 2019 und der Ergänzung eines eigenständigen KRITIS-Moduls bekannt, sondern bereits durch die BSI-Kritisverordnung und den damit in Zusammenhang stehenden gesetzlichen Anforderungen. Hierbei sind in den befragten Unternehmen Unterschiede in der Wahrnehmung des Aufwands zur Umsetzung der Anforderungen aus der BSI-Kritisverordnung und den Vorgaben des KRITIS-Moduls der VAIT zu erkennen. Generell entsteht aus der zunehmenden Relevanz der KRITIS durch die Vorbereitung von Audits und Folgeprozessen ein erheblicher Mehraufwand für die befragten Unternehmen. Während sich dies für einen Teil der Versicherer überwiegend in einem hohen Arbeitsaufwand für die erstmalige Umsetzung widerspiegelt, ergeben sich hieraus für die anderen Unternehmen dieser Befragtengruppe langfristig ein deutlich gestiegener Arbeitsaufwand und ein höherer personeller Ressourcenbedarf. Die betroffenen Versicherungsunternehmen unterliegen erhöhten Dokumentations-, Berichts- und Zertifizierungspflichten. Zusätzlich kommen gestiegene Anforderungen im Bereich des Notfall- sowie Ausfallmanagements in Form von gesonderten Prüfungen auf die Unternehmen zu. Daneben werden auch die Dienstleister verstärkt in diesen Auditprozess einbezogen, wodurch die Kooperation mit Vertragspartnern erschwert wird. Von einem befragten Unternehmen wird angegeben, dass es grundsätzlich bereit ist die Anforderungen des KRITIS-Moduls freiwillig zu erfüllen, jedoch können aus einer Einstufung als KRITIS auch erhebliche Nachteile resultieren. Die Mehrheit der Versicherungsunternehmen sind aktuell von Vorgaben des KRITIS-Moduls nicht betroffen, jedoch wird sich nach Ansicht der Befragungsteilnehmer durch eine mögliche Anpassung der Schwellenwerte der Adressatenkreis zukünftig deutlich ausweiten.

4.2.3 Umsetzungsstände der VAIT in den Unternehmen

Mehrheitlich wurde die Umsetzung der in den VAIT definierten Anforderungen von den befragten Unternehmen auf Projektbasis abgewickelt und nur vereinzelt erfolgte eine Integration

der Umsetzungsvorgänge in die betrieblichen Regelprozesse. Bei der Beurteilung des aktuellen Umsetzungsstandes der VAIT in der Praxis zeigen sich in den einzelnen Befragtengruppen deutliche Unterschiede. Während die Experten aus der Versicherungswirtschaft den Umsetzungsstand überwiegend als hoch einschätzen, wird dieser von den Unternehmensberatern und Wirtschaftsprüfern zumeist als niedrig beurteilt. Insbesondere bei der Umsetzung der Anforderungen im Bereich der Ausgliederungen besteht in den Versicherungen noch ein deutlicher Nachholbedarf.

Während die Versicherer vornehmlich Schwierigkeiten in der Umsetzung der Module *IRM*, *IT-Projekte und Anwendungsentwicklung*, *BBM* sowie *Ausgliederungen und sonstiger Fremdbezug von IT-Dienstleistungen* als Grund für die bisher unvollständige Anforderungsumsetzung angeben, sind in zwei Unternehmen speziell Probleme bei der Implementierung der Module *IT-Strategie, IT-Governance*, *ISM*, *IT-Betrieb* und *KRITIS* ursächlich für den geringen Umsetzungsstand. Demgegenüber sind Anforderungen an die *IT-Strategie* und *IT-Governance* bei den übrigen befragten Versicherern bereits fast vollständig umgesetzt. Die von der BaFin festgelegten Mindestinhalte bzw. -bestandteile der Strategie boten den befragten Versicherern hierbei einen guten Leitfaden für einen anforderungskonformen Aufbau. Die Governance-Strukturen mussten teilweise im Zuge des Projektes großflächig angepasst werden, um die geforderte Verzahnung sowie Abstimmung zwischen Strategie und Governance zu gewährleisten. Das *ISM* ist nach Meinung der Versicherer überwiegend umgesetzt. Nur in einem Fall lag bisher noch kein umfassender und fachbereichsübergreifender Sollmaßnahmenkatalog für die Informationssicherheit vor.

Als ausschlaggebend für den niedrigen Umsetzungsstand der VAIT war für einige Versicherer das Modul *IRM*. Dabei gestaltet sich häufig die praktische Darstellung des Informationsverbundes und die damit einhergehende Schutzbedarfsanalyse schwierig. Teilweise liegt keine vollständige oder übergreifende CMDB vor. Der Informationsverbund wird noch aus zu vielen einzelnen Systemen abgeleitet, die nicht miteinander verknüpft sind. Als Folge sind die Schutzbedarfsfeststellungen noch nicht vollumfänglich erfolgt. Das Modul *Ausgliederungen und sonstiger Fremdbezug von IT-Dienstleistungen* ist bei einigen Versicherern immer noch vollständig umgesetzt. Die Ausgliederungsrichtlinien sind u. a. zu oberflächlich und beziehen die Kontrolle von Sub-Dienstleistern nicht ausreichend ein. Darüber hinaus fehlt z. B. in einem der befragten Unternehmen ein Ausgliederungsbeauftragter, sodass die Verantwortlichkeiten dort nicht klar formuliert sind. Bei fehlender Dokumentation von Verantwortlichkeiten wird von der BaFin

laut eines Experten grundsätzlich eine Anforderung als nicht erfüllt angesehen. In diesem Unternehmen existiert zudem kein stringenter Prozess zur Klassifizierung von Ausgliederungen und zur nachgelagerten Kontrolle der Dienstleister. Im Bereich *IT-Projekte* erfolgten in den Versicherungen umfassende Umstrukturierungen, sodass diesbezüglich in den Unternehmen keine umsetzungsrelevanten Aspekte mehr offen sind. Kritische Auswirkungen auf den Umsetzungsstand hat die Thematik IDV innerhalb der *Anwendungsentwicklung*. Für zwei Unternehmen stellen die Anforderungen zur IDV aufgrund ihrer bisherigen Organisation laut eigener Aussage keine Herausforderung dar und sie konnten diese problemlos umsetzen. Sieben der elf befragten Versicherungsgesellschaften haben bis zum Erhebungszeitpunkt der Studie jedoch noch nicht alle Anforderungen des Moduls umgesetzt. Es existieren zudem noch größere Unsicherheiten hinsichtlich der Reichweite und des Umfangs des notwendigen Anpassungsbedarfs in den Unternehmen. Die hohe Anzahl von IDV in den Versicherungen und die diesbezüglichen Anforderungen, wie z. B. Testverfahren oder Berechtigungskonzepte, erschweren die zentrale Kontrolle durch die Abgabe der Verantwortung in die Fachbereiche. Eine kleinere Versicherung hat bspw. noch nicht mit der Umsetzung dieses Anforderungsmoduls begonnen. Die Fachabteilungen wurden bislang nicht mit diesen Themen betraut, um eine mögliche Überlastung zu vermeiden. Das Modul *BBM* wurde bei neun von elf Unternehmen als wichtiger, noch nicht vollständig abgeschlossener Teilbereich bei der Umsetzung der VAIT genannt. Das Modul gestaltet sich in der Umsetzung als sehr zeit- und aufwandsintensiv. So ist zwar die Richtlinienebene weitestgehend fertiggestellt, aber die Konzeption der regelmäßigen Rezertifizierungen bzw. die Erstellung von Berechtigungsprozessen für die einzelnen Anwendungen ist nur schwer bzw. langsam umsetzbar. Gleiches gilt für die damit verbundene Dokumentation, wozu auch die Überwachung kritischer oder konfliktärer Berechtigungen gehört.

Die drei zuletzt genannten Anforderungsmodule sind auch von den Experten der Wirtschaftsprüfung und Unternehmensberatung als kritische Aspekte der Umsetzung genannt worden. Beim Management von Ausgliederungen ergeben sich offene Punkte in der initialen und kontinuierlichen Risikobewertung der Services und Dienstleister. Zudem sind häufig keine lückenlose Erstaufnahme der IDV in den Gesellschaften und kein stetiger Überprüfungsprozess vorhanden. Im BBM erschwert die historisch bedingte Heterogenität und Vielfalt der Systemlandschaften in den Versicherungsunternehmen die Umsetzung der geforderten Regelungen der VAIT. Gleichzeitig ist der Umgang mit administrativen bzw. kritischen Berechtigungen nur unzureichend geregelt. Ein Experte erklärt in diesem Gesamtkontext, dass einige Unternehmen ihren tatsächlichen Umsetzungsstand überschätzen und gleichzeitig den damit eingehenden Arbeitsaufwand unterschätzen.

4.2.4 Umsetzungsaufwand und Ressourcenverwendung für die Einführung der VAIT

Bezogen auf den Umsetzungsaufwand der VAIT zeigen sich in den Versicherungen hinsichtlich der Bewertung des Arbeitsaufwands für die erstmalige Umsetzung der regulatorischen Anforderungen und deren sich anschließenden regelmäßigen Einhaltung deutliche Unterschiede. Die kleinen und mittelständischen Versicherer haben i. d. R. die in den VAIT formulierten Anforderungen innerhalb ihrer bisherigen Prozesse ohne große finanzielle Mehrbelastungen und einen unverhältnismäßig hohen Umsetzungsaufwand im Vergleich zu den übrigen laufenden IT-Projekten implementiert. Jedoch wird von den Interviewpartnern die eindeutige Zuordnung der Aufwendungen für die Umsetzung als problematisch eingeschätzt, da bspw. die Anforderungen aus den VAIT bereits schon vor deren Inkrafttreten durch die vorherige Implementierung international anerkannter Standards mit IT-Sicherheitsaspekten erfüllt wurden. Zudem wird die die Aufwandszuordnung durch die aufwendige Dokumentation der vielfach kleinteiligen und dezentral stattfindenden Umsetzungsaktivitäten, die vornehmlich auf Abteilungs- und Mitarbeiterebene erledigt werden, erschwert. Ebenfalls gestaltet sich in diesem Zusammenhang insbesondere für kleine und mittelständische Versicherer die Kalkulation der finanziellen Aufwendungen schwierig, da diese häufig nicht über eine ausreichende personelle, infrastrukturelle und prozessuale Ausstattung verfügen. Hierdurch wird von einem Interviewpartner der Umsetzungsaufwand für die VAIT höher als die Implementierung der Solvency-II-Anforderungen oder der Regelungen aus der EU-DSGVO bewertet, sodass die Einführung der VAIT ohne Unterstützung durch externe Beratungsunternehmen nicht möglich erscheint. So zeigen sich in den von den befragten Versicherern genannten Spannweiten der Aufwandsschätzungen für die Einführungsprojekte erhebliche Unterschiede, da diese von 500 bis hin zu 1500 Personentagen reichen und dadurch als Großprojekte mit langfristiger Ressourcenbindung klassifiziert werden.

Bezogen auf die Anforderungsmodule lassen sich in der Aufwandsbetrachtung Parallelen zu offenen Feldern aus der Evaluation des Umsetzungsstandes erkennen. Als wesentliche Aufwandtreiber in den Unternehmen lassen sich die Module IRM, Ausgliederungen und sonstiger Fremdbezug von IT-Dienstleistungen, IT-Projekte und Anwendungsentwicklung wie auch das BBM identifizieren. Hierbei weist im Modul IRM der initiale Aufbau und die Verwaltung aktueller Informationsverbünde eine Vielzahl von Interdependenzen zu anderen Themenfelder auf. Im Bereich der Ausgliederungen gestaltet sich die Umsetzung der Anforderungen zur Dienstleistersteuerung deutlich umfangreicher, wodurch die Arbeitsprozesse durch die zusätzlichen Vorgänge, wie z. B. die Ausgliederungsklassifizierung oder Risikobewertung, zeitlich

verlangsamt werden, sodass sich die Abwicklung von Routineaktivitäten zukünftig zeitlich deutlich verlängert. Hiervon sind durch die gestiegenen Anforderungen der VAIT jedoch nicht nur die Beschaffungsprozesse, sondern auch die komplexen Unternehmensaktivitäten, wie z. B. die Anwendungsentwicklung, betroffen. Insbesondere der sich aus den regulatorischen Vorgaben zur IDV ergebende Mehraufwand für die Fachabteilungen wird von den befragten Experten übereinstimmend hervorgehoben. Im Berechtigungsmanagement werden die Schwierigkeiten weniger in der Art und Weise der Umsetzung der VAIT-Anforderungen, sondern vielmehr im hohen Zeitaufwand der Einführung bzw. Anpassung der notwendigen Berechtigungsprozesse für alle Anwendungen gesehen.

Der durch die Umsetzung der VAIT entstandene Ressourcenaufwand wird von den Versicherern bezogen auf die Personalsituation überwiegend als temporär eingeschätzt. Während für die Umsetzungsprojekte die Beschaffung und Nutzung umfangreicher externer Ressourcen notwendig war, konnte die sich an die Einführung anschließenden Regelprozesse größtenteils mit bestehenden internen Ressourcen realisiert werden. Ein zusätzlicher Personalbedarf entsteht in den befragten Unternehmen vorwiegend durch die Besetzung von aus der Umsetzung der VAIT-Anforderungen resultierenden neu zu schaffenden Stellen. So hat sich in den befragten Unternehmen teilweise auch durch die Erfüllung der Anforderungen des KRITIS-Moduls zusätzlicher Bedarf an spezifischen Fachkräften ergeben. Die Experten aus den Beratungs- und Wirtschafsprüfungsunternehmen teilen die Einschätzung der Assekuranzen und sehen ebenfalls einen aus der Umsetzung der VAIT resultierenden personellen Mehrbedarf, der sich nur bedingt durch Mehrarbeit den vorhandenen Ressourcen kompensieren lässt und mittel- bis langfristig zu einem erhöhten Personalbedarf an speziell ausgebildeten Fachkräften führen wird.

4.3 Prüfungsaktivitäten und -praxis der VAIT durch die BaFin

Seit der Veröffentlichung der VAIT im Jahr 2018 haben im deutschen Versicherungsmarkt bis zum Erhebungszeitpunkt der Studie nur vereinzelt Prüfungen zum Umsetzungsstand der neu geltenden IT-Regulatorik durch die BaFin in den Unternehmen stattgefunden. So rechnet auch nur die Hälfte der befragten Unternehmen mit einer Prüfung durch die BaFin innerhalb der nächsten zwei bis drei Jahre. Insbesondere die Unternehmensgröße stellt aus Sicht der Befragten ein wichtiges Merkmal für die Auswahl der zu prüfenden Versicherer dar, sodass große Versicherer tendenziell aufgrund ihrer wirtschaftlichen Bedeutung eine zeitnahe und kleinere Unternehmen eine spätere VAIT-Prüfung erwarten. Demgegenüber wird diese Einschätzung von den Interviewpartnern aus der Unternehmensberatungs- und Wirtschaftsprüfungsbranche

nicht geteilt, da diese auch kurzfristig mit vermehrten Prüfungsaktivitäten bei kleinen und mittelständischen Versicherungen rechnen. Aus Sicht dieser Befragtengruppe wird die Bedeutung der VAIT und deren Wichtigkeit für die Versicherungsaufsicht von den Unternehmen deutlich unterschätzt. Jedoch sind aus Sicht dieser Expertengruppe die fehlenden Übergangsfristen zur Umsetzung der in den VAIT formulierten Anforderungen für die Unternehmen unproblematisch, da eine Prüfung vieler Einzelanforderungen in der Vergangenheit bereits im Rahmen der Jahresabschlussprüfungen durchgeführt wurde.

Nahezu alle befragten Versicherungsunternehmen, bei denen bislang noch keine VAIT-Prüfung stattgefunden hat, sehen sich auf mögliche zukünftige Überprüfung durch die BaFin ausreichend vorbereitet. Nur eine Assekuranz sieht sich aufgrund des aktuell noch sehr geringen Umsetzungsstandes der VAIT auf eine potenzielle zukünftige Unternehmensprüfung durch die BaFin als unzureichend vorbereitet. Neben der BaFin werden die VAIT-Prüfungen auch auf Veranlassung der Aufsichtsbehörden durch externe Wirtschaftsprüfungsunternehmen durchgeführt. Jedoch erwarten die befragten Versicherer mehrheitlich nicht, dass sich in der Praxis die Zeitdauer, der Ablauf oder die Intensität der von den Wirtschaftsprüfungsunternehmen durchgeführten Prüfungen, von denen durch die BaFin selbst durchgeführten wesentlich unterscheiden. Allerdings sehen einige Assekuranzen die aktuell bei der BaFin vorgehaltenen personellen Personalressourcen und fachlichen Kompetenzen für den Umfang der zukünftig angestrebten Unternehmensprüfungen als zu gering an. Dies spiegelt sich derzeit in der Praxis insbesondere an der Vielzahl von Vergaben der Prüfungsaufträge an externe Parteien und den deutlichen Zeitverzögerungen bei der Fertigstellung der Prüfberichte wider.

Abgeleitet aus den eigenen Prüfungserfahrungen der befragten Unternehmen und den aus dem Marktumfeld verfügbaren Informationen zu den Prüfungen, betreffen die Feststellungen der Prüfer überwiegend folgende Sachverhalte:

- die administrativen Berechtigungen im Modul BRM,
- die erstmalige Aufnahme und kontinuierliche Überprüfung der IDV im Modul IT-Projekte und Anwendungsentwicklung,
- die initialen Risikobewertungen und Folgerisikobewertung der Ausgliederungen sowie
- die Mängel in der Dokumentation des Informationsverbundes und der Schutzbedarfsklassifizierung im Modul IRM.

Im Anschluss an eine VAIT-Prüfung wird den Versicherungsunternehmen eine Frist zur Vorlage eines Maßnahmenpaketes zur Nachbesserung und ggf. zur Berichterstattung über den Umsetzungsstand der Nachbesserungen gesetzt. Nach Aussagen der befragten Experten beträgt diese Fristdauer hierfür in der Praxis i. d. R. weniger als ein Jahr. Dabei stehen der BaFin unterschiedliche Mittel zur Durchsetzung der geforderten Verbesserungsmaßnahmen zur Verfügung. Einerseits kann durch die Ankündigung einer zeitnahen strengen Nachprüfung zeitlicher Druck auf die Versicherungsunternehmen erzeugt werden und andererseits hat die BaFin darüber hinaus die Möglichkeit in den Geschäftsbetrieb, z. B. durch die Übernahme von Schlüsselfunktionen, einzugreifen oder diesen bei gravierenden Unregelmäßigkeiten sogar komplett stillzulegen. Jedoch ist eine Verhängung finanzieller Sanktionen seitens der BaFin gegen die betroffenen Versicherer nicht möglich. Hinsichtlich des Umfangs und der Intensität der VAIT-Prüfung herrscht bei den befragten Experten Uneinigkeit. Vereinzelt gehen die Befragten davon aus, dass die VAIT-Prüfungen keine wesentlichen Unterschiede und keinen höheren Aufwand zu den anderen von der BaFin durchgeführten Prüfungen aufweisen. Demgegenüber wird jedoch auch eine strengere Herangehensweise der BaFin in der technischen Prüfungstiefe von IT-Systemen wie auch durch sehr exakte und starre Ergebniserwartungen in der Anforderungsumsetzung ausgegangen. Analog zu den in der Praxis bereits durchgeführten BAIT-Prüfungen wird hier eine stetige Steigerung der Prüfungsintensität erwartet, da aufgrund der zunehmenden vollständigen Umsetzung der regulatorischen Anforderungen durch die Unternehmen eine Steigerung der Anspruchshaltung bei den Ergebnissen seitens der Aufsichtsbehörde zu beobachten war.

In den VAIT wird vielfach eine Umsetzung der Anforderungen in Anlehnung an das Proportionalitätsprinzip gemäß den individuellen Risikoprofilen der Unternehmen vorausgesetzt. Eine konsequente Berücksichtigung des Proportionalitätsprinzips in der Praxis ist jedoch nach übereinstimmender Meinung der Befragtengruppe aus der Versicherungsbranche bei den bisherigen VAIT-Prüfungen nicht zu erkennen. Stattdessen gelten die im Rundschreiben formulierten Anforderungen überwiegend als Mindeststandards der umzusetzenden Vorgaben. Hierdurch kommt es nach Ansicht der Befragten nicht zu einer Lockerung der Anforderungen für die kleinen und mittelständischen Versicherer, sondern vielmehr zu einer Anforderungsverschärfung für die großen Unternehmen.

4.4 Zukünftige Entwicklungen im Bereich der IT-Regulatorik und der VAIT

Von einem Experten wird die Ansicht vertreten, dass trotz der stattfindenden Debatte zur Festlegung der einzelnen Anforderungen, letztlich nur die Prüfungspraxis der BaFin ausschlaggebend für die Interpretation der VAIT ist. Generell schätzen die Befragtengruppe aus den Assekuranzen die Mitwirkungsmöglichkeiten als sehr gering ein. Als Gründe hierfür werden von den Unternehmen die durch die BaFin angestrebte möglichst hohe Einheitlichkeit der definierten Anforderungen in den VAIT, BAIT und Kapitalverwaltungsaufsichtlichen Anforderungen an die IT (KAIT) wie auch die zu anderen rechtlichen Vorgaben bestehenden Interdependenzen genannt.

Insgesamt sehen die unterschiedlichen Befragtengruppen in den VAIT mit dessen aktuellen Detailierungsgrad ein erstes, anwendbares rechtliches Rahmenwerk zur Organisation der Informationssicherheit, insbesondere für kleine und mittelständische Versicherungsunternehmen. Als wichtigster Treiber für die in Zukunft zu erwartenden kontinuierlichen Anpassungen und Erweiterungen der VAIT werden von allen Experten die stetig zunehmenden Digitalisierungstendenzen in der Versicherungswirtschaft genannt. Insbesondere für den Einsatz neuer Technologien, wie z. B. Best Practices für das Management von CC-Services, den Einsatz von Künstlicher Intelligenz für unternehmerische Entscheidungen oder der Nutzung von Robotik in den IDV-Anwendungen erwarten die befragten Versicherer in den nächsten Jahren schrittweise Konkretisierungen der VAIT durch die BaFin. Gleichzeitig erscheint eine exaktere Formulierung der bestehenden Anforderungen im Hinblick auf die zeitliche Dauer von Dokumentations- und Protokollierungspflichten sinnvoll.

Im Kontext der europäischen Versicherungsaufsicht ist aktuell noch nicht abschätzbar, wie sich zukünftig die Integration der VAIT in die Richtlinien zur IT-Regulatorik der EIOPA gestalten wird. Hierbei ist nach Auffassung der befragten Experten nicht zu erwarten, dass zwischen den übergeordneten europäischen und nationalen Vorschriften keine wesentlichen Kontradiktionen bestehen werden, da bei der Formulierung der VAIT inhaltlich die Vorgaben des Versicherungsaufsichtsgesetzes (VAG), der Mindestanforderungen an die Geschäftsorganisation von Versicherungsgesellschaften (MaGo), der Delegierten Verordnung (DVO) und der Solvency II-Richtlinie bereits berücksichtigt wurden. Demgegenüber erwarten die Unternehmen jedoch, dass die BaFin bei der Umsetzung der europäischen Richtlinien erfahrungsgemäß deutliche Konkretisierungen und Verschärfung der Anforderungen vornehmen wird. Langfristig werden die VAIT einem kontinuierlichen Veränderungsprozess unterliegen, der durch die schrittweise

Einführung neuer Module und die Integration von aus der Prüfungspraxis stammenden Erkenntnissen gekennzeichnet ist.

5 Diskussion und kritische Würdigung

Die Ergebnisse der qualitativen Studie zeigen, dass die Unternehmen einem unterschiedlichen Umsetzungsstand der VAIT unterliegen. Die Bedeutung der Digitalisierung als Treiber für den technologischen Fortschritt in der Versicherungsbranche ist dabei jedoch unumstritten. Insbesondere größere Versicherungsunternehmen haben die Anforderungen an die VAIT bereits in Teilen umgesetzt. Vornehmlich infolge von Prüfungen sowie Vorprüfungen durch die BaFin und Wirtschaftsprüfungsgesellschaften konnte diese Entwicklung im Vergleich zu kleineren Versicherungsunternehmen zunehmend vorangetrieben werden. In diesem Zusammenhang ist auf Grundlage der Studie erkennbar, dass Unternehmen ohne Prüfungserfahrung den Einfluss der VAIT unterschätzen. Ferner wird der Umsetzungsstand der Versicherungsgesellschaften mit geringer Erfahrung zur Prüfungspraxis der BaFin tendenziell überschätzt. Dies zeigt sich dadurch, dass nach Meinung der Experten die wesentlichen Anforderungen über alle Module hinweg erfüllt sind, jedoch eine Tiefe der Anforderungsumsetzung nicht wiedergegeben werden konnte. Insgesamt erkennen Versicherungsgesellschaften zumeist nicht die tatsächliche Reichweite der Anforderungen aus den VAIT und setzen diese oftmals nur oberflächlich um. Insbesondere kleinere und mittelständische Versicherungsunternehmen schätzen den Umsetzungsaufwand der VAIT geringer ein als größere Unternehmen. Ein möglicher Grund dafür besteht darin, dass das Proportionalitätsprinzip nach Meinung der Experten in der Praxis keine Anwendung findet. Nahezu alle Anforderungen werden auch von kleinen Versicherungsunternehmen gefordert, was für diese aufgrund fehlender Fachexpertise erschwert umzusetzen ist. Fraglich ist in diesem Kontext, inwieweit das Proportionalitätsprinzip generell dahingehend einer klaren Definition unterliegt, dass dieses in die Prüfungspraxis zukünftig angemessen übertragen werden kann.

Sofern Versicherungsunternehmen die VAIT in der Fassung zum Erhebungszeitpunkt der Studie aus dem Jahr 2019 nicht vollumfänglich umgesetzt hatten, mussten diese ohne etwaige Karenzzeit die Anforderungen aus dem Rundschreiben 10/2018 (VA) in der Fassung vom 3. März 2022 anpassen.[4] Dazu gehörten bspw. die neu integrierten Kapitel zur operativen Informationssicherheit und dem IT-Notfallmanagement. Kleine Versicherungsunternehmen, die zu diesem

[4] Siehe zu der Ausgestaltung und den Änderungen der VAIT ausführlich das novellierte Rundschreiben 10/2018 (VA) in der Fassung vom 3. März 2022 (BaFin 2022).

Zeitpunkt bisher keiner Prüfung oder Vorprüfung unterzogen wurden, blieben damit weiterhin in der Unsicherheit ob die bisherigen Umsetzungen mit den jeweiligen Anforderungen konform sind. Aufgrund der kurzfristigen Veröffentlichung des neuen Rundschreibens sind Erfahrungsberichte derzeit nicht ausreichend vorhanden, weshalb dieser Aspekt in der vorliegenden Studie nicht vertiefend untersucht wurde. Da die Anpassungen aus dem Jahr 2022 verstärkt an die Sichtweise der EIOPA angelehnt sind, ist zudem fraglich wie sich die VAIT zukünftig weiterentwickeln werden, z. B. ob sich diese weiterhin auf den deutschen Versicherungsmarkt fokussieren oder sich die VAIT vermehrt an europäische und/oder internationale Regelwerke anlehnen werden. Grundsätzlich werden derartige Anpassungen die Unternehmen vor neue Herausforderungen stellen.

Zusammenfassend liefert die vorliegende empirische Studie einen ersten Überblick zum Umsetzungsstand der VAIT (Rundschreiben 10/2018 (VA) in der Fassung vom 20. März 2019) in deutschen Versicherungsunternehmen. Infolge der gewählten Stichprobe ist die Generalisierbarkeit und Repräsentativität der Ergebnisse jedoch eingeschränkt (Firestone 1993; Miles und Hubermann 1994; Lee und Baskerville 2003; Groleau et al. 2009). Zudem handelt es sich bei den Studienergebnissen zur VAIT um ein spezifisches Thema für den deutschen Versicherungsmarkt, wodurch eine Übertragung auf den internationalen Markt nicht möglich ist. Aufgrund des dynamischen Entwicklungsprozesses und der Einführung der neuen Fassung aus dem Jahr 2022 sollte der Umsetzungsstand zukünftig erneut erhoben und fortlaufend evaluiert werden. Eine Ausweitung der Analyse des Status quo der Umsetzung auf vergleichbare Regelwerke in internationale Versicherungsmärkte wäre ebenfalls denkbar. Über den Vergleich der Ergebnisse im Zeitverlauf sowie zu anderen Märkten könnten wertvolle Erkenntnisse für die Praxis generiert werden.

6 Schlussbetrachtung

Der vorliegende Beitrag analysiert den Status quo der Umsetzung der VAIT in den deutschen Versicherungsunternehmen wie auch die in der Praxis unternehmensseitig bestehenden Probleme und Herausforderungen für eine anforderungskonforme Implementierung der Regelungen der VAIT. Zudem sind die aktuellen Schwerpunkte der bislang diesbezüglich durchgeführten aufsichtsrechtlichen Prüfungen untersucht worden. Hinsichtlich des Umsetzungsstandes der Regelungen der VAIT zeigt die Untersuchung, dass sich in den befragten Unternehmen deutliche Unterschiede ergeben. So setzen die Versicherer infolge einer Unterschätzung der tatsächlichen Reichweite der einzelnen Anforderungen aus den VAIT diese in der Praxis häufig nur

oberflächlich um. Insgesamt weist der deutsche Versicherungsmarkt seit dem Inkrafttreten der VAIT im Jahr 2018 aktuell noch geringe Prüfungsaktivitäten der zuständigen Aufgabenträger auf und es hat nur eine kleine Anzahl von Prüfungen stattgefunden. Jedoch ist zukünftig mit einer deutlichen Intensivierung der diesbezüglichen aufsichtsrechtlichen Prüfungsaktivitäten zu rechnen. Angesichts der im Jahr 2022 stattgefundenen Novellierung der VAIT und der hieraus resultierenden Neuregelungen und Anpassungen der einzelnen Anforderungen bleibt jedoch abzuwarten, inwieweit sich aus diesen Entwicklungen und dem Fehlen von Übergangsfristen Auswirkungen auf die bisherige Umsetzungspraxis der Anforderungen in den Unternehmen und die Prüfungsaktivitäten der Versicherungsaufsicht ergeben werden.

Literatur

Albrecher, H., Bommier, A., Filipović, D., Koch-Medina, P., Loisel, S., Schmeiser, H.: Insurance: models, digitalization, and data science. European Actuarial Journal 9(2), 349–360 (2019)

Aldasoro, I., Gambacorta, L., Giudici, P., Leach, T.: The drivers of cyber risk. Journal of Financial Stability 60, 100989. DOI: https://doi.org/10.1016/j.jfs.2022.100989 (2022)

Aleatrati Khosroshahi, P., Roth, S., Hauder, M.: Impact of Solvency II on the Enterprise Architecture of Insurances: A Qualitative Study in Germany. In: Proceedings of the Multikonferenz Wirtschaftsinformatik 2014 (MKWI), Paderborn, Germany, February 26–28, 2014 (2014)

Ammann, T.: Der Einsatz Künstlicher Intelligenz in der Finanz- und Versicherungswirtschaft — Markttrend und regulatorische Herausforderungen. Computer und Recht 36(10), 633–640 (2020)

Aschenbrenner, M.: Informationsverarbeitung – Überblick. In: Aschenbrenner, M., Dicke, R., Karnarski, B., Schweiggert, F. (Hrsg.) Informationsverarbeitung in Versicherungsunternehmen, S. 15–25. Springer, Berlin, Heidelberg (2010)

Bassellier, G., Benbasat, I., Reich, B.H.: The influence of business managers' IT competence on championing IT. Information Systems Research 14(4), 317–336 (2003)

Basten, D., Joosten, D., Mellis, W., Wallmueller, C.: Keep IT simple – The challenge of interlaced IT architecture at Gothaer Systems. Journal of Information Technology Teaching Cases 4(1), 34–40 (2014)

Bauer, S.: A literature review on operational IT risks and regulations of institutions in the financial service sector. In: Proceedings of the 5th International Conference on Information Resources Management (CONF-IRM), Vienna, Austria, May 21–23, 2012 (2012)

Beltratti, A., Corvino, G.: Why are insurance companies different? The limits of convergence among financial institutions. The Geneva Papers on Risk and Insurance – Issues and Practice 33(3), 363–388 (2008)

Berger, A.N.: The economic effects of technological progress: Evidence from the banking industry. Journal of Money, Credit and Banking 35(2), 141–176 (2003)

Bierth, C., Friedrich, K., Linderkamp, T., Lohse, U., Schröder, M.: Zukunft der Versicherung – Versicherung der Zukunft. Zeitschrift für die gesamte Versicherungswissenschaft 107(2), 127–141 (2018)

Bogner, A., Littig, B., Menz, W.: Interviews mit Experten: Eine praxisorientierte Einführung. Springer VS, Wiesbaden (2014)

Bohnert, A., Fritzsche, A., Gregor, S.: Digital agendas in the insurance industry: The importance of comprehensive approaches. The Geneva Papers on Risk and Insurance – Issues and Practice 44(1), 1–19 (2019)

Bonsón, E., Cortijo, V., Escobar, T., Flores, F., Monreal, S.: Solvency II and XBRL: New rules and technologies in insurance supervision. Journal of Financial Regulation and Compliance 18(2), 144–157 (2010)

Brady, T., Targett, D.: Strategic Information Systems in the Banking Sector: Holy Grail or Poison Chalice. Technology Analysis & Strategic Management 7(4), 387–406 (1995)

Braun, A., Eder, H., Maier, S.C., Schmeiser, H., Schreiber, F., Vogel, R.: Die Chancen der IT in der Digitalisierung von Versicherern. EY Innovalue Management Advisors GmbH und Universität St. Gallen Institut für Versicherungswirtschaft (I•VW), St. Gallen. https://www.ivw.unisg.ch/wp-content/uploads/2020/02/DigitalisierungAB2019-EY.pdf (2017), Zugegriffen: 15. März 2023

Braunwarth, K.S., Kaiser, M., Müller, A.-L.: Economic evaluation and optimization of the degree of automation in insurance processes. Business & Information Systems Engineering 2(1), 29–39 (2010)

Buhl, H.U., Kundisch, D.: Transformation von Finanzintermediären durch Informationstechnologie. WIRTSCHAFTSINFORMATIK 45(5), 503–508 (2003)

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Rundschreiben 10/2018 (VA) in der Fassung vom 20.03.2019: Versicherungsaufsichtliche Anforderungen an die IT (VAIT) (2019)

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin): Rundschreiben 10/2018 (VA) in der Fassung vom 03.03.2022: Versicherungsaufsichtliche Anforderungen an die IT (VAIT) (2022)

Burla, L., Knierim, B., Barth, J., Liewald, K., Duetz, M., Abel, T.: From Text to Codings: Intercoder Reliability Assessment in Qualitative Content Analysis. Nursing Research 57(2), 113–117 (2008)

Bussmann, K.-D., Salvenmoser, S., Lescher, G.: Wirtschaftskriminalität in der analogen und digitalen Wirtschaft. PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft und Martin-Luther-Universität Halle-Wittenberg, Halle (2017)

Bussmann, K.-D., Lescher, G., Salvenmoser, S.: Wirtschaftskriminalität 2018 – Compliance in der Versicherungswirtschaft: Wachsende Risiken bei digitaler Wirtschaftskriminalität. PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft und Martin-Luther-Universität Halle-Wittenberg, Halle (2018)

Cappiello, A.: Technology and the insurance industry: Re-configuring the competitive landscape. Palgrave Pivot, Cham (2018)

Cappiello, A.: The European insurance industry: Regulation, risk management, and internal control. Palgrave Macmillan, Cham (2020)

Cavanagh, S.: Content analysis: concepts, methods and applications. Nurse Researcher 4(3), 5–16 (1997)

Channon, D.F.: The strategic impact of IT on the retail financial services industry. The Journal of Strategic Information Systems 7(3), 183–197 (1998)

Codington, S., Wilson, T.D.: Information system strategies in the UK insurance industry. International Journal of Information Management 14(3), 188–203 (1994)

Christiaans, T., Steden, S.: Cloud-computing in the insurance industry – An application of the theory of club-goods. In: Bakırcı, F., Heupel, T., Kocagöz, O., Özen, Ü. (Hrsg.) German-Turkish perspectives on IT and innovation management: Challenges and approaches, S. 275–290. Springer Gabler, Wiesbaden (2018)

Didenko, A.N.: Cybersecurity regulation in the financial sector: Prospects of legal harmonization in the European Union and beyond. Uniform Law Review 25(1), 125–167 (2020)

Downe-Wamboldt, B.: Content analysis: Method, applications, and issues. Health Care for Women International 13(3), 313–321 (1992)

Dreher, M.: Die Veröffentlichungspflichten von Versicherungsunternehmen gegenüber der BaFin: Umfang und Grenzen der versicherungsaufsichtsrechtlichen Offenlegungspflichten. Zeitschrift für die gesamte Versicherungswissenschaft 98(2), 187–219 (2009)

Dreher, M.: Versicherungsaufsicht über IT und Governance. Versicherungsrecht – VersR 70(19), 1177–1191 (2019)

Eckert, C., Eckert, J., Zitzmann, A.: The status quo of digital transformation in insurance sales: an empirical analysis of the german insurance industry. Zeitschrift für die gesamte Versicherungswissenschaft 110(2-3), 133–155 (2021)

Eckert, C., Osterrieder, K.: How digitalization affects insurance companies: Overview and use cases of digital technologies. Zeitschrift für die gesamte Versicherungswissenschaft 109(5), 333–360 (2020)

Egan, R., Cartagena, S., Mohamed, R., Gosrani, V., Grewal, J., Acharyya, M., Dee, A., Bajaj, R., Jaeger, V.-J., Katz, D., Meghen, P., Silley, M., Nasser-Probert, S., Pikinska, J., Rubin, R., Ang, K.: Cyber operational risk scenarios for insurance companies. British Actuarial Journal 24, e6. DOI: https://doi.org/10.1017/S1357321718000284 (2019)

Eisenhardt, K.M.: Building Theories from Case Study Research. The Academy of Management Review 14(4), 532–550 (1989)

Eisenhardt, K.M., Graebner, M.E.: Theory Building From Cases: Opportunities And Challenges. Academy of Management Journal 50(1), 25–32 (2007)

Eling, M.: Cyber risk and cyber risk insurance: Status quo and future research. The Geneva Papers on Risk and Insurance – Issues and Practice 43(2), 175–179 (2018)

Eling, M., Lehmann, M.: The impact of digitalization on the insurance value chain and the insurability of risks. The Geneva Papers on Risk and Insurance – Issues and Practice 43(3), 359–396 (2018)

Eling, M., Nuessle, D., Staubli, J.: The impact of artificial intelligence along the insurance value chain and on the insurability of risks. The Geneva Papers on Risk and Insurance – Issues and Practice 47(2), 205–241 (2022)

Engelke, L.: IT-Alignment in einem Versicherungsunternehmen auf der Grundlage einer Corporate- und IT-Governance. In: Aschenbrenner, M., Dicke, R., Karnarski, B., Schweiggert, F. (Hrsg.) Informationsverarbeitung in Versicherungsunternehmen, S. 63–70. Springer, Berlin, Heidelberg (2010)

Elo, S., Kyngäs, H.: The qualitative content analysis process. Journal of Advanced Nursing 62(1), 107–115 (2008)

European Insurance and Occupational Pensions Authority (EIOPA): Cyber risk for insurers – Challenges and opportunities. https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf (2019), Zugegriffen: 15. März 2023

Francalanci, C., Galal, H.: Information technology and worker composition: Determinants of productivity in the life insurance industry. Management Information Systems Quarterly 22(2), 227–241 (1998)

Firestone, W.A.: Alternative arguments for generalizing from data as applied to qualitative research. Educational Researcher 22(4), 16–23 (1993)

Gal, J.: Corporate governance of insurers in Germany. *German National Report*. World Congress of the International Insurance Law Association (AIDA) 2018. Zeitschrift für die gesamte Versicherungswissenschaft 109(1), 41–64 (2020)

Gampe, J.: IT-Sicherheit: Aufsicht konkretisiert IT-Anforderungen an die Versicherungswirtschaft. BaFinJournal April 2018, 24–28. URL: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2018/fa_bj_1804_VAIT.html (2018), Zugegriffen: 15. März 2023

Gennen, K.: Ausgewählte rechtliche Implikationen. In: Reuter, C. (Hrsg.) Sicherheitskritische Mensch-Computer-Interaktion: Interaktive Technologien und Soziale Medien im Krisen- und Sicherheitsmanagement, 2. Aufl., S. 155–184. Springer Vieweg, Wiesbaden (2021)

Gioia, D.A., Corley, K.G., Hamilton, A.L.: Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organizational Research Methods 16(1), 15–31 (2013)

Gläser, J., Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen, 4. Aufl. VS Verlag für Sozialwissenschaften, Wiesbaden (2010)

Goldstein, J., Chernobai, A., Benaroch, M.: An event study analysis of the economic impact of IT operational risk and its subcategories. Journal of the Association for Information Systems 12(9), 606–631 (2011)

Graneheim, U.H., Lundman, B.: Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. Nurse Education Today 24(2), 105–112 (2004)

Graneheim, U.H., Lindgren, B.-M., Lundman, B.: Methodological challenges in qualitative content analysis: A discussion paper. Nurse Education Today 56, 29–34 (2017)

Groleau, D., Zelkowitz, P., Cabral, I.E.: Enhancing Generalizability: Moving From an Intimate to a Political Voice. Qualitative Health Research 19(3): 416–426 (2009)

Gruhn, V., Ringel, J., Rosenbaum, M.: Business Alignment: Versicherungsfachwissen als Kernkompetenz der IT. Zeitschrift für die gesamte Versicherungswissenschaft 95(3), 457–470 (2006)

Guest, G., Bunce, A., Johnson, L.: How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. Field Methods 18(1), 59–82 (2006)

Handke, S.: A problem of Chief and Indian—The role of the supervisory authority BaFin and the ministry of finance in German financial market policy. Policy and Society 31(3), 237–247 (2012)

Harris, S.E., Katz, J.L.: Firm size and the information technology investment intensity of life insurers. Management Information Systems Quarterly 15(3), 333–352 (1991)

Harwood, T.G., Garry, T.: An Overview of Content Analysis. The Marketing Review 3(4), 479–498 (2003)

Hsieh, H.-F., Shannon, S.E.: Three Approaches to Qualitative Content Analysis. Qualitative Health Research 15(9), 1277–1288 (2005)

Ifinedo, P.: Information technology security management concerns in global financial services institutions: Is national culture a differentiator?. Information Management & Computer Security 17(5), 372–387 (2009)

International Association of Insurance Supervisors (IAIS): Issues paper on cyber risk to the insurance sector. https://www.iaisweb.org/uploads/2022/01/160812-Issues-Paper-on-Cyber-Risk-to-the-Insurance-Sector_final.pdf (2016), Zugegriffen: 15. März 2023

International Association of Insurance Supervisors (IAIS): Issues paper on increasing digitalisation in insurance and its potential impact on consumer outcomes. https://www.iaisweb.org/uploads/2022/01/181112-Issues-Paper-on-Increasing-Digitalisation-in-Insurance-and-its-Potential-Impact-on-Consumer-Outcomes.pdf (2018), Zugegriffen: 15. März 2023

Kaczynski, D., Salmona, M., Smith, T.: Qualitative research in finance. Australian Journal of Management, 39(1), 127–135 (2014)

Kaigorodova, G.N., Mustafina, A.A., Pyrkova, G.K., Vyukov, M.G., Davletshina, L.M.: Cyber risks for insurance company. In: Ashmarina, S., Mesquita, A., Vochozka, M. (Hrsg.) Digital transformation of the economy: Challenges, trends and new opportunities, S. 669–677. Springer, Cham (2020)

Kane, A.T., Goldstein, P.A.: Cybersecurity is not a product, it's a process: Financial service regulators hold insurance company boards responsible for cybersecurity. Emory Corporate Governance and Accountability Review 4(2), 353–362 (2017)

Kao, M.B.: Regulating the Cybersecurity of Insurance Companies in the United States. Transactions: The Tennessee Journal of Business Law 21(1), 11–38 (2020)

Kappenberg, W., Drews, P.: Softwarealterung aus Sicht des IT-Managements – Ergebnisse einer qualitativ-empirischen Analyse in der Finanzindustrie. In: Proceedings of the 44. Jahrestagung der Gesellschaft für Informatik e. V. (GI) (INFORMATIK), Stuttgart, Germany, September 22–26, 2014 (2014)

Kashyap, A.K., Wetherilt, A.: Some principles for regulating cyber risk. AEA Papers and Proceedings 109, 482– 487 (2019)

Koch, G.: Versicherungsinformatik — Eine versicherungswissenschaftliche Fachdisziplin. Zeitschrift für die gesamte Versicherungswissenschaft 95(Supplement 1), 359–372 (2006)

Köhne, T., Brömmelmeyer, C.: The New Insurance Distribution Regulation in the EU—A Critical Assessment from a Legal and Economic Perspective. The Geneva Papers on Risk and Insurance – Issues and Practice 43(4), 704–739 (2018)

Kuckartz, U.: Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4. Aufl. Beltz Juventa, Weinheim, Basel (2018)

KPMG AG Wirtschaftsprüfungsgesellschaft: Neues Denken, Neues Handeln – Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil A: Digitalisierung. https://assets.kpmg/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-digitalization-de.pdf (2017), Zugegriffen: 15. März 2023

Lagazio, M., Sherif, N., Cushman, M.: A multi-level approach to understanding the impact of cyber crime on the financial sector. Computers & Security 45, 58–74 (2014)

Lamnek, S.: Qualitative Sozialforschung: Lehrbuch, 4. Aufl. Beltz, Weinheim, Basel (2005)

Lanfranchi, D., Grassi, L.: Examining insurance companies' use of technology for innovation. The Geneva Papers on Risk and Insurance – Issues and Practice 47(3), 520–537 (2022)

Lee, A.S., Baskerville, R.L.: Generalizing Generalizability in Information Systems Research. Information Systems Research 14(3), 221–243 (2003)

Lehmann, C.: Zur Regulierung von Versicherungen: Rechtfertigungsanalyse und ausgewählte Praxisbeispiele. Zeitschrift für die gesamte Versicherungswissenschaft 108(3-4), 227–253 (2019)

Linderkamp, T., Schneider U., Graf von der Schulenburg, J.-M., Lohse, U., Schwarzbach, C.: Versicherungen und Krisen – Aus der Vergangenheit für die Zukunft lernen. Zeitschrift für Versicherungswesen 74(1), 8–10 (2023)

Manning, R.L., Stephenson, M.K., Todd, J.D.: Information technology in the insurance industry: A forecast of utilization and impact. Journal of Risk and Insurance 52(4), 711–722 (1985)

Mayring, P.: Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12. Aufl. Beltz, Weinheim, Basel (2015)

McLellan, E., MacQueen, K.M., Neidig, J.L.: Beyond the Qualitative Interview: Data Preparation and Transcription. Field Methods 15(1), 63–84 (2003)

Melliou, M., Wilson, T.D.: Business process redesign and the UK insurance industry. International Journal of Information Management 15(3), 181–198 (1995)

Miles, M.B., Huberman, A.M.: Qualitative Data Analysis: An Expanded Sourcebook, 2nd ed. SAGE Publications, Thousand Oaks, CA, London, New Delhi (1994)

Modrow-Thiel, B.: Qualitative Interviews - Vorgehen und Probleme. Zeitschrift für Personalforschung, Sonderheft: EMPIRISCHE PERSONALFORSCHUNG, 129–146 (1993)

Moormann, J., Schmidt, G.: IT in der Finanzbranche: Management und Methoden. Springer, Berlin, Heidelberg (2007)

Morse, J.M.: Confusing Categories and Themes. Qualitative Health Research 18(6), 727–728 (2008)

Myers, M.D., Newman, M.: The qualitative interview in IS research: Examining the craft. Information and Organization 17(1), 2–26 (2007)

Naylor, M.: Insurance transformed: Technological disruption. Palgrave Macmillan, Cham (2017)

Neirotti, P., Paolucci, E.: Assessing the strategic value of information technology: An analysis on the insurance sector. Information & Management 44(6), 568–582 (2007)

Nicoletti, B.: Digital insurance: Business innovation in the post-crisis era. Palgrave Macmillan, London (2016)

Nicoletti, B.: Insurance 4.0: Benefits and challenges of digital transformation. Palgrave Macmillan, Cham (2021)

Noordhoek, D.: Regulatory considerations for digital insurance business models. The Geneva Association, Zurich. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/digitalinsurance_web.pdf (2021), Zugegriffen: 15. März 2023

Olaisen, J.: Information versus information technology as a strategic resource: Areas of application of information and information technology in Norwegian banks and insurance companies. International Journal of Information Management 10(3), 192–214 (1990)

Oletzky, T., Reinhardt, A.: Herausforderungen der Regulierung von und der Aufsicht über den Einsatz Künstlicher Intelligenz in der Versicherungswirtschaft. Zeitschrift für die gesamte Versicherungswissenschaft 111(4), 495–513 (2022)

Pauch, D., Bera, A.: Digitization in the insurance sector – challenges in the face of the Covid-19 pandemic. Procedia Computer Science 207, 1677–1684 (2022)

Petsch, M., Nissen, V.: IT-Systeme in der Versicherungswirtschaft auf Basis kundenorientierter Prozesse. In: Proceedings of the 39. Jahrestagung der Gesellschaft für Informatik e. V. (GI) (INFORMATIK), Lübeck, Germany, September 28 – October 2, 2009 (2009)

Pisoni, G.: Going digital: Case study of an Italian insurance company. Journal of Business Strategy 42(2), 106–115 (2021)

Pohlmann, P., Vossen, G., Everding, J., Scheiper, J.: Künstliche Intelligenz, Bias und Versicherungen – Eine technische und rechtliche Analyse. Zeitschrift für die gesamte Versicherungswissenschaft 111(2), 135–175 (2022)

Puschmann, T.: Fintech. Business & Information Systems Engineering 59(1), 69–76 (2017)

Uzquiano, J.L.: Anwendungslandschaften von Versicherungsunternehmen. In: Aschenbrenner, M., Dicke, R., Karnarski, B., Schweiggert, F. (Hrsg.) Informationsverarbeitung in Versicherungsunternehmen, S. 151–162. Springer, Berlin, Heidelberg (2010)

Qu, S.Q., Dumay, J.: The qualitative research interview. Qualitative Research in Accounting & Management 8(3), 238–264 (2011)

Roßmehl, M., Leider, Y., Redman, M., Rütten, M., Hovestadt, C., Basten, D., Werner, M.: Need for a smart solution: Developing a sourcing strategy for a policy system at a German insurance company. Journal of Information Technology Teaching Cases 7(1), 9–16 (2017)

Schiro, J.J.: External forces impacting the insurance industry: Threats from regulation. The Geneva Papers on Risk and Insurance – Issues and Practice 31(1), 25–30 (2006)

Schmidt, C.: Insurance in the digital age: A view on key implications for the economy and society. The Geneva Association, Zurich. https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/insurance_in_the_digital_age_01.pdf (2018), Zugegriffen: 15. März 2023

Schnell, R., Hill, P.B., Esser, E.: Methoden der empirischen Sozialforschung, 9. Aufl. Oldenbourg, München (2011)

Schultze, U., Avital, M.: Designing interviews to generate rich data for information systems research. Information and Organization 21(1), 1–16 (2011)

Singh, A., Akhilesh, K.B.: The Insurance Industry—Cyber Security in the Hyper-Connected Age. In: Akhilesh, K.B., Möller, D.P.F. (Hrsg.) Smart Technologies: Scope and Applications, S. 201–219. Springer, Singapore (2020)

Smits, M.T., Van der Poel, K.G., Ribbers, P.M.A.: Assessment of information strategies in insurance companies in the Netherlands. The Journal of Strategic Information Systems 6(2), 129–148 (1997)

Stankat, R.: Bedeutung der Informationsverarbeitung für das Geschäft einer Versicherung. In: Aschenbrenner, M., Dicke, R., Karnarski, B., Schweiggert, F. (Hrsg.) Informationsverarbeitung in Versicherungsunternehmen, S. 39–49. Springer, Berlin, Heidelberg (2010)

Streitz, S.H.: Von FAIT zu VAIT: Nur ein ausgetauschter Buchstabe oder grundlegend neue Anforderungen für Vorstand und IT-Steuerung?. In: Looschelders, D., Michael, L. (Hrsg.) Versicherungsaufsichtsrechtliche Anforderungen an die Informationstechnologie von Versicherungsunternehmen: VAIT, IT-Sicherheit, IT-Governance, Risikomanagement, Geschäftsleiterverantwortung, S. 39–61. Verlag Versicherungswirtschaft, Karlsruhe (2019)

Surminski, M.: Das Versicherungsjahr 2022 – ein Rückblick. Zeitschrift für Versicherungswesen 74(1), 3–4 (2023)

Taylor, M.: Technological changes in IT and their influence on insurance: The change ahead (II). The Geneva Papers on Risk and Insurance – Issues and Practice 26(1), 89–104 (2001)

Thalhofer, T., Beck, M.: Auswirkungen von Solvency II auf das IT-Outsourcing bei Versicherungen. Computer und Recht 32(1), 1–6 (2016)

Theis, A.: Regulierung und Versicherungswirtschaft: Chancen und Herausforderungen aus ökonomischer Perspektive. Volkswirtschaftliche Themen und Analysen Nr. 7. Gesamtverband der Deutschen Versicherungswirtschaft e. V. (GDV), Berlin. https://www.gdv.de/resource/blob/9308/57a39eeeb369416223979c92afb2c959/volkswirtschaftliche-themen-und-analysen-nr--7---pdf-data.pdf (2015), Zugegriffen: 15. März 2023

Thoma, A., Widemann, P.: Nächste Liste abarbeiten. Zu den bestehenden Anforderungen an die IT-Sicherheit der Versicherer ist die VAIT-Liste hinzugekommen. Steht nun der zu erwartende Aufwand bei der Umsetzung in einem angemessenen Verhältnis zum Aufsichtsziel der Bafin?. Versicherungswirtschaft 73(7), 40–43 (2018)

Timofeyev, Y., Dremova, O.: Insurers' responses to cyber crime: Evidence from Russia. International Journal of Law, Crime and Justice 68, 100520. DOI: https://doi.org/10.1016/j.ijlcj.2021.100520 (2022)

Tsindeliani, I.A., Proshunin, M.M., Sadovskaya, T.D., Popkova, Z.G., Davydova, M.A., Babayan, O.A.: Digital transformation of the banking system in the context of sustainable development. Journal of Money Laundering Control 25(1), 165–180 (2022)

Vaismoradi, M., Turunen, H., Bondas, T.: Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. Nursing & Health Sciences 15(3), 398–405 (2013)

Varga, S., Brynielsson, J., Franke, U.: Cyber-threat perception and risk management in the Swedish financial sector. Computers & Security 105, 102239. DOI: https://doi.org/10.1016/j.cose.2021.102239 (2021)

Werth, O., Schwarzbach, C., Rodríguez Cardona, D., Breitner, M.H., Graf von der Schulenburg, J.-M.: Influencing factors for the digital transformation in the financial services sector. Zeitschrift für die gesamte Versicherungswissenschaft 109(2-4), 155–179 (2020)

Wilson, C., Gaidosch, T., Adelmann, F., Morozova, A.: Cybersecurity Risk Supervision. Departmental Paper No. 2019/014. International Monetary Fund (IMF), Washington, DC. https://www.imf.org/-/media/Files/Publications/DP/2019/English/CRSEA.ashx (2019), Zugegriffen: 15. März 2023

Wojcik, K.-P., Annoscia, D., Kerr, S.: Report from Brussels: Pending legislative initiatives by the European Commission in the area of financial services in the EU – content and state of play. Zeitschrift für Bankrecht und Bankwirtschaft 34(5), 312–332 (2022)

Wrede, D.: Mind the (IT-)System – Ein Vorschlag zur Gestaltung einer IT Due Diligence von Versicherungsunternehmen. Zeitschrift für die gesamte Versicherungswissenschaft 110(4-5), 269–313 (2021)

Yin, R.K.: Case Study Research: Design and Methods, 3rd ed. SAGE Publications, Thousand Oaks, CA, London, New Delhi (2003)

Zgraggen, R.R.: Cyber security supervision in the insurance sector: Smart contracts and chosen issues. In: Proceedings of the 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Oxford, United Kingdom, June 3–4, 2019 (2019)

Modul 3

Influences of Digital Innovations on Advisory Work in the Financial Services Sector

Theresa Eden
Oliver Werth
Davinia Rodríguez Cardona
Christoph Schwarzbach
Michael H. Breitner
Johann-Matthias Graf von der Schulenburg

Die Unternehmung, 76 (1), S. 6–27
Verfügbar unter: https://www.nomos-elibrary.de/10.5771/0042-059X-2022-1-6/influences-of-digital-innovations-on-advisory-work-in-the-financial-services-sector-jahrgang-76-2022-heft-1?page=1

Modul 4

Digital Transformation in Back-Offices of German Insurance Companies

Christoph Schwarzbach
Theresa Eden
Oliver Werth
Ute Lohse
Michael H. Breitner
Johann-Matthias Graf von der Schulenburg

International Journal of Innovation and Technology Management, 2023, S. 1–27
Verfügbar unter: https://www.worldscientific.com/doi/epdf/10.1142/S0219877023500505

Modul 5

Chances and Challenges of Business Intelligence: Insights from the German Insurance Market

Theresa Eden
Oliver Werth
Claus Marcus Aschenbach
Michael H. Breitner

eingereicht bei:

Zeitschrift für die gesamte Versicherungswissenschaft

Chances and Challenges of Business Intelligence: Insights from the German Insurance Market

Theresa Eden, Oliver Werth, Claus Marcus Aschenbach, Michael H. Breitner

Theresa Eden (korrespondierende Autorin)
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover
Deutschland
E-Mail: te@ivbl.uni-hannover.de

Oliver Werth
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Wirtschaftsinformatik
Königsworther Platz 1
D-30167 Hannover
Deutschland

Claus Marcus Aschenbach
Gottfried Wilhelm Leibniz Universität Hannover
Welfengarten 1
D-30167 Hannover
Deutschland

Michael H. Breitner
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Wirtschaftsinformatik
Königsworther Platz 1
D-30167 Hannover
Deutschland

Chances and Challenges of Business Intelligence: Insights from the German Insurance Market

Zusammenfassung

Im Rahmen der digitalen Transformation bieten neue Analyseverfahren und Visualisierungen für Versicherungsunternehmen die Möglichkeit bestehende Geschäftsprozesse zu unterstützen, neue Geschäftsprozesse zu ermöglichen und neue Kunden zu gewinnen. Insbesondere infolge einer schnellen, hochwertigen und intuitiven Datenaufbereitung können erhebliche Wettbewerbsvorteile generiert werden. Business Intelligence (BI) Systeme unterstützen und ermöglichen dabei die Datenverarbeitung und sind in Finanzdienstleistungsunternehmen von besonderem Interesse, da große Datenmengen an Kundeninformationen wertschöpfend genutzt werden können. Mit qualitativen Interviews mit Experten aus der deutschen Versicherungsbranche untersucht dieser Beitrag die aktuellen Einsatzpotentiale von BI in Versicherungsunternehmen sowie die mit der Einführung und Nutzung resultierenden Chancen und Herausforderungen. Die Ergebnisse und Erkenntnisse zeigen, dass der Einsatz von BI als vorteilhaft angesehen wird und die Nutzung in Versicherungsunternehmen deutlich zunehmen wird, da potentielle Einsatzmöglichkeiten derzeit ungenügend ausgeschöpft werden. Unsere Forschung unterstützt auch den Entscheidungsprozess von Praktikern, in welchem Umfang die Implementierung von BI sinnvoll ist.

Abstract

In the context of digital transformation, new analysis and visualization methods and tools offer insurance companies the opportunity to support existing and enable new business processes and acquire new clients. In particular, competitive advantages can be generated through fast and intuitive high-quality data processing. Business Intelligence (BI) systems support and enable data processing and create significant value for financial services companies, as large amounts of customer data can be used profitably. Based on qualitative interviews with experts from the German insurance industry, this paper examines possible applications of BI in insurance companies and, moreover, opportunities and challenges resulting from BI implementation and use. Our results and findings show that the use of BI is beneficial and an expansion in the insurance sector is expected, as potential use cases currently are not fully exploited. Our research also supports decision-making of practitioners to implement new BI tools and processes.

1 Introduction

Digital transformation and the enduring value of information as a crucial success factor affect all business areas and sectors, e.g., insurance, in these times. In a world of big data, companies are urged to analyze and use it profitably (e.g., Davenport 2014). New analytics procedures and visualizations allow companies to support existing business processes and acquire new clients (Keller 2018). However, without appropriate relating or visualization, the volumes of data do not deliver any immediate intended use but rather represent pure information. Competitive advantages thus arise from fast and high-quality data processing. Business intelligence (BI) systems support processing this information and can therefore be seen as a useful technology within insurance companies (Gehra et al. 2005). With the help of statistical and visualization options, the data volumes can be processed and evaluated for business purposes. BI is particularly interesting to financial services companies because they are technology-driven, collect a high quantity of data about their customers, and the customer information received can be used profitably in various ways (Rostek 2009). Overall, there are several possible BI applications. This paper addresses the question of how insurance companies can benefit from the use of BI applications. Past literature on BI investigated it in the context of, e.g., in higher education (Gupta et al. 2015) and its effective usage (Trieu et al. 2022). However, BI has been neglected so far by exploratory and recent investigations of useful use cases tailored to the specificities of the (German) insurance sector, e.g., lack of use of the potential of digital technologies (Catlin et al. 2015), changing value creation due to digitalization, competitive pressure (Eling and Lehmann 2017), and regulatory requirements (Schmidt 2018). From a theoretical perspective, we shed light on possible use cases and their associated chances and challenges of BI within this business area. In doing so, we interviewed eight (n=8) experts from the insurance sector in Germany. Interviewees were invited to talk about possible and already existent use cases, their observations, and their understandings of BI in the German insurance sector. Interview transcripts were analyzed with qualitative content analysis (Kuckartz 2018) and discussed. In this context, qualitative research offers the opportunity to generate new insights through systematically analyzing experts' practical experiences. With this work, we support the decision-making process for practitioners as to whether and to what extent BI can be implemented within insurance companies. Also, practitioners in the insurance sector can use the findings provided in this study for a more focused discussion on BI for insurance. Motivated by these statements, we answer the following research questions (RQs) with this study:

Which established and new BI tools and processes exist in insurance companies?

The rest of our paper is structured as follows: First, we provide the theoretical background of BI and its relationship to insurance companies. Then, we introduce our research design and research methods. Results, our discussion, findings, and implications presented subsequentially. Finally, limitations, further research directions, and conclusions conclude our paper.

2 Business Intelligence in Insurance Companies

BI and their associated systems "combine data gathering, data storage, and knowledge management with analytical tools to present complex internal and competitive information to planners and decision-makers." (Negash 2004, p. 178). However, there is no common definition of BI available (Philips-Wren et al. 2021). An influential review of BI by Chee et al. (2009) identifies various definitions in the academic literature. They found that the interpretations of the term fall into three aspects: the management aspect, the technological aspect, and the product aspect. For example, according to Petrini and Pozzeborn (2008), in the management aspect, the focus is on the coordination and management of the process, which ensures that the data from various sources of information, both internal and external, is integrated and analyzed to sources are integrated and analyzed to support the decision-making process. The technological aspect focuses on finding, collecting, organizing, and accessing information from different data sources; it is directly related to the software. In line with Davenport (2014, p. 46), BI uses "tools to support data-driven decisions, with emphasis on reporting," while the term Business Analytics (BA) "focuses on statistical and mathematical analysis for decisions." With the help of Big Data and/or data mining, the BI software should generate insights that are not immediately apparent. For this case, external and/or internal, as well as structured and/or unstructured data, can be used. In the product aspect, on the other hand, BI is the result of a detailed analysis of comprehensive business data and analytical practices. The processed data as the product is the goal of this approach (Chee et al. 2009).

Like several other business areas, the insurance sector is affected by digital transformation, the threat of new market entrants, and the introduction of technological possibilities (Werth et al. 2020; Eckert et al. 2021). The usage and introduction of new technologic possibilities for insurance companies, e.g., cloud computing or Artificial Intelligence, have been recently reviewed (Eckert and Osterrieder 2020; Eling et al. 2022). Insurance companies need to constantly analyze the needs and requirements of their customers to ensure that these can be met at

all times (Rostek 2009). In addition, the business processes within the value chain and the products must be constantly adapted to new needs. Companies collect and centralize information about their customers and use it to gain valuable insights into data, thus supporting the company's decision-makers. Focusing on BI and BA, several application areas have been discussed. For example, insurance companies can use BI for managing internal documents and integrate them into document management or use it for specific knowledge management (e.g., Negash 2004; Dreyer et al. 2022). Also, BI can automatically handle all incoming customers' data, e.g., from smart home devices, and examine new marketing possibilities and new insurance product specifications from it (Schulte-Noelle 2001; Eggert and Alberts 2020; Huang et al. 2022). Another application area for BI and BA can be seen in call centers of insurance companies (Kyper et al. 2009). Here, decision trees, derived with BA based on data from call centers, can leverage the overall performance of the call center's responsiveness. Another application of BI comes from Amini et al. (2021). In this Iranian study, BI is used for better risk prediction in different areas for insurance companies. Also, BI can be used for calculating and monitoring key performance indicators, e.g., managing reserves, calculating large losses or solvency predictions, and against insurance fraud (Ngai et al. 2011; Helfand 2017; Eckert and Osterrieder 2020). Another qualitative approach to the chances and challenges of BI usage comes from Baars et al. (2009). Their study, with a look at the financial services sector, i.e., banks and insurances, reveal challenges such as a lack of integration into existing IT backends and restricted time and monetary budgets as barriers to the usage of BI. However, their study and examinations are somewhat outdated for such a vital topic as BI.

It can be summarized that researchers from an information systems or business perspective have extensively studied BI. Also, different application areas have been studied so far. However, the German insurance sector has been somewhat neglected, and the literature is fragmented. The efficient usage of BI and its associated chances and challenges in an insurance environment remains somewhat unclear. Therefore, more timely exploratory research on this topic is necessary to accumulate current knowledge for academics and practitioners.

3 Research Design and Research Methods

Given the lack of context-specific research findings on the chances and challenges related to implementing and using BI in insurance companies and the explorative nature of the research questions, qualitative case interviews with insurance experts were conducted (Yin 2009). Qualitative research offers the opportunity to generate new insights through a systematic analysis

regarding the practice-based experiences of interviewed experts in the area of digital transformation in the financial services sector (Gioia et al. 2013; Schnell et al. 2011). Therefore, potential interview participants in insurance companies were contacted via email after prior research regarding relevant expertise to analyze the research questions. For this purpose, the experts had to have distinctive experience with the use of BI in insurance companies, such as regular use of BI applications or experience with implementing BI in their company. The chosen form of questioning was oral with partially standardized and open guideline interviews. We chose this form of questioning because it is established in the analysis of expert knowledge (Myers and Newman 2007; Schultze and Avital 2011). Seven semi-structured open guideline-based interviews with eight experts could be conducted from May to July 2022. With the seventh interview, no new insights were generated, and theoretical saturation of the results was achieved. The interview duration varied between approximately 45 and 60 minutes. Table 1 shows the expert number and the position within the respective insurance companies.

Interview	Expert	Position
1	E.1	Team Leader Sales Controlling
2	E.2	Team Leader Controlling
3	E.3	Member of the Board
4	E.4	Controller
5	E.5	Team Lead Customer Management
6	E.6	Controller
7	E.7	Team Lead Sales Controlling
	E.8	Team Lead BI and Analytics Competence Center

Table 1 Interview Experts

The interview guideline was developed based on the previous literature review and is divided into four parts, containing six subordinate questions. Initially, general explanations about the research project and the collection of information about the person, professional occupation, and position of the interviewed experts were used at the beginning of the interview. Subsequently, an introduction question on the conceptual understanding of BI is asked in the second part. The third part deals with the potential uses and challenges of BI. Questions on the potential influence of BI on decision-making constitute the last part of the interview. The interviews were held in German, recorded, and fully transcribed afterward. We did not send out the interview guideline in advance but briefly introduced our study as part of the interview invitations.

The evaluation was conducted using the current version of the qualitative data analysis software MAXQDA following the qualitative content analysis, according to Kuckartz (2018), which allows a systematic and rule-based evaluation of the data material. After analyzing the interviews, a deductive-inductive category system with anchor examples was developed (Mayring 2015). Potential categories were identified deductively from the interview guide and inductively from the interview material. The deductive categories were additionally reviewed based on the transcripts, and the inductive development of subcategories followed (Hsieh and Shannon 2005). An overview of the category system is shown in Table 2.

Main codes	**Subcodes**	**Definition of the Subcodes**	**Anchor examples**
Definition of BI	/	Text passages indicating the interpretation of the term BI	E.3: "(...) break it down into two different points. On the one hand, you have a business point, i.e., what everyday life involves for us in the company. That always involves numbers, data, and facts, especially the focus on controlling. Intelligence is the area we can feed."
Chances	Reporting system	Indications for possible applications of BI regarding reporting in insurance companies	E.5: "But where you definitely use it is in controlling (...)."
	Sales analysis	Indications for possible applications of BI regarding sales analyses in insurance companies	E.2: "We use it for reporting capabilities, so sending standard reports for the sales part."
	Market forecasts	Indications for possible applications of BI regarding market forecasts in insurance companies	E.3: "I would say to generate past-related insights for the future from the data obtained. That's how I would describe it in one sentence. That means enlightening a bit of a glass ball in order to be able to predict certain things or recognize them at an early stage."
	Usability	Indications for possible applications of BI regarding usability in insurance companies	E.1: "We want to expand this even further in the future and open up additional areas of application, such as operational business for ad hoc information."
Challenges	Data and privacy	Text passages about data used and the handling of data in the respective company	E.4: "That is, of course, Prio 1, that the data we control is reliable and that we can derive the right decisions and measures from them."

	IT landscape and programming	Text passages about the technical infrastructure and programming in the company	E.2: "When you use software solutions, you naturally have programming in front of your nose. The system we use is very flexible, but also has its own software language, which has presented us as a company with small challenges, wherein the depth of detail the topics were not quite easy to implement and which also cost a lot of time."
	Employee involvement	Text passages about the involvement of employees in dealing with BI as an innovation in the company	E.4: "Well, the challenge is basically to bring the employees along and to change the perspective."
Impact on processes	Management process	Text passages about the impact of BI on management processes	E.2: "(...) that the processes or the calculations that lead to the key figures are always followed according to a precise definition and can therefore also be less prone to error. This has increased the confidence of the sales department, and thus it has been possible to tap into the key figures more and more."
	Decision-making process	Text passages about the impact of BI on decision-making processes	E.5: "So that ultimately we make decisions that are secure for the long term, not just a gut feeling."

Table 2 Category system

The final category system, based on which the transcripts were coded, contained the four main codes "Definition," "Chances," "Challenges," and "Impact on processes", and another nine related subcodes, all concerning BI. Based on this, the results of the qualitative content analysis are presented below.

4 Results

4.1 Definition

According to the experts interviewed, BI is defined as the company's internal data handling in an IT landscape. It should also be mentioned that BI is not defined as the program to be operated but as a kind of idea. In other words, experts believe BI is a type of collective term for various functions and uses that can be realized with the support of a software solution.

> E.2: “I think business intelligence can basically be split into two different points. On the one hand, you have the point of business, i.e., what everyday life involves in our company. That always involves numbers, data, and facts, especially the focus on controlling. Intelligence is the area that we can focus on. So from my point of view, the IT machine so that we can put the numbers, data, facts into an intelligent IT machine […].”

Two of the interview participants (E.4 and E.8) mention the goal is what they call a “single place of truth.” This involves the conception and realization of a digital place where all internal company data is bundled and can be evaluated. All visualized data can be viewed by everyone with a high degree of reliability, as there are no other collection, consolidation, and evaluation methods within the company. The BI software solution used within the company also differs between financial service providers. Many programs on the market include BI packages or are described as BI tools. Summarizing the understanding of the term, there is a consensus among experts that BI is defined as an idea and collective term which includes data processing in the company, analysis, and visualization. A software application is required for support and realization, which is company-dependent.

4.2 Chances

Reporting system

All the experts interviewed mentioned controlling as the most frequently used option. This primarily involves generating standard reports (e.g., to Federal Financial Supervisory Authority (BaFin)) from both the operational and sales areas. The financial services companies consolidate and visualize the information, which can be accessed via the BI tool. The advantage is that this information can be generated automatically and sent to the intended users at the required time. After one-time programming, the information is kept up to date continuously, and the created dashboards and evaluations can be exported and sent independently. The controlling department can also include direct comments when communicating the results. In addition, only limited programming skills are required for the BI tool to create the reporting to collect and analyze the requested data from the data warehouse.

> E.4: “Standard reporting is a main focus of the BI tool, but of course also the possibility to easily browse the data warehouse via a BI tool, to create ad-hoc evaluations without having great SQL knowledge, but to assemble evaluations via drag and drop and then just analyze the data accordingly […].”

Reporting for executive positions also serves as the basis for financial services companies' budgeting, revenue, and expense planning. The evaluations and findings determined can ultimately be incorporated into the company's internal planning processes. Furthermore, financial services companies are subject to many regulatory measures. In this context, BI provides support to present and fulfill the requirements related to the reporting system. In addition, the support of actuaries with BI was highlighted as a usage.

Sales analysis

Financial services companies focus particular attention on reporting from sales controlling. Sales is an important core variable in many insurance companies. Therefore, it is important to analyze and optimize the sales channels with the support of BI evaluations. In this way, the sales partner is informed which products offered are in high demand and which are less in demand. In case of doubt, a sales partner can assess this independently, but this provides a clear evaluation, and comparisons can be made with other sales partners and channels. On the one hand, an evaluation of the sales data is important for the success of the individual sales employee since the performance is secured in the long term through sales and continuous customer care. On the other hand, evaluating and comparing product groups and sales channels is important for the insurance company itself, as sales are one of the company's main sources of income. An analysis of the distribution can protect against damages in the long run, and important distribution channels can be developed.

Another point to be addressed is, according to one of the experts interviewed, the area of sales analyses is also explicitly used for customer management. Evaluations of new as well as existing customers are performed, showing profitability. Whether the remaining respondents perform these evaluations on their customers cannot be explicitly confirmed based on the data material, but it cannot be excluded either.

Market forecasts

Most of the experts interviewed stated that BI is used to evaluate and visualize historical data and to show upcoming changes in income and expenses. The data can be analyzed, and the program can be configured to provide warning signals in case of discrepancies. According to the experts (E.1, E.2, E.6, and E.8), discrepancies are defined as deviations between target and actual figures, and BI is therefore used primarily in the company's accounting system. As a result, the company is in a position to react to potential risks at an early stage or to implement measures to improve the key figures in the BI system:

> E.2: “[...] where the management can actively go into the figures and see for themselves whether there are points somewhere in the key operating figures that trigger warning signals and must be reacted to.”

Concerning the future, any upcoming market and industry developments should be available and readable. This information is used to create an edge over existing and potential competitors. Not only trends for products can be identified, but also potential threats for the company, which may result in a loss of sales. Development opportunities can be observed too:

> E.8: “So far, you’ve only looked at ex-post things with BI, but you can easily enrich that with predictive things or simulations so that you have a good basis for decision-making when you want to weigh two negotiation alternatives against each other for corporate management.”

Usability

It is further noticeable that most financial services companies do not use all the functions and benefits of BI. The experts are aware of more areas that support the use of BI solutions. There is a need for expansion in the frequency of use. Only two of the interview participants said that BI is used in almost all areas of the company (E.2 and E.4)

The interviews showed that the experts’ main focus about the application areas of BI is the analysis of operational and sales-related company data. Mainly the controlling department uses its functions to create a standardized reporting system, which can be customized to the target groups. Probably the main advantage, in this case, is the simple operation by drag and drop and the possibility of automated creation of reporting. Sales analyses are performed to assess the profitability of sales partners and channels. Market analyses and forecasts are feasible with BI solutions, enabling an edge over competitors. Furthermore, the experts interviewed are aware that the application areas are diverse, and not all potential functions of the software are exploited.

4.3 Challenges

Data and privacy

The quality of the data implemented in the BI software is mentioned by only one interviewee (E.4). According to the interviewee, data quality, in this sense, means reliability. Reliable data contributes to increasing the company’s value and constitutes the basis for business decisions.

Resource-intensive corrections of previous decisions and sales activities that are not optimally controlled are named as risks for the use of poor data quality.

In addition, the handling of data in the context of data protection was mentioned. Even regardless of the European General Data Protection Regulation (GDPR), the secure handling of customer data in the insurance sector is regulated in the Code of Conduct (CoC) of the German Insurance Association. The CoC defines principles for the quality of data processing and data security. These rules of conduct extend the European regulations and are voluntary. Compared to many other countries, the requirements in this regard are high in Europe, according to the experts (E.2, E.5, E.7, and E.8). Data protection concerning BI is legally highly complex. Which customer data may be collected, who is allowed to access and use this customer data, up to the same assurance that only those persons are granted access who are authorized, are some examples.

> E.5: "These are simply legal requirements. The topic of data is very sensitive in Europe and is becoming even more sensitive. I don't want to judge that here, whether it's good or bad. It's just the way it is because we have extremely high legal requirements compared to other countries, such as China or the USA."

IT landscape and programming

The experts report that the existing IT landscape in the backend can become problematic during an implementation (E.1 and E.5). When attempting to combine reporting and other uses of BI in a software application, it can be seen that in most cases, the IT infrastructure has grown and developed without precise guidelines. The subsequent task is to simplify the highly evolved and complex processes and models to make them more flexible. In addition, the use of data in the company has changed compared to the past. Today, deep insights can be obtained from data through data mining and similar evaluation methods, which can provide an important competitive advantage for the company. This means that the available information was not evaluated to the extent that is possible but was only considered as part of the application and not discussed.

It should also be mentioned that one expert points out the issues encountered when implementing BI solutions about the IT landscape as a subsidiary of a corporate group (E.6). Existing guidelines and requirements of the parent company must be complied with. Once the subsidiary decides to integrate a BI tool into the company on its own, special customized solutions have to be found. Existing security measures of the working group have to be changed to be able to access, read and analyze the data from the data warehouse. Suppose the working group itself

does not use a BI software solution. In that case, the subsidiary cannot fall back on expertise in information technology and must ultimately build up its own know-how successively through training and experience:

> E.6: "[…] but even with the special solution, we are completely responsible for the tool ourselves. That means we don't get any support from the group's IT, and accordingly, some things take a bit longer because we have to get to grips with it ourselves."

Additionally, the implementation effort of the software solution was mentioned. The programs must be designed to extract data from the desired digital repositories. As BI tools use a proprietary programming language, companies are bound to the support of the software solution providers. There is some scope for action, but companies depend on the appropriate support in the case of complex and specific internal company requests or even general technical problems. Consequently, the implementation of BI is not only time-consuming but also cost-intensive.

Employee involvement

The company's employees are mentioned in a similar context. They must be trained and qualified to be able to use the new programs in the company adequately. Thus, the employees contribute significantly to the company's success and organizational change. Likewise, employees must understand the purpose and the company-internal goal of the BI application, which requires appropriate communication. This is a process that, similar to the application's programming, is both time-consuming and cost-intensive. Previous ways of working and the employees' perspectives are thus changed.

Furthermore, an understanding of the advantages of BI is to be established among employees across departments. Employee resistance to change has been part of innovation management research for many years. These resistances and disruptions occur in the transition period from the current state, i.e., the time without BI, to the future state. The reason for this is a self-perceived inconsistency between the two states. This can occur at all levels of the organization. The resistance can be based on many factors, such as perceived unfairness or a fear of loss. The experts interviewed describe an attempt to communicate a data-driven world to employees:

> E.6: "[…] then there is the other view, which would be to trim the employees to really use the data, i.e., to really work with the dashboards and simply admit that this is now our data-driven world."

It can be seen that companies are aware of the upcoming innovation management when they want to implement BI applications. Costly training programs are launched, and employees are involved in the implementation to familiarize the workforce with the systems from the beginning. The benefits of use seem to outweigh the costs and issues, as these investments are amortized shortly after implementation. Insurance companies are willing to invest time and money to ensure BI education and maximize their benefits.

Overall, financial services companies that have decided to implement BI solutions are facing issues from previous decisions and current problems. The existing IT infrastructure needs to be redesigned and simplified, and the data for the analyses should be high quality. It is also important to involve employees and to comply with legal requirements, such as the GDPR or the voluntary CoC. Employees who evaluate and use the data are crucial to the success of BI in insurance companies. They must be trained accordingly and involved in the development process to generate the best possible benefit for the company. Companies make this resource-intensive investment because the benefits outweigh the costs of the investment.

4.4 Impact on processes

Management processes

The use of BI is one of the most important application areas in sales. Due to information technology, sales partners can evaluate and compare their own production and their employees' production. This way, incentives can be set to increase production, and difficulties can be eliminated. Without the need for consultation with the controlling department and the associated reporting, the sales departments have access to the intended evaluations. Since implementing BI solutions in the company, the sales partners have recognized the added value and demanded analyses to control themselves and the employees. Therefore, it can be deduced that the evaluations in the sales department are involved in the management processes and change them. In this respect, management can discuss and interpret the results and production with the sales department. But also the sales units receive an overview of their performance. Additionally, BI uses resources more efficiently, and development potentials can be targeted. Compared to the business organization without BI, searching for potential errors is time-consuming.

In the context of the transformation of the management processes, the interdepartmental possibility of discussion should be mentioned. On the one hand, operational and sales results can be interpreted within management and the board of directors, influencing future processes and communication with employees. In this case, BI positively influences management methods and processes. On the other hand, a department's management can deal with the results without

waiting for consultation with the top management. Thus an operational decision-making scope is established within the department. By using resources more efficiently and improving communication within the company, the company gains flexibility. Furthermore, there is the possibility of clear communication of management goals across departments, using the reports of the BI applications for support:

> E.2: "You can also discuss and use the key performance indicators through that, and I think that always provides the opportunities for internal and external exchange, also to discuss across departments about the individual topics and therefore provides more flexibility and more opportunities for the whole company."

To conclude, communication within the company is increased because BI can provide precise definitions used consistently across departments. Explanations of terms can be provided in the system with threshold values. In summary, it can be confirmed that the sales department of insurance companies, in particular, can change its management processes by using BI. Thus, the sales partners can evaluate the production of their employed sales partners. Resources can be used efficiently to solve specific problems and are not spent searching for potential sources of errors. A certain scope for decision-making allows the departments to flexibly and responsibly carry out management tasks and communicate these to the employees.

Decision-making processes

The analysis of data is even more important in today's world, as the insights gained have an impact on management decision-making. This link between data and decision-making is also confirmed by the interviewee, a board member of a financial services company. Furthermore, the interviewees agree that quantifying and measuring the impact of BI systems on decision-making is not simple. The implementation in the company is successive, so a direct assessment of the impact is difficult:

> E.5: "It's just not that easy to measure, and because you don't implement something like this, I don't know, within a month, but it takes years. It's just such a gradual process."

According to the interview participants, the quality of data evaluations has increased. As data from many sources can converge in the BI application, it is possible to trace the results in great detail. This allows the exact origin of a problem to be identified more easily and quickly. Subsequently, targeted action measures can be taken and initiated. The reporting system in the BI software is designed interactively to the extent that the core of the problem that occurred can

be displayed with a few clicks and drill-down menus. This type of data analysis leads to better decision-making:

> E.1: “I can create dashboards that I can navigate relatively interactively, which is obviously great for decision-making. And later, when I’ve identified a problem issue, I can drill down through what is called drill-downs or drill-throughs into the core information again, so what’s really the core cause of the problem, or the identified problem at that moment.”

The data quality resulting from BI is also relevant with regard to future-related forecasts. Market forecasts and potential future issues for the insurance company can be better justified and communicated with the available depth of detail. It is also mentioned that decision-making and communication are simplified due to BI. In addition, according to the experts surveyed, there is an improvement in the plausibility of the results and data. In the absence of BI, decisions are often made based on experience and gut feeling. As a consequence of the intelligent system, the decision-makers are in a better position to justify their decisions and assessments and communicate them reasonably. The susceptibility to errors decreases, and the decisions are less regretted in retrospect. This ensures the company’s success, especially in the long term.

As a further positive impact, the speed of decision-making in the information material becomes apparent. Based on the fact that data is uploaded to the reporting system at regular times and in an automated manner and that this data is constantly up to date, data analyses and comments can be carried out considerably faster. Decision-making is influenced by the fact the data does not have to be uploaded, compiled, and visualized individually. Due to the automated process, the decision-makers in the company have quick access to the analyses, and internal ad-hoc decisions can be made in a short-term manner. The time saved in decision-making provides resources in the form of time capacities that can be invested otherwise. In addition, spontaneous decisions can be made more quickly by constantly monitoring sales and revenue figures. The changes in the figures are continuously displayed in the BI system so that the necessary decision-making processes can be performed faster. As a result, reacting faster to trends and fluctuations in the insurance market is possible.

According to the experts, the fact that one software solution is now sufficient to perform data analyses and visualizations also contributes to a higher speed of decision-making. There is no longer a need to extract data from different data sources. Since the program aggregates the data, a time saving is created, directly affecting the turnaround time and speed of decision-making.

Furthermore, not only is time capacity created, but it also allows existing resources to be better invested. The surveyed experts stated that BI influences investment decisions. For example, data analyses and market forecasts lead to more informed decisions. By making the right investments, there is the possibility of securing the long-term success of the company. According to the interviewees, investments are not only in capital but also in time, employees, or product groups. A quick and plausible investment decision can help to stay one step ahead of competitors in the insurance sector.

5 Discussion and Implications

The qualitative study showed a consensus among the experts that the use of BI in internal and external reporting is the most important function and generates an advantage over previous systems. For insurance companies, the main focus is on analyses of sales partners and channels, as well as market forecasts. In this context, Huang et al. (2022) show that BI can significantly influence financial performance and customer behavior. Curko et al. (2007) also name customer categorization and segmentation as valuable benefits of BI. In our interview study, one expert works as a team leader for customer management, but the job description does not indicate that customer segmentation and targeted selling are performed using BI. In the literature, BI is also highlighted as a possible application for calculating insurance premiums and managing insurance policies (Rostek 2009; Helfand 2017). One expert also highlighted this use. Overall, BI has the potential to improve the calculation and monitoring of key performance indicators as well as the management of internal risks (Helfand 2017; Eckert and Osterrieder 2020). Amini et al. (2021) also use the example of agricultural insurance to show that the use of BI can drastically reduce imprecise estimations caused by uncertainties. In addition, possible predictions for handling financial risks could be made. Overall, the experts surveyed focus more on business than technology in the context of BI. In contrast, Petrini and Pozzeborn (2009) show that in the Brazilian companies surveyed, BI management focuses on technology. As a result, the BI systems were implemented predominantly with a technological focus.

According to Watson (2009), improved decision-making and business process enhancement are among the most important reasons for using BI systems. Also, visualization through the use of BI is highlighted as an advantage (Chung 2009; Toreini et al. 2022). At the same time, they are also one of the most difficult to measure or quantify. The interview participants confirm this aspect. It is expressed that implementation of BI does not take place in the short term but successively over a longer period of time. The interviewed participants confirm that the application potential within the company has not yet been fully exhausted. Insurance companies are aware

that further fields of application, such as the detection of insurance fraud, can be developed. Potential barriers to the further expansion of BI within the company are the difficulties listed regarding data protection, infrastructure, and innovation management between employees. Furthermore, the experts interviewed stated that an investment in the employees and their handling of BI applications is necessary to ensure the best possible use of the systems. Cost and time savings are expected for internal company processes with the use of BI in the literature (Wanda and Stian 2015). It is noticeable that all experts mentioned faster decision-making and, thus, time savings. Grounding and plausibility of decisions were also mentioned as positive outcomes by respondents. However, cost savings were not explicitly named concerning the process change in the company. In summary, Table 3 provides an overview of our interview study's key findings and implications.

Main codes	Subcodes	Key findings	Implications
Chances	Reporting system	• To use BI for standard reporting, technological know-how is only required to a minor extent.	• Standard reporting (e.g., to BaFin) should be supported by establishing dashboards and specific evaluations using BI.
	Sales analysis	• BI can be used to analyze and optimize the sales channels clearly. Evaluations of possible new and existing customers provide information on profitability as part of customer management.	• To optimize sales analyses, BI should be used for evaluations in this context (e.g., customer evaluations).
	Market forecasts	• Competitive advantages can be achieved by analyzing the upcoming market and industry developments (e.g., product trends).	• BI should be used to implement market forecasts, and in this context, the definition of key figures is needed in order to be able to use deviations between target and actual in accounting as a warning signal.
	Usability	• BI provides a wide range of functions that can be used for sales analysis, market analysis, and for assessing the profitability of sales partners and channels. For e.g., the drag-and-drop operation and the possibility of automating reports are an advantage compared to other tools.	• A knowledge transfer between employees on BI-specific know-how should be established to increase the potential for usability.
Challenges	Data and privacy	• High-quality data makes a decisive contribution to increasing the value of a company. In contrast, poor-quality data can lead to resource-intensive corrections and inadequately managed sales channels.	• It should always be ensured that high-quality data is provided across all business sections to achieve good results with BI.

	IT landscape and programming	• The use of BI depends on the IT landscape of the parent company and its subsidiaries. Existing guidelines and requirements of the parent company must be complied with.	• The IT landscape should be prepared, e.g., through adapting to regulatory requirements, for implementing BI applications.
	Employee involvement	• Employees contribute significantly to the success of the company and to organizational change.	• For the company's success, employees should be actively involved in the innovation process, i.e., the implementation and use of BI, via adequate training. In this context, employees have to understand the internal goal of BI.
Impact on processes	Management process	• The management department has direct access to cross-departmental analyses, which improves communication. BI also leads to more efficient use of resources and the optimization of development potential.	• Incentives to increase profitability should be provided through the use of BI, as communication can be optimized. Therefore, these incentives have to be forced top-down.
	Decision-making process	• The use of BI leads to the simplification of decision-making and communication. For data analysis and visualization, BI is sufficient as a software solution in this context.	• Extracting data from only one source reduces the susceptibility to errors in the decision-making process and increases the speed of decision-making using BI.

Table 3 Overview of key findings and implications

6 Limitations, Future Research Directions and Conclusions

Due to the unavoidable limited generalizability and limited objectivity, our results can only be considered as a first trend regarding the use of BI in insurance companies. Moreover, the study focuses only on the German insurance market. In order to generate better generalizable results, an increase in the sample size and an extension to international insurance markets is advisable. A comparison with international insurance markets can provide valuable and more holistic insights for various industry sectors. While our research takes a general view of the use of BI in insurance companies in Germany, the interviews suggest that further research can investigate the specific use of BI in individual lines of business, such as property or life insurances. In this context, it is interesting to analyze what influence BI has on individual insurance lines and how BI can support the calculation of insurance premiums and the detection of insurance fraud.

Our paper analyzed established and new applications of BI in insurance companies and identified chances and challenges associated with implementing and using BI. Eight experts from

German insurance companies were interviewed. Our results show that the use of BI is generally perceived as advantageous and a further expansion of BI in insurance companies is expected. In particular, employees should be increasingly involved in the use of BI in the future. Overall, application possibilities of BI in insurance companies are not fully exploited. Even in literature, BI in insurance companies is discussed to a limited extent. In the future, the use of BI should be extended to specific lines of business. In an increasingly digital world, insurance companies can profitably use data insights gained through BI for a broader understanding and discussions among practitioners and researchers.

References

Amini, M., Salimi, S., Yousefinejad, F., Tarokh, M.J., Haybatollahi, S.M.: The Implication of Business Intelligence in Risk Management: A Case Study in Agricultural Insurance. Journal of Data, Information and Management. **3**(2), 155–166 (2021)

Baars, H., Zimmer, M., Kemper, H.G.: The ICT Convergence Discourse in the Information Systems Literature–A Second-Order Observation. In: Proceedings of the 17th European Conference on Information Systems (ECIS), Verona, Italy, June 8–10, 2009 (2009)

Catlin, T., Hartmann, R., Segev, I. and Tentis, R. (2015) The Making of a Digital Insurer: The Path to Enhanced Profitability, Lower Costs and Stronger Customer Loyalty (2015). http://www.mckinsey.com/industries/financial-services/our-insights/the-making-of-a-digital-insurer, Accessed 11 Dec 2022

Chee, T., Chan, L., Chuah, M., Tan, C., Wong, S., Yeoh, W.: Business Intelligence Systems: State-of-the-art Review and Contemporary Applications. In: Proceedings of the 2009 Symposium on Progress in Information and Communication Technology (SPICT'09), Kuala Lumpur, Malaysia, December 7–8, 2009 (2009)

Chung, W.: Enhancing Business Intelligence Quality with Visualization: An Experiment on Stakeholder Network Analysis. Pacific Asia Journal of the Association for Information Systems, **1**(1), 33–54 (2009)

Curko, K., Bach, M.P., Radonic, G.: Business Intelligence and Business Process Management in Banking Operations. In: Proceedings of the 29th International Conference on Information Technology Interfaces (ITI), Cavtat, Croatia, June 25–28, 2007 (2007)

Davenport, T.H.: How Strategists Use "Big Data" to Support Internal Business Decisions, Discovery and Production. Strategy & Leadership. **42**(4), 45–50 (2014)

Dreyer, S., Werth, O., Olivotti, D., Guhr, N., Breitner, M.H.: Knowledge Management Systems for Smart Services: A Synthesis of Design Principles. e-Service Journal. **13**(2), 27–67 (2022)

Eckert, C., Eckert, J., Zitzmann, A.: The Status Quo of Digital Transformation in Insurance Sales: An Empirical Analysis of the German Insurance Industry. Zeitschrift für die gesamte Versicherungswissenschaft. **110**(2), 133–155 (2021)

Eckert, C., Osterrieder, K.: How Digitalization affects Insurance Companies: Overview and Use Cases of Digital Technologies. Zeitschrift für die gesamte Versicherungswissenschaft. **109**(5), 333–360 (2020)

Eggert, M., Alberts, J.: Frontiers of Business Intelligence and Analytics 3.0: A Taxonomy-based Literature Review and Research Agenda. Business Research. **13**(2), 685–739 (2020)

Eling, M., Lehmann, M.: The Impact of Digitalization on the Insurance Value Chain and the Insurability of Risks. The Geneva Papers on Risk and Insurance–Issues and Practice. **43**(3), 359–396 (2018)

Eling, M., Nuessle, D., Staubli, J.: The Impact of Artificial Intelligence Along the Insurance Value Chain and on the Insurability of Risks. The Geneva Papers on Risk and Insurance–Issues and Practice. **47**(2), 205–241 (2022)

Gehra, B., Gentsch, P., Hess, T.: Business Intelligence for the Masses. Controlling & Management Review. **49**(3), 236–242 (2005)

Gioia, D.A., Corley, K.G., Hamilton, A.L.: Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organizational Research Methods. **16**(1), 15–31 (2013)

Gupta, B., Goul, M., Dinter, B.: Business Intelligence and Big Data in Higher Education: Status of a Multi-Year Model Curriculum Development Effort for Business School Undergraduates, MS Graduates, and MBAs. Communications of the Association for Information Systems. **36**(1), 450–476 (2015)

Helfand, R.D.: Big Data and Insurance: What Lawyers Need to Know and Understand. Journal of Internet Law. **21**(3), 2–35 (2017)

Hsieh, H.-F., Shannon, S.E.: Three Approaches to Qualitative Content Analysis, Qualitative Health Research. **15**(9), 1277–1288 (2005)

Huang, Z.X., Savita, K.S., Dan-yi, L., Omar, A.H.: The Impact of Business Intelligence on the Marketing with Emphasis on Cooperative Learning: Case-study on the Insurance Companies. Information Processing & Management. **59**(2), 1–10 (2022)

Keller, B.: Big Data and Insurance: Implications for Innovation, Competition and Privacy (2018). https://www.genevaassociation.org/research-topics/cyber-and-innovation-digitalization/big-data-andinsurance-implications-innovation, Accessed 10 Dec 2022

Kuckartz, U.: Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 3rd Ed. Beltz Juventa, Weinheim, Basel (2018)

Kyper, E.S., Douglas, M.J., Lievano, R.J.: Operational Business Intelligence: Applying Decision Trees to Call Centers. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS), San Francisco, California, USA, August 6–9, 2009 (2009)

Mayring, P.: Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12th Ed. Beltz, Weinheim, Basel (2015)

Myers, M.D., Newman, M.: The Qualitative Interview in IS Research: Examining the Craft. Information and Organization. **17**(1), 2–26 (2007)

Negash, S.: Business Intelligence. Communications of the Association for Information Systems. **13**(2004), 177–195 (2004)

Ngai, E.W., Hu, Y., Wong, Y.H., Chen, Y., Sun, X.: The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature. Decision Support Systems. **50**(3), 559–569 (2011)

Petrini, M., Pozzeborn, M.: What Role is "Business Intelligence" Playing in Developing Countries? A Picture of Brazilian Companies. In: Rahman, H. (Hrsg.) Data Mining Applications for Empowering Knowledge Societies, S. 237–257. Information Science Reference, Hershey, New York (2008)

Phillips-Wren, G., Daly, M., Burstein, F.: Reconciling Business Intelligence, Analytics and Decision Support Systems: More Data, Deeper Insight. Decision Support Systems. **146**(2021), 1–10 (2021)

Rostek K.: Business Intelligence for Insurance Companies. Foundations of Management. **1**(1), 65–82 (2009)

Schmidt, C.: Insurance in the Digital Age: A View on Key Implications for the Economy and Society (2018). https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/insurance_in_the_digital_age_01.pdf, Accessed 11 Dec 2022

Schnell, R., Hill, P.B., Esser, E.: Methoden der empirischen Sozialforschung, 9th Ed. Oldenbourg, München (2011)

Schulte-Noelle, H.: Technological Changes in IT and Their Influence on Insurance: The Change Ahead (I). The Geneva Papers on Risk and Insurance–Issues and Practice. **26**(1), 83–88 (2001)

Schultze, U., Avital, M.: Designing Interviews to Generate Rich Data for Information Systems Research. Information and Organization. **21**(1), 1–16 (2011)

Toreini, P., Langner, M., Maedche, A. Morana, S., Vogel, T.: Designing Attentive Information Dashboards. Journal of the Association for Information Systems. **23**(2), 521–552 (2022)

Trieu, V.H., Burton-Jones, A., Green, P., Cockcroft, S.: Applying and Extending the Theory of Effective Use in a Business Intelligence Context. MIS Quarterly. **46**(1), 645–678 (2022)

Wanda, P., Stian, S.: The Secret of my Success: An Exploratory Study of Business Intelligence Management in the Norwegian Industry. Procedia Computer Science. **64**(2015), 240–247 (2015)

Watson, H.J.: Business Intelligence – Past, Present, and Future. In: Proceedings of the 15th Americas Conference on Information Systems (AMCIS), San Francisco, California, USA, August 6–9, 2009 (2009)

Werth, O., Schwarzbach, C., Rodríguez Cardona, D., Breitner, M. H., Graf von der Schulenburg, J.-M.: Influencing Factors for the Digital Transformation in the Financial Services Sector. Zeitschrift für die gesamte Versicherungswissenschaft, **109**(2), 155–179 (2020)

Yin, R.K.: Case Study Research: Design and Methods. 4th Ed. SAGE Publications, Thousand Oaks, CA, London, New Delhi (2009)

Modul 6

Human Factor Influences on Early Warning in Cyber Security: A Content-analysis based Literature Review

Theresa Eden
Dirk Wrede
Johann-Matthias Graf von der Schulenburg

eingereicht bei:

Management Review Quarterly

Human Factor Influences on Early Warning in Cyber Security: A Content-analysis based Literature Review

Theresa Eden, Dirk Wrede, Johann-Matthias Graf von der Schulenburg

Theresa Eden (Corresponding Author)

Gottfried Wilhelm Leibniz Universität Hannover
Institute for Risk and Insurance
Otto-Brenner-Straße 7
D-30159 Hannover
Germany
E-Mail: te@ivbl.uni-hannover.de

Dirk Wrede

Gottfried Wilhelm Leibniz Universität Hannover
Institute for Risk and Insurance
Otto-Brenner-Straße 7
D-30159 Hannover
Germany

Johann-Matthias Graf von der Schulenburg

Gottfried Wilhelm Leibniz Universität Hannover
Institute for Risk and Insurance
Otto-Brenner-Straße 7
D-30159 Hannover
Germany

Human Factor Influences on Early Warning in Cyber Security: A Content-analysis based Literature Review

Abstract

This study examines the influence of human factors on early warnings in cyber security through a content-analysis based literature review. The search in the selected databases provided 13,998 articles. Following the defined inclusion and exclusion criteria, a total of 67 articles could be considered for further analysis. The results show that in addition to organizational factors, infrastructure, technology, law, and regulation, human factors have a significant impact on cyber security in an organization. While awareness training can be used to increase the sensitivity toward conspicuousness and accompanying cyber-attacks, the evaluations of such training can serve as a possible early warning indicator. In particular, the use of surveys and comparisons of changes over time could be used. In this context, early warning has the potential to reduce damage resulting from attacks, errors, or failures and should be considered as well as prevention measures in companies.

Keywords: cyber security; information security; human factor; early warning indicator; literature review

1 Introduction

The relevance of cyber security has increased in recent years and is one of the most strategically important tasks for companies (Kayworth and Whitten 2010; Marotta and McShane 2018; Tam et al. 2021). Because of digitalization, the frequency, complexity, and extent of cyber-attacks are growing (Chertoff 2008; Choo 2011; Eling and Wirfs 2019). The damage resulting from such attacks is not only technical but also financial. This can result in an existential threat to business economic success and competitiveness (Cavusoglu et al. 2004; Fielder et al. 2016; Järveläinen 2013; Rakes et al. 2012; Smith 2004; Srinidhi et al. 2015). Overall, cyber security is difficult to measure because of multiple influencing factors; thus, it requires a holistic and practical approach (Anderson and Moore 2006; Fielden 2010; Soomro et al. 2016; Werlinger et al. 2009; Zafar and Clark 2009). Consequently, to prevent cyber-attacks, it is important to consider both technical and non-technical practices while generating cross-disciplinary collaboration (Choobineh et al. 2007; Crossler et al. 2013; Eling et al. 2021; Falco et al. 2019; Marotta

and McShane 2018; Tu et al. 2019; Von Solms and Von Solms 2004; Zafar and Clark 2009).

> "Computer security is not just about technology and systems. It is also about the people who use these systems and how their vulnerable behaviors can lead to exploitation" (Bowen et al. 2011).

In this context, the human factor is an additional dimension and significant issue in cyber security, representing the weakest link in an organization's security construct and a potential target for attackers (Azmi et al. 2018; De Maggio et al. 2019; Pfleeger et al. 2014; Stewart and Jürjens 2017; Von Solms and Van Niekerk 2013). In information security, the human factor is defined as the role of humans in the security process. In cybersecurity, the additional dimension of the human being as a potential target of cyberattacks is included (Von Solms and Van Niekerk 2013). Therefore, this factor should not be forgotten in the prevention measures. In the course of prevention measures, early warning is another component that is considered in technical research (Bernsmed and Tøndel 2013; Disterer 2015; Kalutarage et al. 2016; Petrenko 2018). Early warning has the potential to reduce damage resulting from attacks, errors, or failures (Disterer 2015).

The focus of the current research is predominantly on the area of intrusion detection (Buczak and Guven 2015; Mitchell and Chen 2014; Mohammadi et al. 2019; Robinson et al. 2015) and, concerning the human factor, on the establishment of cyber or information security awareness as a preventive measure for cyber-attacks (Abawajy 2014; Kritzinger and Smith 2008; Nosworthy 2000; Siponen 2001; Thomson and Von Solms 1998; Tsohou et al. 2012). In this context, the potential of early warning is highlighted only at the technical level. The aim of this study is to fill the research gap regarding the influence of the human factor on early warning in cyber security using a holistic and practical approach and to thus construct employee-based early warning indicators. The following research question (RQ) was investigated: What impact do human factors have on early warnings in cyber security?

The article is structured as follows. First, the theoretical background related to previous research in this area is presented. A special focus is on the factors influencing information security and the relevance of human factors. This is followed by the presentation of the selected research methodology, including the description of the material collection, descriptive analysis, and selection and definition of the categories. Next, we present our analysis framework, followed by the material evaluation, which includes the developed categories and the resulting framework. We then present the results of the literature review of the developed categories. Finally, we

discuss the results and address the limitations of the applied research method before concluding our study.

2 Theoretical Background

Rashid et al. (2018) emphasized that "the foundational knowledge on which the field of cybersecurity is being developed is fragmented." Previous research on information security has mostly focused on considering security from either a socio-technical (Backhouse and Dhillon 1996; Hitchings 1996; James 1996; Mujinga et al. 2017), socio-philosophical (Ratnasingham 1998), socio-organizational (Dhillon and Backhouse 2001), or purely technical (Bass 2000; Li and Guo 2007; Wong et al. 2000; Yang and Huang 2007) perspective. Such delineation may have led to security being widely viewed as an area that has not been comprehensively explored in information security research (Kotulic and Clark 2004; Paulson 2002; Siponen and Willison 2007; Zafar and Clark 2009). Thus, the need for a holistic approach to information security has been increasingly highlighted in the literature (Fielden 2010; Soomro et al. 2016; Zafar and Clark 2009).

Accordingly, research on information security is wide-ranging and includes technical, behavioral, managerial, philosophical, and organizational approaches that address securing and protecting the confidentiality, integrity, and availability of information and information systems (Crossler et al. 2013; Zafar and Clark 2009). Although non-technical factors are increasingly emphasized in information security research, they are rarely studied in an integrated framework (Tu et al. 2019). The literature emphasizes the multidimensional nature of information security (Choo et al. 2021; Posthumus and Von Solms 2004; Von Solms 2001). For example, according to Da Veiga and Eloff (2007), information security includes technology, processes, and people. Information security in organizations consists of complex processes that are influenced by a wide variety of factors and should be managed in a single framework, if possible (Yildirim et al. 2011). Silic and Back (2014), among others, identified organizational and human aspects of information security as 2 of the 13 main topics of research in this area. Singh et al. (2014) emphasized the importance of the organizational factors of information security. Tu et al. (2019) also focused on the analysis of the organizational and human aspects of information security management. Kraemer et al. (2009) investigated the relationship between human and organizational factors and technical vulnerabilities of computers and information security. Werlinger et al. (2009) took a holistic view and examined human, organizational, and technological factors, including existing interrelationships, as challenges for information technology security management. Monfelt et al. (2011) described a 14-layered framework that includes organizational

and social aspects in information security management. In addition to the organizational dimension, Choraś et al. (2015) distinguished the operational and infrastructural dimensions of cyber security. Schuessler (2007) emphasized the importance of regulatory factors in information security. Karyda et al. (2006) considered legal aspects in addition to technical and organizational aspects in the framework for outsourcing information security/information technology security services. The literature emphasizes the importance of human aspects as the most important factor for information security (Ashenden 2008; Azmi et al. 2018; Stewart and Jürjens 2017). For example, Al-Darwish and Choe (2019) investigated the direct and indirect factors influencing human aspects of information security. Spears and Barki (2010) examined user participation in information systems security risk management. Young et al. (2018) analyzed the impact of human behavioral changes on cyber security. Alavi et al. (2014) developed a conceptual framework to analyze human factors in information security management systems. Concerning the RQ considered in this study, in addition to the human factor, the current state of research on early warning in the field of information security needs to be examined.

So far, the aspect of early warning in the field of information security has been less researched. The literature indicates the relevance of early warning for information security (Disterer 2015; Petrenko 2018). However, the consideration is mainly limited to discussing the potential uses of weak signals in the context of information security (Kajava et al. 2005; Disterer 2015) and describing the identification, selection, and implementation of early warning indicators for the management of information security incidents (Bernsmed and Tøndel 2013).

3 Research Methodology

3.1 Content-analysis based Literature Review

Researchers have published a variety of studies on cyber security (Fujs et al. 2019; Suryotrisongko and Musashi 2019) using diverse research methods (Edgar and Manz 2017; Fujs et al. 2019). This research was conducted as a content-analysis based literature review using the approach of Seuring and Gold (2012) following the recommendations of Fisch and Block (2018) with the extension by Clark et al. (2021), as predominantly qualitative research methods are used to study all key cyber security areas (Fujs et al. 2019). Fink (2014) defined a literature review as "a systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners." Saunders et al. (2009) described the process of reviewing literature as an iterative cycle of defining and specifying parameters and keywords, searching for literature

based on these keywords, and evaluating and collecting the existing literature. Literature reviews provide a summary of the existing state of a research area by identifying patterns, themes, and questions, and they serve to capture the conceptual content of a research area (Meredith 1993).

Using a literature review, the representative literature on a topic is analyzed, critiqued, and summarized in a holistic manner to generate new conceptual frameworks and perspectives (Bem 1995; Palmatier et al. 2018; Snyder 2019; Torraco 2005). Seuring et al. (2005) and Seuring and Müller (2008) indicated that, from a methodological perspective, a literature review can be understood as a content analysis combining quantitative and qualitative aspects to examine both structural (descriptive) and content criteria. Hsieh and Shannon (2005) referred to the use of qualitative content analysis to review the literature. Accordingly, Seuring and Gold (2012) suggested integrating content analysis (Mayring 2015) into the systematic review process to further enhance the validity of literature reviews. In this context, the performance of content analysis requires preliminary theoretical considerations and a clear process structure (Kassarjian 1977). Content analysis is a method for categorizing and quantifying qualitative, text-based data in a structured, rule-guided, and theory-driven manner to extend beyond the purely descriptive analysis of the collected data (Mayring and Brunner 2009). We used this structured approach for data analysis, based on Mayring's qualitative content analysis model, for our literature review (Rowe 2014) to analyze both the formal qualitative and quantitative substantive aspects in the literature we studied (Duriau et al. 2007). Following Seuring and Gold's (2012) process model for content analysis, the approach in our study includes the following four steps:

(1) Material collection: The material to be collected was defined and delimited. In addition, the unit of analysis (i.e., individual paper) was determined.
(2) Descriptive analysis: The formal aspects of the material were recorded, for example, the number of publications per year, which formed the background for the subsequent theoretical analysis.
(3) Selection and definition of categories: The structural dimensions and associated analytical categories were determined, which were used to analyze the collected material, for example, the number of publications per year. The structural dimensions constituted the main topics of the analysis and comprised individual analytical categories.
(4) Material evaluation: The evaluation of the material to be analyzed according to the selected structural dimensions takes place to enable the identification of relevant topics and the interpretation of the results (Seuring and Gold 2012).

A description of the material evaluation process (steps 3 and 4) is presented in Figure 1. The following section outlines in detail the four-step content analytic approach, following Mayring (2015), as used in this study to conduct a systematic literature analysis (Rowe 2014).

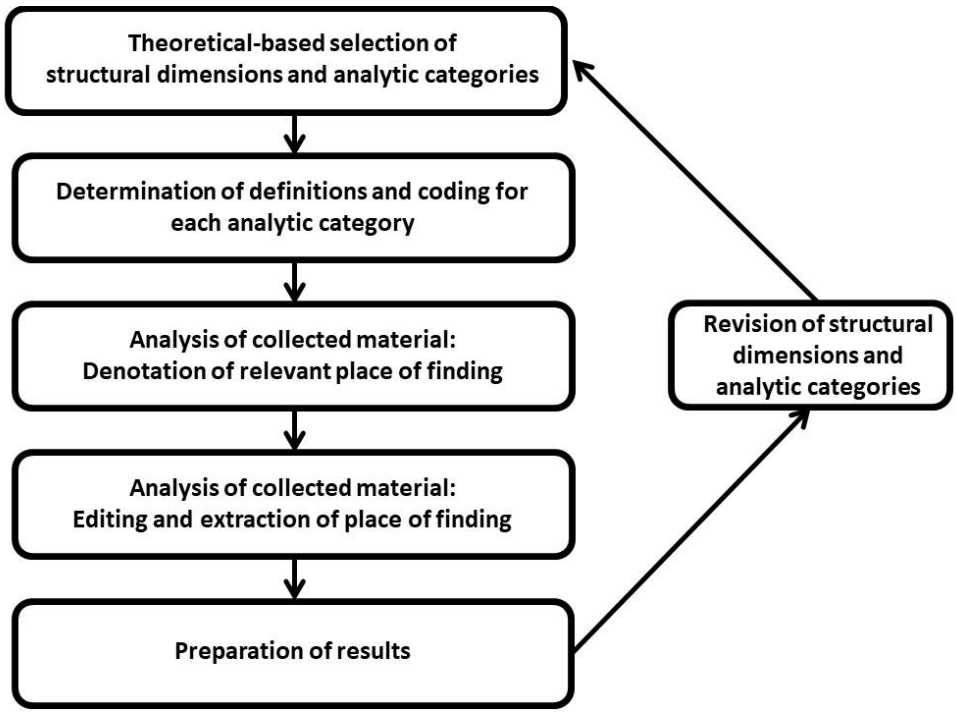


Figure 3: Research process of a structured content analysis, following Mayring (2015)

3.2 Material Collection

The quality of a literature review is significantly determined by the quality of the process (Vom Brocke et al. 2009). The first step was to identify and define keywords and search terms (Hart 1998; Tranfield et al. 2003). The keywords were selected inductively based on a review of numerous publications in the field of information, cyber, and information technology security, considering not only the keywords of the articles but also the existence of the searched terms in the respective abstracts (Vom Brocke et al. 2015). Subsequently, a trial-and-error procedure was performed to identify the best initial keywords and generate a set of comprehensive search terms (Pickering and Byrne 2014) covering all important scientific papers related to our RQ (Wolfswinkel et al. 2013). Finally, the selected search terms were discussed with experts in the field, and necessary adjustments were made. We finally used the following search terms, which were combined via Boolean operators to form our final search string (Table 1).

Table 2: Overview search string

Topic	Keywords	Appearing in
Academic database search		
Security	"Cyber Security," "Cybersecurity," Information Security," "Informationssicherheit," "IT Security"	EconBiz, Science Direct, Wiso, Springer, Senior Scholars' Basket of Journals
Metrics	"Metrics," "Indicator," "Indikator," "Kennzahl"	
ISMS	"ISMS," "Informationssicherheitsmanagementsystem," "Information Security Management System"	
Bolean Formula: (Cyber Security OR Cybersecurity OR Information security OR Informationssicherheit OR IT Security) AND (Metrics OR Indicator OR Indikator OR Kennzahl) AND (ISMS OR Informationssicherheitsmanagementsystem OR Information Security Management System)		
Google Scholar Search		
Security	"Cyber Security"	All fields
Metrics	"Indicator"	
ISMS	"ISMS"	

Search terms were used to search anywhere in the document, i.e., title, abstract, and main text. The time period for the search was constrained to the period from January 1, 2000 to May 15, 2020. In a literature review, it is vital to define an analytical framework for research and to delimit the research problem. In this regard, four important notes were provided.

(1) This analysis targeted papers in peer-reviewed scientific journals as well as conference papers in English and German, which are subject to the focus of frameworks, metrics, or indicators in the field of informatics security, cyber security, and/or illustrate influencing factors on named aspects. Following the guidelines for the consideration of gray literature (Garousi et al. 2019), book contributions were included in the analysis, as this

approach has already been used in multi-vocal literature reviews in the research area of cyber security and crime (Cascavilla et al. 2021; Islam et al. 2019).

(2) Literature in other languages was excluded, as well as those that addressed predominantly focused technical or model-based aspects.

(3) To generate a holistic approach of influencing topics related to the development and application of early warning indicators, publications with an industry-specific focus are not part of further analysis.

(4) Publications prior to the turn of the century were excluded to ensure a certain degree of currency.

The search for relevant publications was mainly performed as a structured keyword search. The combinations of descriptors were used to search the following databases: EconBiz (www.econbiz.de), ScienceDirect (www.sciencedirect.com), Wiso (www.wiso-net.de), SSRN (www.ssrn.com), and Springer (www.springerlink.com). In addition, the Senior Scholars' Basket of Journals[1], as defined by the Association for Information Systems (AIS) in December 2011, were included in the literature search. Furthermore, a non-systematic literature search in the search service Google Scholar was conducted to identify further publications that were not listed in the above-mentioned databases and scientific journals.

When searching the individual literature databases or scientific journals, the search string had to be adapted to the specifications of the search engine (Appendix 1). The literature search was conducted based on a structured search and identification process following Vom Brocke et al. (2009) and Webster and Watson (2002), which essentially involves querying scientific databases using keywords and searching backward or forward based on relevant articles. While backward search refers to reviewing the literature sources of the articles obtained from keywords, forward search refers to reviewing other sources that cited the article (Levy and Ellis 2006; Okoli 2015; Schryen 2015). After an initial quick content check, the identified articles were included or excluded from the analysis. To increase the reliability of the research method, databases and journals, as well as individual articles, were reviewed by a second researcher. When reading the articles, cited literature sources were used as secondary sources; however, this did not result in many additional articles, which can be taken as an indication of the validity of the research (Seuring and Müller 2008). The selection process for identifying the relevant literature was based on the procedure of the PRISMA Transparent Reporting of Systematic

[1] The following journals were selected by the Association for Information Systems (AIS) Senior Scholars as a top basket of journals: European Journal of Information Systems, Information Systems Journal, Information Systems Research, Journal of the Association for Information Systems, Journal of Information Technology, Journal of Management Information Systems, Journal of Strategic Information Systems, and Management Information Systems Quarterly (Association for Information Systems (AIS) 2011).

Reviews and Meta-Analyses (Moher et al. 2009). Thus, as part of the literature selection process for evaluating the content of the articles, we conducted an analysis of the titles, abstracts, and full texts (Moher et al. 2009; Vom Brocke et al. 2009). A detailed description of the selection process for the identification of relevant literature is shown in Figure 2.

The search in the above-mentioned databases provided 13,998 articles. By searching the Association for Information Systems (AIS) Senior Scholars' Basket of Journals, an additional 113 publications were identified. In the search results, 118 duplicates were removed from further analysis. Based on the defined inclusion and exclusion criteria, 13,744 publications were excluded. Through a subsequent review of the full texts of 249 publications, 208 publications were excluded. Subsequently, a backward or forward search, as suggested by Webster and Watson (2002), was performed to find 19 relevant papers. Further, seven papers were identified through a non-systematic literature search on Google Scholar using the defined keywords. This provided 67 articles with relevant content as a result of the literature selection process, considering the defined inclusion and exclusion criteria.

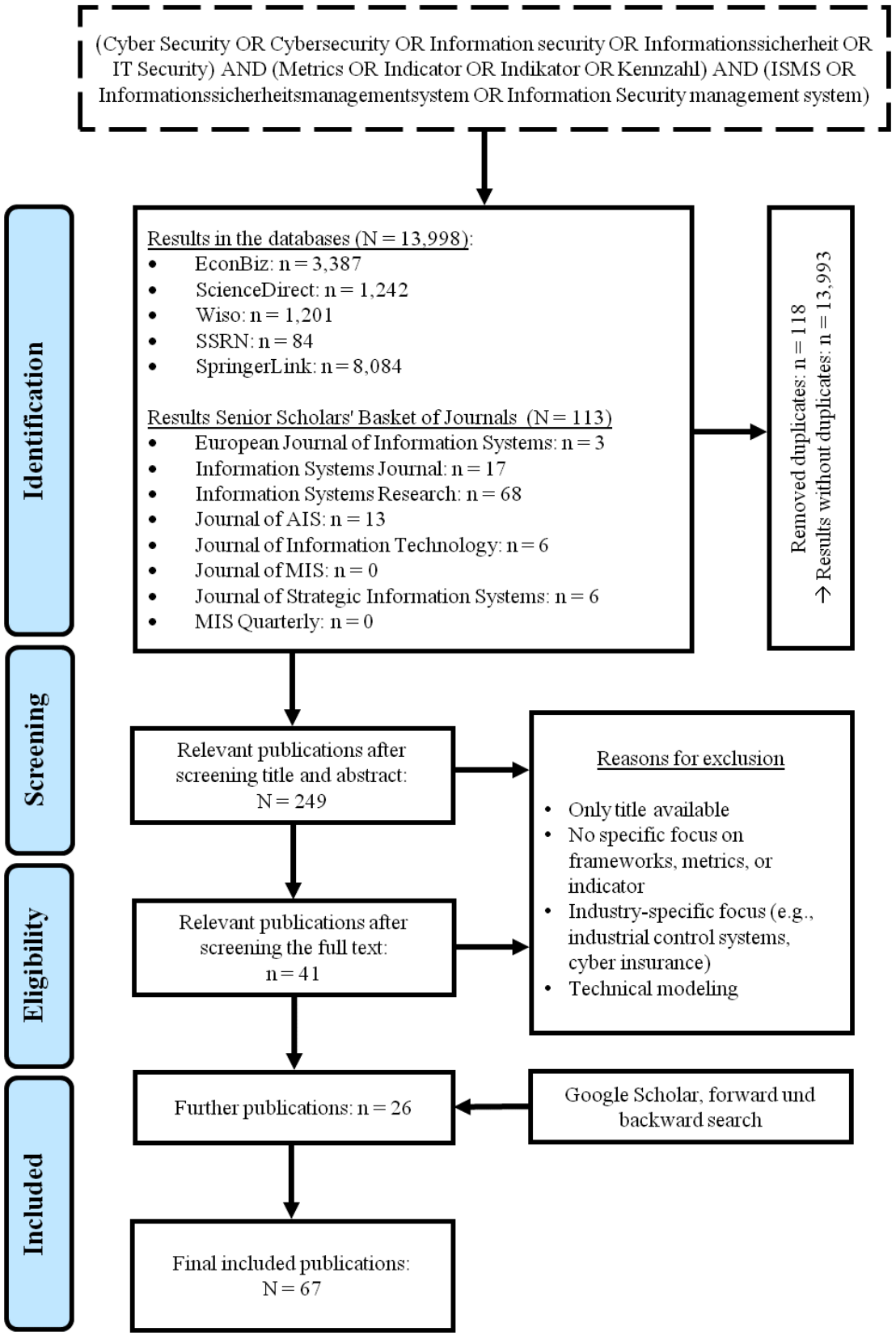


Figure 4: Flowchart illustrating the literature selection process, following Moher et al. (2009)

3.3 Descriptive Analysis

In the descriptive analysis, the formal aspects of the papers examined were evaluated, with a focus on the distribution in terms of time period and thematic focus (Seuring and Müller 2008).

Sixty-seven identified articles were distributed over the publication period from 2000 to 2020. The exact distribution within each year is shown in Figure 3. This figure shows that many publications could be identified, especially in the years 2007, 2009, 2011, and 2014.

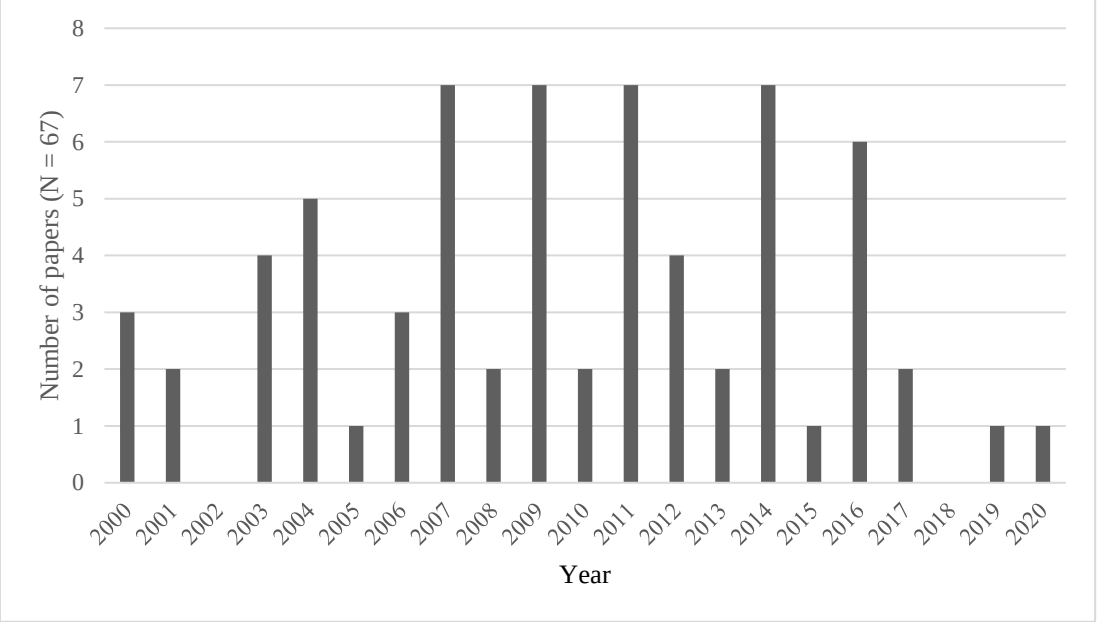


Figure 5: Distribution across the time period

In assigning the publications to various topics, we followed the aim and scope of the respective journals and books. In addition, the partial lack of discriminatory power between the journals was discussed, and a decision was made for one topic.

Regarding the focus of the respective journals and book contributions, most of the selected publications were from the security and resilience field (Figure 4). Specifically, we included, for example, the following journals in this category: *Computers & Security*, *Computers Fraud & Security*, and *Safety Science*. The second most common thematic focus is information systems with the following journals: *MIS Quarterly*, *Information Systems Management*, and *Information Systems Research*. Journals within the third topic, Management Science, include the *Information Resources Management Journal* and the *Journal of Cleaner Production*.

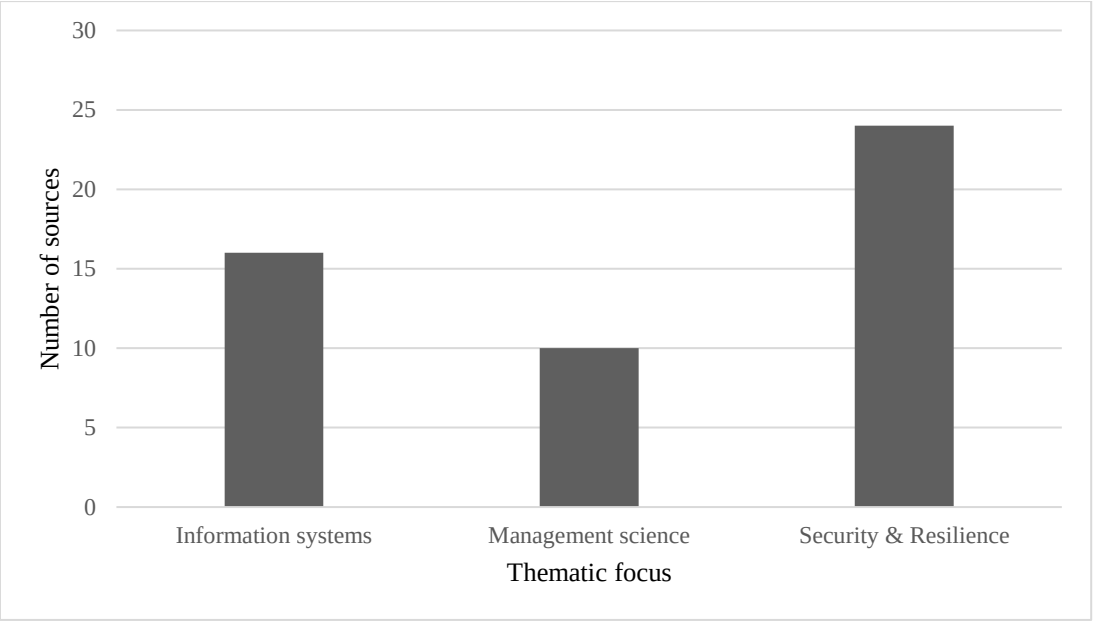


Figure 6: Distribution across the thematic focus

3.4 Selection and Definition of Categories

The coding process was based on the work of Gioia et al. (2013) and Saldaña (2013). We used an abductive approach to category formation, derived from the question of the influence of human factors on early warnings in cyber security. For better interpretation, this was done in consistent alignment with previous literature (Mantere and Ketokivi 2013). Accordingly, based on inductive coding, we conducted a qualitative analysis of the literature (Gioia et al. 2013; Saldaña 2013). Next, in an iterative process, the inductive codes and categories derived directly from the literature were compared with the analysis of the previous theory and revised until a robust conceptual framework emerged (Mantere and Ketokivi 2013; Saldaña 2013; Seuring and Gold 2012).

As suggested by Gioia et al. (2013), all selected publications were subsequently coded according to consecutive levels or cycles of analysis. The first step involved open coding, and the included informant terms were elaborated after reading each paper. This resulted in more than 50 codes occurring in the documents that related to the named influencing factors. The second step involved the search for first-order concepts that explored similarities and differences as a descriptive analysis of the data (Gioia et al. 2013). The third coding step was based on second-order codes that looked for highly abstracted concepts, resulting in 24 categories. We reviewed and compared these 24 categories to finally refine them into four main elements: framework information security, safety indicators and metrics, human factors in information security, and security threat classification. These were used to provide content to the aggregated

dimensions of the analysis—all of which represent the highest level of abstraction (Gioia et al. 2013).

The four dimensions are discriminant to each other, and together they provide a complete picture of the phenomenon under study (human factors influencing early warning in cyber security). In the following sections, we examine these four dimensions along with their dynamic interrelationships. The categories were identified through an iterative process of category formation, testing, and revision through constant comparison of categories and data (Eisenhardt 1989; Mayring 2015).

4 Analysis Framework

The conceptualization of the analysis framework was based on previously developed categories. Overall, this framework is structured around the five pillars of cyber security, which represent the factors human, organizational, infrastructure, technology, and law and regulation (Figure 5). These pillars support and strengthen cyber security in companies. The pillar "Human" is the most fundamental and, concurrently, the weakest element of cyber security owing to lack of awareness and insufficient knowledge. Addressing knowledge deficiencies requires training and time while promoting employees' acceptance (Azmi et al. 2018). Because humans are the most vulnerable pillar of cyber security, we analyzed this pillar in depth.

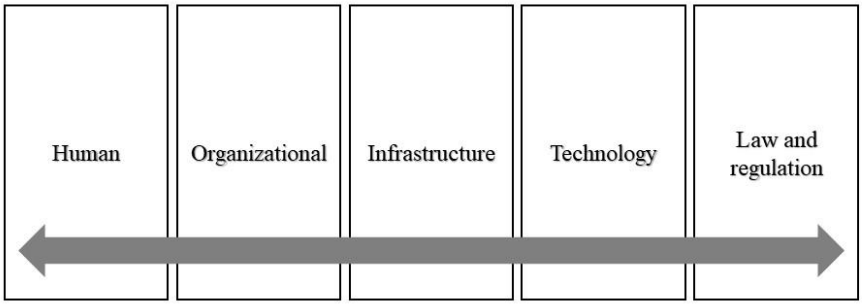


Figure 7: Five pillars of cyber security, following Azmi et al. (2018)

In this analysis framework, the organizational pillar comprises the functional structure, which includes both inward-looking strategic measures and outward-looking strategic measures to control cyberspace. The goal of this pillar is to increase the ability to respond to cyber threats. The infrastructure pillar represents the environment of cyberspace and is often depicted in cyber security frameworks as an elementary component. Within the technology pillar, the goal is to

adopt leading technologies that support the maintenance of cyber security. Last, law and regulation serves to provide the regulatory framework of existing systems in cyberspace (Azmi et al. 2018).

In addition to the aforementioned five pillars of cyber security, another component of the analysis framework is the potential for early warning in connection with the weakest element of cyber security: the human pillar. Because cyber-attacks are increasingly dynamic in their development and change, our focus is on integrating the human factor as an early warning indicator. This involves technical data security, which is complemented by human dimensions (Mattern et al. 2014). The need to develop early warning systems for cyber-attacks, including social and not purely technical origins, has also been reported (Hoffman 2013).

5 Material Evaluation

The retrieved papers were analyzed based on the previously developed categories and the resulting framework (Figure 6).

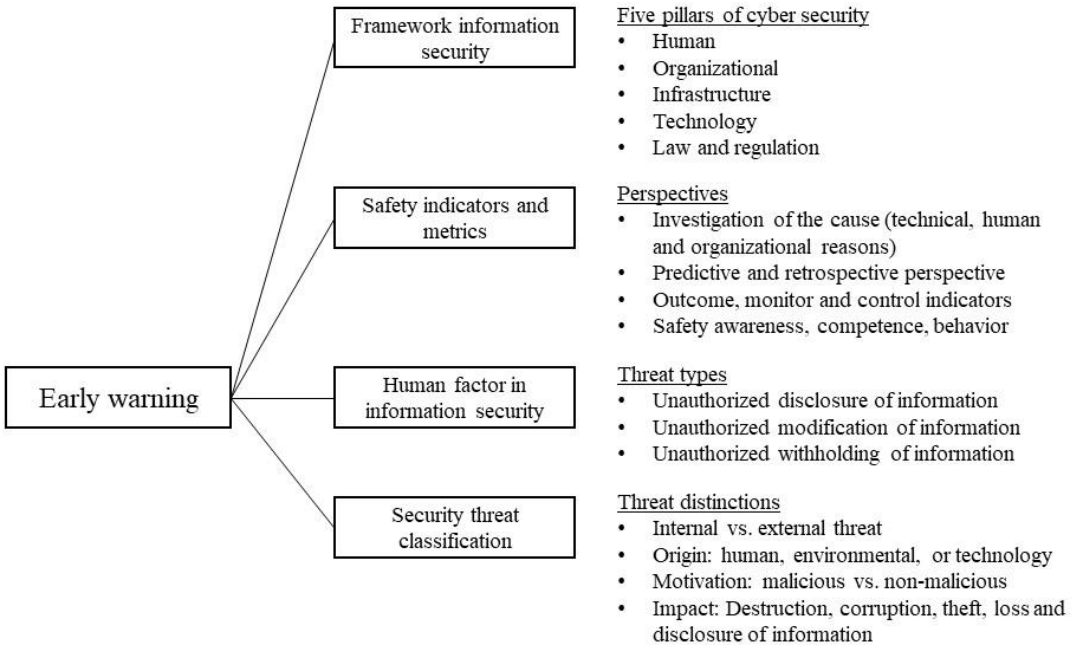


Figure 8: Framework Early Warning

The first category includes six frameworks in the context of information security. Based on these frameworks, factors that are decisive for the effective implementation of information security and associated systems should be considered in the subsequent development of potential early warning indicators for maintaining information security. Based on the knowledge gained, an analysis of general and specific security indicators and key figures was conducted. Awareness-raising measures have the potential to provide early warnings. Furthermore, the resulting security threats can be classified in different ways. This classification is the fourth component for the construction of early warning indicators to align them accordingly. The theoretically based category scheme increased the reliability of the coding and internal validity of the results. The transparency and replicability of the research method are ensured by careful documentation of the entire research process (Seuring and Gold 2012).

6 Results

6.1 Information Security Frameworks

For the analysis of information security, six frameworks were identified in the systematic literature review (from 2003 to 2012; Table 2). Table 2 presents a matrix concept that summarizes the relevant components in the literature (Webster and Watson 2002). Frameworks focusing on information security culture, information security architecture, and information security governance or industry-specific categorizations were excluded owing to the primary consideration of generally applicable frameworks (AlHogail 2015; Da Veiga and Eloff 2007; Eloff and Eloff 2005; Vithanwattana et al. 2016). The analysis of the six included frameworks identified five pillars: human, organizational, infrastructure, technology, law, and regulation.

Table 3: Overview information security frameworks

References	Human	Organizational	Infrastructure	Technology	Law and regulation
Al-Tameem A, Zairi M, Kamala M (2009) Critical factors of information security implementation.	✓	✓	✓	✓	✓
Park S, Ahmad A, Ruighaver AB (2010) Factors influencing the implementation of information systems security strategies in organizations.		✓	✓	✓	
Saleh MS, Alrabiah A, Bakry SH. (2007) Using ISO 17799:2005 information security management: A STOPE view with six sigma approach.	✓	✓	✓	✓	
Torres JM, Sarriegi JM, Santos NS (2006) Managing information systems security: Critical success factors and indicators to measure effectiveness.	✓	✓		✓	✓
Trček D (2003) An integral framework for information systems security management.	✓	✓		✓	✓
Uffen J, Pomes R, Breitner MH (2012) Toward a sustainable and efficient component-based information security framework.	✓	✓	✓	✓	

Comparing the different frameworks, we found that the five pillars differ in their importance. Only the organizational and technical factors are included in all the frameworks examined, which is why these components are expected to have a significant influence on the implementation of information security and related systems in the context of the literature. However, the sub-items that comprise the aforementioned factors vary within each framework owing to a lack of consistent definitional approaches. While Al-Tameem et al. (2009) highlighted strategy, awareness, top management support, risk management, training, financial resources, and corporate culture as sub-items within the organizational factors, Park et al. (2010) referred to these factors as the alignment, balance, and effectiveness of strategies. Saleh et al. (2007) emphasized the handling of resources and management of security incidents in the area of organization. In Torres et al. (2006), organizational factors such as the information system security strategy, dynamic evaluation of effectiveness, and integration of information security were grouped under the formal components. While Trček (2003) did not present the scope of organizational factors as well as technological factors in depth within the layered multi-plane model, organizational factors—according to Uffen et al. (2012)—include top management support for holistic identification and control of security risks. Similarly, the level of detail of technical factors differed between frameworks. Although access controls, encryption, and information technology infrastructure recovery were mentioned as sub-items in Al-Tameem et al. (2009) and Saleh et al.'s (2007) Strategy, Technology, Organization, People, and Environment (STOPE) approach also includes access controls as well as communication and operations management, as well as acquisition, development, and maintenance of information systems. In this context, Park et al. (2010) addressed a simple implementation of the strategy, whereas Torres et al. (2006) grouped the information system security architecture and business relationships under technical factors. Uffen et al. (2012) included the implementation of information system security architecture among the factors mentioned.

In addition to organizational and technical factors, the human factor was the third most frequently mentioned component and influencing factor of information security systems. This factor was addressed in five of the six selected frameworks. Although Al-Tameem et al. (2009) did not explicitly include the human factor among the three main parts within their critical factors, this factor was implicitly included in the organizational factors under awareness and training. Torres et al. (2006) equally implicitly included the human factor in their informal components as awareness of information security. Regarding matters before, during, and after termination of employment, Saleh et al. (2007) defined the human factor. In the layered multi-plane model, security mechanisms include interactions between humans and between humans and

machines (Trček 2003). Furthermore, the human factor can be used to reduce the internal misuse of information system resources, which can be achieved by increasing awareness and training and, according to Uffen et al. (2012), is a key component in the implementation of information security. In summary, awareness was the main component of human factors in three frameworks. Only Park et al. (2010) did not include human factors in their frameworks.

Furthermore, infrastructure was important in four of six frameworks. Law and regulation was found in three frameworks. Although the focus differed depending on the orientation of the frameworks, insight for further analysis was provided regarding potential early warning indicators; specifically, organizational and technological components as well as human factors are important for maintaining information security and implementing the associated management systems (Table 2).

6.2 Safety Indicators and Metrics

In addition to the frameworks listed above, an understanding of security indicators and metrics provides another basis for developing an early warning indicator in information security. Indicators comprise condensed data to inform about economic facts regarding business analysis and control. Not only is the past orientation relevant, but key indicators can also serve as early warning indicators via target-performance comparisons, which support the initiation of countermeasures regarding future orientation. Key performance indicators also include metrics; although, these primarily report on a reality that is difficult to depict. These are mostly not directly measurable facts (i.e., "soft factors"). Nevertheless, the use of the terms "key performance indicator," "indicator," and "metric" is often synonymous (Gladen 2014; Piontek 2009; Rodrigues et al. 2016; Weber and Schäffer 2016). Some security indicators regarding technological, formal, and informal components can already be found in the information security framework by Torres et al. (2006). Examples of information technology security indicators, according to Kütz (2011), circumscribe response times to error messages, resolution times in the processing of incidents, and open problems at the time of the survey. Dal Moro (2020) also identified the number of viruses or intrusions being blocked as a potential information technology security indicator.

In most cases, retrospective observations in other safety areas have shown that prior analysis and management of signals and early warnings could have prevented or at least reduced undesirable events (Hopkins 2000). Early warning indicators in the form of safety or risk indicators are updated regularly and cover only selected determinants of overall safety or risk to remain manageable in their application (Øien et al. 2011a; Paltrinieri et al. 2012; Patriarca et

al. 2019). These indicators can be structured based on two perspectives (Øien et al. 2011a). The first refers to the exploration of the root cause, which leads from technical to human and organizational reasons (Leveson 2004). These three causes support the previously obtained finding that technical, human, and organizational aspects have a significant influence on safety-related issues. The second is a predictive and retrospective view. In this context, there is a difference between predicting an incident, including all possible causes, and determining the cause after the incident has occurred (Øien et al. 2011a).

Based on the perspective representation of safety indicators according to Øien (2001), there are parallels to the components of the frameworks presented earlier. In both safety indicators and frameworks, organizational, human, and technical factors are elementary components. For the prediction of risks, the development of technical, human, and organizational causes can be assumed. Risk prediction is a fundamental element for the development and effective implementation of early warning indicators. While within the frameworks, the components of the different factors vary, it can also be seen in the context of safety indicators that the organizational factors are not classified in a uniform way (Takano et al. 2004; Wilpert 2000).

Safety indicators can further play a central role in the area of performance in providing information that increases organizational safety potential by motivating people to improve safety. In this framework, safety indicators can be divided into three types, which are applied in organizational safety management: outcome, monitor, and drive indicators. Outcome indicators are lagging indicators because they result from other situational factors. An example of an outcome indicator is the number of safety events. Although safety itself is not an outcome and therefore cannot be measured by an outcome indicator, in practice, these indicators are used to define safety priorities or to draw conclusions about the level of safety. In contrast, monitor and drive indicators can be categorized as early warning indicators of their predictive capacity. The drive indicators are subject to transformation into control measures, which serve to optimize the system. The coordination of socio-technical activities for the motivation of safety-relevant measures constitutes the main function of the drive indicators. Monitor indicators provide an overview of the company's development, which includes procedures, competences, and the motivation of the personnel. Furthermore, the organizational safety potential is mapped (Reiman and Pietikäinen 2012). Safety culture or safety climate can be used as a safety indicator (Grabowski et al. 2007; Mearns 2009). Lagging safety indicators are most commonly used in practice, but early warning indicators are becoming increasingly important for anticipation. However, changes cannot be fully monitored; therefore, their selection is crucial (Reiman and Pietikäinen 2012). The following quote from Hollnagel and Woods (2006) summarizes the need

to consider different time perspectives: “In order to be in control, it is necessary to know what has happened (the past), what is happening (the present) and what may happen (the future), as well as knowing what to do and having the required resources to do it.” In addition, security has evolved into a dynamic and system-oriented concept, which includes more than just the absence of risk (Reiman and Pietikäinen 2012). The recognition that security is subject to a dynamic business environment is equally confirmed by information security frameworks (Abbas et al. 2011; Andersen et al. 2004; Melara et al. 2003; Park et al. 2010; Safa et al. 2016; Torres et al. 2006). To the extent that security encompasses more than the absence of risk, indicators should also focus on the positive side of security (Hollnagel 2008). In summary, the role of safety indicators in performance is to provide information about safety that motivates people to improve and further develop the safety situation (Reiman and Pietikäinen 2012). Consequently, the human factor is an essential part of the construct and will be analyzed more intensively.

The motivation of employees regarding the security situation in a company can be examined as a “non-technical” aspect using employee-oriented key performance indicators and ultimately controlled as a result. The significance of human factors is becoming increasingly important alongside organizational regulations and technical protective measures and should be considered in its role in information security (Dlamini et al. 2009; Lacey 2009; Metalidou et al. 2014a; Zerr and Benner 2017). Employee-oriented security management includes the consideration of human behaviors and motives, which have an impact on the development and implementation of measures to optimize information security (Luo et al. 2011; Zerr and Benner 2017). However, management’s knowledge of employee behaviors and motives is insufficient in the context of information security (Albrechtsen and Hovden 2009). Information technology users can have both positive and negative roles in creating or averting security risks (Soomro et al. 2016). A negative role in this context is that employees are involved in theft of information with malicious intent or to violate access policies (Vance et al. 2013; Yao et al. 2014). However, compliance with security policy and awareness of risks have a positive influence on information security (Siponen 2001; Soomro et al. 2016). The goal of employee-oriented security management is to develop measures that increase the security level of a company by reducing the risks regarding information protection, from which three categories can be derived: 1. sensitize, 2. inform and qualify, and 3. motivate and regulate. In addition to the human factors already mentioned within an employee-oriented safety management, organizational and technical framework conditions belong to the fields of action, which are in an indispensable dependency rela-

tionship (Zerr and Benner 2017). These components have already been identified in the frameworks and generally valid safety metrics (Al-Tameem et al. 2009; Leveson 2004; Park et al. 2010; Trček 2003). In addition, it is important to make the goals of employee-oriented safety management measurable. For this purpose, relevant target variables are identified and determined at the theoretical level, as well as defined and specified. In the last step at the theoretical level, the dimensions of the target variables are determined. Subsequently, observable indicators are determined at the empirical level, and the measurement procedure is defined. By influencing personal characteristics, three key figures can be determined: safety awareness, safety competence, and safety behavior (Zerr and Benner 2017). Within the framework of safety awareness, safety risks must be minimized by employees recognizing and assuming their own roles and following the associated rules. Personal responsibility describes the competence to identify one's function in avoiding risks and to act independently without primarily delegating such activities. A survey and observation of employees can be used to assess safety awareness (Kritzinger and Smith 2008; Zerr 2007). The different types of security awareness are listed in Table 3.

Table 4: Types of security awareness, following Zerr (2007)

		Unobservable	
	Attitude / Behavior	Positive	Negative
Observable	Safety compliant	Safety awareness by conviction	Apparent security awareness
	Not safety compliant	"Prevented" security awareness	No security awareness

From Table 3, security-compliant or non-security-compliant behavior is observable. An example of this is the quality of a password. The attitudes of employees, on the other hand, are not observable but can be collected through a survey. A positive attitude can be derived using a questionnaire targeting security awareness. Observation and questioning methods should therefore be combined when surveying safety awareness. The results can be used to influence security awareness by developing a suitable awareness campaign. The survey expresses the degree of agreement or disagreement, which is queried via rating scales on various topics (Zerr 2007).

Safety competence describes the ability of employees to recognize safety risks, classify them correctly, and react appropriately. This requires knowledge of the internal rules of conduct, standards, and norms. Safety competence can be represented by three different perspectives: self-assessment, external assessment, and actual competence. A comparison of these perspectives provides indications of a possible need for action. While self-assessment, such as the attitude toward security awareness, can be surveyed with the help of a questionnaire, an expert survey must be used for external assessment. Actual competence can be determined through observations in critical situations (Zerr and Benner 2017).

The last key performance indicator of the influence of person-related characteristics is safety behavior, whereby the conformity of the behavior to the rules must be observed. To determine this, non-participant observation is suitable, which minimizes the risk of result distortion. However, covert observations are usually not feasible in practice, as they are associated with high costs and data protection hurdles. Therefore, surveys were conducted to measure compliant behavior. The methods that are suitable for companies depend on various criteria, such as the number of employees and the available budget. In principle, regular data collection is required to analyze the changes over time. Conclusions can be drawn about said changes, which can serve as an early warning indicator. The integration of available data from observations and surveys can be done via a "security dashboard" (Zerr and Benner 2017), which enables managers to realize the development of their area as a control center for key figures and supports them in the resulting decision-making (De Oliveira Alves et al. 2006).

6.3 Human Factor in Information Security

The management of a company is responsible for the control of human resources, which includes planning, motivation, and control of activities regarding information security (Soomro et al. 2016). An essential component of information security in the context of employees and information security policies is influenced by awareness and targeted training (Eminağaoğlu et al. 2009; Puhakainen and Siponen 2010). These policies have a significant impact on successful business operations and information systems security; thus, the relevance of the human factor should not be underestimated (Metalidou et al. 2014b; Soomro et al. 2016). The most critical factor in information security involves a complex interaction between humans and technical factors (Trček et al. 2007). Many information security vulnerabilities and data breaches are owing to ignorant employees (Yildirim et al. 2011). Reasons that employees are a major cause of vulnerabilities can include lack of awareness, simple ignorance, low compliance or violation of information security policies, and bad motives (Vance et al. 2013).

In this context, three threats to information systems can be identified concerning information security: unauthorized disclosure of information, unauthorized modification of information, and unauthorized withholding of information (Harris 2003; Saydjari 2004; Tryfonas et al. 2000). While combating external threats has been a central concern in the past, insider actions in particular constitute a significant threat. In this context, insider attacks can be both unintentional and intentional (Denning 2003).

Insiders are trusted individuals who have privileged access to business-critical systems and data and are advantageously positioned to attack the organization (Nurse et al. 2014; Probst et al. 2007). One possible scenario describes a recently fired employee whose system privileges have not yet been revoked. In another case, the software developer who designed the company systems and thus has a knowledge advantage also has privileged access. In the third scenario, an unknown person uses the already logged-in computer without the authenticated user being aware of it. The janitor is also considered an insider because of their privileged physical access. In addition, the following distinctions should be considered: malicious and non-malicious threats, obvious and clandestine actions, and actions that cause damage by people with stolen passwords or as a result of naive use by legitimate users. The motivation behind insider attacks, their consequences, and how to deal with them are also important issues. Motivation can range from fun, technical challenges and criminal intentions to espionage. In this context, the intention of an insider attack can be retaliation and personal financial gain. To minimize such attacks, the focus is on the prevention, detection, and response. Best practices include recording, monitoring, and auditing employees' online activities (Cappelli et al. 2012). Many attacks can also be detected through non-technical means, such as employees noticing suspicious behavior. Such suspicious behavior may be equally subject to detection by law enforcement, business partners, or customers (Eldardiry et al. 2013; Moore et al. 2011). While there is growing interest in automated insider threat detection, there are approaches to anomaly analysis that examine employees' behavior that deviates from the norm. The difficulty, however, is determining what constitutes normal behavior and what deviations lead to classification as a potential insider threat. Automated detection of insider threats requires careful management by system analysts (Legg 2017; Patcha and Park 2007).

6.4 Security Threat Classification

Because of different types of threats within information systems, equally different types of damage are caused, ranging from small losses to destruction of the information system. Because the impact of such threats varies, a classification of security threats is useful. In the context of

this classification, the following principles should be adhered to: each threat is assigned to exactly one category. There is no overlap in a category, and they are subject to a logical structure, thus achieving broad acceptance. Furthermore, threat characteristics should be fully included in category classification. The classification criteria must be formulated unambiguously and precisely so that repeated applications lead to identical classifications (Jouini et al. 2014; Jouini and Rabai 2016).

Jouini et al. (2014) used a multidimensional model to classify threats, with the goal of considering all principles. This model extends the cyber security incident presented in this study by insider attacks. The following criteria are applied in the multidimensional model of Jouini et al. (2014): the first criterion for classifying security threats is the origin of that threat. A distinction is made between internal and external threats. This origin is specified by different agents, which are differentiated by Jouini et al. (2014) according to human, environment, and technology. Human threats include those caused by humans and result in damage or risk within the systems. Examples of human threats include insiders and hackers. Environmental threats, such as natural disasters (floods, fires, storms), in contrast, are caused by non-human influences and therefore belong to a different category. Technological threats are divided into physical and technical processes. Physical processes include access to restricted areas. Technical processes include hardware and software technologies. Threats are triggered either within a company or from an external starting point. In addition, the motivation behind security threats is another component of multidimensional models. Threats can be both malicious and non-malicious, as well as intentional or accidental in origin. Examples of intentional threats include spying and identity theft. Accidental threats include data corruption owing to programming or operator errors. In the context of classification by agents, environmental threats are natural threats that occur without malicious intent. Because technological threats, according to Jouini et al. (2014), are caused by physical or technical processes over which humans have no direct influence, they are not subject to malicious acts. Based on this criterion, it is possible to reconstruct the attack behavior and understand the intention behind it. The factor is thus predictable and helps to conclude a security incident with high accuracy, minimizing the risks and speeding up future reconnaissance (Rasmi and Jantan 2011). Threat impact finds its application in classification. The following impacts were identified: destruction, corruption, theft, loss and disclosure of information, denial of use, elevation of privilege, and illegal use (Swiderski and Snyder 2004).

In summary, the security threats to a system are classified according to five basic criteria, which lead to several elementary threat classes. Overall, the multidimensional model proposed by Jouini et al. (2014) offers a holistic approach to the classification of security threats

compared to other models, which is why this model was selected for this study as part of a systematic literature review (see Cebula et al. 2014 for the classification of cyber risks).

6.5 Summary of the Findings

Owing to the lack of specific publications on early warning indicators in information security, a conceptual framework was developed and presented using a systematic literature review. The conceptual framework includes information security frameworks, security indicators, and metrics; the relevance of the human factor in information security; and the classification of security threats resulting from cyber-attacks.

Within the frameworks for information security, three dominant components could be ascertained that support the successful implementation and maintenance of information security and associated systems, relating to the areas of organization, technology, and human factors. However, owing to a lack of definitional approaches in the various business units and different orientations of the frameworks, there was a variation in the specific scope of the components listed, which made a generalized analysis difficult.

The analysis of generally applicable security indicators provided a basis for the development of powerful early warning indicators in the area of information security. Early warning indicators should only cover selected determinants of overall security or risk; otherwise, the manageability of such an indicator is compromised (Øien et al. 2011a). In addition, for safety indicators, just as for the previously listed frameworks, organizational, technical, and human factors are elemental components that support root cause exploration. Based on the investigation of the cause, a risk prediction can be developed, which is essential for an early warning (Leveson 2004; Øien et al. 2011a). Furthermore, safety indicators in the area of performance can be differentiated into result, monitor, and drive indicators regarding the provision of information to improve safety. While outcome indicators focus on lagging events, monitor and drive indicators have a forward-looking characteristic, which allows them to be classified as early warning indicators. Although drive indicators can be transformed into control measures, monitor indicators provide an overview of the security-relevant aspects of a company, enabling the derivation of the maturity level of companies in organizational security (Reiman and Pietikäinen 2012). Based on the characteristics of the monitor indicators, three key figures of employee-oriented security management generate information about the degree of security awareness, security competence, and security behavior (Zerr and Benner 2017). Many vulnerabilities in information security can be traced back to ignorant employees and thus have a key impact on security (Yildirim et al. 2011). However, the extent that such metrics are considered useful

in practice is questionable. The classification of security threats according to Jouini et al. (2014) also provided the opportunity to differentiate threats in their origin and motivation, with the human factor occupying a significant position.

7 Discussion and Limitations

The most critical factor influencing information security is the complex interaction of human and technical factors, with the most significant vulnerabilities attributable to employees (Eminağaoğlu et al. 2009; Trček et al. 2007; Weber et al. 2019; Yildirim et al. 2011). Humans are considered the weakest link in the defensive chain. Studies show that attackers targeting unauthorized access to internal corporate information actually prefer humans to technology as targets (De Maggio et al. 2019). Potential reasons for human vulnerability can be both lack of awareness and the malicious motive to harm the company (Vance et al. 2013). Thus, on the one hand, threats come from external attacks that exploit employee ignorance and, on the other hand, from internal perpetrators who have privileged access to mission-critical systems and malicious intent (Denning 2003; Nurse et al. 2014; Vance et al. 2013; Yildirim et al. 2011). To reduce threats triggered by unintentional employee actions, awareness measures are essential elements (Diesch et al. 2020; Soomro et al. 2016). However, awareness measures are not effective against the threat of internal perpetrators who intentionally want to harm the company, triggered by a lack of appreciation and dissatisfaction. This type of threat can be limited by a distinct corporate culture (Caldwell 2016; Chang and Lin 2007; Weber et al. 2019).

As a result of a lack of technology regarding the automatic detection and response of cyber-attacks, people can support the information security concept in that anomalies in emails are passed on, provided that targeted sensitization measures have taken place (Weber et al. 2019). An experiment by Heartfield and Loukas (2018) showed that 90% of simulated attacks, such as social engineering simulations and externally obtained USB sticks, were detected by employees. In contrast, technical sensors did not alert 81% of the time (Heartfield and Loukas 2018). However, exploiting this potential is only possible if employees are sufficiently sensitized to such threats. Employees should behave in an information-security-compliant manner in this context by either consciously or unconsciously compromising the security of information and actively reporting detected threats. Information security-compliant behavior includes, for example, the secure handling of passwords to the effect that they are not passed on to third parties, and that they comply with password guidelines and the screen lock is activated when leaving the workplace, which can prevent unauthorized access. Furthermore, it is necessary to

check the emails for credibility, for which the first step is to educate employees about the recognition features of phishing emails. In addition, the use of USB sticks is only permitted if they originate from a source known to the employee (Weber et al. 2019). In this context, awareness training should not be implemented only when damage has already occurred because of a lack of awareness but should protect against it preventively (Cole et al. 2019).

It is also important to implement an awareness campaign adapted to the company (Zerr 2007). These campaigns can be designed in a variety of ways but should include the provision of information on the one hand and training in the application of the information provided on the other (Siponen 2000). Internet-based training is widely used in this context to educate employees about information security issues (Shaw et al. 2009; Willems and Meinel 2008). Moreover, gamification in awareness campaigns is a procedure in which employees are motivated to deal with information security threats through playful aspects (Gjertsen et al. 2017). In addition, incentives are provided through rewards (Cole et al. 2019). A complementary component of the campaigns is the simulation of phishing emails, where the previously imparted knowledge regarding the salience of such cyber-attacks can be tested. Possible phishing simulation techniques are based on the content classified as phishing or observing behavior during fake phishing attacks (Hale et al. 2015). To measure human factors in cyber security, Bowen et al. (2011) focused on measuring susceptibility to phishing attacks at the enterprise level. This survey also shows that employee training can effectively reduce the vulnerability of such attacks (Bowen et al. 2011). Alternatively, employee skills could be measured using the cyber security skills index. Skills that are asked for, for example, prevent the leakage of confidential digital information to unauthorized individuals or malware via non-secure websites (Carlton et al. 2019).

In this context, when investigating the potential of employee awareness for early warning, there is a need to make the success of this factor measurable and comparable. In particular, conclusions can be drawn about changes over time and the realistic assessment of the information security situation before and after security measures, which can serve as an early warning indicator (Torres et al. 2006; Zerr and Benner 2017). In terms of measuring the success of awareness training, this shows the extent to which employees recognize potential threats. Poor success measurement results provide an early warning that employees are not sufficiently sensitized and that they pose an increased threat (Eminağaoğlu et al. 2009; Weber et al. 2019). Torres et al. (2006) further presented potential early warning indicators following the human factor in the enterprise. An associated indicator reflects the percentage of qualified personnel in the area of information security. If, after defining a critical threshold, the number of qualified personnel falls below the threshold, this could be used as an indicator for early warning, since

sufficient qualified personnel are needed to maintain information security. Responsibilities should also be subject to a balanced distribution to identify an overwhelming workload at an early stage, which can also be mapped using an indicator. The average number of information security training hours received and the level of awareness, differentiated by management level, information technology staff, and end users, can be used as an early warning indicator via an internal survey (Torres et al. 2006). Zerr (2007) took a similar approach, focusing on measuring security awareness, security literacy, and security behavior. These security indicators are also determined through surveys or observations and can support early warning of resulting vulnerabilities based on lack of awareness (Kritzinger and Smith 2008; Zerr 2007; Zerr and Benner 2017).

In addition to response capacity and support, resilience-based early warning indicators also use risk awareness to assess the organization's resilience via self-assessment measures (Bernsmed and Tøndel 2013; Øien et al. 2010, 2011b). When employees' awareness increases, they behave more securely and pose less of a threat to information security (Jaeger 2018). Employees should not be viewed exclusively as a vulnerability, but equally as a potential security sensor to support information security (Heartfield and Loukas 2018; Weber et al. 2019). For early warning, system parameters must be described to trigger warnings when a certain tolerance limit is exceeded. In relation to the employee, these would be, for example, the proportion of former employees who are still granted access rights to information systems three days after leaving the company or the number of failed login attempts in relation to all login attempts. If the tolerance limit is exceeded, staggered warning levels can be issued according to the severity of the violation (Disterer 2015). In addition, the consideration of so-called "weak signals" (Ansoff 1975) offers the potential to indicate latent threats that are not yet apparent. It is assumed that threats are usually announced in advance by weak signals, which can provide the opportunity for early reactions (Ansoff 1975; Reinhardt 1984; Zelewski 1987). The use of external sources, such as the results of structured surveys of experts, threat catalogs, and evaluations of current specialist literature, is suitable for detecting such weak signals (Krystek 2006). It also seems useful to establish inter-company cooperation for the exchange of knowledge to take up divergent experiences as impulses for further internal analyses (Disterer 2015).

This systematic literature review has several limitations in its methodological approach. One limitation is the selected time period (until the beginning of 2020). Over time, science tends to self-correct as fraudulent or invalid research can be retracted, and false hypotheses or theories can be disproved by new data. However, this self-correcting process can take years or even decades, and the public often cannot wait for science to bring forth the correct solution to a

perceived problem, especially during a public health crisis such as the COVID-19 pandemic (Shamoo 2020). The COVID-19 pandemic is changing the context for research and thus poses many challenges for information security research (e.g., the disruption of carefully thought-out data collection efforts and significant methodological challenges due to a lack of continuity; Fink 2020; Prommegger et al. 2021). Therefore, we decided to exclude literature from the beginning of the COVID-19 pandemic. Moreover, as a result of the developed search string, which provides the basis for the search, there is the possibility that relevant publications regarding the development of a conceptual framework for early warning indicators in the area of information security have not been involved. Furthermore, for a complete consideration of the literature relevant to early warning indicators in the field of information security, an extension of the literature search to other databases may be useful. Databases that could be used for this purpose include IEEE Xplore and ACM Digital Library, which primarily refer to the field of computer science. Additionally, owing to the formulation of inclusion and exclusion criteria (Kuckertz and Block 2021), relevant publications may not have been considered. It is quite conceivable that such publications were published before the turn of the century or in languages other than German and English. In addition, the results of the descriptive analysis indicate that relevant papers may not have been included in the systematic literature review. The assignment of the journals and conferences to the respective topics was also made more difficult because there was hardly any separation between the topics. In particular, there are overlaps between information security and security. In conclusion, there are challenges in conducting a systematic literature review. Despite careful checking of the results against the previously established search string and defined inclusion and exclusion criteria, the evaluation of the resulting publications is subject to a subjective view, with the risk that publications relevant to the context of the RQ may have been excluded. Although the literature research was comprehensive, the completeness of the selected material cannot be guaranteed, which is why the generalizability of the findings may be limited. To generate the greatest possible objectivity, it is preferable that the formulation of the search criteria, as well as the review of the generated hits, be performed independently by more than two persons and that the results be subsequently combined.

8 Conclusion

The increasing relevance of cyber risks has led companies to focus on the prevention of cyber-attacks. In addition to prevention measures, early warning in the area of cyber security has the potential to reduce or, at best, prevent potential damage.

We used a content-analysis based literature review to investigate the influence of human factors on early warnings in cyber security. The results show that the human factor as a whole has a major impact on cyber security in an organization. While awareness training can serve to increase sensitivity to anomalies and related cyber-attacks, evaluations of such training can be used as an early warning indicator. In this context, surveys and comparisons of changes over time should be used in particular. Overall, the findings from this content-analysis based literature review should be validated in future research by interviewing experts in the field. Through the integration of the qualitative interview study, practice-oriented experiences can be included and combined into a holistic approach. In addition, the technical aspects that we excluded in this research design should be considered in future research approaches in this area. The consideration of technical frameworks seems to be useful in this context.

References Papers contained in the Literature Review[2]

Abbas H, Magnusson C, Yngstrom L, Hemani A (2011) Addressing dynamic issues in information security management. Inf Manag Comput Secur 19(1):5–24. https://doi.org/10.1108/09685221111115836

Albrechtsen E, Hovden J (2009) The information security digital divide between information security managers and users. Comput Secur 28(6):476–490. https://doi.org/10.1016/j.cose.2009.01.003

AlHogail A (2015) Design and validation of information security culture framework. Comput in Hum Behav 49:567–575. https://doi.org/10.1016/j.chb.2015.03.054

Andersen DF, Cappelli DM, Gonzalez JJ, Mojtahedzadeh M, Moore AP, Rich E, Sarriegui JM, Shimeall TJ, Stanton JM, Weaver EA, Zagonel A (2004) Preliminary System Dynamics Maps of the Insider Cyber-Threat Problem. In: Proceedings of the 22nd International Conference of the System Dynamics Society, Oxford, United Kingdom, July 25–29, 2004

Al-Tameem A, Zairi M, Kamala M (2009) Critical factors of information security implementation. In: Proceedings of the 2009 First International Conference on Networked Digital Technologies (NDT), Ostrava, Czech Republic, July 28–31, 2009

Cappelli DM, Moore AP, Trzeciak RF (2012) The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley, Upper Saddle River, NJ, Boston, MA, Indianapolis, IN, San Francisco, CA, New York, NY, Toronto, Montreal, London, Munich, Paris, Madrid, Capetown, Sydney, Tokyo, Singapore, Mexico City

Cebula JL, Popeck M, Young LR (2014) A Taxonomy of Operational Cyber Security Risks Version 2 (Technical Note CMU/SEI-2014-TN-006). Software Engineering Institute. Carnegie Mellon University, Pittsburgh, PA. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf. Accessed 18 December 2022

[2] The references for this paper are given in two parts: this part of the references section present the papers contained in the literature review (results section). The papers included in both the literature review and the other sections of this paper are listed in both parts of the references section.

Dal Moro E (2020) Towards an Economic Cyber Loss Index for Parametric Cover Based on IT Security Indicator: A Preliminary Analysis. Risks 8(2):45. https://doi.org/10.3390/risks8020045

Da Veiga A, Eloff JHP (2007) An Information Security Governance Framework. Inf Syst Manag 24(4):361–372. https://doi.org/10.1080/10580530701586136

De Oliveira Alves GA, Da Costa Carmo LFR, De Almeida ACRD (2006) Enterprise Security Governance; A practical guide to implement and control Information Security Governance (ISG). In: Proceedings of the 1st IEEE/IFIP International Workshop on Business-Driven IT Management (BDIM), Vancouver, BC, Canada, April 3–7, 2006

Denning DE (2003) Information technology and security. Georgetown University Press, Washington, DC

Dlamini MT, Eloff JHP, Eloff MM (2009) Information Security: The moving target. Comput Secur 28(3–4):189–198. https://doi.org/10.1016/j.cose.2008.11.007

Eldardiry H, Bart E, Liu J, Hanley J, Price B, Brdiczka O (2013) Multi-Domain Information Fusion for Insider Threat Detection. In: Proceedings of the 2013 IEEE Security and Privacy Workshops, San Francisco, CA, USA, May 23–24, 2013

Eloff JHP, Eloff MM (2005) Information security architecture. Comput Fraud Secur 2005(11):10–16. https://doi.org/10.1016/S1361-3723(05)70275-X

Eminağaoğlu M, Uçar E, Eren Ş (2009) The positive outcomes of information security awareness training in companies – A case study. Inf Secur Technic Rep 14(4):223–229. https://doi.org/10.1016/j.istr.2010.05.002

Gladen W (2014) Performance Measurement: Controlling mit Kennzahlen. 6th edn. Springer Gabler, Wiesbaden

Grabowski M, Ayyalasomayajula P, Merrick J, Harrald JR, Roberts K (2007) Leading indicators of safety in virtual organizations. Saf Sci 45(10):1023–1024. https://doi.org/10.1016/j.ssci.2006.09.007

Harris S (2003) CISSP All-in-One Exam Guide, 2nd edn. McGraw-Hill, New York, NY, Chicago, IL, San Francisco, CA, Lisbon, London, Madrid, Mexico City, Milan, New Delhi, San Juan, Seoul, Singapore, Sydney, Toronto

Hollnagel E (2008) Safety Management – Looking Back or Looking Forward. In: Hollnagel E, Nemeth CP, Dekker S (eds) Remaining Sensitive to the Possibility of Failure. CRC Press, London, pp 63–77

Hollnagel E, Woods DD (2006) Epilogue: Resilience Engineering Precepts. In: Hollnagel E, Woods DD, Leveson N (eds) Resilience Engineering: Concepts and Precepts. CRC Press, London, pp 347–358

Hopkins A (2000) An AcciMap of the Esso Australia Gas Plant Explosion. In: Proceedings of the 18th European Safety Reliability & Data Association (ESReDA) Seminar, Karlstad, Sweden , June 15–16, 2000

Jouini M, Rabai LBA, Aissa AB (2014) Classification of security threats in information systems. Procedia Comput Sci 32:489–494. https://doi.org/10.1016/j.procs.2014.05.452

Jouini M, Rabai LBA (2016) A Scalable Threats Classification Model in Information Systems. In: Proceedings of the 9th International Conference on Security of Information and Networks (SIN), Newark, NJ, USA, July 20–22, 2016

Kritzinger E, Smith E. (2008) Information security management: An information security retrieval and awareness model for industry. Comput Secur 27(5–6):224–231. https://doi.org/10.1016/j.cose.2008.05.006

Kütz M (2011) Kennzahlen in der IT – Werkzeuge für Controlling und Management, 4th edn. dpunkt.verlag, Heidelberg

Lacey D (2009) Managing the Human Factor in Information Security: How to win over staff and influence business managers. John Wiley & Sons, Hoboken, NJ

Legg PA (2017) Human-Machine Decision Support Systems for Insider Threat Detection. In: Palomares I, Carrascosa H, Kalutarage K, Huang Y (eds) Data Analytics and Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Applications. Springer, Cham, pp 33–53

Leveson N (2004) A new accident model for engineering safer systems. Saf Sci 42(4):237–270. https://doi.org/10.1016/S0925-7535(03)00047-X

Luo X, Brody R, Seazzu A, Burd S (2011) Social Engineering: The Neglected Human Factor for Information Security Management. Inf Resour Manag J 24(3):1–8. http://doi.org/10.4018/irmj.2011070101

Mearns K (2009) From reactive to proactive – Can LPIs deliver?. Saf Sci 47(4):491–492. https://doi.org/10.1016/j.ssci.2008.07.028

Melara C, Sarriegui JM, Gonzalez JJ, Sawicka A, Cooke DL (2003) A System Dynamics Model of an Insider Attack on an Information System. In: Proceedings of the 21st International International Conference of the System Dynamics Society, New York, NY, USA, July 20–24, 2003

Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Skourlas C, Giannakopoulos G (2014a) The Human Factor of Information Security: Unintentional Damage Perspective. Procedia Soc Behav Sci 147:424–428. https://doi.org/10.1016/j.sbspro.2014.07.133

Metalidou E, Marinagi C, Trivellas P, Eberhagen N, Giannakopoulos G, Skourlas C (2014b) Human factor and information security in higher education. J Syst Inf Technol 16(3):210–221. https://doi.org/10.1108/JSIT-01-2014-0007

Moore AP, Cappelli DM, Caron TC, Shaw E, Spooner D, Trzeciak RF (2011) A Preliminary Model of Insider Theft of Intellectual Property (Technical Note CMU/SEI-2011-TN-013). Software Engineering Institute. Carnegie Mellon University, Pittsburgh, PA. https://resources.sei.cmu.edu/asset_files/TechnicalNote/2011_004_001_15362.pdf. Accessed 18 December 2022

Nurse JRC, Legg PA, Buckley O, Agrafiotis I, Wright G, Whitty M, Upton D, Goldsmith M, Creese S (2014) A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. In: Tryfonas T, Askoxylakis I (eds) Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22–27, 2014, Proceedings. Springer, Cham, pp 270–281

Øien K (2001) A framework for the Establishment of Risk Indicators. Reliab Eng Syst Saf 74(2):147–167. https://doi.org/10.1016/S0951-8320(01)00068-0

Øien K, Utne IB, Herrera IA (2011a) Building Safety indicators: Part 1 – Theoretical foundation. Saf Sci 49(2):148–161. https://doi.org/10.1016/j.ssci.2010.05.012

Paltrinieri N, Øien K, Cozzani V (2012) Assessment and comparison of two early warning indicator methods in the perspective of prevention of atypical accident scenarios. Reliab Eng Syst Saf 108:21–31. https://doi.org/10.1016/j.ress.2012.06.017

Park S, Ahmad A, Ruighaver AB (2010) Factors Influencing the Implementation of Information Systems Security Strategies in Organizations. In: Proceedings of the 2010 International Conference on Information Science and Applications (ICISA), Seoul, South Korea, April 21–23, 2010

Patcha A, Park J-M (2007) An overview of anomaly detection techniques: Existing solutions and latest technological trends. Comput Netw 51(12):3448–3470. https://doi.org/10.1016/j.comnet.2007.02.001

Patriarca R, Falegnami A, De Nicola A, Villani ML, Paltrinieri N (2019) Serious games for industrial safety: An approach for developing resilience early warning indicators. Saf Sci 118:316–331. https://doi.org/10.1016/j.ssci.2019.05.031

Piontek J (2009) Bausteine des Logistikmanagements: Supply Chain Management. E-Logistics. Logistikcontrolling, 3rd edn. NWB Verlag, Herne

Probst CW, Hansen RR, Nielson F (2007) Where Can an Insider Attack?. In: Dimitrakos T, Martinelli F, Ryan PYA, Schneider S (eds) Formal Aspects in Security and Trust: Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26–27, 2006, Revised Selected Papers. Springer, Berlin, Heidelberg, pp 127–142

Puhakainen P, Siponen MT (2010) Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. Manag Inf Syst Q 34(4):757–778. https://doi.org/10.2307/25750704

Rasmi M, Jantan A (2011) Attack Intention Analysis Model for Network Forensics. In: Zain JM, Mohd WMBW, El-Qawasmeh E (eds) Software Engineering and Computer Systems: Second International Conference, ICSECS 2011, Kuantan, Pahang, Malaysia, June 27–29, 2011, Proceedings, Part II. Springer, Berlin, Heidelberg, pp 403–411

Reiman T, Pietikäinen E (2012) Leading indicators of system safety – Monitoring and driving the organizational safety potential. Saf Sci 50(10):1993–2000. https://doi.org/10.1016/j.ssci.2011.07.015

Rodrigues VP, Pigosso DCA, McAloone TC (2016) Process-related key performance indicators for measuring sustainability performance of ecodesign implementation into product development. J Clean Prod 139:416–428. https://doi.org/10.1016/j.jclepro.2016.08.046

Safa NS, Von Solms R, Futcher L (2016) Human aspects of information security in organisations. Comput Fraud Secur 2016(2):15–18. https://doi.org/10.1016/S1361-3723(16)30017-3

Saleh MS, Alrabiah A, Bakry SH (2007) Using ISO 17799: 2005 information security management: a STOPE view with six sigma approach. Int J Netw Manag 17(1):85–97. https://doi.org/10.1002/nem.616

Saydjari OS (2004) Multilevel Security: Reprise. IEEE Secur Priv 2(5):64–67. https://doi.org/10.1109/MSP.2004.78

Siponen MT (2001) Five dimensions of information security awareness. ACM SIGCAS Comput Soc 31(2):24–29. https://doi.org/10.1145/503345.503348

Soomro ZA, Shah MH, Ahmed J (2016) Information security management needs more holistic approach: A literature review. Int J Inf Manag 36(2):215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Swiderski F, Snyder W (2004) Threat modeling. Microsoft Press, Redmond, WA

Takano KI, Tsuge T, Hasegawa N, Hirose A (2004) Development of a safety assessment system for promoting a safe organizational climate and culture. In: Itoigawa N, Wilpert B, Fahlbruch B (eds) Emerging Demands for the Safety of Nuclear Power Operations: Challenge and Response, CRC Press, Boca Raton, FL, pp 45–60

Torres JM, Sarriegi JM, Santos J, Serrano N (2006) Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. In: Katsikas SK, López J, Backes M, Gritzalis S, Preneel B (eds) Information Security: 9th International Conference, ISC 2006, Samos Island, Greece, August 30 – September 2, 2006, Proceedings. Springer, Berlin, Heidelberg, pp 530–545

Trček D, Trobec R, Pavešić N, Tasič JF (2007) Information systems security and human behavior. Behav Inf Technol 26(2):113–118. https://doi.org/10.1080/01449290500330299

Trček D (2003) An integral framework for information systems security management. Comput Secur 22(4):337–360. https://doi.org/10.1016/S0167-4048(03)00413-9

Tryfonas T, Gritzalis D, Kokolakis S (2000) A Qualitative Approach to Information Availability. In: Qing S, Eloff JHP (eds) Information Security for Global Information Infrastructures: IFIP TC11, Sixteenth Annual Working Conference on Information Security, August 22–24, 2000, Beijing, China. Springer, New York, NY, pp 37–47

Uffen J, Pomes R, Breitner MH (2012) Towards a Sustainable and Efficient Component-based Information Security Framework. In: Proceedings of the Multikonferenz Wirtschaftsinformatik 2012 (MKWI), Braunschweig, Germany, February 29 – March 2, 2012

Vance A, Lowry PB, Eggett D (2013) Using Accountability to Reduce Access Policy Violations in Information Systems. J Manag Inf Syst 29(4):263–290. https://doi.org/10.2753/MIS0742-1222290410

Vithanwattana N, Mapp G, George C (2016) mHealth – Investigating an information security framework for mHealth data: Challenges and possible solutions. In: Proceedings of the 12th International Conference on Intelligent Environments (IE), London, United Kingdom, September 14–16, 2016

Weber J, Schäffer U (2016) Einführung in das Controlling, 15th edn. Schäffer-Poeschel, Stuttgart

Wilpert B (2000) Organizational factors in nuclear safety. In: Proceedings of the 5th International Conference on Probabilistic Safety Assessment and Management (PSAM), Osaka, Japan, November 27 – December 1, 2000

Yao YH, Fan YY, Guo YX, Li Y (2014) Leadership, work stress and employee behavior. Chin Manag Stud 8(1):109–126. https://doi.org/10.1108/CMS-04-2014-0089

Yildirim EY, Akalp G, Aytac S, Bayram N (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. Int J Inf Manag 31(4):360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Zerr K (2007) Security-Awarenss-Monitoring – Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewusstseins bei Mitarbeitern. Datenschutz und Datensicherheit – DuD 31(7):519–523. https://doi.org/10.1007/s11623-007-0178-x

Zerr K, Benner A (2017) Kennzahlen eines mitarbeiterorientierten Sicherheitsmanagements. Datenschutz und Datensicherheit – DuD 41(2):80–87. https://doi.org/10.1007/s11623-017-0733-z

Further References[3]

Abawajy J (2014) User preference of cyber security awareness delivery methods. Behav Inf Technol 33(3):237–248. https://doi.org/10.1080/0144929X.2012.708787

Al-Darwish AI, Choe P (2019) A Framework of Information Security Integrated with Human Factors. In: Moallem A (ed) HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019. Proceedings. Springer, Cham, pp 217–229

Alavi R, Islam S, Mouratidis H (2014) A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations. In: Tryfonas T, Askoxylakis I (eds) Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22–27, 2014, Proceedings. Springer, Cham, pp 297–305

Anderson R, Moore T (2006) The Economics of Information Security. Science 314(5799):610–613. https://doi.org/10.1126/science.1130992

Ansoff HI (1975) Managing Strategic Surprise by Response to Weak Signals. Calif Manag Rev 18(2):21–33. https://doi.org/10.2307/41164635

Ashenden D (2008) Information Security management: A human challenge?. Inf Secur Techn Rep 13(4):195–201. https://doi.org/10.1016/j.istr.2008.10.006

Association for Information Systems (AIS) (2011) Senior Scholars' Basket of Journals. http://aisnet.org/general/custom.asp?page=SeniorScholarBasket. Accessed 10 January 2023

Azmi R, Tibben W, Win KT (2018) Review of cybersecurity frameworks: context and shared concepts. J Cyber Pol 3(2):258–283. https://doi.org/10.1080/23738871.2018.1520271

Backhouse J, Dhillon G (1996) Structures of responsibility and security of information systems. Eur J Inf Syst 5(1):2–9. https://doi.org/10.1057/ejis.1996.7

Bass T (2000) Intrusion detection systems and multisensor data fusion. Commun ACM 43(4):99–105. https://doi.org/10.1145/332051.332079

Bernsmed K, Tøndel IA (2013) Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management. In: Proceedings of the 7th International Conference on IT Security Incident Management and IT Forensics (IMF), Nuremberg, Germany, March 12–14, 2013

Bem DJ (1995) Writing a review article for Psychological Bulletin. Psychol Bull 118(2):172–177. https://doi.org/10.1037/0033-2909.118.2.172

Bowen BM, Devarajan R, Stolfo S (2011) Measuring the human factor of cyber security. In: Proceedings of the 2011 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, November 15–17, 2011

Buczak AL, Guven E (2015) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Commun Sur Tutor 18(2):1153–1176. https://doi.org/10.1109/COMST.2015.2494502

[3] The references for this paper are given in two parts: this part of the references section present the papers not contained in the literature review (results section). The papers included in both the literature review and the other sections of this paper are listed in both parts of the references section.

Caldwell T (2016) Making security awareness training work. Comput Fraud Secur 2016(6):8–14. https://doi.org/10.1016/S1361-3723(15)30046-4

Carlton M, Levy Y, Ramim M (2019) Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Inf Comput Secur 27(1):101–121. https://doi.org/10.1108/ICS-11-2016-0088

Cascavilla G, Tamburri DA, Van Den Heuvel WJ (2021) Cybercrime threat intelligence: A systematic multi-vocal literature review. Comput Secur 105:102258. https://doi.org/10.1016/j.cose.2021.102258

Cavusoglu H, Cavusoglu H, Raghunathan S (2004) Economics of IT Security Management: Four Improvements to Current Security Practices. Commun Assoc Inf Syst 14:65–75. https://doi.org/10.17705/1CAIS.01403

Chang SE, Lin CS (2007) Exploring organizational culture for information security management. Inf Manag Data Syst 107(3):438–458. https://doi.org/10.1108/02635570710734316

Chertoff M (2008) The cybersecurity challenge. Regul Gov 2(4):480–484. https://doi.org/10.1111/j.1748-5991.2008.00051.x

Choo K-KR (2011) The cyber threat landscape: Challenges and future research directions. Comput Secur 30(8):719–731. https://doi.org/10.1016/j.cose.2011.08.004

Choo K-KR, Gai K, Chiaraviglio L, Yang Q (2021) A multidisciplinary approach to Internet of Things (IoT) cybersecurity and risk management. Comput Secur 102:102–136. https://doi.org/10.1016/j.cose.2020.102136

Choobineh J, Dhillon G, Grimaila MR, Rees J (2007) Management of Information Security: Challenges and Research Directions. Commun Assoc Inf Syst 20:958–971. https://doi.org/10.17705/1CAIS.02057

Choraś M, Kozik R, Renk R, Hołubowicz W (2015) A Practical Framework and Guidelines to Enhance Cyber Security and Privacy. In: Herrero Á, Baruque B, Sedano J, Quintián H, Corchado E (eds) International Joint Conference: CISIS'15 and ICEUTE'15. Springer, Cham, pp 485–495

Clark WR, Clark LA, Raffo DM, Williams Jr RI (2021) Extending Fisch and Block's (2018) tips for a systematic review in management and business literature. Manag Rev Q 71(1):215–231. https://doi.org/10.1007/s11301-020-00184-8

Cole JR, Pence T, Cummings J, Baker E (2019) Gamifying Security Awareness: A New Prototype. In: Moallem A (ed) HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings. Springer, Cham, pp 115–133

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville RL (2013) Future directions for behavioral information security research. Comput Secur 32:90–101. https://doi.org/10.1016/j.cose.2012.09.010

Da Veiga A, Eloff JHP (2007) An Information Security Governance Framework. Inf Syst Manag 24(4):361–372. https://doi.org/10.1080/10580530701586136

Denning DE (2003) Information technology and security. Georgetown University Press, Washington, DC

De Maggio MC, Mastrapasqua M, Tesei M, Chittaro A, Setola R (2019) How to Improve the Security Awareness in Complex Organizations. Eur J Secur Res 4(1):33–49. https://doi.org/10.1007/s41125-017-0028-2

Dhillon G, Backhouse J (2001) Current directions in IS security research: towards socio-organizational perspectives. Inf Syst J 11(2):127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Disterer G (2015) Frühwarnsysteme für das IT-Sicherheits- und Risikomanagement. HMD Prax Wirtschaftsinf 52(5):790–801. https://doi.org/10.1365/s40702-015-0171-z

Diesch R, Pfaff M, Krcmar H (2020) A comprehensive model of information security factors for decision-makers. Comput Secur 92:1–21. https://doi.org/10.1016/j.cose.2020.101747

Duriau VJ, Reger RK, Pfarrer MD (2007) A Content Analysis of the Content Analysis Literature in Organization Studies: Research Themes, Data Sources, and Methodological Refinements. Organ Res Method 10(1):5–34. https://doi.org/10.1177/1094428106289252

Edgar TW, Manz DO (2017) Research Methods for Cyber Security. Syngress, Cambridge, MA

Eisenhardt KM (1989) Building Theories from Case Study Research. Acad Manag Rev 14(4):532–550. https://doi.org/10.2307/258557

Eling M, McShane M, Nguyen T (2021) Cyber risk management: History and future research directions. Risk Manag Insur Rev 24(1):93–125. https://doi.org/10.1111/rmir.12169

Eling M, Wirfs JH (2019) What are the actual costs of cyber risk events?. Eur J Operat Res 272(3):1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021

Eminağaoğlu M, Uçar E, Eren Ş (2009) The positive outcomes of information security awareness training in companies – A case study. Inf Secur Techn Rep 14(4):223–229. https://doi.org/10.1016/j.istr.2010.05.002

Falco G, Eling M, Jablanski D, Weber M, Miller V, Gordon LA, Wang SS, Schmit J, Thomas R, Elvedi M, Maillart T, Donavan E, Dejung S, Durand E, Nutter F, Scheffer U, Arazi G, Ohana G, Lin H (2019) Cyber risk research impeded by disciplinary barriers. Science 366(6469):1066–1069. https://doi.org/10.1126/science.aaz4795

Fielden K (2010) Information Security Framework. Proceedings of the 2010 International Conference on Information Society (i-Society), London, United Kingdom, June 28–30, 2010

Fielder A, Panaousis E, Malacaria P, Hankin C, Smeraldi F (2016) Decision support approaches for cyber security investment. Decis Support Syst 86:13–23. https://doi.org/10.1016/j.dss.2016.02.012

Fink A (2014) Conducting Research Literature Reviews: From the Internet to Paper, 4th edn. SAGE Publications, Los Angeles, CA, London, New Dehli, Singapore, Washington, DC

Fink L (2020) Conducting Information Systems Research in the Midst of the COVID-19 Pandemic: Opportunities and Challenges. Inf Syst Manag 37(4):256–259. https://doi.org/10.1080/10580530.2020.1814460

Fisch C, Block J (2018) Six tips for your (systematic) literature review in business and management research. Manag Rev Q 68(2):103–106. https://doi.org/10.1007/s11301-018-0142-x

Fujs D, Mihelič A, Vrhovec SLR (2019) The power of interpretation: Qualitative methods in cybersecurity research. Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES), Canterbury, United Kingdom, August 26–29, 2019

Garousi V, Felderer M, Mäntylä MV (2019) Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. Inf Softw Technol 106:101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gioia DA, Corley KG, Hamilton AL (2013) Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. Organ Res Method 16(1):15–31. https://doi.org/10.1177/1094428112452151

Gjertsen EGB, Gjære EA, Bartnes M, Flores WR (2017) Gamification of Information Security Awareness and Training. In: Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP), Porto, Portugal, February 19–21, 2017

Hale ML, Gamble RF, Gamble P (2015) CyberPhishing: A game-based platform for phishing awareness testing. In: Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS), Kauai, HI, USA, January 5–8, 2015

Hart C (1998) Doing a Literature Review: Releasing the Social Science Research Imagination. SAGE Publications, London, Thousand Oaks, CA, New Dehli

Heartfield R, Loukas G (2018) Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Comput Secur 76:101–127. https://doi.org/10.1016/j.cose.2018.02.020

Hitchings J (1996) A practical solution to the complex human issues of information security design. In: Katsikas SK Gritzalis D (eds) Information Systems Security: Facing the information society of the 21st Century. Chapman & Hall, London, pp 3–12

Hoffman LJ (2013) Social Science, Computer Science, and Cybersecurity Workshop Summary Report (Report GW-CSPRI-2013-02). Cyber Security Policy and Research Institute. The George Washington University, Washington, DC. https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/Final+08+22+13+1301+Report+Social+Science.pdf. Accessed 12 January 2023

Hsieh H-F, Shannon SE (2005) Three Approaches to Qualitative Content Analysis. Qual Health Res 15(9):1277–1288. https://doi.org/10.1177/1049732305276687

Islam C, Ali Babar M, Nepal S (2019) A Multi-Vocal Review of Security Orchestration. ACM Comput Surv 52(2):1–45. https://doi.org/10.1145/3305268

Jaeger L (2018) Information security awareness: literature review and integrative framework. In: Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS), Big Island, HI, USA, January 2–6, 2018

James HL (1996) Managing information systems security: a soft approach. In: Proceedings of the 1996 Information Systems Conference of New Zealand (ISCNZ), Palmerston North, New Zealand, October 30–31, 1996

Järveläinen J (2013) IT incidents and business impacts: Validating a framework for continuity management in information systems. Int J Inf Manag 33(3) 583–590. https://doi.org/10.1016/j.ijinfomgt.2013.03.001

Kalutarage HK, Shaikh S, Lee B-S, Lee C, Kiat YC (2016) Early Warning Systems for Cyber Defence. In: Camenisch J, Kesdoğan D (eds) Open Problems in Network Security: IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October 29, 2015, Revised Selected Papers. Springer, Cham, pp 29–42

Kajava J, Savola R, Varonen R (2005) Weak Signals in Information Security Management. In: Hao Y, Liu J, Wang Y, Cheung Y-M, Yin H, Jiao L, Ma J, Jiao Y-C (eds) Computational

Intelligence and Security: International Conference, CIS 2005, Xi'an, China, December 15–19, 2005, Proceedings, Part II. Springer, Berlin, Heidelberg, pp 508–517

Karyda M, Mitrou E, Quirchmayr G (2006) A framework for outsourcing IS/IT security services. Inf Manag Comput Secur 14(5):403–416. https://doi.org/10.1108/09685220610707421

Kassarjian HH (1977) Content Analysis in Consumer Research. J Consum Res 4(1):8–18. https://doi.org/10.1086/208674

Kayworth T, Whitten D (2010) Effective Information Security Requires a Balance of Social and Technology Factors. Manag Inf Syst Q Exec 9(3):163–175. https://aisel.aisnet.org/misqe/vol9/iss3/5

Kotulic AG, Clark JG (2004) Why there aren't more information security research studies. Inf Manag 41(5):597–607. https://doi.org/10.1016/j.im.2003.08.001

Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: Pathways to vulnerabilities. Comput Secur 28(7):509–520. https://doi.org/10.1080/10580530701586136

Kritzinger E, Smith E (2008) Information security management: An information security retrieval and awareness model for industry. Comput Secur 27(5–6):224–231. https://doi.org/10.1016/j.cose.2008.05.006

Krystek U (2006) Frühwarnsysteme. In: Hutzschenreuter T, Griess-Nega T (eds) Krisenmanagement: Grundlagen – Strategien – Instrumente. Gabler, Wiesbaden, pp 221–244

Kuckertz A, Block J (2021) Reviewing systematic literature reviews: ten key questions and criteria for reviewers. Manag Rev Q 71(3):519–524. https://doi.org/10.1007/s11301-021-00228-7

Levy Y, Ellis TJ (2006) A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. Infor Sci: Int J Emerg Transdiscipl 9:181–212. https://doi.org/10.28945/479

Li Y, Guo L (2007) An active learning based TCM-KNN algorithm for supervised network intrusion detection. Comput Secur 26(7–8):459–467. https://doi.org/10.1016/j.cose.2007.10.002

Mantere S, Ketokivi M (2013) Reasoning in Organization Science. Academy Manag Rev 38(1):70–89. https://doi.org/10.5465/amr.2011.0188

Marotta A, McShane M (2018) Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. Risk Manag Insur Rev 21(3):435–452. https://doi.org/10.1111/rmir.12109

Mattern T, Felker J, Borum R, Bamford G (2014) Operational levels of cyber intelligence. Int J Intel Count Intel 27(4):702–719. https://doi.org/10.1080/08850607.2014.924811

Mayring P (2015) Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12th edn. Beltz, Weinheim, Basel

Mayring P, Brunner E (2009) Qualitative Inhaltsanalyse. In: Buber R, Holzmüller HH (eds) Qualitative Marktforschung: Konzepte – Methoden – Analysen, 2nd edn. Gabler, Wiesbaden, pp 669–680

Meredith J (1993) Theory Building through Conceptual Methods. Int J Operat Prod Manag 13(5):3–11. https://doi.org/10.1108/01443579310028120

Mitchell R, Chen I-R (2014) A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv 46(4):1–29. https://doi.org/10.1145/2542049

Mohammadi S, Mirvaziri H, Ghazizadeh-Ahsaee M, Karimipour H (2019) Cyber intrusion detection by combined feature selection algorithm. J Inf Secur Applic 44:80–88. https://doi.org/10.1016/j.jisa.2018.11.007

Moher D, Liberati A, Tetzlaff J, Altman DG, The PRISMA Group (2009) Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement. Annal Intern Med 151(4):264–269. https://doi.org/10.7326/0003-4819-151-4-200908180-00135

Monfelt Y, Pilemalm S, Hallberg J, Yngström L (2011) The 14-layered framework for including social and organizational aspects in security management. Inf Manag Comput Secur 19(2):124–133. https://doi.org/10.1108/09685221111143060

Mujinga M, Eloff MM, Kroeze JH (2017) A Socio-Technical Approach to Information Security. In: Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, USA, August 10–12, 2017

Nosworthy JD (2000) Implementing Information Security In The 21st Century — Do You Have the Balancing Factors?. Comput Secur 19(4):337–347. https://doi.org/10.1016/S0167-4048(00)04021-9

Nurse JRC, Legg PA, Buckley O, Agrafiotis I, Wright G, Whitty M, Upton D, Goldsmith M, Creese S (2014) A Critical Reflection on the Threat from Human Insiders – Its Nature, Industry Perceptions, and Detection Approaches. In: Tryfonas T, Askoxylakis I (eds) Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22–27, 2014, Proceedings. Springer, Cham, pp 270–281

Øien K, Massaiu S, Tinmannsvik RK, Størseth F (2010) Development of Early Warning Indicators based on Resilience Engineering. In: Proceedings of the 10th International Probabilistic Safety Assessment & Management Conference (PSAM), Seattle, WA, USA, June 7–11, 2010

Øien K, Utne IB, Tinmannsvik RK, Massaiu S (2011b) Building Safety indicators: Part 2 – Application, practices and results. Saf Sci 49(2):162–171. https://doi.org/10.1016/j.ssci.2010.05.015

Okoli C (2015) A Guide to Conducting a Standalone Systematic Literature Review. Commun Assoc Inf Syst 37:879–910. https://doi.org/10.17705/1CAIS.03743

Palmatier RW, Houston MB, Hulland J (2018) Review articles: purpose, process, and structure. J Acad Mark Sci 46(1):1–5. https://doi.org/10.1007/s11747-017-0563-4

Paulson LD (2002) Wanted: More Network-Security Graduates and Research. Computer 35(2):22–24. https://doi.org/10.1109/2.982909

Petrenko S (2018) Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation. Springer, Cham

Pfleeger SL, Sasse MA, Furnham A (2014) From Weakest Link to Security Hero: Transforming Staff Security Behavior. J Homel Secur Emerg Manag 11(4):489–510. https://doi.org/10.1515/jhsem-2014-0035

Pickering C, Byrne J (2014) The benefits of publishing systematic quantitative literature reviews for PhD candidates and other early-career researchers. High Educ Res Developm 33(3):534–548. https://doi.org/10.1080/07294360.2013.841651

Posthumus S, Von Solms R (2004) A framework for the governance of information security. Comput Secur 23(8):638–646. https://doi.org/10.1016/j.cose.2004.10.006

Prommegger B, Thatcher JB, Wiesche M, Krcmar H (2021) When your data has COVID-19: how the changing context disrupts data collection and what to do about it. Eur J Inf Syst 30(1):100–118. https://doi.org/10.1080/0960085X.2020.1841573

Rakes TR, Deane JK, Rees LP (2012) IT security planning under uncertainty for high-impact events. Omega – Int J Manag Sci 40(1):79–88. https://doi.org/10.1016/j.omega.2011.03.008

Rashid A, Danezis G, Chivers H, Lupu E, Martin A, Lewis M, Peersman C (2018) Scoping the Cyber Security Body of Knowledge. IEEE Secur Priv 16(3):96–102. https://doi.org/10.1109/MSP.2018.2701150

Ratnasingham P (1998) Trust in Web-based electronic commerce security. Inf Manag Comput Secur 6(4):162–166. https://doi.org/10.1108/09685229810227667

Reinhardt WA (1984) An early warning system for strategic planning. Long Range Plan 17(5):25–34. https://doi.org/10.1016/0024-6301(84)90034-7

Robinson M, Jones K, Janicke H (2015) Cyber warfare: Issues and challenges. Comput Secur 49:70–94. https://doi.org/10.1016/j.cose.2014.11.007

Rowe F (2014) What literature review is not: diversity, boundaries and recommendations. Eur J Inf Syst 23(3):241–255. https://doi.org/10.1057/ejis.2014.7

Saldaña J (2013) The Coding Manual for Qualitative Researchers, 2nd edn. SAGE Publications, Los Angeles, CA, London, New Dehli, Singapore, Washington, DC

Saunders M, Lewis P, Thornhill A (2009) Research methods for business students, 5th edn. Pearson Education, Harlow

Schryen G (2015) Writing Qualitative IS Literature Reviews—Guidelines for Synthesis, Interpretation, and Guidance of Research. Commun Assoc Inf Syst 37:286–325. https://doi.org/10.17705/1CAIS.03712

Schuessler J (2007) An Information Systems Security Framework. In: Proceedings of the 13th Americas Conference on Information Systems (AMCIS), Keystone, CO, USA, August 9–12, 2007

Seuring S, Gold S (2012) Conducting content analysis based literature reviews in supply chain management. Supply Chain Manag: Int J 17(5):544–555. https://doi.org/10.1108/13598541211258609

Seuring S, Müller M (2008) From a literature review to a conceptual framework for sustainable supply chain management. J Clean Prod 16(15):1699–1710. https://doi.org/10.1016/j.jclepro.2008.04.020

Seuring S, Müller M, Westhaus M, Morana R (2005) Conducting a Literature Review — The Example of Sustainability in Supply Chains. In: Kotzab H, Seuring S, Müller M, Reiner G (eds) Research Methodologies in Supply Chain Management. Physica-Verlag HD, Heidelberg, pp 91–106

Shamoo AE (2020) Validate the integrity of research data on COVID 19. Account Res 27(6):325–326. https://doi.org/10.1080/08989621.2020.1787838

Shaw RS, Chen CC, Harris AL, Huang HJ (2009) The impact of information richness on information security awareness training effectiveness. Comput Educ 52(1):92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Silic M, Back A (2014) Information security: Critical review and future directions for research. Inf Manag Comput Secur 22(3):279–308. https://doi.org/10.1108/IMCS-05-2013-0041

Singh AN, Gupta MP, Ojha A (2014) Identifying factors of "organizational information security management". J Enterp Inf Manag 27(5):644–667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen MT (2000) A conceptual foundation for organizational information security awareness. Inf Manag Comput Secur 8(1):31–41. https://doi.org/10.1108/09685220010371394

Siponen MT (2001) Five dimensions of information security awareness. ACM SIGCAS Comput Soc 31(2):24–29. https://doi.org/10.1145/503345.503348

Siponen MT, Willison R (2007) A Critical Assessment of IS Security Research between 1990-2004. In: Proceedings of the 15th European Conference on Information Systems (ECIS), St. Gallen, Switzerland, June 7–9, 2007

Smith GS (2004) Recognizing and Preparing Loss Estimates from Cyber-Attacks. Inf Syst Secur 12(6):46–57. https://doi.org/10.1201/1086/44022.12.6.20040101/79786.8

Snyder H (2019) Literature review as a research methodology: An overview and guidelines. J Bus Res 104:333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Soomro ZA, Shah MH, Ahmed J (2016) Information security management needs more holistic approach: A literature review. Int J Inf Manag 36(2):215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Spears JL, Barki H (2010) User Participation in Information Systems Security Risk Management. Manag Inf Syst Q 34(3):503–522. https://doi.org/10.2307/25750689

Srinidhi B, Yan J, Tayi GK (2015) Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors. Decis Support Syst 75:49–62. https://doi.org/10.1016/j.dss.2015.04.011

Stewart H, Jürjens J (2017) Information security management and the human aspect in organizations. Inf Comput Secur 25(5):494–534. https://doi.org/10.1108/ICS-07-2016-0054

Suryotrisongko H, Musashi Y (2019) Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspective. In: Proceedings of the 12th IEEE International Conference on Service-Oriented Computing and Applications (SOCA), Kaohsiung, Taiwan, November 18–21, 2019

Tam T, Rao A, Hall J (2021) The good, the bad and the missing: A Narrative review of cybersecurity implications for australian small businesses. Comput Secur 109:1–56. https://doi.org/10.1016/j.cose.2021.102385

Thomson ME, Von Solms R (1998) Information security awareness: educating your users effectively. Inf Manag Comput Secur 6(4):167–173. https://doi.org/10.1108/09685229810227649

Torraco RJ (2005) Writing Integrative Literature Reviews: Guidelines and Examples. Hum Resour Dev Rev 4(3):356–367. https://doi.org/10.1177/1534484305278283

Torres JM, Sarriegi JM, Santos J, Serrano N (2006) Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness. In: Katsikas SK, López J, Backes M, Gritzalis S, Preneel B (eds) Information Security: 9th International Conference, ISC 2006, Samos Island, Greece, August 30 – September 2, 2006, Proceedings. Springer, Berlin, Heidelberg, pp 530–545

Tranfield D, Denyer D, Smart P (2003) Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. Br J Manag 14(3):207–222. https://doi.org/10.1111/1467-8551.00375

Trček D, Trobec R, Pavešić N, Tasič JF (2007) Information systems security and human behavior. Behav Inf Technol 26(2):113–118. https://doi.org/10.1080/01449290500330299

Tsohou A, Karyda M, Kokolakis S, Kiountouzis E. (2012) Analyzing trajectories of information security awareness. Inf Technol People 25(3):327–352. https://doi.org/10.1108/09593841211254358

Tu CZ, Adkins J, Zhao GY (2019) A Review of Information Systems Security Management: An Integrated Framework. In: Proceedings of the 14th Annual Conference of the Midwest United States Association for Information Systems (MWAIS), Oshkosh, WI, USA, May 21–22, 2019

Vance A, Lowry PB, Eggett D (2013) Using Accountability to Reduce Access Policy Violations in Information Systems. J Manag Inf Syst 29(4):263–290. https://doi.org/10.2753/MIS0742-1222290410

Vom Brocke J, Simons A, Niehaves B, Riemer K, Plattfaut R, Cleven A (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In: Proceedings of the 17th European Conference on Information Systems (ECIS), Verona, Italy, June 8–10, 2009

Vom Brocke J, Simons A, Riemer K, Niehaves B, Plattfaut R, Cleven A (2015) Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. Commun Assoc Inf Syst 37:205–224. https://doi.org/10.17705/1CAIS.03709

Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102. https://doi.org/10.1016/j.cose.2013.04.004

Von Solms SH (Basie) (2001) Information Security — A Multidimensional Discipline. Comput Secur 20(6):504–508. https://doi.org/10.1016/S0167-4048(01)00608-3

Von Solms SH (Basie), Von Solms R (2004) The 10 deadly sins of information security management. Comput Secur 23(5):371–376. https://doi.org/10.1016/j.cose.2004.05.002

Weber K, Schütz A, Fertig T (2019) Grundlagen und Anwendung von Information Security Awareness – Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren. Springer Vieweg, Wiesbaden

Webster J, Watson RT (2002) Analyzing the Past to Prepare for the Future: Writing a Literature Review. Manag Inf Syst Q 26(2):xiii–xxiii. https://www.jstor.org/stable/4132319

Werlinger R, Hawkey K, Beznosov K (2009) An integrated view of human, organizational, and technological challenges of IT security management. Inf Manag Comput Secur 17(1):4–19. https://doi.org/10.1108/09685220910944722

Willems C, Meinel C (2008) Awareness Creation mit Tele-Lab IT-Security: Praktisches Sicherheitstraining im virtuellen Labor am Beispiel Trojanischer Pferde. In: Alkassar A, Siekmann J (eds) SICHERHEIT 2008–Sicherheit, Schutz und Zuverlässigkeit. Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik eV (GI). Gesellschaft für Informatik e.V., Bonn, pp 513–523

Wolfswinkel JF, Furtmueller E, Wilderom CPM (2013) Using grounded theory as a method for rigorously reviewing literature. Eur J Inf Syst 22(1):45–55. https://doi.org/10.1057/ejis.2011.51

Wong CK, Gouda M, Lam SS (2000) Secure Group Communications Using Key Graphs. IEEE/ACM Transact Netw 8(1):16–30. https://doi.org/10.1109/90.836475

Yang J, Huang S-HS (2007) Mining TCP/IP packets to detect stepping-stone intrusion. Comput Secur 26(7–8):479–484. https://doi.org/10.1016/j.cose.2007.07.001

Yildirim EY, Akalp G, Aytac S, Bayram N (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. Int J Inf Manag 31(4):360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Young H, Van Vliet T, Van de Ven J, Jol S, Broekman C (2018) Understanding Human Factors in Cyber Security as a Dynamic System. In: Nicholson D (ed) Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17−21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA. Springer, Cham, pp 244–254

Zafar H, Clark JG (2009) Current State of Information Security Research In IS. Commun Association Inf Syst 24:557–596. https://doi.org/10.17705/1CAIS.02434

Zelewski S (1987) Frühwarnung und Künstliche Intelligenz: Möglichkeiten zur Fortentwicklung von Frühwarnsystemen durch Beiträge der Künstlichen Intelligenz. Die Unternehmung 41(4):256–265. https://www.jstor.org/stable/24178830

Zerr K (2007) Security-Awarenss-Monitoring – Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewusstseins bei Mitarbeitern. Datenschutz und Datensicherheit – DuD 31(7):519–523. https://doi.org/10.1007/s11623-007-0178-x

Zerr K, Benner A (2017) Kennzahlen eines mitarbeiterorientierten Sicherheitsmanagements. Datenschutz und Datensicherheit – DuD 41(2):80–87. https://doi.org/10.1007/s11623-017-0733-z

Statements and Declarations

Funding:

The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Competing Interests:

The authors have no relevant financial or non-financial interests to disclose.

Author Contributions:

The idea was developed by Theresa Eden and Dirk Wrede. All authors contributed to the study conception and design. Literature search and data analysis were performed by Theresa Eden. The first draft of the manuscript was written by Dirk Wrede, Theresa Eden and Johann-Matthias Graf von der Schulenburg. All authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Availability of data and material:

Available upon request.

Modul 7

Practice-oriented Early Warning Indicators in Cybersecurity: Insights from a Qualitative Empirical Study in Germany

Theresa Eden
Dirk Wrede
Christoph Schwarzbach
Tobias Basse

eingereicht bei:

Journal of Information Technology

Practice-oriented Early Warning Indicators in Cybersecurity: Insights from a Qualitative Empirical Study in Germany

Theresa Eden, Dirk Wrede, Christoph Schwarzbach, Tobias Basse

Theresa Eden (Corresponding Author)

Gottfried Wilhelm Leibniz Universität Hannover
Institute for Risk and Insurance
Otto-Brenner-Straße 7
D-30159 Hanover
Germany
E-Mail: te@ivbl.uni-hannover.de

Dirk Wrede

Gottfried Wilhelm Leibniz Universität Hannover
Institute for Risk and Insurance
Otto-Brenner-Straße 7
D-30159 Hanover
Germany

Christoph Schwarzbach

Gottfried Wilhelm Leibniz Universität Hannover
Information Systems Institute
Königsworther Platz 1
D-30159 Hanover
Germany

Tobias Basse

Norddeutsche Landesbank Girozentrale
Friedrichswall 10
D-30159 Hanover
Germany

Practice-oriented Early Warning Indicators in Cybersecurity: Insights from a Qualitative Empirical Study in Germany

Abstract

This paper aims to examine practice-oriented early warning indicators (EWI) in the field of cybersecurity respectively to conceptualize them based on theoretical considerations. A qualitative research approach was chosen due to a lack of available data. For the qualitative study, 25 experts from various business sectors were interviewed. The expert interviews were analyzed using qualitative content analysis according to Kuckartz (2018). The analysis of the expert interviews shows that early warning systems (EWS) in the area of cybersecurity need, on the one hand, to be implemented technically. Still, on the other hand, the significance of the human factor should not be disregarded. The human element, in particular, substantially influences the success of security measures. It should be included in potential EWI in addition to the technical aspects and the current state of IT hygiene. The focus of the constructed EWI is not on early warnings (EW) against cyber-attacks but on examining weak spots within IT hygiene and insufficient employee sensitization. The topic examined in this research paper is of particular importance due to the increasing relevance of cybersecurity. To the best of our knowledge, no studies have been published on practice-oriented EWI in the field of cybersecurity. The findings are valuable for risk managers due to the holistic approach.

Keywords Cybersecurity, Information Security, Early Warning, Early Warning Indicators, Cyber-Risk Management, Information Security Management

1. Introduction

Cyber perils are among the most critical business risks for companies worldwide in the 21st century (Allianz Global Corporate & Specialty (AGCS), 2023). Damages caused by cybercrime can be both financial and non-financial (Mainelli, 2013; Eling & Schnell, 2016). In addition to conventional cyber-risk management, early warning systems (EWS) as part of a proactive and holistic cyber-risk management provide the potential to reduce damages caused by such events (Marotta & McShane, 2018). However, the early warning (EW) aspect of this field is relatively unexplored. The relevance of such risk management frameworks for information security (InfoSec) has already been stressed (Disterer, 2015; Petrenko, 2018), and also the identification,

selection, and implementation of early warning indicators (EWI) for the management of InfoSec incidents have been described (Bernsmed & Tøndel, 2013). EWI are indicators that attempt to detect known threats and provide information about organizational resilience before those threats result in actual problems (Øien et al., 2010; Ramaki & Atani, 2016). To the best of our knowledge, a systematic analysis and conceptualization of potential practice-oriented EWI in the field of cybersecurity has not yet been conducted. We fill the gap regarding EW and provide a first assessment of which aspects should be included in the context of potential EWI. Consequently, the following research question will be investigated:

> RQ: What is the status quo of EW in the field of cybersecurity/InfoSec, and what aspects should be incorporated in the design of potential practice-oriented EWI?

The article is structured as follows: First, the research area's existing theoretical background is presented. Afterward, our research methodology is laid out, including the data collection and the formation of categories. The results are presented in the fourth section in line with the recommendations by Yin (2003) at a primarily aggregate level and along the previously developed categories. Finally, we discuss the results and address the limitations of the adopted research methodology before we finalize our study with a brief conclusion.

2. Theoretical Background

In the academic literature, different terms are frequently used synonymously for the concept of InfoSec. These terms do not have a common definition and are not precisely differentiated (Diesch et al., 2018; Eling et al., 2021). For example, in addition to the term InfoSec (Anderson, 2003; Dlamini et al., 2009; Lundgren & Möller, 2019), one may find synonymous use of the terms computer security (ComSec) (Landwehr, 2001; Bishop, 2003; Andrews & Whittaker, 2004), information system security (Loch & Carr, 1991; De Paula et al., 2005), IT security (ITSec) (Spruit & Looijen, 1996; Oppliger, 2007), or cybersecurity (Von Solms & Van Niekerk, 2013; Cains et al., 2022). This multitude of terminologies resulted in numerous efforts aiming to reduce semantic ambiguity (Finne, 2000; Alshaikh et al., 2014; Schatz et al., 2017). As a result, the concept of InfoSec also went through different evolutionary phases over the years (Althonayan & Andronache, 2018). Von Solms (2010) divides these development phases starting in the 1980s into five waves. However, the evolution and existence of various terms related to cybersecurity continue to create ambiguity and impede an integrated solution for both enterprise cyber-risk management and interdisciplinary research approaches (Eling et al., 2021).

Furthermore, these definition ambiguities foster difficulties in measuring security or risk within an industry or an organization (Falco et al., 2019). Thus, the research community recognizes

the urgent need for effective security metrics. Although various qualitative and quantitative methods for security measures are suggested in the literature, so far, only a few of them have found a widespread practical application (Rudolph & Schwarz, 2012). The reason is that current proposals for ITSec metrics are not based on uniform, methodologically grounded requirements (Yasasin & Schryen, 2015). Thus, quantitative security measures, in particular, constitute one of the major challenges in ITSec (Fenz, 2010; Almasizadeh & Azgomi, 2014). In practice and literature, the terms metric and measure are mainly used synonymously (Diesch & Krcmar, 2020). In particular, research on security indicators and the development of metrics for InfoSec are still at a very early research stage and relatively underdeveloped (Diesch et al., 2018). Respective publications address, among other things, the derivation of quality criteria (Savola, 2013) and requirements (Yasasin & Schryen, 2015) for ITSec metrics, the development and implementation of security measures (Chew et al., 2008), the identification of proactive InfoSec management system metrics (Hajdarevic & Allen, 2013), the identification and specification of metrics and indicators for the management of security incidents (Cadena et al., 2020), the development of a classification framework to categorize and compare security indicators (Rudolph & Schwarz, 2012), and the design of EWI for the management of InfoSec incidents (Bernsmed & Tøndel, 2013).

The multidimensional character of InfoSec is emphasized in the literature (Von Solms, 2001; Posthumus & Von Solms, 2004; Von Solms & Von Solms, 2004). Consequently, many different research activities on various dimensions of InfoSec have been conducted in recent decades. This includes, e.g., legal and regulatory aspects (Karyda et al., 2006; Schuessler, 2007); the technological dimension (Eloff & Von Solms, 2000); infrastructural factors (Choraś et al., 2015); the importance of the human factor (Spears & Barki, 2010; Stewart & Jürjens, 2017); and organizational elements (Kraemer et al., 2009). Collier et al. (2013) distinguish four domains of cybersecurity: the physical, informational, cognitive, and social domain. Accordingly, the need for a holistic approach to InfoSec is increasingly emphasized (Dutta & Roy, 2008; Zafar & Clark, 2009; Soomro et al., 2016). Research on InfoSec is wide-ranging and includes technical, behavioral, managerial, philosophical, and organizational approaches to protecting the confidentiality, integrity, and availability of information and information systems (Crossler et al., 2013).

The importance of non-technical factors is also highlighted in information systems security research, although they are rarely analyzed in an integrated framework (Tu et al., 2019). In the corporate environment, InfoSec usually includes technologies, processes, and people (Da Veiga & Eloff, 2007), which are influenced by various factors and should be managed within a single

framework (Yildirim et al., 2011). Notably, human aspects are emphasized as the most important factor for InfoSec (Backhouse & Dhillon, 1996; Dhillon & Backhouse, 2001; Trček, 2003; Schultz, 2005; Siponen & Willison, 2007; Trček et al., 2007; Furnell & Clarke, 2012; Safa et al., 2015; Connolly et al., 2017; Azmi et al., 2018). For Scala et al. (2019), human aspects constitute one of the five complex cybersecurity problems. In this context, e.g., Al-Darwish and Choe (2019) evaluate the direct and indirect influencing factors on the human aspects of InfoSec, while Young et al. (2018) investigate the impact of changes in human behavior on cybersecurity, and Alavi et al. (2014) develop a conceptual framework to analyze the human factors of InfoSec management systems. The recent literature has increasingly highlighted the importance of the organizational factors of InfoSec (Kotulic & Clark, 2004; Ransbotham & Mitra, 2009; Bulgurcu et al., 2010; Singh et al., 2014). For Kraemer and Carayon (2003), human and organizational issues are among the most significant barriers to an effective InfoSec and ComSec. Similarly, Silic and Back (2014) identify organizational and human aspects of InfoSec as two of the 13 major research topics in this area. Consequently, in addition to the mere investigation of human aspects, organizational factors of InfoSec are also included in the analysis (Tu et al., 2019). Werlinger et al. (2009), in their holistic view of ITSec management, further expand the analysis of human and organizational aspects by including technological factors. Beznosov and Beznosova (2007) analyze the technological, human, and social dimensions of ComSec activities. Choraś et al. (2015) identify an organizational and, more broadly, an operational and infrastructural dimension of cybersecurity. Monfelt et al. (2011) describe a 14-layered framework that includes organizational and social aspects in InfoSec management. Regulatory factors for InfoSec are also emphasized (Schuessler, 2007). Karyda et al. (2006), e.g., consider technical, organizational, and legal aspects in their framework for outsourcing IS/ITSec services.

The aspect of EW in InfoSec is rarely investigated, although some authors emphasize its importance for InfoSec (Disterer, 2015; Petrenko, 2018). However, the discussion so far is limited mainly to potential applications of weak signals in the context of InfoSec (Kajava et al., 2005; Disterer, 2015) and describing the identification, selection, and implementation of EWI for the management of InfoSec incidents (Bernsmed & Tøndel, 2013).

3. Method and Data

Due to the lack of context-specific research findings on EW in the field of cybersecurity and the explorative nature of the research question, we chose a qualitative empirical research design in the form of expert interviews, for which Figure 1 provides an overview.

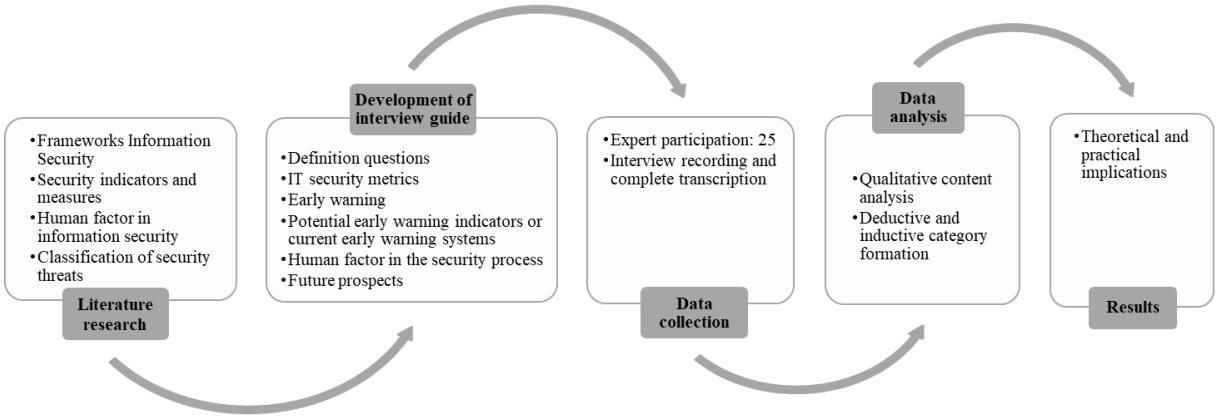


Figure 1. Elements of the research design

The method chosen for the study was oral questioning using partly standardized interviews. This approach is well established in qualitative research, especially for identifying expert knowledge (Schultze & Avital, 2011). The expert interviews were conducted using an open interview guide (Myers & Newman, 2007; Qu & Dumay, 2011), which included all relevant issues as independent thematic areas. The guided expert interviews took place between October 2019 and March 2021. With a response rate of 34.74%, 25 of 72 requested experts were interviewed. They were chosen from different business sectors based on their extensive practice-based knowledge and experience in InfoSec. The participants were not selected to meet representativeness criteria, which is why this is not a random sample. Since qualitative studies primarily aim to generate a better understanding of the research subject and to gain insights that go beyond the investigated cases (Hsieh & Shannon, 2005; Eisenhardt & Graebner, 2007; Kaczynski et al., 2014), the sampling criteria were oriented on the questions raised and the theoretical-conceptual preliminary considerations (Eisenhardt, 1989). Therefore, potential interview partners were contacted based on these preliminary examinations and snowball sampling. The selection of experts to be interviewed was mainly based on the initial research questions and the interviewees' recommendations (Rowley, 2012). Table 1 presents an overview of the interviewees.

Inter-view	Company	Position
I.1	Consulting	Consultant Cybersecurity
I.2	Public Authority	Chief Detective Cybercrime
I.3	Consulting	Senior Manager Cybersecurity
I.4	Association for IT Security	Chairman of the Board
I.5	Public Authority	Chief Detective Cybercrime
I.6	Logistics and Postal Company	Chief Information Security Officer
I.7	Service Company	Manager
I.8	Trading Company	Information Security Officer
I.9	Trading and Service Company	Manager IT
I.10	Service Company	Manager
I.11	Consulting	Director Cyber-Risk
I.12	Institute for Corporate Security	Head of Cybersecurity
I.13	Technical-Scientific Association	Head of Digital Security
I.14	Primary Insurer	Chief Information Security Officer
I.15	IT Service Provider	Chief Information Security Officer
I.16	IT Service Provider	Head of Risk Management
I.17	Reinsurance	Senior Risk Manager
I.18	Reinsurance	Head of Incident Response
I.19	Service Company	Head of IT
I.20	Service Company	IT Infrastructure Manager
I.21	Public Authority	Member of Economic Protection
I.22	Publishing Group	IT Security Officer
I.23	IT Service Provider	Managing Director
I.24	Primary Insurer	Information Security Officer
I.25	Reinsurance	Cyber Analyst

Table 1. Overview of the interview participants

The interviews lasted between 30 and 90 minutes, with an average of 48 minutes. They were recorded and transcribed to increase reliability (McLellan et al., 2003). The study followed the process model of the structured thematic qualitative content analysis according to Kuckartz (2018), which allows for a systematic and rule-based data analysis. A category system with anchor examples was developed by screening the interviews. The data analysis approach is intended to draw conclusions to answer the research question. The category system was developed deductively-inductively (Mayring, 2015). Some categories were deductively derived from the questions in the interview guideline, while others were inductively inferred from the data material. At the beginning of the analysis, the entire text material was read several times and then coded in successive steps, each increasing the level of abstraction, focusing on the terms

in relevant transcript segments. The analyzed data were checked for text segments relevant to the content during this process. The identified text elements were labeled and given codes that circumscribe the segment as accurately as possible (Gioia et al., 2013).

To ensure coding quality, a ‘double-blind procedure’ was used, whereby two researchers independently developed the codes (Guest et al., 2006). To ensure a common understanding of the codes and their application, two researchers entirely coded parts of the text material to test the developed coding scheme. The researchers then met to go through the material and to clarify as well as finalize the codes and categories. A code description was also prepared, including a brief explanation of the meaning and the code’s intended use. The preliminary coding scheme was discussed by the research team, including the two coders. The created codes were finally harmonized, and further development of the coding scheme took place after consensus among the authors. Special attention was paid to the stability of the developed codes and the structural design of the resulting coding scheme (Hennink et al., 2017). During the coding process, a final coding scheme was developed that contained a list of primarily descriptive codes. In the second step, the coding scheme was structured and transferred into a category system that organized the inductive and deductive categories into a hierarchical order (main and subcategories). The resulting content-analytic category system formed the basis for the subsequent qualitative analysis. Figure 2 shows the structure and content of the developed category system.

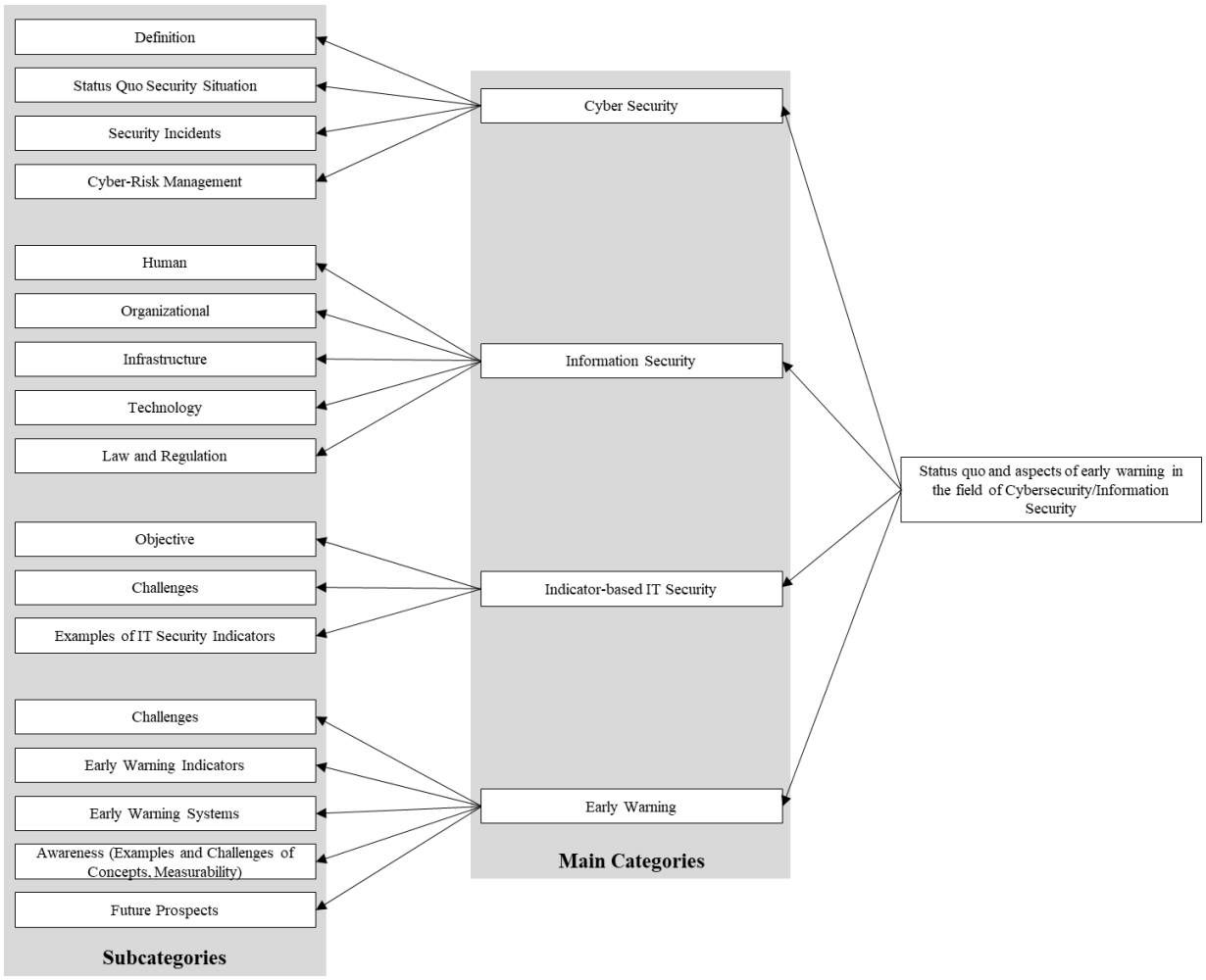


Figure 2. Category system

The final constructed category system, which provided the basis for coding the text material, contained four main categories. These were differentiated further into subcategories and comprised a total of 17 categories. The Comparative Method for Themes Saturation (CoMeTS) by Constantinou et al. (2017) was used to achieve thematic saturation. In this method, all themes from all interviews are first compared with each other. Afterward, the order of the interviews is rearranged several times to recheck saturation because the interview order leads to a different saturation during the review. Hence, readjusting the interviews helps to confirm saturation. We compared our themes on two levels to decide whether thematic saturation was achieved. First, all interviews were compared with each other. Second, the order of the interviews was rearranged several times, and saturation was rechecked to avoid any errors caused by their order and to ensure that thematic saturation was achieved. The latter was reached with regard to the main topics after analyzing 25 interviews. Collecting more data repeatedly did not yield new themes concerning the research question (Bowen, 2008; Morse, 1995, 2015). An overview of the saturation threshold of the codes is provided in Figure 3.

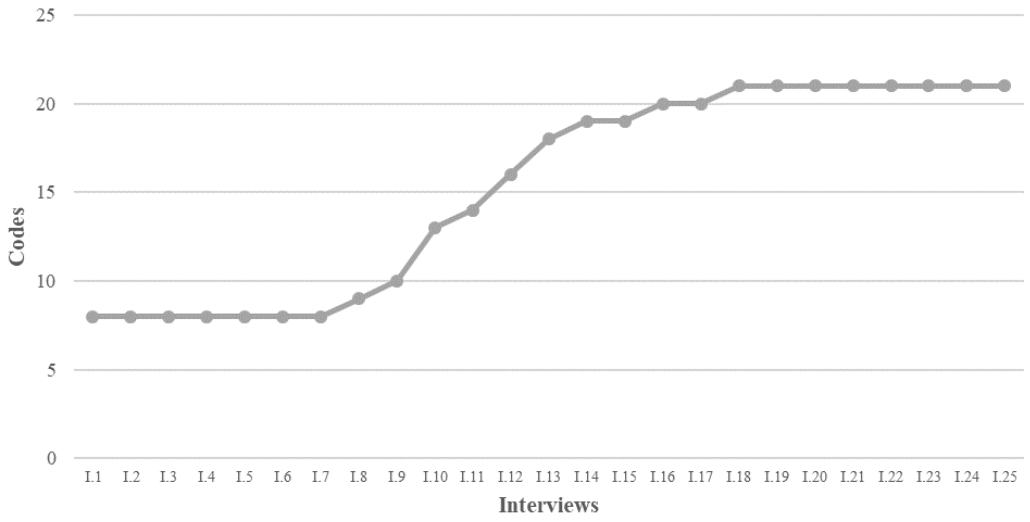


Figure 3. Themes saturation threshold

4. Results

Cybersecurity

Definition

Most experts surveyed associate the term cybersecurity with information and ITSec. In this context, all activities upholding the protection goals of confidentiality, availability, and integrity of assets, as well as the protection of a company against external and intended or unintended internal attacks, are mentioned. At the same time, the human factor that ultimately operates the technology must be considered. Consequently, the employees' awareness of how to handle technology significantly influences cybersecurity in a company.

Status Quo Security Situation

The ability of a company to protect itself preventively against cyber-attacks using a comprehensive ITSec solution varies as a result of the different factors described below. The levels of ITSec to be considered in this context are technical, organizational, personnel, and process dimensions. If companies focus exclusively on one of these levels, it indicates that ITSec is not effectively implemented. Even the best and most cost-intensive processes and technologies in the field of cyberdefense do not provide sufficient protection if, e.g., the personnel dimension is disregarded, and thus awareness among employees is lacking.

The first reason for the differences in the ITSec situation that emerged from the interviews is the size of the company. While InfoSec officers are responsible for maintaining ITSec in medium to large companies, smaller companies cannot dedicate sufficient resources to fill such a position. In addition, SMEs predominantly lack awareness of the need to protect themselves

against potential cyber-attacks. However, while small businesses often believe that they are not a strategic target for cyber-attacks, the threat of randomized attacks is increasingly recognized. A further differentiation is needed regarding the industry in which the companies operate. The first example is provided by comparing banks and insurances, as described by an interviewee from a consulting company. Banks are far more advanced in their ITSec management than insurers due to legal and regulatory requirements. Banks adopted the principle of three lines of defense at least fourteen years ago. The first line of defense includes the IT in terms of processes and operations. The definition of specific requirements and procedural instructions is carried out in the context of the second line of defense, which is part of the compliance department and is implemented by security officers. Finally, the IT audit, which is mandatory for banks, is conducted. A corresponding regulatory framework for insurers was not adopted until 2019 with the Supervisory Requirements for IT in Insurance Undertakings (VAIT), which is why the gap to banks is considerable. The third differentiation made by the interview participants relates to the confrontation a company might already have had with cyber-attacks and the associated threat level. If companies, regardless of their size, have already experienced an attack and suffered resulting damages, they are subsequently better positioned in terms of their ITSec capabilities. Furthermore, the influence of management on the maturity of ITSec shouldn't be underestimated. According to experts, companies are in better position if the management recognizes the relevance and threat situation.

Security Incidents

There is widespread expert consensus that every company, regardless of its industry, is a potential target for cyber-attacks. Unless a company is affected by focused attacks, there is still a risk of damage from randomized attempts. Banks are seen as attractive due to their direct payment transactions. However, protection against cyber-attacks is particularly pronounced in this industry, which significantly increases the effort required by potential hackers to reach their goals. In contrast, in the case of so-called 'low-hanging fruits', the effort needed to penetrate the company's internal systems is comparatively low. In the opinion of some experts, insurance companies cannot be classified as strategic targets because they do not directly handle payments. Within the insurance corporation surveyed, there were no relevant security breaches during the last five years.

Depending on how the company is affected, the interviewees list various security incidents and classify them in terms of their relevance. In addition, the motivation behind an attack is listed as the reason for different attack scenarios, whereby a distinction can be made between standard

attacks and highly professionalized attacks. On the one hand, economic interests are predominant; on the other hand, the theft of know-how and personal identities is also an attractive target for hacker attacks on innovative companies. According to two interview participants, this kind of theft is particularly attractive from larger but still medium-sized companies that offer innovative solutions in their field of business in which they are world market leaders and can be referred to as 'hidden champions'.

According to the consulting companies' experience, their customers are continuously subject to attacks. In most cases, these are ransomware attacks, in which infrastructure systems are encrypted, and ransom is demanded. Ransomware attacks, along with phishing e-mails, are among the most commonly cited security threats. Another threat originates from using USB drives not belonging to the company, through which malware can infiltrate the company's internal systems. From the perspective of the interviewees working for the public sector, malware distributed via macros is also a typical attack scenario. Furthermore, the bombardment of interfaces with password requests is a sign of a cyber-incident, which can lead to a denial-of-service attack aimed at overloading the data network. Another common cause of intrusions by external hackers can be attributed to simple things, such as the careless use of passwords in the private and business environment.

Cyber-Risk Management

Concerning cyber-risk management, there is a mostly consistent view among the companies regarding its orientation. Individual interviewees mentioned an awareness shift to the point that risk management used to be perceived as having a complete preventive function, which precluded any need for reactive measures. In the meantime, this view has changed for the most part. Companies increasingly recognize that prevention alone is not enough and a fast response time is also required in order to minimize financial damage in the event of a cyber-incident. Nevertheless, prevention should make it as difficult as possible for attackers to penetrate the company's systems. Alongside the preventive and responsive aspects, detection should also be considered a component of cyber-risk management. As is the case with the ITSec situation, it is challenging for small and medium-sized companies to maintain prevention and detection mechanisms in their risk management, as the necessary measures are difficult to implement due to a lack of resources.

Information Security

Human, Organizational, Infrastructure, Technology, Law, and Regulation

Since the majority of the interviewees consider InfoSec as cybersecurity, the mentioned components of the term do not differ compared to the specified aspects of cybersecurity. On the one hand, InfoSec includes the objectives of protecting confidentiality, availability, and integrity. On the other hand, a three-pillar model is mentioned on which InfoSec is built. The first pillar of the concept is technology, which also includes the technical infrastructure in companies. Within the second pillar, specifications and procedural regulations are relevant. Finally, there is the third pillar, consisting of the human factor, which uses the technology and the processes of a company. Secure and informed users are, therefore, essential for maintaining InfoSec. The experts view regulatory requirements as a primary driver for improved company security.

Indicator-based IT Security

Objectives and Challenges

The small and medium-sized companies in our sample do not use key performance indicators (KPI), which is why we excluded this topic for experts belonging to this company category. The objective of using KPI in corporate consulting with a focus on banks and insurance companies is divided into three parts: The first objective is risk monitoring, for which so-called key risk indicators are used to provide an overview. The second objective is to meet regulatory requirements. The last objective is performance monitoring in a company in conjunction with the use of KPI. KPI also serve for internal and external benchmarking, which can stimulate the motivation to improve the company's situation. It is questionable, though, how comparable these KPI are in terms of an external benchmarking between different companies. The first problem already exists in the definition of an indicator. As long as, e.g., only serious security incidents are considered, the term 'serious' is a matter of interpretation if it is not subject to prior definition.

Another challenge in the use of metrics can be attributed to the definition of a threshold value. There is a need for continuous revision as to when a metric triggers in a crisis situation. Furthermore, it is relevant not only at which threshold a metric sets off but also whether this reaction is justified. The occurrence of false positives, whereby key indicators falsely state that they are above a defined threshold, is not unusual.

Examples of IT Security Indicators

The experts mentioned various examples of ITSec indicators that are either hypothetical or already in practical use. The respondent from a reinsurance company describes a hypothetical ITSec indicator. This metric produces a potential alarm signal based on a combination of the vulnerability management and corresponding Internet activities. For example, suppose a vulnerability is discovered in remote maintenance security, and at the same time, it is known on the Internet that such vulnerabilities are currently targeted. In that case, the company should be warned of this by the reaction of the associated key indicator. ITSec metrics already used in practice by consulting companies include, e.g., the number of unpatched systems, system up-to-dateness, number of unfixed vulnerabilities, time taken to update and fix vulnerabilities, number of security incidents/phishing attacks, and number of antivirus cases on user devices. A complementary approach is to use indicators to identify attack vectors and anomalies as well as to utilize them to differentiate between standard and highly sophisticated attacks.

Early Warning

Challenges

The most frequently cited challenge is due to the fact that attack scenarios change continuously, making EW considerably more difficult because it is not possible to draw on known patterns. Additionally, the monitoring of potential cyber-attacks generates a large number of events. Provided each event is classified as a security-relevant incident, the company's 'fire department' is busy for the most part with insignificant incidents, and the resulting volume of data is hardly manageable. In contrast, the participating insurance company is able to fully automatically filter potentially safety-relevant incidents from all events with a low false positive rate of below 20%. As a result, more than 70% of the detected incidents are safety-relevant. However, this approach is currently only feasible for very few companies. High false positive rates lead to the complete discontinuation of EWS. Altogether, the predictive capabilities of companies of all sizes are limited.

Early Warning Indicators

The essential characteristic of a potential EWI mentioned by the experts is its reliability. The indicator should be reliable in threat situations, keep false-positive rates to a minimum, and should be comprehensibly constructed to ensure that the evaluation of the results is clearly interpretable. A possible traffic lights system is also considered helpful for classifying security incidents using indicators. In this context, the definition of criticality within the different traffic

light phases is necessary to determine reaction periods. A sufficiently large database in relation to the size of the company is also required.

Differences exist between experts regarding the measures to be implemented in response to an EWI being triggered. On the one hand, an automatic reaction in the form of shutting down the affected systems or isolating them from the Internet is considered sensible. This should be followed by a manual evaluation of the incident by the IT department. Based on this automated response, an opportunity exists to stop an acute threat. On the other hand, the lack of willingness of the management to implement such a system and the frequency of false positive warnings, which is considered to be too high to justify an automated response. Furthermore, an attack probability given by the indicator would help to adapt potential security measures to the threat level. Finally, the question of what specifically constitutes an EWI is subject to consideration from various perspectives. The question about examples of potential EWI in the area of InfoSec could only be answered by some interviewees by means of hypothetical considerations. Monitoring network communication by employing key indicators is considered a potential EWI. One expert already classified an improved information supply regarding current cyber-attacks or the assessment of the 'information security readiness' as possible EWI.

Early Warning Systems

In connection with the research question concerning the status quo of EWS in the area of cybersecurity, the interviews revealed that companies have already been using intrusion detection and intrusion prevention systems for many years to support EW of cyber-attacks. Moreover, many experts are aware of the use of security information and event management (SIEM) solutions in this area. The implementation of SIEM solutions is an indicator of a company's high level of ITSec maturity, predominantly found in larger companies. The existence of EWS also is of major importance taking a risk management perspective. Modern risk management frameworks more or less have to be forward-looking (Jorion, 2009; Kunze et al., 2020). Rochette (2009), e.g., has stressed that risk managers should not just be waiting for bad things to happen. Most probably, this is especially true for the financial services industry (Rodriguez Gonzalez et al., 2018; Kunze et al., 2020).

In any case, there is no one perfect solution for EW of cyber-attacks. Instead, various processes and systems should be combined. In particular, the combination of SIEM solutions and threat intelligence currently provides the biggest potential for EW from the perspective of consulting companies. Within SIEM solutions, potential anomalies can be detected by monitoring and comparing events. This involves collecting, processing, and correlating numerous event data.

In addition, it is necessary to determine how companies should react to certain irregularities. SIEM solutions often fail in this context due to their complexity. Threat intelligence, in contrast, provides complementary data about what is gathered in the area of cyber-attacks at companies worldwide. Using a combination of information obtained from SIEM solutions and threat intelligence, it is possible to detect a threat at an early stage. One expert cited the 'Malware Information Sharing Platform' (MISP) as an example of a freely accessible threat intelligence platform used to share so-called 'Indicators of Compromise' (IoC). A complementary topic is Predictive Threat Intelligence, which is at the beginning of its development and, therefore, cannot be described in detail by the expert.

In response to the aforementioned challenges of continuously changing attack scenarios, experts are considering approaching EW from a different perspective. The focus of the forecast is not on potential cyber-attacks as such but on the general state of a company's IT hygiene. The main focus is on analyzing company-internal vulnerabilities that may present an attractive target in the future. An example are unpatched systems, which will require considerably less effort by an attacker than updated systems. This means that there is a certain probability that an attack will target these systems in the future. Based on the approach of using the state of the company's security situation for EW, the analysis of the maturity level of employee awareness is particularly significant.

Awareness

Investing in the most innovative and expensive technologies to defend oneself against cyber-attacks hardly improves the security situation unless the employees are able to recognize harmful anomalies. Ultimately, the people in an organization are the ones using the technology. They have a significant security impact simply as a result of their utilization. This insight is also highly relevant from the perspective of risk managers. Consequently, people should be the foundation of the security setup. Within a company, the security can only be as good as the weakest link, which usually is the employee. The relevance of the human factor in the security process is increasingly recognized by companies, which raises the willingness to invest in awareness campaigns and therefore constitutes a growth market. One of the reasons for the increasing awareness is that both companies and employees are sensitized by the broader media presence of cyber-incidents. Contrary to the growing awareness, many employees still act very naïve due to a lack of training.

Based on these findings, there is consensus among the participants that awareness should be given the highest priority in a security concept. In the case of attack scenarios such as CEO

fraud, ransomware, or phishing e-mails, the trigger is primarily the employee who carelessly opens such e-mails and enables the attacker to gain access to the company's internal network or to benefit financially. In this context, it is essential that employees are familiar with the reason for awareness measures and what can happen if the accompanying regulations are violated. They must be attentive, act cautiously and report conspicuous e-mails immediately to the appropriate department. In addition, the measures must reach the entire workforce, regardless of whether they are directly involved in the ITSec concept or not. According to the respondent from a public authority, the losses in companies with awareness measures are 50% to 70% lower than in companies where awareness is not addressed.

Examples of awareness concepts and associated challenges

A button in e-mail programs through which suspicious e-mails can be reported is an often-used and comparatively simple tool. The IT administrator must check these e-mails. In the case of malicious e-mails, an attack wave can be detected comparatively quickly, which in turn facilitates the warning of employees. In this context, employees must be educated on detecting anomalies in e-mails and the typical tricks of phishing e-mails. The mandatory use of Internet-based training is widespread in companies. In the IT services company, participation within the first four weeks after the program's publication is rewarded. Current trends show that gamified measures and the opportunity to win something increase the employees' motivation to participate.

The expert from an Institute for Corporate Security offers package solutions for SMEs, which include an awareness package with six modules. Central training subjects are InfoSec and data protection. Following this education, evaluations are conducted to determine if the previously taught content can be applied. Experience has shown that employees are more engaged with these topics after such training. In the medium-sized retail and service company, the annual employee dialog is used as an awareness measure. It is communicated verbally that tickets should be written in the event of anomalies. These tickets are then checked by the IT department. The reinsurance company surveyed has introduced a 'Cyber Awareness Month'. Throughout the month, employees were offered various opportunities for awareness training, primarily designed based on gamification. One example of this is the Cyber Escape Room. Employees can only get out of this room if they possess and correctly apply cybersecurity skills. The service provider for security awareness focuses on the effect of repetition and integration into the daily work routine in its awareness campaigns. A training plan includes recurring components, with individual sessions lasting only five minutes. Within the campaign goal in the corporate objectives also increases success.

Measurability of awareness measures

The most frequently mentioned survey methods for measuring awareness are questionnaires and performance reviews. Various aspects can be determined with the help of a questionnaire. One consideration by the experts is to record the level of investment made by companies in awareness measures, which in turn can provide information about their importance within the security concept. Other points of interest include the number of people responsible for cybersecurity and questions about training measures. Based on the answers to these questions, it is possible to determine a value that provides information about the maturity of awareness in a company. Success controls after a training generate information about the outcome and progress of the education. Internet-based training courses offer the opportunity to measure whether employees click on certain training options and how much time they spend on the course. Similar to a reward system, awarding achievable points can also provide information about the employee's learning status.

In addition to the surveys, the evaluation of phishing simulations is often mentioned as a means of assessing the effectiveness of awareness measures. This involves sending phishing e-mails to employees in order to determine how many react to the fakes subsequently. If this procedure is combined with training measures in which employees are informed about the characteristics of phishing e-mails, a comparative value can be determined. If more fake phishing e-mails were opened before the training measure than after the campaign, this would indicate higher awareness and, thus, a successful outcome. To ensure comparability, the phishing e-mails must be similarly well prepared, since otherwise, the results would be distorted by the divergent quality. Furthermore, awareness trends can be derived by repeating and comparing the results of such simulations. Despite various suggestions for the measurement of awareness, it is seen as a challenge since it concerns measuring a 'soft factor' or a behavior. The latter is often made difficult by the workers' council.

Future Prospects

The interviewees are convinced that the importance of cybersecurity and cyberdefense will increase in the years ahead. In addition, the topic of EW should increasingly be addressed in order to reduce or, at best, prevent damaging effects in the future. Overall, there is great potential for improvement among companies in the area of cybersecurity. However, this potential can only be harnessed if the topic of cybersecurity is transformed from a niche subject to a societal issue. Thus, companies should be aware that every digitization investment requires a cybersecurity investment, regardless of whether it concerns SMEs, public authorities, or large corporations.

Although it is only natural to lock doors and physically secure buildings, it is equally important to spread this understanding to the digital world.

An upcoming challenge in cybersecurity lies in the fact that, due to the increasing professionalism of cybercrime, there is an escalating need for corresponding specialists who are, however, not available on the market. In the future, hacking SMEs will hardly be a challenge for cybercriminals anymore. The value of information has already increased enormously in recent years. Another difficulty for companies is to stay up to date technologically and to raise sufficient financial resources for preventive measures. In addition to digitization aspects, insurance experts see the greatest opportunity of the current development in cyber-insurances. Cyber policies are becoming more attractive because there is no absolute protection against cyber-attacks, and an increasing number of companies will fall victim to such incidents. The market for cyber-insurances is seen as a large growth market (KPMG AG Wirtschaftsprüfungsgesellschaft 2017).

5. Discussion

Both the relevant literature and the expert interviews show that the terms InfoSec, cybersecurity, and ITSec are not uniformly defined. In particular, InfoSec is subject to highly complex interpretations due to its various components. However, since cybersecurity is also understood as a general term encompassing cybersecurity, InfoSec, and ComSec, we regard it in a more comprehensive way for reasons of simplicity (Singer & Friedman, 2014; Tirumala et al., 2019).

In terms of EWI in cybersecurity, Torres et al. (2006) introduce an indicator relating to the percentage of classified hardware and software. This indicator detects illegally downloaded software, verified licenses, and company-external devices. The interviewed experts described a similar approach with the ITSec indicators, where the number of unpatched systems, their up-to-dateness, and the number of unresolved vulnerabilities is recorded. Such indicators help to generate information that supports EW in the area of InfoSec, even if they are not designed for this purpose initially. Illegally downloaded software or using non-company hardware (e.g., USB sticks) can already enable malicious software to reach the company's internal IT systems. In addition, insufficient patch management and non-updated systems present vulnerabilities that facilitate system access for an attacker. If indicators provide information about the existence of the problems mentioned above, companies should regard this as an EW of an increased likelihood of attack and address the identified weaknesses as quickly as possible.

When a security incident occurs, response time is also crucial. Identified long response times are a warning that the extent of damages could be more significant than would be the case with faster response times. Additionally, the sum of identified potential threats, the sum of newly

identified threats, as well as the number of security incidents and phishing attacks provides information about the current threat level (Torres et al., 2006). With respect to the research question, it is evident that technical aspects, and general IT hygiene, should be mapped within the scope of potential EWI. The quality of an indicator depends on the underlying data basis. If only quantitative data is analyzed without including the necessary qualitative information, there is a risk of misinterpreting complex issues. In particular, causal relationships should be considered during interpretation to avoid ambiguities and to capture interdependencies. Moreover, the challenge of potential EWI is to adjust the threshold values and reduce false positives (Reichmann et al., 2017). Concerning the thresholds, it is conceivable that after exceeding a tolerance limit, staggered warning levels are issued depending on the severity of the breach (Disterer, 2015).

Furthermore, incorporating so-called ‘weak signals’ (Ansoff, 1975) offers the potential to warn of not yet apparent threats. The premise is that threats usually announce themselves through weak signals, which consequently provides the opportunity for early responses (Ansoff, 1975; Reinhardt, 1984; Zelewski, 1987). In order to identify such weak signals, utilizing external sources, such as the results of structured expert surveys and evaluations of current literature, is suitable (Krystek, 2006). It also seems sensible to establish cross-company collaborations to exchange knowledge and learn from divergent experiences as stimuli for further internal analyses (Disterer, 2015). Our qualitative study also highlights an improved news coverage of current cyber-attacks, which is primarily due to EWS such as threat intelligence.

A complementary approach is provided by IoC, which detect the presence of malicious software in IT systems and often are used as part of malware investigations (Catakoglu et al., 2016). IoC provide detailed information on illegal activities in the organization’s internal networks and systems. While the analysis of these indicators does not have EW properties by itself, an extension to the exchange of IoC data could generate this capability. An exemplary basis for such an exchange platform is the ‘Structured Threat Information Expression’ (STIX) (Rhoades, 2014; Fransen et al., 2015). A structured language for information on cyber threats facilitates the consistent exchange and analysis of these (Barnum, 2012). The potential of threat intelligence to provide EW of cyber-attacks via information sharing was already highlighted in our qualitative study. In recent years, cyber threat intelligence (CTI) gained importance in the context of InfoSec and is used increasingly in companies. The idea is to exchange evidence-based knowledge about known and emerging cyber threats. Building on this information, the opportunity, in turn, arises to decide on possible responses to such threats (Quiang et al., 2016).

Moreover, ensuring data quality is problematic. Whereas internal and public sources are available free of charge, commercial sources are based on fees. Compared to freely available threat information, the data quality of paid sources is more ensured (Amoroso, 2012). To facilitate and accelerate the exchange of information between companies, it needs to be structured and automated. In this regard, the STIX mentioned above is considered the standard for describing threat intelligence data. In addition, threat intelligence exchange platforms support an automated and accelerated exchange. An example of such a platform is the MISP (Fransen et al., 2015; Sillaber et al., 2016). The MISP grants the collection and sharing of critical IoC on targeted attacks and threat intelligence on vulnerabilities used for current cyber-attacks. Collaborative knowledge exchange thus enables the early detection of current threats (Wagner et al., 2016).

However, limitations are evident in the area of CTI and associated exchange platforms. As a consequence of innumerable threat information, there is a risk that the resulting amounts of data are hardly manageable. However, for an early detection of and timely response to potential cyber threats, threat information must be available as quickly as possible (Johnson et al., 2016; Sillaber et al., 2016). Even between existing exchange platforms, interoperability is impossible due to diverging standards. Furthermore, the quality of the threat data is often insufficient, resulting in the need for additional preparation measures. It also remains controversial which data can be shared in light of data protection regulations or which information is withheld for fear of reputational damages and thus cannot be used by other companies for EW (Barnum, 2012; Vázquez et al., 2012; Sillaber et al., 2016). Overall, CTI is at an early development stage, so further research and development is necessary (Oosthoek & Doerr, 2021).

Torres et al. (2006) also present potential EWI for companies in the context of the human factor. One indicator reflects the proportion of qualified personnel in the field of InfoSec. Based on a predefined critical threshold for the number of qualified personnel, falling below this value yields a potential EW signal. The average number of training hours received and the level of InfoSec awareness can be assessed via a survey and used as a potential EWI (Torres et al., 2006). Zerr (2007) takes a similar approach focusing on measuring security awareness, security literacy, and security behavior. These security indicators are also determined through surveys or observations and can provide EW of problems resulting from a lack of awareness (Zerr, 2007; Kritzinger & Smith, 2008; Zerr & Benner, 2017).

The aforementioned inclusion of qualitative information in EWI can be achieved, e.g., through the measurement of awareness measures. The most critical determinant influencing InfoSec is

the complex interaction of human and technical factors, which must be included in potential EWI. Employees are seen as the most vulnerable point since humans are the preferred target for attacks in comparison to technology (Eminağaoğlu et al., 2009; De Maggio et al., 2019). Awareness measures are essential in reducing threats caused by an employee's unintentional actions (Weber et al., 2019). To analyze the potential of employee awareness for EW, it is necessary to be able to measure and compare this factor and its variations. Conclusions can be drawn, from changes over time and the assessment of the InfoSec situation before and after security measures. This can also serve as an EWI (Torres et al., 2006; Zerr & Benner, 2017).

Limitations to conducting and evaluating a cross-industry qualitative study are founded mainly on the distinctive features of a qualitative methodology. One criticism is that the presented sample of interviewed cross-industry experts does not meet the requirement of representativeness. Consequently, the generalizability and objectivity of the findings are limited (Firestone, 1993; Miles & Hubermann, 1994; Lee & Baskerville, 2003; Groleau et al., 2009; Williams & Tsang, 2015). The results can only be regarded as a first trend in the context of a partial observation. This is especially true for the relevance of the discussed EWS and procedures, as well as the potential EWI derived from our findings, which are based on the maturity level of identified factors, such as awareness. In addition, this study focuses on the German market only. An increase in the sample size, as well as more comprehensive and international studies, seem necessary to obtain generalizable results. In addition, an industry-specific survey appears reasonable to be able to cover potentially unique characteristics of the companies. A supplementary quantitative study could also support the findings. Another limitation to the informational value of this study results from the assessment of the interviewees. As experts, they evaluate the topic on the basis of their professional experience. Therefore, their assessments are somewhat subjective.

6. Conclusion

The ongoing digitization and interconnection of the economy, coupled with the growing complexity of IT systems, show a rising vulnerability to cybercrime in recent years. As a result, the importance of cybersecurity in companies should also increase. Potential EWI provide a relevant approach to reducing damages resulting from cyber-attacks. On the one hand, such EW must be implemented on a technical level, but on the other hand, the significance of the human factor should not be disregarded. In particular, the human factor significantly influences the success of security measures. It should be included in EWI in addition to technical aspects and the current state of IT hygiene. By implementing and monitoring technical and organizational

protective measures and raising employee awareness, it should be as hard as possible for attackers to obtain a financial advantage at the expense of a company. Since achieving complete protection against cyber-attacks is impossible, cyber-insurances also assume significant importance.

References

Alavi R, Islam S, Mouratidis H (2014) A Conceptual Framework to Analyze Human Factors of Information Security Management System (ISMS) in Organizations, Tryfonas T, Askoxylakis I. (Eds.), *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014, Proceedings*, Springer, Cham, pp. 297–305.

Al-Darwish AI, Choe P (2019) A Framework of Information Security Integrated with Human Factors", Moallem A (Ed.), *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26-31, 2019, Proceedings*, Springer, Cham, pp. 217–229.

Allianz Global Corporate & Specialty SE (AGCS) (2023) Allianz Risk Barometer: Identifying the major business risks for 2023 – The most important corporate concerns for the year ahead, ranked by 2,712 risk management experts from a record 94 countries and territories., available at: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf (accessed 16 February 2023).

Almasizadeh J, and Azgomi MA (2014) Mean privacy: A metric for security of computer systems. *Computer Communications* 52: 47–59.

Alshaikh M, Ahmad A, Maynard SB, Chang S (2014) Towards a Taxonomy of Information Security Management Practices in Organisations, paper presented at the 25th Australasian Conference on Information Systems (ACIS), December 8–10, Auckland, New Zealand.

Althonayan A, Andronache A (2018) Shifting from Information Security towards a Cybersecurity Paradigm, paper presented at the 10th International Conference on Information Management and Engineering (ICIME), September 22–24, Manchester, United Kingdom.

Amoroso E (2012) *Cyber Attacks: Protecting National Infrastructure*, 1st ed., Elsevier, Amsterdam, Boston, MA, Heidelberg, London, New York, NY, Oxford, Paris, San Diego, CA, San Francisco, CA, Singapore, Sydney, Tokyo.

Anderson JM (2003) Why we need a new definition of information security. *Computers & Security* 22(4): 308–313.

Andrews M, Whittaker JA (2004) Computer Security. *IEEE Security & Privacy* 2(5): 68–71.

Ansoff HI (1975) Managing Strategic Surprise by Response to Weak Signals. *California Management Review* 18(2): 21–33.

Azmi R, Tibben W, Win KT (2018) Review of cybersecurity frameworks: context and shared concepts. *Journal of Cyber Policy* 3(2): 258–283.

Backhouse J, Dhillon G (1996) Structures of responsibility and security of information systems. *European Journal of Information Systems* 5(1): 2–9.

Barnum S (2012) Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™), working paper, The MITRE Corporation, Bedford, MA, McLean, VA, available at: https://www.mitre.org/sites/default/files/publications/stix.pdf (accessed 26 September 2022).

Bernsmed K, Tøndel IA (2013) Forewarned is Forearmed: Indicators for Evaluating Information Security Incident Management, paper presented at the 7th International Conference on IT Security Incident Management and IT Forensics (IMF), March 12–14, Nuremberg, Germany.

Beznosov K, Beznosova O (2007) On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security* 15(5): 420–431.

Bishop M (2003) What is computer security?. *IEEE Security & Privacy* 1(1): 67–69.

Bulgurcu B, Cavusoglu H, Benbasat I (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *Management Information Systems Quarterly* 34(3): 523–548.

Bowen GA (2008) Naturalistic inquiry and the saturation concept: a research note. *Qualitative Research* 8(1): 137–152.

Cadena A, Gualoto F, Fuertes W, Tello-Oquendo L, Andrade R, Tapia F, Torres J (2020) Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study, Rocha Á, Pereira RP (Eds.), *Developments and Advances in Defense and Security: Proceedings of MICRADS 2019*, Springer, Singapore, pp. 507–519.

Cains MG, Flora L, Taber D, King Z, Henshel DS (2022) Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis: An International Journal* 42(8): 1643–1669.

Catakoglu O, Balduzzi M, Balzarotti D (2016) Automatic extraction of indicators of compromise for web applications, paper presented at the 25th International Conference on World Wide Web (WWW), April 11–15, Montreal, Canada.

Chew E, Swanson M, Stine K, Bartol N, Brown A, Robinson W (2008) Performance Measurement Guide for Information Security, NIST Special Publication 800–55 Revision 1, National Institute of Standards and Technology (NIST), Gaithersburg, MD, available at: https://doi.org/10.6028/NIST.SP.800-55r1 (accessed 26 September 2022).

Choraś M, Kozik R, Renk R, Hołubowicz W (2015) A Practical Framework and Guidelines to Enhance Cyber Security and Privacy, Herrero, Á., Baruque, B., Sedano, J., Quintián, H., & Corchado, E. (Eds.), *International Joint Conference: CISIS'15 and ICEUTE'15*, Springer, Cham, Heidelberg, New York, NY, Dordrecht, London, pp. 485–495.

Collier ZA, Linkov I, Lambert JH (2013) Four domains of cybersecurity: a risk-based systems approach to cyber decisions. *Environment Systems and Decisions* 33(4): 469–470.

Connolly LY, Lang M, Gathegi J, Tygar DJ (2017) Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information and Computer Security* 25(2): 118–136.

Constantinou CS, Georgiou M, Perdikogianni M (2017) A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research* 17(5): 571–588.

Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville RL (2013) Future directions for behavioral information security research. *Computers & Security* 32: 90–101.

Da Veiga A, Eloff JHP (2007) An Information Security Governance Framework. *Information Systems Management*. 24(4): 361–372.

De Maggio MC, Mastrapasqua M, Tesei M, Chittaro A, Setola R (2019) How to Improve the Security Awareness in Complex Organizations. *European Journal for Security Research*. 4(1): 33–49.

De Paula R, Ding X, Dourish P, Nies K, Pillet B, Redmiles DF, Ren J, Rode JA, Silva Filho RS (2005) In the eye of the beholder: A visualization-based approach to information system security. *International Journal of Human-Computer Studies* 63(1–2): 5–24.

Dhillon G, Backhouse J (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal* 11(2): 127–153.

Diesch R, Krcmar H (2020) SoK: Linking Information Security Metrics to Management Success Factors, paper presented at the 15th International Conference on Availability, Reliability and Security (ARES), August 25–28, Virtual Event, Ireland.

Diesch R, Pfaff M, Krcmar H (2018) Prerequisite to Measure Information Security - A State of the Art Literature Review, paper presented at the 4th International Conference on Information Systems Security and Privacy (ICISSP), January 22–24, Funchal, Madeira, Portugal.

Disterer G (2015) Frühwarnsysteme für das IT-Sicherheits- und Risikomanagement, *HMD – Praxis der Wirtschaftsinformatik* 52(5): 790–801.

Dlamini MT, Eloff JHP, Eloff MM (2009) Information security: The moving target. *Computers & Security* 28(3–4): 189–198.

Dutta A, Roy R (2008) Dynamics of organizational information security. *System Dynamics Review* 24(3): 349–375.

Eisenhardt KM (1989) Building Theories from Case Study Research *The Academy of Management Review* 14(4) 532–550.

Eisenhardt KM, Graebner ME (2007) Theory Building From Cases: Opportunities And Challenges *Academy of Management Journal* 50(1): 25–32.

Eling M, McShane M, Nguyen T (2021) Cyber risk management: History and future research directions. *Risk Management and Insurance Review* 24(1): 93–125.

Eling M, Schnell W (2016) What do we know about cyber risk and cyber risk insurance?. *The Journal of Risk Finance* 17(5): 474–491.

Eloff MM, Von Solms SH (2000) Information Security Management: A Hierarchical Framework for Various Approaches. *Computers & Security* 19(3): 243–256.

Eminağaoğlu M, Uçar E, Eren Ş (2009) The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*. 14(4): 223–229.

Falco G, Eling M, Jablanski D, Weber M, Miller V, Gordon LA, Wang SS, Schmit J, Thomas R, Elvedi M, Maillart T, Donavan E, Dejung S, Durand E, Nutter F, Scheffer U, Arazi G, Ohana G, Lin H (2019) Cyber risk research impeded by disciplinary barriers. *Science* 366(6469): 1066–1069.

Fenz S (2010) Ontology-based Generation of IT-Security Metrics, paper presented at the 25th Annual ACM Symposium on Applied Computing (SAC), March 22–26, Sierre, Switzerland.

Finne T (2000) Information Systems Risk Management: Key Concepts and Business Processes. *Computers & Security* 19(3): 234–242.

Firestone WA (1993) Alternative arguments for generalizing from data as applied to qualitative research. *Educational Researcher* 22(4): 16–23.

Fransen F, Smulders A, Kerkdijk R (2015) Cyber security information exchange to gain insight into effects of cyber threats and incidents. *e & i Elektrotechnik und Informationstechnik* 132(2): 106–112.

Furnell SM, Clarke N (2012) Power to the people? The evolving recognition of human aspects of security. *Computers & Security* 31(8): 983–988.

Gioia DA, Corley KG, Hamilton AL (2013) Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology. *Organizational Research Methods* 16(1): 15–31.

Groleau D, Zelkowitz P, Cabral IE (2009) Enhancing Generalizability: Moving From an Intimate to a Political Voice. *Qualitative Health Research* 19(3): 416–426.

Guest G, Bunce A, Johnson L (2006) How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods* 18(1): 59–82.

Hajdarevic K, Allen P (2013) A new method for the identification of proactive information security management system metrics, paper presented at the 36th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), May 20–24, Opatija, Croatia.

Hennink MM, Kaiser BN, Marconi VC (2017) Code Saturation Versus Meaning Saturation: How Many Interviews Are Enough?. *Qualitative Health Research* 27(4): 591–608.

Hsieh H-F, Shannon SE (2005) Three Approaches to Qualitative Content Analysis. *Qualitative Health Research* 15(9): 1277–1288.

Johnson C, Badger L, Waltermire D, Snyder J, Skorupka C (2016) Guide to Cyber Threat Information Sharing, NIST Special Publication 800-150, National Institute of Standards and Technology (NIST), Gaithersburg, MD, available at: http://dx.doi.org/10.6028/NIST.SP.800-150 (accessed 26 September 2022).

Jorion P (2009) Risk Management Lessons from the Credit Crisis. *European Financial Management* 15(5): 923–933.

Kaczynski D, Salmona M, Smith T (2014) Qualitative research in finance. *Australian Journal of Management* 39(1): 127–135.

Kajava J, Savola R, Varonen R (2005) Weak Signals in Information Security Management, Hao Y, Liu J, Wang Y, Cheung Y-M, Yin H, Jiao L, Ma J, Jiao Y-C (Eds.), *Computational Intelligence and Security: International Conference, CIS 2005, Xi'an, China, December 15–19, 2005, Proceedings, Part II*, Springer, Berlin, Heidelberg, New York, NY, pp. 508–517.

Karyda M, Mitrou E, Quirchmayr G (2006) A framework for outsourcing IS/IT security services *Information Management & Computer Security* 14(5): 403–416.

Kotulic AG, Clark JG (2004) Why there aren't more information security research studies. *Information & Management* 41(5): 597–607.

KPMG AG Wirtschaftsprüfungsgesellschaft (2017) Neues Denken, Neues Handeln – Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber, available at: https://assets.kpmg.com/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf (accessed 26 September 2022).

Kraemer S, Carayon P (2003) A Human Factors Vulnerability Evaluation Method for Computer and Information Security. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* 47(12): 1389–1393.

Kraemer S, Carayon P, Clem J (2009) Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security* 28(7): 509–520.

Kritzinger E, Smith E (2008) Information security management: An information security retrieval and awareness model for industry. *Computers & Security* 27(5–6): 224–231.

Krystek U (2006) Frühwarnsysteme, Hutzschenreuter T, Griess-Nega T (Eds.), *Krisenmanagement: Grundlagen – Strategien – Instrumente*, Gabler, Wiesbaden, pp. 221–244.

Kuckartz U (2018) *Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung*, 4th ed., Beltz Juventa, Weinheim, Basel.

Kunze F, Basse T, Rodriguez Gonzalez M, Vornholz G (2020) Forward-looking financial risk management and the housing market in the United Kingdom: is there a role for sentiment indicators?. *The Journal of Risk Finance* 21(5): 659–678.

Landwehr CE (2001) Computer security, *International Journal of Information Security* 1(1): 3–13.

Lee AS, Baskerville RL (2003) Generalizing Generalizability in Information Systems Research. *Information Systems Research* 14(3): 221–243.

Loch KD, Carr HH (1991) Threats To Information System Security: An Organizational Perspective, paper presented at the 24th Hawaii International Conference on System Sciences (HICSS), January 8–11, Kauai, HI, USA.

Lundgren B, Möller N (2019) Defining Information Security. *Science and Engineering Ethics* 25(2): 419–441.

Mainelli M (2013) Learn from insurance: cyber bore. *The Journal of Risk Finance* 14(1): 100–102.

Marotta A, McShane M (2018) Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach. *Risk Management and Insurance Review* 21(3): 435–452.

Mayring P (2015) *Qualitative Inhaltsanalyse: Grundlagen und Techniken*, 12th ed., Beltz, Weinheim, Basel.

McLellan E, MacQueen KM, Neidig JL (2003) Beyond the Qualitative Interview: Data Preparation and Transcription. *Field Methods* 15(1): 63–84.

Miles MB, Huberman AM (1994) *Qualitative Data Analysis: An Expanded Sourcebook*, 2nd ed., SAGE Publications, Thousand Oaks, CA, London, New Delhi.

Monfelt Y, Pilemalm S, Hallberg J, Yngström L (2011) The 14-layered framework for including social and organizational aspects in security management. *Information Management & Computer Security* 19(2): 124–133.

Morse JM (1995) The Significance of Saturation. *Qualitative Health Research* 5(2): 147–149.

Morse JM (2015) "Data Were Saturated . . . ". *Qualitative Health Research* 25(5): 587–588.

Myers MD, Newman M (2007) The qualitative interview in IS research: Examining the craft. *Information and Organization* 17(1): 2–26.

Øien K, Massaiu S, Tinmannsvik RK, Størseth F (2010) Development of Early Warning Indicators based on Resilience Engineering, paper presented at the 10th International Probabilistic Safety Assessment & Management Conference (PSAM), June 7–11, Seattle, WA, USA.

Oosthoek K, Doerr C (2021) Cyber Threat Intelligence: A Product Without a Process?. *International Journal of Intelligence and Counter Intelligence* 34(2): 300–315.

Oppliger R (2007) IT Security: In Search of the Holy Grail. *Communications of the ACM* 50(2): 96–98.

Petrenko S (2018) *Big Data Technologies for Monitoring of Computer Security: A Case Study of the Russian Federation*, Springer, Cham.

Posthumus S, Von Solms R (2004) A framework for the governance of information security. *Computers & Security* 23(8): 638–646.

Qu SQ, Dumay J (2011) The qualitative research interview. *Qualitative Research in Accounting & Management* 8(3): 238–264.

Quiang L, Zeming Y, Baoxu L, Zhengwei J, Jian Y (2016) Framework of cyber attack attribution based on threat intelligence, Mitton N, Chaouchi H, Noel T, Watteyne T, Gabillon A, Capolsini P (Eds.), *Interoperability, Safety and Security in IoT: Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers*, Springer, Cham, pp. 92–103.

Ramaki AA, Atani RE (2016) A survey of IT early warning systems: architectures, challenges, and solutions. *Security and Communication Networks* 9(17): 4751–4776.

Ransbotham S, Mitra S (2009) Choice and Chance: A Conceptual Model of Paths to Information Security Compromise. *Information Systems Research* 20(1): 121–139.

Reichmann T, Kißler M, Baumöl U, (2017) *Controlling mit Kennzahlen: Die systemgestützte Controlling-Konzeption*, 9th ed., Vahlen, München.

Reinhardt WA (1984) An early warning system for strategic planning. *Long Range Planning* 17(5): 25–34.

Rhoades D (2014) Machine actionable indicators of compromise, paper presented at the 2014 International Carnahan Conference on Security Technology (ICCST), October 13–16, Rome, Italy.

Rochette M (2009) From risk management to ERM. *Journal of Risk Management in Financial Institutions* 2(4): 394–408.

Rodriguez Gonzalez M, Basse T, Kunze F, Vornholz G (2018) Early warning indicator systems for real estate investments: Empirical evidence and some thoughts from the perspective of financial risk management. *Zeitschrift für die gesamte Versicherungswissenschaft* 107(4): 387–403.

Rowley J (2012) Conducting research interviews. *Management Research Review* 35(3/4): 260–271.

Rudolph M, Schwarz R (2012) A Critical Survey of Security Indicator Approaches, paper presented at the 7th International Conference on Availability, Reliability and Security (ARES), August 20–24, Prague, Czech Republic.

Safa NS, Sookhak M, Von Solms R, Furnell SM, Ghani NA, Herawan T (2015) Information security conscious care behaviour formation in organizations. *Computers & Security* 53: 65–78.

Savola RM (2013) Quality of security metrics and measurements. *Computers & Security* 37: 78–90.

Scala NM, Reilly AC, Goethals PL, Cukier M (2019) Risk and the Five Hard Problems of Cybersecurity. *Risk Analysis: An International Journal* 39(10): 2119–2126.

Schatz D, Bashroush R, Wall J (2017) Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law* 12(2): 53–74.

Schuessler J (2007) An Information Systems Security Framework, paper presented at the 13th Americas Conference on Information Systems (AMCIS), August 9–12, Keystone, CO, USA.

Schultz E (2005) The human factor in security. *Computers & Security* 24(6): 425–426.

Schultze U, Avital M (2011) Designing interviews to generate rich data for information systems research. *Information and Organization* 21(1): 1–16.

Silic M, Back A (2014) Information security: Critical review and future directions for research. *Information Management & Computer Security* 22(3): 279–308.

Sillaber C, Sauerwein C, Mussmann A, Breu R (2016) Data Quality Challenges and Future Research Directions in Threat Intelligence Sharing Practice, paper presented at the 3rd ACM on Workshop on Information Sharing and Collaborative Security (WISCS), October 24, Vienna, Austria.

Singer PW, Friedman A (2014) *Cybersecurity and Cyberwar: What everyone needs to know*, Oxford University Press, Oxford, New York, NY, Auckland, Cape Town, Dares Salaam, Hong Kong, Karachi, Kuala Lumpur, Madrid, Melbourne, Mexico City, Nairobi, New Delhi, Shanghai, Taipei, Toronto.

Singh AN, Gupta MP, Ojha A (2014) Identifying factors of "organizational information security management". *Journal of Enterprise Information Management* 27(5): 644–667.

Siponen MT, Willison R (2007) A Critical Assessment of IS Security Research between 1990–2004, paper presented at the 15th European Conference on Information Systems (ECIS), June 7–9, St. Gallen, Switzerland.

Soomro ZA, Shah MH, Ahmed J (2016) Information security management needs more holistic approach: A literature review. *International Journal of Information Management* 36(2): 215–225.

Spears JL, Barki H (2010) User Participation in Information Systems Security Risk Management. *Management Information Systems Quarterly* 34(3): 503–522.

Spruit MEM, Looijen M (1996) IT security in Dutch practice. *Computers & Security* 15(2): 157–170.

Stewart H, Jürjens J (2017) Information security management and the human aspect in organizations. *Information and Computer Security* 25(5): 494–534.

Tirumala SS, Valluri MR, Babu GA (2019) A survey on cybersecurity awareness concerns, practices and conceptual measures, paper presented at the 9th International Conference on Computer Communication and Informatics (ICCCI), January 23–25, Coimbatore, India.

Torres JM, Sarriegi JM, Santos J, Serrano N (2006) Managing Information Systems Security: Critical Success Factors and Indicators to Measure Effectiveness, Katsikas SK, López J, Backes M, Gritzalis S, Preneel B (Eds.), *Information Security: 9th International Conference, ISC 2006, Samos Island, Greece, August 30–September 2, 2006, Proceedings*, Springer, Wiesbaden, pp. 530–545.

Trček D (2003) An integral framework for information systems security management. *Computers & Security* 22(4): 337–360.

Trček D, Trobec R, Pavešić N, Tasič JF (2007) Information systems security and human behavior. *Behaviour & Information Technology* 26(2): 113–118.

Tu CZ, Adkins JK, Zhao GY (2019) A Review of Information Systems Security Management: An Integrated Framework, paper presented at the 14th Annual Conference of the Midwest United States Association for Information Systems (MWAIS), May 21–22, Oshkosh, WI, USA.

Vázquez DF, Acosta OP, Spirito C, Brown S, Reid E (2012) Conceptual framework for cyber defense information sharing within trust relationships, paper presented at the 4th International Conference on Cyber Conflict (CYCON), June 5–8, Tallinn, Estonia.

Von Solms SH (2001) Information Security – A Multidimensional Discipline. *Computers & Security* 20(6): 504–508.

Von Solms SH (2010) The 5 Waves of Information Security – From Kristian Beckman to the Present, Rannenberg K, Varadharajan V, Weber C (Eds.), *Security and Privacy – Silver Linings in the Cloud: 25th IFIP TC-11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia, September 20-23, 2010, Proceedings*, Springer, Berlin, Heidelberg, pp. 1–8.

Von Solms R, Van Niekerk J (2013) From information security to cyber security. *Computers & Security* 38: 97-102.

Von Solms SH, Von Solms R (2004) The 10 deadly sins of information security management. *Computers & Security* 23(5): 371–376.

Wagner C, Dulaunoy A, Wagener G, Iklody A (2016) MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform, paper presented at the 3rd ACM on Workshop on Information Sharing and Collaborative Security (WISCS), October 24, Vienna, Austria.

Weber K, Schütz AE, Fertig T (2019) *Grundlagen und Anwendung von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren*, Springer, Wiesbaden.

Werlinger R, Hawkey K, Beznosov K (2009) An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security* 17(1): 4–19.

Williams JN, Tsang EW (2015). Classifying generalization: paradigm war or abuse of terminology?. *Journal of Information Technology* 30(1): 18–29.

Yasasin E, Schryen G (2015) Requirements for IT Security Metrics – An Argumentation Theory Based Approach, paper presented at the 23rd European Conference on Information Systems (ECIS), May 26–29, Münster, Germany.

Yildirim EY, Akalp G, Aytac S, Bayram N (2011) Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management* 31(4): 360–365.

Yin RK (2003) *Case Study Research: Design and Methods*, 3rd ed., SAGE Publications, Thousand Oaks, CA, London, New Delhi.

Young H, Van Vliet T, Van de Ven J, Jol S, Broekman C (2018) Understanding Human Factors in Cyber Security as a Dynamic System, Nicholson D (Ed.), *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17–21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA*, Springer, Cham, pp. 244–254.

Zafar H, Clark JG (2009) Current State of Information Security Research in IS. *Communications of the Association for Information Systems* 24: 557–596.

Zelewski S (1987) Frühwarnung und Künstliche Intelligenz: Möglichkeiten zur Fortentwicklung von Frühwarnsystemen durch Beiträge der Künstlichen Intelligenz. *Die Unternehmung* 41(4): 256–265.

Zerr K (2007) Security-Awareness-Monitoring – Ein sozialwissenschaftlicher Ansatz zur Messung des Sicherheitsbewusstseins bei Mitarbeitern. *Datenschutz und Datensicherheit – DuD* 31(7): 519–523.

Zerr K, Benner A (2017) Kennzahlen eines mitarbeiterorientierten Sicherheitsmanagements. *Datenschutz und Datensicherheit – DuD* 41(2): 80–87.

Modul 8

Silent Cyber-Risiken als Herausforderung für das Pricing und Underwriting in deutschen Versicherungsunternehmen – Ergebnisse einer qualitativ-empirischen Analyse

Theresa Eden

Dirk Wrede

Niclas Max Meyer

eingereicht bei:
Zeitschrift für die gesamte Versicherungswissenschaft

Silent Cyber-Risiken als Herausforderung für das Pricing und Underwriting in deutschen Versicherungsunternehmen – Ergebnisse einer qualitativ-empirischen Analyse

Theresa Eden, Dirk Wrede, Niclas Max Meyer

Theresa Eden (korrespondierende Autorin)
Wissenschaftliche Mitarbeiterin
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover
E-Mail: te@ivbl.uni-hannover.de

Dirk Wrede
Wissenschaftlicher Mitarbeiter
Gottfried Wilhelm Leibniz Universität Hannover
Institut für Versicherungsbetriebslehre
Otto-Brenner-Straße 7
D-30159 Hannover

Niclas Max Meyer
Gottfried Wilhelm Leibniz Universität Hannover
Welfengarten 1
D-30167 Hannover

Silent Cyber-Risiken als Herausforderung für das Pricing und Underwriting in deutschen Versicherungsunternehmen – Ergebnisse einer qualitativ-empirischen Analyse

Zusammenfassung Infolge der impliziten und unbeabsichtigten Mitversicherung von Cyber-Risiken in den traditionellen Policen, entstehen für Versicherungsunternehmen Silent Cyber-Risiken, die erhebliches Haftungspotenzial implizieren können. Insbesondere die Bewertung der Cyber-Risiken im Underwriting- und Pricing-Prozess gestalten sich für Versicherungsunternehmen als herausfordernd (Romanosky et al. 2019). Aufbauend auf den Erkenntnissen von Romanosky et al. (2019) und Nurse et al. (2020) zum Underwriting und Pricing von Cyber-Versicherungen, ist das Ziel dieses Forschungsbeitrags einen Überblick über den Umgang mit resultierenden Silent Cyber-Risiken zu geben. Aufgrund der Aktualität sowie unzureichenden wissenschaftlichen Betrachtung praktischer Erfahrungen im Umgang mit Silent Cyber-Risiken, werden 21 Interviews mit 24 Fachexperten aus der deutschen Versicherungswirtschaft durchgeführt. Die Ergebnisse zeigen, dass ein einheitlicher Umsetzungsstand zum Management von Silent Cyber-Risiken bei den Versicherungsunternehmen nicht erkennbar ist. Vielmehr sind in diesem Kontext Quantifizierungsschwierigkeiten der Risiken zu beobachten. Hieraus resultiert, dass Maßnahmen, wie ein präzises Underwriting und Pricing der Silent Cyber-Policen, derzeit schwer umsetzbar sind.

Silent Cyber Risks as a Challenge for Pricing and Underwriting in German Insurance Companies – Findings of a Qualitative-Empirical Analysis

Abstract As a result of the implicit and unintended co-insurance of cyber risks in traditional policies, silent cyber risks arise for insurance companies, which can imply significant liability potential. In particular, the evaluation of cyber risks in the underwriting and pricing process is relevant for insurance companies due to a lack of transparency (Romanosky et al. 2019). Following the findings of Romanosky et al. (2019) and Nurse et al. (2020) on the pricing and underwriting of cyber insurance, the aim of this research paper is to provide further insights into managing resulting silent cyber risks. Due to the topicality and insufficient scientific consideration of practical experiences in dealing with silent cyber risks, 21 interviews with 24 experts from the German insurance industry are conducted. The results show that a uniform implementation status for the management of silent cyber risks at the insurance companies is not recognizable. Rather, difficulties in quantifying can be observed in this context. Consequently, measures such as precise underwriting and pricing are currently difficult to implement.

1 Motivation und Problemstellung

Aktuell stellen Cyber-Risiken das größte globale Geschäftsrisiko für Unternehmen dar (Allianz Global Corporate & Specialty SE (AGCS) 2022). Infolge der voranschreitenden Digitalisierung ist ein signifikanter Anstieg der Häufigkeit, Komplexität und Intensität von Cyber-Angriffen zu beobachten (Chertoff 2008; Eling und Wirfs 2019). Aufgrund der aus Cyber-Angriffen resultierenden datenschutzbezogenen Pflicht- und Vertraulichkeitsverletzungen, Betriebsunterbrechungen und Datendiebstählen können hohe finanzielle Vermögensschäden sowie Reputationsverluste entstehen (Cavusoglu et al. 2004; Bulgurcu et al. 2010; Järveläinen 2013). So sind infolge gezielter Cyber-Angriffe jährlich insgesamt 102,9 Milliarden Euro Schaden für die deutsche Wirtschaft zu verzeichnen (Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) 2020).

In diesem Zusammenhang erscheint der Risikotransfer von Cyber-Bedrohungen über Versicherungslösungen als umfassende Absicherung der Schadenauswirkungen sinnvoll, wobei diese überwiegend auf die Absicherung finanzieller Schäden ausgerichtet sind (Böhme und Schwartz 2010; Haas und Hofmann 2014; Tonn et al. 2019). Neben Cyber-Versicherungen, die Cyber-Risiken affirmativ einschließen, können auch traditionelle Policen Versicherungsdeckungen für Cyber-Schäden beinhalten, sofern diese Verträge sie nicht explizit ausschließen oder aufgrund unklar formulierter Versicherungsbedingungen unbewusst einbeziehen. Diese Besonderheiten werden als Silent Cyber-Risiken bezeichnet (Bank of England Prudential Regulation Authority (PRA) 2017; European Insurance and Occupational Pensions Authority (EIOPA) 2022). Neben den mit Cyber-Risiken einhergehenden Herausforderungen, wie z. B. ein erhöhtes Änderungsrisiko und mögliche Kumulrisiken, stellen Silent Cyber-Risiken die Versicherungsunternehmen vor weitere Schwierigkeiten. Insbesondere die fehlende Eindeutigkeit der Versicherungsbedingungen und die damit einhergehende Identifizierung und Bewertung von Silent Cyber-Risiken ist aufgrund unzureichender Datenverfügbarkeit erschwert. In Bezug auf die fehlende Eindeutigkeit bei der Auslegung der Versicherungsbedingungen ist das Gerichtsverfahren zwischen Mondelez und der Zurich Versicherung ein prominentes Beispiel. Der Lebensmittelkonzern Mondelez International Inc. hatte bei der Zurich American Insurance Company eine All-Risk-Sachversicherungspolice abgeschlossen. Diese Versicherungsdeckung umfasste die Risiken von physischen Schäden am Eigentum des Unternehmens vollumfänglich ab, insbesondere den physischen Verlust oder die Beschädigung von elektronischen Daten, Programmen oder Software einschließlich materieller Verluste oder Schäden, die durch die böswillige Einbringung eines Maschinencodes oder Instruktionen verursacht werden. Zusätzlich waren in dieser Versi-

cherungspolice tatsächliche Verluste sowie zusätzliche Kosten, die infolge von Betriebsunterbrechungen entstehen und unmittelbar auf den Ausfall des IT-Systems zurückzuführen sind, versichert. Im Rahmen eines Cyber-Angriffs des Malware-Programms ‚NotPetya' wurden im Juni 2017 1.700 Server und 24.000 Laptops des Unternehmens Mondelez beschädigt, wodurch ein Schaden in Höhe von über 100 Millionen US-Dollar entstanden ist. Zurich verweigerte jedoch die Schadensdeckung und berief sich auf den Ausschluss derartiger Schäden, die durch kriegerische Handlung einer Regierung entstanden sind. Bisher ist keine endgültige Entscheidung in diesem Rechtsstreit getroffen worden (Ferland 2019; Chopra 2021; Tatar et al. 2021).

Auch wenn Silent Cyber-Risiken u. a. durch den Rechtsstreit zwischen Mondelez und Zurich sowohl in der Forschung als auch in der Praxis mehr Aufmerksamkeit erlangt haben, handelt es sich immer noch um ein vergleichsweise wenig erforschtes Themenfeld (Haas 2016; Eling 2018; Cartagena et al. 2020; Wrede et al. 2020). Insbesondere der unternehmensinterne Umgang mit derartigen Risiken findet in der wissenschaftlichen Literatur bisher kaum Beachtung. Im Schriftum werden im Zusammenhang mit Silent Cyber insbesondere Versicherungspolicen erforscht (Armbrüster 2020; Cartagena et al. 2020; Woods und Weinkle 2020; Wrede et al. 2020). Wrede et al. (2020) analysieren die allgemeinen Versicherungsbedingungen ausgewählter traditioneller Cyber-Policen und liefern einen ersten grundlegenden Überblick zum Umgang mit Silent Cyber-Deckungen in deutschen Versicherungsunternehmen im Unternehmenskontext. Aufgrund der hohen Relevanz der Thematik ist eine weiterführende Studie aus Perspektive der Versicherer sinnvoll. Romanosky et al. (2019) und Nurse et al. (2020) geben zudem einen Einblick in den Underwriting-Prozess sowie das Pricing von Cyber-Risiken im Cyber-Versicherungsgeschäft. Die Analyse des Pricings von Silent Cyber-Risiken findet allerdings nach unserem Kenntnisstand in der Forschung bisher keine Anwendung. Ziel dieses Beitrages ist es das Pricing und Underwriting sowie das Risikomanagement von Silent Cyber-Risiken in Versicherungsunternehmen zu untersuchen und dabei einen Beitrag zur Schließung der Forschungslücke für den deutschen Markt zu liefern. Folgende Forschungsfragen werden in diesem Zusammenhang analysiert:

1. Wie ist der Status quo der Wahrnehmung von Silent Cyber-Risiken in der deutschen Versicherungswirtschaft?
2. Wie werden die Gefährdungspotenziale von Silent Cyber-Risiken eingeschätzt und welche Maßnahmen ergreifen die Versicherer im Umgang mit Silent Cyber-Risiken hinsichtlich des Underwritings und Pricings?
3. Wie schätzt die Versicherungswirtschaft die zukünftige Entwicklung der Silent Cyber-Problematik ein?

Zur Beantwortung der oben genannten Forschungsfragen ist der vorliegende Artikel wie folgt strukturiert: Zunächst erfolgt in Abschn. 2 die Beschreibung des aktuellen Forschungsstandes der Ausgestaltung von Cyber-Deckungen in traditionellen Versicherungspolicen und der Silent Cyber-Risiken. Abschn. 3 dient der Beschreibung von Forschungsdesign sowie Vorgehensweise bei der Datenerhebung und -auswertung. In Abschn. 4 werden die Ergebnisse der analysierten Experteninterviews dargestellt. Eine entsprechende Diskussion der herausgearbeiteten Ergebnisse ist Gegenstand des Abschn. 5. In Abschn. 6 finden sich eine kurze Zusammenfassung der Ergebnisse und einige Schlussfolgerungen.

2 Stand der Forschung

Infolge von Cyber-Angriffen sind Unternehmen vielfältigen Schadensszenarien ausgesetzt. Diese können aufgrund von datenschutzbezogenen Pflicht- und Vertraulichkeitsverletzungen, Betriebsunterbrechungen, Datendiebstählen in hohen finanziellen Vermögensschäden sowie auch Reputationsverlusten resultieren (Cavusoglu et al. 2004; Smith 2004; Salmela 2008; Bulgurcu et al. 2010; Järveläinen 2013;). Ferner sind die Zerstörung von Software und IT-Systemen (Jouini et al. 2014; Romanosky 2016; Amin 2019) und der Ausfall oder die Zerstörung von Produktionseinrichtungen mögliche Folgen von Cyber-Angriffen (Lathrop und Stanisz 2016; Elhabashy 2019). In diesem Zusammenhang führen Cyber-Angriffe jedoch nicht ausschließlich zu finanziellen Verlusten (Gandhi et al. 2011; Jouini et al. 2014), sondern zugleich vermehrt zu physischen Schäden, wie Sach- und Personenschäden (Zelle und Whitehead 2014; Lathrop und Stanisz 2016; Amin 2019).

Zur Absicherung derartiger Cyber-Risiken stellen Versicherungslösungen eine Möglichkeit des Risikotransfers dar (Böhme und Kataria 2006; Faisst et al. 2007; Bandyopadhyay und Shidore 2011; Tosh et al. 2017; Tonn et al. 2019). Konkret lassen sich auf dem Versicherungsmarkt drei Deckungskonzepte differenzieren: Stand-Alone-Cyber-Policen, Cyber-Deckungen in einem Versicherungsbündel (Add-on-Police) und Silent Cyber-Deckungen (Coburn et al. 2016; Organisation for Economic Cooperation and Development (OECD) 2017; EIOPA 2018). Die Literatur zeigt, dass sich Stand-Alone-Cyber-Policen nicht als ganzheitliche Lösung am Markt etabliert haben. Gründe dafür sind sowohl auf die Nachfrage- als auch auf die Angebotsseite zurückzuführen (Wrede et al. 2020). Als Marktbarriere für das Angebot von Cyber-Versicherungen werden in der Literatur vielfach bestehende Informationsasymmetrien sowie stark korrelierte Schadenspotenziale von Cyber-Risiken genannt (Young et al. 2016; Baban et al. 2017a, b; Bodin et al. 2018). Auch die hohe Dynamik von Cyber-Bedrohungen wird als Herausforde-

rung hervorgehoben (Zhao et al. 2013). Zudem sind fehlende historische Daten zu den Schadenhäufigkeiten und -ausmaßen von Cyber-Vorfällen sowie mangelnde Erfahrungswerte bei der Schadenregulierung als weitere Ursache zu nennen (Baban et al. 2017a, b; Strupczewski 2017; Siegel et al. 2018). Nachfrageseitig sind die in Unternehmen bestehenden Informationsdefizite über angebotene Cyber-Versicherungsprodukte und deren Deckungsumfang wie auch die unzureichende Wahrnehmung von Cyber-Risiken als potenzielle Bedrohung anzuführen (Moore 2010; Baban et al. 2017a; Meland et al. 2017; Eling 2018). Zudem zeigen Strupczewski und Thlon (2021), dass die Unternehmensgröße als ein Indikator für den Abschluss einer Cyber-Versicherung herangezogen werden kann. Insgesamt werden bei Cyber-Versicherungsprodukten die Ergänzung einer Cyber-Deckungskomponente (Add-on-Police) in bestehenden Versicherungsprodukten gegenüber einer eigenständigen Cyber-Police präferiert (Middleton und Kazamia 2016). In Bezug auf Cyber-Deckungen in einem Versicherungsbündel zeigen Haas und Hofmann (2014) wie auch Siegel et al. (2018), dass derartige Cyber-Produkte von den Kunden zwar gewünscht sind, jedoch die resultierende Komplexität der Produkte eine Herausforderung für die Nachvollziehbarkeit darstellt.

Cyber-Versicherungen umfassen jedoch vornehmlich die Deckung finanzieller Schäden (Böhme und Schwartz 2010; Haas und Hofmann 2014; Castriotta 2022). Ein Versicherungsschutz für Sach- und Personenschäden infolge von Cyber-Angriffen besteht zumeist nicht (Lathrop und Stanisz 2016; Franke 2017). Derartige Schäden sind in traditionellen Policen ausschließlich dann enthalten, sofern kein expliziter Ausschluss besteht oder Versicherungsbedingungen einer unklaren Formulierung unterliegen (Marotta et al. 2015, 2017). Bisweilen umfassen am Markt bestehende Deckungskonzepte für Cyber-Risiken häufig unzureichende Beschreibungen des Leistungsumfangs sowie unpräzise Formulierungen der Versicherungsbedingungen (Baer 2003; Meland et al. 2017; Marotta et al. 2015, 2017). Zur Analyse der Deckungskonzepte und Vertragsbedingungen von Versicherungslösungen für Cyber-Risiken in den traditionellen Versicherungspolicen existieren in der wissenschaftlichen Literatur unterschiedliche Veröffentlichungen. Eine Übersicht der Forschungsarbeiten zur Ausgestaltung von Cyber-Deckungen in Versicherungsprodukten zeigt Tabelle 1.

Tab. 1 Übersicht des aktuellen Forschungsstandes

Veröffentlichung	Datengrundlage	Wesentliche Ergebnisse
Jerry II und Mekel (2001): Cybercoverage for Cyber-Risks: An Overview of Insurers' Responses to the Perils of E-Commerce	• Deckungskonzepte für Cyber-Risiken in einzelnen klassischen Versicherungen wie z. B. Haftpflichtversicherungen	• Unternehmen können nicht davon ausgehen, dass Cyber-Risiken über traditionelle Policen abgedeckt sind • Versicherungsschutz sollte hinsichtlich potenzieller Lücken analysiert werden
Kesan et al. (2005): Cyberinsurance as a Market-based Solution to the Problem of Cybersecurity – A Case Study	• Leistungsumfang der Deckungs-konzepte von Cyber-Policen im Allgemeinen	• Probleme der Adversen Selektion und Moral Hazard können zu Marktversagen führen • Soziale Wohlfahrtsgewinne könnten über Cyber-Versicherungsbranche erzielt werden
Baer und Parkinson (2007): Cyberinsurance in IT Security Management	• Deckungskonzepte von Cyber-Versicherungen	• Absicherung von Schäden durch Betriebsunterbrechungen in Stand-Alone-Deckungen aller führenden Versicherer
Coburn et al. (2016): Managing Cyber Insurance Accumulation Risk	• Deckungskonzepte und Produktkomponenten von 26 Cyber-Versicherungen im britischen Versicherungsmarkt	• Unterschiedlicher Versicherungsschutz innerhalb der Policen • Kein Versicherungsprodukt mit gleicher Anzahl und Art von Deckungen
Haas (2016): Management von Cyber-Risiken und Möglichkeiten des Risikotransfers: eine ökonomische und versicherungstechnische Analyse	• Zehn Cyber-Deckungskonzepte in traditionellen Versicherungsprodukten • Musterbedingungen des Gesamtverbandes der Deutschen Versicherungswirtschaft e.V. (GDV) für Betriebshaftpflicht-, Elektronik-, Sach-, Betriebsunterbrechungs- sowie Daten- und Softwareversicherung	• Ergänzende Policen unterliegen gegenüber Stand-Alone-Deckungen restriktiveren Auslegungen der Versicherungsbedingungen
Marotta et al. (2017): Cyber-Insurance Survey sowie Marotta et al. (2015): A Survey on Cyber-Insurance. Technical Report IIT TR-17/2015	• Versicherungsdeckungen von 14 Cyber-Policen international tätiger Versicherer	• Eigenschadendeckung beinhaltet Verlust und Beschädigung digitaler Vermögenswerte, Schäden durch Betriebsunterbrechungen, Cyber-Erpressungen sowie Diebstahl von Geld und digitalen Vermögenswerten
Woods et al. (2017): Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms	• 24 Cyber-Versicherungsantragsformulare in Bezug auf Risikofragebögen verschiedener Cyber-Policen im US-amerikanischen und britischen Versicherungsmarkt	• Bis 2012 wurden Cyber-Versicherungspolicen ohne Kriegsausschlussklausel angeboten
Nieuwesteeg und de Waard (2018): The Law & Economics of Cyber Insurance Contracts: A Case Study	• Deckungskonzepte von Cyber-Versicherungen, Preisen und Marktteilnehmern im niederländischen Versicherungsmarkt	• Versicherer verfolgen zwei Optionen: Marktdurchdringung mit leicht zugänglichen und attraktiven Versicherungsprodukten oder Strategie der umfangreichen Absicherung korrelierter Risiken

Franke (2018): Cyber Insurance against Electronic Payment Service Outages: A Document Study of Terms and Conditions from Electronic Payment Service Providers and Insurance Companies	• Deckungskonzepte von fünf Cyber-Versicherungen • Geschäftsbedingungen von drei elektronischen Zahlungsverkehrsdienstleistern hinsichtlich der Absicherung von Ausfällen, wie z. B. die Unterbrechung Zahlungsdienstes	• Cyber-Versicherungen bieten Schutz vor Ausfällen elektronischer Zahlungsdienste • Versicherungsdeckung variiert zwischen angebotenen Versicherungsoptionen
Talesh (2018): Data Breach, Privacy, and Cyber Insurance: How Insurance Companies act as "Compliance Managers" for Businesses	• Angebot von Risikomanagement-Dienstleistungen in über 30 Cyber-Versicherungsprodukten	• Versicherer agieren als Compliance-Manager • Versicherer bieten Risikomanagementdienste an, die Einfluss auf die Einhaltung des Datenschutzes innerhalb der Unternehmen ausüben
Hunt (2019): The Internet of Buildings: Insurance of Cyber Risks for Commercial Real Estate	• Berücksichtigung von Cyber-Deckungen in ausgewählten traditionellen Versicherungsprodukten (z. B. Allgefahrenversicherung und allgemeine Haftpflichtversicherung) für den Bereich der Gewebeimmobilienwirtschaft im US-amerikanischen Versicherungsmarkt	• Silent Cyber-Risiken sind oder werden zukünftig aus betrachteten Policen ausgeschlossen • Auch Cyber-Policen bieten keinen vollumfänglichen Schutz vor genannten Risiken
Romanosky et al. (2019): Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?	• Deckungskonzepte von über 200 Cyber-Policen im US-amerikanischen Versicherungsmarkt	• Insgesamt sind die Versicherungsdeckungen sehr ähnlich • Ausschlüsse variieren jedoch stärker • Preisgestaltung der Prämien hinsichtlich der Messgrößen und Gleichungen sind sehr unterschiedlich • Keine verbindliche Quelle für die Bewertung von Cyber-Risiken
Woods und Weinkle (2020): Insurance Defnitions of Cyber War	• 56 Cyber-Policen im US-amerikanischen Versicherungsmarkt	• Bis 2012 wurden Cyber-Versicherungspolicen ohne Kriegsausschlussklausel angeboten • 41 der betrachteten Policen enthielten Kriegsausschlussklausel • Versicherer sind gezwungen Versicherungsausschlüsse eindeutig zu beschreiben und klar zu formulieren
Wrede et al. (2020): Affirmative and Silent Cyber Coverage in Traditional Insurance Policies: Qualitative Content Analysis of Selected Insurance Products from the German Insurance Market	• 43 allgemeine Versicherungsbedingungen traditioneller Versicherungspolicen ausgewählter Produktsparten hinsichtlich der in den Verträgen enthaltenen impliziten und expliziten Cyber-Deckungen sowie den hieraus entstehenden Silent-Cyber-Risiken im deutschen Versicherungsmarkt	• Aus derzeitigen Ausgestaltungen der Versicherungsbedingungen einzelner Sparten ergeben sich erhebliche Silent Cyber-Deckungen

French (2021): Five Approaches to Insuring Cyber Risks	• Status quo des Versicherungsmarktes und verschiedene Deckungskonzepte zur Versicherung von Cyber-Risiken	• Fünf Ansätze zur Versicherung von Cyber-Risiken: Selbstlösung des Marktes, Absicherung von Cyber-Risiken im Rahmen von gewerblichen Haftpflicht- und Sachversicherungspolicen, Einführung einheitlicher eigenständiger Haftpflicht- und Sachversicherungen für Cyber-Risiken, Bundesregierung als Exzedentenversicherer oder Rückversicherer von Cyber-Risiken, All-Risk Private-Public Ansatz
Baker und Shortland (2022): Insurance and Enterprise: Cyber Insurance for Ransomware	• 25 Interviews mit Fachexperten aus den Bereichen Versicherung, Recht, Sicherheit und Politik zur Versicherungsdeckung von Cyber-Versicherung	• Cyber-Versicherungen haben Lösungen entwickelt, um die befallenen IT-Systeme schnell wiederherzustellen aber auch die Haftung einzuschränken • Sicherheitsentscheidungen sind weitestgehend den Versicherten überlassen
Charalambous et al. (2022): Analyzing Coverages of Cyber Insurance Policies Using Ontology	• Analyse von Versicherungsverträgen bekannter Versicherungsunternehmen wie AXA, Vero, RSA, Allianz, Tokio Marine, Travelers, Philadelphia, Delta, Hartford, Zurich und Hiscox	• Methodik und einen Prototyp eines Systems, das potenzielle Versicherungskunden dabei unterstützt Verträge auf der Grundlage einer vordefinierten Ontologie mit Begrifflichkeiten zur Cyberversicherung zu vergleichen

Die Übersicht verdeutlicht, dass sich bisherige Forschungsarbeiten primär auf den Einschluss der Policen in traditionelle Versicherungssparten mit länderspezifischen Schwerpunkten fokussieren (Hunt 2019; Romanosky 2019; Woods und Weinkle 2020). Diese Erkenntnisse lassen sich aufgrund der Besonderheiten des bspw. amerikanischen Versicherungsmarktes und Rechtssystem jedoch nicht auf den deutschen Markt übertragen. Wrede et al. (2020) liefern in diesem Kontext die erste systematische Analyse von traditionellen Versicherungsprodukten hinsichtlich der in den Verträgen enthaltenen impliziten und expliziten Cyber-Deckungen sowie den hieraus entstehenden Silent Cyber-Risiken für den deutschen Versicherungsmarkt. Im Folgenden ist es das Ziel die Erkenntnisse von Wrede et al. (2020) um die Analyse des Pricings und Underwritings sowie das Risikomanagement von Silent Cyber-Risiken in deutschen Versicherungsunternehmen zu erweitern.

3 Methodik und Daten

Aufgrund des Mangels an kontextspezifischen Forschungserkenntnissen über den Umgang mit dem Pricing und Underwriting von Silent Cyber-Deckungen, wie auch des explorativen Charakters der Fragestellungen, wurde ein qualitativ-empirischer Forschungsansatz in Form von

qualitativen Expertenbefragungen gewählt (Mayring 2015). Das Ziel dabei ist es, durch eine systematische Auswertung des erhobenen praxisbasierten Erfahrungswissens der befragten Experten neue Erkenntnisse zu generieren (Schnell et al. 2011). Da sich die mündliche Befragung mittels teilstandardisierter Interviews zur Ermittlung von Expertenwissen in der qualitativen Forschung etabliert hat, wurde diese Befragungsform gewählt und mithilfe eines offenen Leitfadens durchgeführt (Myers und Newman 2007; Schultze und Avital 2011). Auf die Durchführung eines Pretests konnte aufgrund der Möglichkeit einer inhaltlichen Anpassung und Ergänzung des Interviewleitfadens nach Erhebung der ersten Interviews verzichtet werden (Gläser und Laudel 2010). Die leitfadengestützten Experteninterviews wurden von Anfang 2020 bis Mitte 2021 durchgeführt. Insgesamt fanden 21 Interviews mit 24 Fachexperten aus der deutschen Versicherungswirtschaft statt, die aufgrund ihres umfassenden praxisbasierten Handlungs- und Erfahrungswissens in dem Bereich Cyber-Risiken und der Ausgestaltung entsprechender Versicherungsdeckungen befragt wurden. Die Kontaktierung der potentiellen Interviewpartner erfolgte anhand der getroffenen Vorüberlegungen hinsichtlich der aufgeworfenen Fragestellungen. Ergänzend hierzu wurde zur Gewinnung von Umfrageteilnehmern das Prinzip des Snowball-Sampling angewandt (Yin 2003; Rowley 2012; Bogner et al. 2014). Eine Übersicht über die befragten Experten zeigt Tabelle 2.

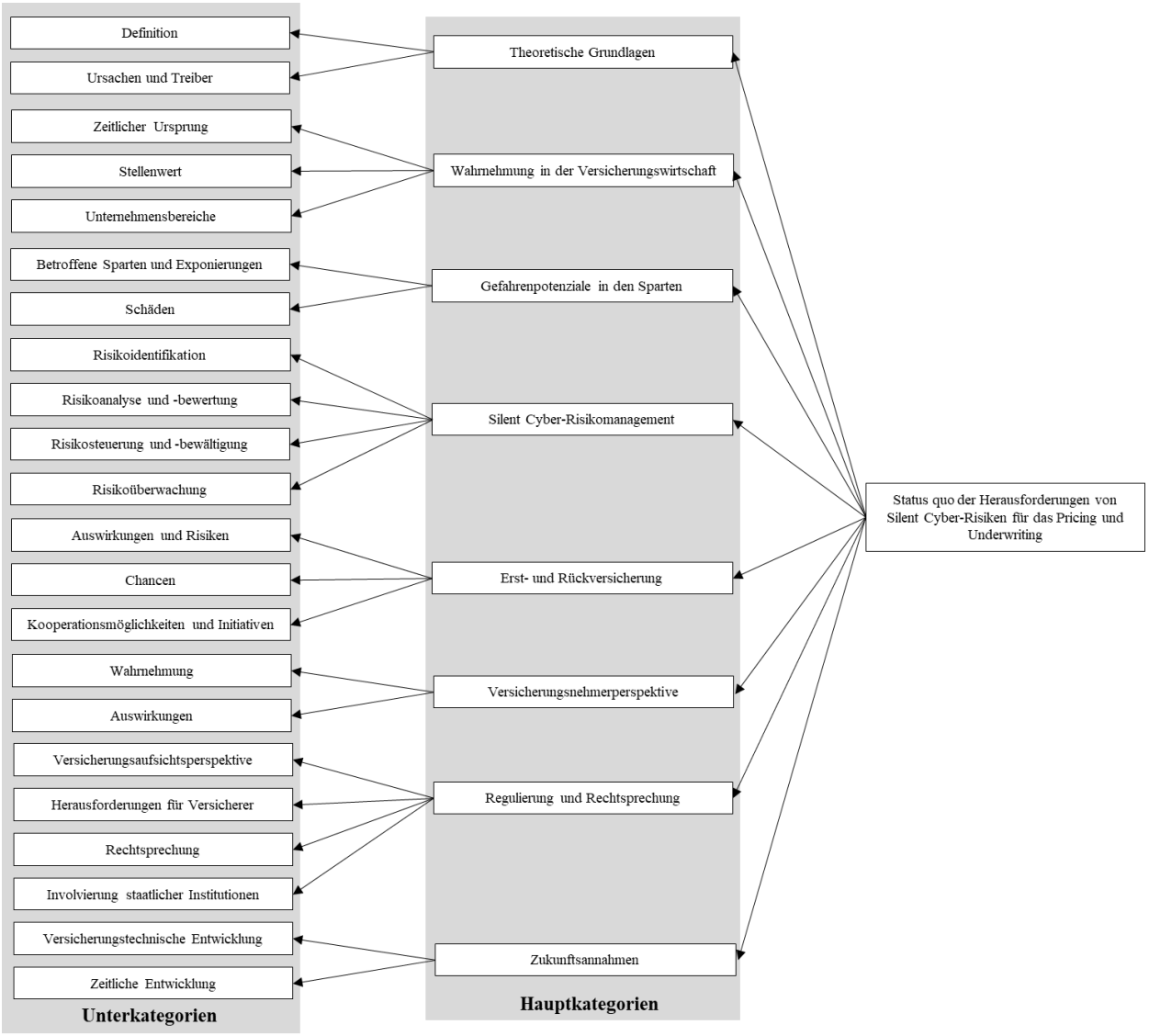
Tab 2. Übersicht Teilnehmenden der Expertenbefragung

Interview	Experte	Unternehmensbranche	Position/Bereich
1	A	Erstversicherer	Leiter Underwriting
2	B	Erstversicherer	Leiter Management
3	C	Erstversicherer	Mitarbeiter Finanzabteilung
4	D	Erstversicherer	Mitarbeiter Technische Versicherung
5	E	Rückversicherer	Senior Corporate Underwriter
	F	Rückversicherer	Senior Underwriter Unfallversicherung
6	G	Rückversicherer	Underwriter Rückversicherung Nichtleben
7	H	Rückversicherer	Leiter Property & Engineering
8	I	Ruckversicherer	Senior Underwriter
9	J	Interessenverband	Leiter Haftpflicht und Kreditversicherung
10	K	Versicherungsmakler	Spezialist Cyber Versicherung
11	L	Versicherungsmakler	Geschäftsführungsmitglied
12	M	Versicherungsmakler	Leiter Produktbereich Cyber-Risk
13	N	Rückversicherer	Mitarbeiter Underwriting
14	O	Rückversicherer/ Rückversicherungsmakler	Mitarbeiter Underwriting
	P	Rückversicherer/ Rückversicherungsmakler	Mitarbeiter Underwriting
15	Q	Rückversicherer	Senior Underwriter Cyber-Risk
16	R	Erstversicherer	Mitarbeiter Underwriting
	S	Erstversicherer	Abteilungsleiter Underwriting
17	T	Rückversicherer	Abteilungsleiter Spartenmanagement
18	U	Erstversicherer	Senior Underwriter Cyber-Risk
19	V	Erstversicherer	Projektleiter Silent Cyber
20	W	Erstversicherer	Abteilungsleiter Produkte & Recht
21	X	Interessenverband	Abteilungsleiter

Die Interviews dauerten zwischen 30 und 100 Minuten, wobei die durchschnittliche Interviewdauer 58 Minuten betrug. Die Gesprächsinhalte wurden aufgezeichnet und vollumfänglich transkribiert. Im Anschluss an die Transkription erfolgte die inhaltliche Überprüfung der angefertigten Transkripte auf Vollständigkeit und Korrektheit (McLellan et al. 2003). Die 21 Experteninterviews bieten somit eine zulässige Ausgangsbasis für die qualitative Untersuchung und erlauben die Ableitung von Tendenzen (Hartley 1994; Merkens 1997). Die Auswertung erfolgt nach dem Ablaufmodell der inhaltlich strukturierenden qualitativen Inhaltsanalyse nach Kuckartz (2018), welche eine systematische und regelgeleitete Auswertung des Datenmaterials ermöglicht. Zur systematischen Auswertung wurde die aktuelle Version der Datenanalysesoftware MAXQDA genutzt. Die Ableitung eines auf den Forschungsfragen basierenden Kategoriensystems ist charakteristisch für die qualitative Inhaltsanalyse (Harwood und Garry 2003; Graneheim und Lundman 2004). Die Entwicklung des Kategoriensystems mit Ankerbeispielen erfolgte deduktiv-induktiv (Gläser und Laudel 2010; Mayring 2015). Mögliche Kategorien wurden deduktiv aus dem Interviewleitfaden und weitere Kategorien induktiv aus dem Material erschlossen. Hierbei wurden die deduktiven Kategorien nochmals mittels der angefertigten Transkripte überprüft und zusätzlich das Material auf induktive Kategorien untersucht. Daran anknüpfend erfolgte anhand des Datenmaterials die induktive Bildung von Unterkategorien. Abschließend fand eine nochmalige Überprüfung des gesamten Datenmaterials einschließlich einer Anpassung und Ergänzung des formulierten Kategoriensystems statt (Hsieh und Shannon 2005).

Zur Gewährleistung der Qualität der Kodierung haben zwei Forscher die Entwicklung der Kodes unabhängig voneinander durchgeführt (Guest et al. 2006). Das entwickelte inhaltsanalytische Kategoriensystem stellte die Basis für die anschließende qualitative Auswertung dar und ist in Abbildung 1 dargestellt.

Abb. 1 Kategoriensystem



Das final konstruierte Kategoriensystem beinhaltet 8 Hauptkategorien und weitere 22 Unterkategorien, welches als Grundlage für die sich anschließende Ergebnisdarstellung dient. Die Darstellung der Ergebnisse erfolgt im nachfolgenden Abschnitt entsprechend der Empfehlungen von Yin (2003) auf weitgehend aggregierter Ebene.

4 Ausgewählte Ergebnisse der Studie

4.1 Wahrnehmung in der Versicherungswirtschaft und Gefahrenpotenziale in den Sparten

Die Mehrheit der Unternehmen in der Versicherungswirtschaft beschäftigt sich seit drei bis vier Jahren mit Silent Cyber-Risiken. Auffällig dabei ist, dass sich vornehmlich Rückversicherer bereits länger mit dem Themenfeld befassen. Hinzukommend unterliegt die Einschätzung der

thematischen Relevanz von Silent Cyber-Risiken bei den befragten Unternehmen einer unterschiedlichen Bewertung. Während einige Versicherer Silent Cyber-Risiken eine geringe Bedeutung zuschreiben, verfügt dieses Themengebiet für andere Unternehmen über eine hohe Priorität innerhalb der Risikobewertung. Als Grund dafür lassen sich unterschiedliche Aspekte anführen. Einerseits stellt die Orientierung der Versicherer einen Einflussfaktor dar. Silent Cyber-Risiken betreffen vermehrt den industriellen Bereich und somit sind Versicherer, die primär das Privatkundensegment bedienen, weniger stark betroffen. Andererseits besteht die Möglichkeit, dass Versicherungsunternehmen bisher nicht mit Silent Cyber-Schäden konfrontiert wurden. Auch der Einfluss der Aufsichtsbehörden ist als weiterer Einflussfaktor aufzuführen.

Bei den Befragungsteilnehmern herrscht überwiegend Einigkeit darüber, dass die Sparten Sach-, Haftpflicht-, Vertrauensschaden- sowie Transportversicherungen hinsichtlich der Silent Cyber-Risiken am stärksten exponiert sind. Zudem wird von den befragten Experten hervorgehoben, dass grundsätzlich jede Produktsparte von Silent Cyber-Risiken betroffen sein kann, aber insbesondere die genannten Versicherungsarten aktuell die größten Gefährdungspotenziale aufweisen.

Im Rahmen der Haftpflichtversicherung sind im Wesentlichen folgende Versicherungsarten betroffen: die Betriebs- und Berufshaftpflichtversicherung, die Vermögensschadenhaftpflichtversicherung und die D&O-Versicherung. Innerhalb der Betriebshaftpflichtversicherung, die u. a. Produkthaftpflicht umfasst, können bspw. Personen-, Vermögens- und Sachschäden infolge von Hackerangriffen entstehen, sofern Cyber-Risiken nicht ausgeschlossen werden. Neben der Betriebshaftpflichtversicherung werden auch die klassische Berufshaftpflicht- und die Vermögensschadenhaftpflichtversicherung als für Silent Cyber-Risiken exponiert angesehen. Als Grund dafür wird angeführt, dass genannte Versicherungsarten als Pflichtversicherungen nur begrenzt Ausschlüsse ermöglichen. Des Weiteren ist im Zusammenhang mit den Haftpflichtversicherungen die Vertrauensschadenversicherung zu nennen, da Mitarbeiter z. B. den Diebstahl von digitalen Währungen ausüben können. An dieser Stelle wird jedoch von Experten der Erstversicherer erwähnt, dass Cyber-Risiken zum Teil explizit in Vertrauensschadenversicherungen mitversichert sind und es sich infolgedessen um affirmative Deckungen handelt. Ferner wird neben der Haftpflicht- und der Sachversicherung der Transportbereich als exponiert angesehen, da vernetzte Transportmittel zunehmend zum Einsatz kommen. Gleichermaßen ist nach Meinung der Befragungsteilnehmer im Bereich der Kraftfahrzeugversicherung aufgrund der steigenden Automatisierung der Fahrzeuge eine zukünftige Exponierung zu erwarten.

4.2 Silent Cyber-Risikomanagement

Risikoidentifikation

Ein zentraler Bestandteil des Risikomanagements ist die Risikoidentifikation. Dabei gilt es für Versicherungsunternehmen Silent Cyber-Risiken innerhalb ihrer Bestände zu identifizieren. Im Prozess der qualitativen Erfassung von Silent Cyber-Risiken werden die Bestände hinsichtlich möglicher Exponierungen analysiert. Die Versicherer im deutschen Markt erhalten durch den Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) Unterstützung bei der Identifikation von Silent Cyber-Exponierungen. Dies umfasst beispielsweise sowohl eine Silent Cyber-bezogene Arbeitsgruppen als auch ein Risikofragebogen zur Identifizierung von Silent Cyber-Exponierungen. Der GDV hat in der Vergangenheit explizit die Haftpflicht-, Sach-, Vertrauensschadenversicherung sowie die technischen Versicherungen analysiert. Diese Initiative endete im Jahr 2020. Ziel der Initiative war es die qualitative Erfassung möglicher Cyber-Risiken in den genannten Sparten zu vereinfachen. Zudem ist der Risikofragebogen im Rahmen des Versicherungsantrages ein wesentlicher Bestandteil zur Identifikation der potenziellen Cyber-Exponierung angehender Versicherungsnehmer.

Risikoanalyse und -bewertung

Bei den Befragungsteilnehmern besteht grundsätzlich Einigkeit darüber, dass die Risikomessung respektive die Quantifizierung der Risiken für die Mehrheit der Versicherer als schwierig und für einzelne Versicherer unmöglich erweist, da einerseits Silent Cyber-Risiken bzw. Cyber-Schäden generell eine neue Thematik für die Unternehmen darstellen und eine Vielzahl dieser Schäden bislang noch nicht versichert waren. Hieraus resultiert, dass unternehmensseitig derzeit nur wenige Daten und Erfahrungen im Umgang mit solchen Schäden vorhanden sind. Andererseits unterliegen die Cyber-Risiken hohen Änderungsrisiken, wodurch sich eine zusätzliche Verschärfung der zuvor beschriebenen Problematik ergibt. Dies hat zur Folge, dass in der Praxis aktuell bei der Modellierung von Silent Cyber-Risiken vornehmlich mit qualitativen Annahmen und Schätzungen gearbeitet wird.

Zunächst sind von dem genannten Erstversicherer die eigenen Bestände derart ausgewertet worden, dass eine jederzeitige Wiederholung der Risikomessung grundsätzlich möglich ist. Hierzu fand die Entwicklung von Datenmodellen statt, welche die Nutzung derselben Daten und Modellierungen ermöglicht. Dies ist im Hinblick auf die Dynamik des Risikos relevant, da hierdurch dem Risikomodell jederzeit neue Szenarien und relevante Informationen hinzugefügt werden können. Dieser Modellierungsansatz ist angelehnt an die Methodik zur Modellierung von Naturkatastrophenrisiken, wo gleichermaßen die Problematik von Kumulrisiken besteht. Unter Einsatz von Musterszenarien hat der Versicherer für die Produktsparten vollumfängliche

Einzelbewertungen vorgenommen. Die daraus gewonnenen Erkenntnisse werden anschließend in Relation zum gesamten Portfolio gesetzt. Der Grund dafür ist, dass jedes Szenario über eine unterschiedliche Intensität in den einzelnen Versicherungssparten verfügt, wobei ebenfalls die verschiedenen Gewichtungen der Sparten innerhalb des Versicherungsbestandes berücksichtigt werden müssen. In diesem Kontext ist eine gewisse Dynamik innerhalb des Versicherungsbestandes zu beachten, da sich die Rahmenbedingungen und Parameter verändern können. Ein Rückversicherer lässt sämtliche Modellierungen von einem Versicherungsmakler durchführen. Der Vorgang der Risikomodellierung von Silent Cyber-Risiken wird folgendermaßen beschrieben: Im Anschluss an die Risikoidentifikation erfolgt zur Identifikation der Wahrscheinlichkeit des jeweiligen Szenarios die Betrachtung verschiedener Schadensszenarien. Anhand der resultierenden Schätzungen werden anschließend die Exponierungen kalkuliert. Hinsichtlich des Kumulrisikos werden von dem Rückversicherer ebenfalls Modellierungen eingesetzt. Die Risikomodellierung ist nach Meinung eines Befragungsteilnehmers wiederum ein elementarer Bestandteil für die auf die Risikoanalyse folgende Risikobeurteilung. Neben den Bewertungen der Risiken ist die Gesamtbewertung hingegen auf Konzernebene durchzuführen, da den Underwritern kein Einblick in die gesamte Silent Cyber-Exponierung vorliegt. Ein Rückversicherer gibt in diesem Zusammenhang an, dass die Underwriter bei der Bewertung von Silent Cyber-Risiken einem Leitfaden zum Beurteilungsprozess folgen.

Für die zuvor erläuterten Prozesse sind aufgrund der fehlenden Daten oftmals qualitative Annahmen notwendig. Insbesondere hinsichtlich der Quantifizierung der Risiken und somit dem Underwriting ist eine fundierte themenspezifische Expertise unabdingbar. Dahingehend wird jedoch kritisiert, dass insbesondere kleinere Versicherer nicht über ausreichendes Fachwissen verfügen. Erste Versicherungsunternehmen haben infolgedessen bereits mit dem unternehmensinternen Know-how-Aufbau begonnen. Als Beispiel dafür werden verpflichtende interne Trainings für die Mitarbeiter des Underwritings der traditionellen Sparten veranlasst. Zudem ist zu erkennen, dass im Bereich Underwriting vermehrt IT- oder Cyber-Experten eingesetzt werden.

Risikosteuerung und -bewältigung

Eine Möglichkeit im Umgang mit Silent Cyber-Risiken ist der Ausschluss sämtlicher Cyber-Risiken aus den traditionellen Sparten. Ein Erstversicherer hat bereits cyberbezogene Deckungsausschlüsse in kleineren Sparten, wie z. B. in Ausfallversicherungen, umgesetzt. Bei den Haftpflicht- und Sachsparten sind derartige Ausschlüsse hingegen noch nicht explizit integriert. Des Weiteren hebt der Experte hervor, dass zurzeit überwiegend bei neuen Verträgen Cyber-Ausschlüsse integriert werden, wohingegen bestehende Policen bisher erhalten bleiben. Auch

bei der Transport- und Motorsparte besteht derzeit kein Handlungsbedarf. Insgesamt ist bei Deckungsausschlüssen nach Meinung der Experten jedoch zu beachten, dass zuerst die Identifikation der Silent Cyber-Risiken in den Verträgen zu erfolgen hat, bevor Ausschlüsse aufgenommen werden können. In diesem Zusammenhang müssen Cyber-Ausschlüsse klar definiert sein und dürfen nicht über einen Interpretationsspielraum verfügen. Des Weiteren führen Ausschlüsse oftmals zu Diskussionen zwischen Maklern und Kunden.

Zur Steuerung von Silent Cyber-Risiken können diese unbewusst affirmativ in den traditionellen Sparten inkludiert werden. Der von den Versicherern bevorzugte Ansatz für diesen Prozess ist es, zunächst sämtliche Cyber-Risiken aus der Versicherungsdeckung auszuschließen. Insgesamt ist die Definition des Cyber-Risikos erforderlich. Anschließend erfolgt der Wiedereinschluss mit konkretem Versicherungsumfang oder begrenzten Sublimits tragbarer Cyber-Risiken mittels Writeback-Lösung. Am Versicherungsmarkt existieren bereits derartige affirmative Versicherungen, die jedoch oftmals ausschließlich resultierende Vermögensschäden deckt.

Einer der befragten Versicherer veröffentlichte intern bereits eine Arbeitsanweisung hinsichtlich der Wordings bezugnehmend auf alle Sparten. Es bedarf allerdings spartenindividueller Lösungen. Die größten Sparten, wie z. B. die Sachversicherungen, Haftpflichtversicherungen und die technischen Versicherungen, umfassen bereits Cyber-Ausschlüsse mit Writeback-Lösungen, wovon lediglich mit Zustimmung der höheren Führungsebene abgewichen werden darf. Bei der Sachversicherung gibt es bestimmte Risiken, die stets in der Versicherungsdeckung enthalten sein müssen – auch wenn dieser Schaden auf eine cyberbedingte Ursache zurückzuführen ist (z. B. infolge eines durch einen Cyber-Angriff ausgelösten Lagerhallenbrandes). Der daraus resultierende Sachschaden wäre in diesem Fall folglich versichert. Dahingegen wäre der Verlust von Daten oder Datenwiederherstellungskosten aufgrund des beispielhaften Feuers in der Lagerhalle nicht von der Sachversicherung gedeckt. Die aus cyberbedingten Ursachen resultierenden Personen- und Sachschäden in der Haftpflichtversicherung bleiben jedoch weiterhin gedeckt, wobei cyberbedingte Vermögensschäden stark limitiert oder aufgrund der hohen Exponierung ausgeschlossen werden. Insgesamt sollen somit die klassischen Risiken, auch wenn diese einer cyberbedingten Ursache unterliegen, in den Sparten verbleiben. Konkret cyberbedingte Risiken, wie bspw. Datenverluste und Datenwiederherstellungen, sind wiederum über die Cyber-Police zu decken. Resultierend daraus soll eine klare Trennung zwischen den konventionellen Sparten und der Cyber-Police erfolgen. Dies erscheint nach den Aussagen der befragten Experten auch der von der Versicherungswirtschaft bevorzugte Ansatz zu sein. Ein

weiteres befragtes Versicherungsunternehmen sieht gleichermaßen die Lösung der Silent Cyber-Problematik im Ausschluss mit dezidierten Wiedereinschluss tragbarer Cyber-Risiken. Versicherungsmakler versuchen dieser Verfahrensweise jedoch entgegenzuwirken.

Eine weitere Möglichkeit zur Bewältigung von Silent Cyber-Risiken umfasst die Bepreisung dieser Risiken. Den Aussagen der befragten Experten ist jedoch zu entnehmen, dass dem Pricing von Silent Cyber-Risiken aktuell keine große Bedeutsamkeit beigemessen wird. Der Grund dafür ist, dass für einige Versicherer diese Risiken kaum quantifizierbar sind. Zudem sei eine Beitragsanpassung aufgrund von Silent Cyber derzeit nicht erforderlich, da keine Veränderung des Schadensgeschehens erkennbar ist. Silent Cyber hat zudem bislang keinen Einfluss auf die erhobenen Rückversicherungsprämien. Ein Erstversicherer kalkuliert hingegen bereits auf Grundlage von Modellierungen einen Preis für Silent Cyber-Risiken. Dabei gilt es spartenindividuelle Zuschläge zu eruieren. In diesem Zusammenhang wird auf die Unterschiede in den jeweiligen Tarifierungen hingewiesen. Bei Sparten, die eine hohe Schadenfrequenz aufweisen (wie z. B. die Kfz-Versicherung), ist eine Prämienkalkulation aufgrund des Einbezugs der Schadensumme am Ende des Jahres für die Berechnung der neuen Prämie weniger komplex. Sofern Silent Cyber-Schäden enthalten wären, sind diese in der neu berechneten Prämie ebenfalls inkludiert. Das befragte Versicherungsunternehmen prüft derzeit, inwieweit sich der kalkulierte Preis für Silent Cyber-Risiken am Markt realisieren lässt. Ein anderer Versicherer inkludiert wiederum geringfügige Mehrprämien für affirmative Bausteine in traditionellen Versicherungsprodukten, wie der Haftpflichtversicherung. Infolgedessen gilt es für diesen Versicherer zunächst Silent Cyber-Risiken zu identifizieren, um diese anschließend bepreisen zu können. Insgesamt werden die Prämien für Cyber-Risiken zunehmend steigen, was bei affirmativen Deckungen ebenfalls eine Preissteigerung zur Folge hat.

Zur Steuerung des aus den Silent Cyber-Risiken resultierende Kumulpotenzials, bieten sich den Versicherungsunternehmen verschiedene Ansätze. Zum einen erfolgt der Rückgriff der Erstversicherer auf Rückversicherungskapazitäten, was der Eingrenzung des Kumulrisikos dient. Dabei gilt es, wie bei den anderen genannten Maßnahmen zur Risikosteuerung, spartenindividuelle Lösungen zu eruieren. Rückversicherer können dieses Risiko folglich mit der Retrozession steuern. In diesem Kontext erläutert ein Experte, dass es zurzeit wenige alternative Risikotransfers im Bereich Cyber für Erst- sowie Rückversicherer gibt, welche die Streuung des Kumulrisikos ermöglichen würden. Ein anderer Experte nennt in diesem Zusammenhang die Möglichkeit von Zeichnungslimits. Ein Rückversicherer versucht sich hingegen rückversicherungsseitig durch die Einführung von Klauseln vor Cyber-Kumulrisiken zu schützen. Rückver-

sicherer bieten dabei sogenannte Cat-Verträge[1] an, die Kumule decken. Anhand von Informationen des Erstversicherers kann der Rückversicherer Implikationen darüber ableiten, wie viele Risiken vom Erstversicherer in dem jeweiligen Areal versichert sind. Dies dient der Einschätzung darüber welche Kosten ein Großschadenereignis, wie z. B. einem Großfeuer, in diesem Gebiet zur Folge hätte. Bei Cyber-Risiken könnte es hingegen der Fall sein, dass bspw. ein Hacker-Angriff mehrere Brände zugleich auslöst. Durch die Einführung von Klauseln soll verhindert werden, dass Cat-Verträge genannte Schäden mit dem vermeintlich selben Auslöser abdecken. lm Kraftfahrtbereich finden derartige Klauseln bereits Anwendung, wodurch die Kumulierung von Sachschäden mit bestimmten Cyber-Hintergründen verhindert wird. Ein Erstversicherer ist dahingehend der Auffassung, dass die Wordings auf Erstversicherungsebene ebenfalls die Kumulproblematik adressieren müssen. Ein anderer Erstversicherer sieht in seinen Beständen zurzeit keine Kumulgefahr, weshalb keinerlei Maßnahmen geplant sind. Ziel ist es lediglich, dass die Kumulgefahr in den bestehenden Versicherungs- sowie Rückversicherungsverträgen stets adressiert ist.

Risikoüberwachung

Nicht wenige Experten empfinden die Implementierung eines Silent Cyber-Schaden-Monitoring als schwierig. Als Grund dafür wird u. a. angeführt, dass die Mitarbeiter im Prozess der Schadenbearbeitung das Vorliegen eines Silent Cyber-Schadens erkennen müssen, was eine erhebliche Herausforderung darstellt. Bereits auf technischer Ebene sei eine derartige Zuordnung derzeit nicht möglich. Ein weiterer Interviewpartner sieht ebenfalls die Herausforderung bei der Identifikation von Silent Cyber-Schäden.

Einige Versicherer geben dahingegen an, dass sie Silent Cyber-Schäden aktuell oder in naher Zukunft quantitativ erfassen können. Als Beispiel wird von einem Erstversicherer ein automatisiertes Erfassungs- bzw. Monitoringsystem angeführt. Auf Grundlage dessen soll einerseits sofort erkennbar sein, wo welche Wordings zum Schutz cyberbedingter Schäden existieren. Andererseits sollen Cyber-Schäden zur weiteren Auswertung automatisch abrufbar sein. Unter Einsatz dieser Informationen sollen die Strategien zur Risikobewältigung und die Lerninhalte für die Underwriter überprüft und angepasst werden. Ausschließlich durch ein derartiges Monitoring besteht die Möglichkeit vertiefende Erkenntnisse über diese Risiken zu generieren. Rückwirkend können cyberbedingte Schäden derzeit nicht erkannt werden, da die dafür benö-

[1] Ein Cat-Vertrag ist ein Ausdruck für die Kumulschadenexzedenten-Rückversicherung. Dieser Vertrag soll Schadengeschehen abdecken, bei denen mehrere Risiken gleichzeitig betroffen sind. Cat-Verträge decken neben typischen Kumulgefahren, wie z. B. Naturkatastrophen, auch akkumulierte Feuerrisiken.

tigen Daten nicht vorhanden sind. Bislang wurden lediglich die führenden 20 Versicherungsnehmer pro Land und Sparte manuell analysiert, womit circa 85% des Prämienaufkommens abgedeckt ist. Ein weiterer Experte gibt an, dass alle Sparten ihre gesamte Silent Cyber-Exponierung quartalsweise statistisch erfassen und an das Risikomanagement weiterleiten müssen.

Ein anderer Erstversicherer hat bereits ein quantitatives Erfassungssystem aufgebaut, das aufbereitete Daten dem GDV zur Verfügung stellen kann. Sollten Silent Cyber-Schäden erkennbar sein, erfolgt die Erfassung im unternehmensinternen System. Dabei werden ausschließlich Verdachtsfälle ab einem bestimmten Schwellenwert hinsichtlich cyberbedingten Ursachen vertiefend analysiert. Bei Schadensfällen unterhalb des definierten Schwellenwertes erfolgt die Sammlung der zugehörigen Daten, wodurch rückwirkend Analysen bezüglich potenzieller Cyber-Attacken getätigt werden können. In Bezug auf das erhöhte Änderungsrisiko von Cyber-Risiken wurde bei dem befragten Versicherungsunternehmen ein Kompetenzcenter etabliert, das im Bereich der Cyber-Versicherung angegliedert ist.

4.3 Kooperationsmöglichkeiten zwischen Erst- und Rückversicherung

Aus Sicht der befragten Experten können Rückversicherer beim Management von Silent Cyber-Risiken für die Erstversicherer als wichtige Ansprechpartner agieren. Dies ist auf zwei wesentliche Gründe zurückzuführen. Zum einen verfügen Rückversicherer über umfangreichere Datenbestände und über eine höhere Schadenerfahrung, da bei ihnen die Portfolios von zahlreichen Erstversicherern zusammenlaufen. Aufgrund der vorhandenen Daten können Rückversicherer das Risiko folglich besser modellieren und bewerten. Darüber hinaus verfügen Rückversicherer über das technische Know-how im Umgang mit Cyber-Risiken. Zum anderen sind viele Rückversicherer vermehrt auf internationalen Märkten vertreten, wodurch auch marktübergreifend Erkenntnisse generiert werden können. Insbesondere in den USA verfügen Cyber-Deckungen über eine längere Historie, weshalb dort gewonnene Erkenntnisse für den deutschen Markt potenziell von Relevanz sind. Aufgrund genannter Aspekte können Rückversicherer die Erstversicherungsunternehmen über den Informationsaustausch im wettbewerbszulässigen Maße beratend unterstützen. Nicht nur für die Erstversicherer ist der Informationsaustausch von Vorteil, sondern auch Rückversicherer profitieren infolge einer möglich geringeren Risikoexponierung auf der Erstversicherungsseite.

4.4 Regulierung

Versicherungsaufsichtsperspektive

Das Thema Silent Cyber-Risiken hat eine hohe Bedeutung bei der Versicherungsaufsicht. Unter den Experten besteht im Wesentlichen Einigkeit darüber, dass das oberste Ziel der Aufsicht die

Sicherstellung der Solvabilität der Versicherungsunternehmen ist. Grund dafür ist einerseits, dass die Versicherungsindustrie gewissen Systemrisiken unterliegt. Andererseits gilt es das Leistungsversprechen gegenüber den Versicherungsnehmern zu garantieren. Ein Experte ist der Meinung, dass Silent Cyber-Risiken das Prämienrisiko in Solvency II adressieren, woraus Konsequenzen für das nachzuweisende Risikokapital resultieren. Dabei geht es um die Frage, ob Versicherer das Risiko überhaupt berücksichtigen und welche Maßnahmen sie hinsichtlich der Beherrschung ergreifen sollten. Ein Experte vermutet, dass der Aufsichtsbehörde aktuell qualitative Annahmen genügen. Des Weiteren ist der Befragte der Auffassung, dass insbesondere die deutsche Versicherungsaufsicht bei diesem Thema in den Rückstand geraten ist. Ein anderer Gesprächspartner verweist entsprechend auf die Bank of England PRA im Vereinigten Königreich, die in Bezug auf Silent Cyber-Risiken bereits explizite Vorgaben für Versicherer entwickelt hat. Sofern Versicherer Cyber-Risiken in traditionellen Sparten decken wollen, müssen sie u. a. nachweisen, dass Underwriter über das entsprechende Know-how verfügen. Zudem muss ein Ressortvorstand abgestellt werden, der hinsichtlich des Themas Verantwortung übernimmt.

Herausforderungen für Versicherer

Für die Versicherungsunternehmen sind die Anfragen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) i. d. R mit einem enormen Zeit- und Personalaufwand verbunden. Neben Meldeobliegenheiten müssen die Versicherer Berichtspflichten nachkommen, die oftmals zu Projekten innerhalb der Versicherungsunternehmen führen. Das Ziel der Versicherungsaufsicht ist es, quantitative Ergebnisse und konkrete Maßnahmen zu evaluieren. Versicherer müssen dafür die gewünschten Aspekte erfassen und modellieren. Oftmals werden hierbei Informationen angefordert, über welche das Versicherungsunternehmen zum gewünschten Zeitpunkt nicht verfügt.

Involvierung staatlicher Institutionen

Unter den Experten besteht überwiegend Konsens darüber, dass neben der BaFin keine weitere Involvierung von staatlichen Institutionen erforderlich ist. Infolgedessen wird für die Bewältigung von Silent Cyber-Risiken nicht die Notwendigkeit gesehen staatliche Institutionen einzubeziehen. Zudem wird angeführt, dass ein staatlicher Eingriff sinnvoll erscheint, wenn Risiken für Versicherer nicht tragbar sind, was nach Meinung der Experten für Silent Cyber-Risiken jedoch aktuell nicht zutrifft. Ein weiterer Aspekt, der bezüglich Cyber-Risiken im Allgemeinen genannt wird, ist ein möglicher Cyber-Pool zur Sammlung von Ereignissen. Für welche Art von Vorfällen dieser dienen könnte, geht aus den Experteninterviews nicht hervor. Die Experten

betonen jedoch, dass die BaFin eine wichtige Institution ist, um ein gesteigertes Problembewusstsein zu schaffen und die Solvabilität der Versicherer sicherzustellen.

4.5 Zukunftsannahmen

Versicherungstechnische Entwicklung des Risikos

Die Erläuterungen der Experten verdeutlichen, dass es in der Praxis zur Kontrolle von Silent Cyber-Risiken zukünftig verschiedene Möglichkeiten geben kann. Hinsichtlich der künftigen versicherungstechnischen Entwicklung von Silent Cyber-Risiken zeigen sich in der deutschen Versicherungswirtschaft jedoch zwei wesentliche Trends. Zum einen werden die Risiken den traditionellen Sparten affirmative Deckungsbausteine hinzugefügt und zum anderen erfolgt gleichzeitig der Einbezug zusätzlicher cyberbezogene Ausschlüsse in den traditionellen Versicherungen.

Ein Experte erläutert in diesem Zusammenhang, dass ein deutsches Versicherungsunternehmen aktuell jegliche Silent Cyber-Risiken in den traditionellen Deckungen ausschließt. Er betont dabei, dass sich in der Vergangenheit gezeigt hat, dass kleine und mittelständige Versicherer vermehrt den Produkten und Lösungen größerer Versicherer folgen. Auch auf anderen Märkten seien derartig weitgehende Ausschlüsse zu beobachten. Durch diesen Ansatz ist es möglich, sämtliche Cyber-Risiken in der Cyber-Versicherung zu bündeln. Dies gilt auch vor dem Hintergrund etwaiger Kumulrisiken. Durch Ausschlüsse lassen sich zudem zukünftig Deckungsüberschneidungen zwischen den traditionellen Versicherungsarten und Cyber-Policen minimieren. Da die Cyber-Versicherung zurzeit aber größtenteils ausschließlich Vermögensschäden deckt, sollten in Zukunft Personen- und Sachschäden in die Cyber-Deckung aufgenommen werden. Ein anderer Experte erwähnt, dass aktuell die Öffnung des Deckungsumfangs der Cyber-Versicherung zu beobachten sei. Allerdings sollten zukünftig nicht prinzipiell alle Cyber-Risiken versichert werden, da bei bestimmten Risiken die Schadensgefahr zu hoch ist.

In diesem Kontext erläutert ein Experte, dass für alle cyberbedingten Vermögensschäden ausschließlich Versicherungsdeckungen in Cyber-Policen existieren und Sach- und Personenschäden in den klassischen Sparten verbleiben sollten. Der Experte ist allerdings der Auffassung, dass dies nicht der zukünftige Weg sein wird. Vielmehr werden die vorhandenen Deckungskonzepte bestehen bleiben und es wird folglich keine Verschiebungen zwischen den unterschlichen Versicherungsdeckungen geben. Ein Grund dafür ist, dass bspw. die Sachversicherung Sachwerte vollumfänglich versichert, wohingegen die Cyber-Versicherung eine Erstrisiko-Deckung impliziert und Schäden nur bis zu einem bestimmten Limit übernimmt. Bezüglich der Versicherungssummen gibt es somit große Unterschiede zwischen den traditionellen Sparten

und der Cyber-Versicherung. Andere Experten schließen sich dieser Position an und ergänzen, dass Verschiebungen zukünftig auch aufgrund des bestehenden Marktdruckes unwahrscheinlich sind. Des Weiteren ist die Cyber-Versicherung ein neuartiges Produkt, das noch keine Markttiefe besitzt. Aufgrund dessen ist eine Bündelung diverser Risiken in der Cyber-Versicherung auch aufgrund der Kumulkontrolle schwerer steuerbar. Entsprechend ist der Vorteil an affirmativen Deckungen in den traditionellen Sparten, dass diese ein größeres Beitragsvolumen aufweisen, wodurch das Risiko aufgrund des Schadenausgleiches versicherbarer ist. Folglich sieht ein Großteil der Experten in der Zukunft affirmative Cyber-Deckungen in den traditionellen Sparten. Die Cyber-Versicherung würde somit weiterhin nur Vermögensschäden umfassen. In diesem Szenario ist entscheidend, dass eine klare Abgrenzung zwischen den traditionellen Versicherungen und den Cyber-Policen vorgenommen wird, um Mehrfachversicherungen von Cyber-Risiken zu vermeiden.

Zeitliche Entwicklung des Risikos

Kurzfristig wird in der deutschen Versicherungsbranche eine intensive Auseinandersetzung mit der Problematik der Silent Cyber-Risiken erwartet. Es gilt zunächst Daten zu sammeln, um diese Risiken besser bewerten zu können. Zudem werden nach Einschätzung der Experten der Erst- und Rückversicherer vermehrt Komplikationen und Haftungsfragen auftauchen. Auch die Versicherungsaufsicht wird sich zukünftig stärker als bisher mit der Thematik beschäftigen. Langfristig glauben die Experten, dass die Problematik der Silent Cyber-Risiken bedeutungslos wird, da Versicherer einen angemessenen Umgang mit diesen Risiken finden werden. Nach Meinung der Experten wird es zwischen den Cyber-Policen und traditionellen Versicherungspolicen eine klare Trennung geben.

5 Diskussion

Wahrnehmung in der Versicherungswirtschaft

Die Ergebnisse der Experteninterviews zeigen, dass sich die Mehrheit der befragten Erst- und Rückversicherer seit ca. drei bis vier Jahren mit der Problematik der Silent Cyber-Risiken beschäftigen. Jedoch befassen sich einzelne Unternehmen bereits deutlich länger mit dieser Herausforderung. In den Versicherungsunternehmen werden Silent Cyber-Risiken unterschiedlich priorisiert. Während für einige der befragten Versicherungsunternehmen der Stellenwert der Thematik einem geringen Risiko gleicht, priorisieren andere die Risiken weit höher. Dabei nehmen u. a. die Portfolioausrichtung der Versicherer und die Aufsichtsbehörden eine zentrale Rolle ein. Die Wahrnehmung der Versicherungsnehmer von Silent Cyber-Risiken wird von den Experten als gering eingeschätzt.

Die Ergebnisse der Expertenbefragung bestätigen die Erkenntnisse der damaligen Untersuchung von Wrede et al. (2020) und zeigen, dass weiterhin erhebliche Unterschiede zwischen den Versicherungsunternehmen in der Wahrnehmung von Silent Cyber-Exponierungen bestehen. So wird auch von der EIOPA (2019) das in der Versicherungspraxis grundsätzlich vorherrschende mangelnde Bewusstsein der Unternehmen für Silent Cyber-Risiken kritisiert. In diesem Zusammenhang kommen auch Cartagena et al. (2020) zu dem Ergebnis, dass erhebliche Schäden und die verstärkte versicherungsaufsichtliche Kontrolle zu einem steigenden Bewusstsein für Silent Cyber-Risiken in den Unternehmen führen können. Die Versicherungsaufsicht ist somit angehalten den Betrachtungsfokus weiterhin verstärkt auf Silent Cyber-Risiken zu richten, um sicherzustellen, dass sich Versicherer tiefergehend mit der Problematik auseinandersetzen und innovative Lösungsansätze für den Umgang mit diesen Risiken entwickeln. In anderen Ländern, wie z. B. Großbritannien, sind die Versicherungsmärkte hinsichtlich der Wahrnehmung von Silent Cyber-Risiken deutlich weiterentwickelt, da die dortigen Versicherungsaufsichtsbehörden den Umgang mit dieser Problematik bereits seit längerer Zeit deutlich stärker adressiert haben.

Einschätzung der Gefahrenpotenziale in den Sparten

Die vorliegende qualitative Studie zeigt, dass zurzeit die Sparten Sach-, Haftpflicht-, Vertrauensschaden- und Transportversicherungen von den Befragungsteilnehmern als hochgradig exponiert eingeschätzt werden. Auch Wrede et al. (2020) schlussfolgern in ihrer Untersuchung, dass neben den in ihrer Studie untersuchten traditionellen Versicherungssparten weitere Produktsparten eine hohe Exponierung durch Silent Cyber-Risiken aufweisen können. Im Bereich der klassischen Haftpflichtversicherung, wie auch der Betriebs- und Berufshaftpflichtversicherung, sehen die Befragten bspw. insbesondere Datenschutzverletzungen als potenzielle Auslöser für Silent Cyber-Schäden, sofern diese nicht explizit ausgeschlossen sind. Da es sich bei Vermögensschadenhaftpflichtversicherung häufig um Pflichtversicherungen handelt, gilt diese aufgrund geringer Ausschlussmöglichkeiten innerhalb der Haftpflichtversicherungen als besonders exponiert. Zudem verdeutlichen die Ergebnisse, dass die Vertrauensschadenversicherung ebenfalls ein erhebliches Potenzial für Silent Cyber-Schäden aufweist. Neben der Sach- und Haftpflichtversicherungssparte weist auch die Produktsparte der Transportversicherung eine starke Silent Cyber-Exponierung auf. Bezogen auf die Zukunft gilt insbesondere die Luft- und als hochgradig gefährdet, da bspw. das autonome Fahren ein Kraftfahrzeug-Versicherungsparte potenzielles Risiko für Cyber-Risiken darstellt. Neben den von den Experten identifizierten Exponierungen zeigen die Untersuchungsergebnisse, dass die identifizierten Schadenfälle bei den deutschen Versicherungsunternehmen in der Praxis bisher gering sind.

Die Literatur zeigt, dass in den Geschäftsinhalts-, Ertragsausfall-, Vermögensschadenhaftpflicht- und D&O-Versicherungen explizite Silent Cyber-Risiken vorhanden sind. Bei den klassischen Betriebs- und Berufshaftpflichtversicherungen sind Deckungsausschlüsse und zusätzliche optionale Leistungsbausteine zur Absicherung von Cyber-Schäden vorgesehen. (Armbrüster 2020; Flagmeier und Heidemann 2020; Gebert und Klapper 2020; Wrede et al. 2020). In der vorliegenden Untersuchung werden etwaige Deckungsausschlüsse ausschließlich von einem befragten Experten thematisiert. So kommen Wrede et al. (2020) ebenfalls zu dem Ergebnis, dass Vertrauensschadenversicherungen affirmative Deckungen beinhalten. Ferner gelangen Wrede et al. (2020) gleichermaßen zur der Erkenntnis, dass hinsichtlich realisierter Silent Cyber-Schäden in der Praxis die Anzahl der bislang unternehmensseitig identifizierten Schadenfälle gering ist. Eine Studie von Willis Towers Watson (2020) zeigt dahingegen, dass Experten der Auffassung sind, dass das Silent Cyber-Risiko infolge der Coronavirus-Pandemie zugenommen hat. Viele Unternehmen mussten aufgrund der Coronavirus-Pandemie dezentralisiert arbeiten, was eine Erhöhung der Cyber-Risiken zur Folge hat. Obgleich die Anzahl der Cyber-Attacken in diesem Zeitraum gleichermaßen deutlich angestiegen ist (Bundesamt für Sicherheit in der Informationstechnik (BSI) 2020).

Während in der Literatur die Transportsparte zunehmend vernachlässigt wird, ist diese nach Meinung der befragten Experten den Sparten mit der stärksten Exponierung zuzuordnen. Des Weiteren gilt es die Kraftfahrt- sowie Luftfahrtsparte vertiefend zu analysieren. Die aktuellen Entwicklungen zeigen, dass eine zeitnahe Exponierung im Kraftfahrtbereich nicht auszuschließen ist und von den Versicherern berücksichtigt werden sollte. Auch im Hinblick auf das resultierende Kumulrisiko sollten Versicherer einen geeigneten Umgang mit möglichen Cyber-Risiken in der Kraftfahrtversicherungssparte etablieren.

Silent Cyber-Risikomanagement

Die Ergebnisse der Expertenbefragung zeigen, dass in den deutschen Versicherungsunternehmen deutliche Unterschiede hinsichtlich des Umsetzungsstandes des Silent Cyber-Risikomanagements bestehen. Grundsätzlich befindet sich die deutsche Versicherungswirtschaft nach Meinung eines Befragungsteilnehmers im Prozess der Risikoidentifikation. Bei der Risikoanalyse und -bewertung zeigen sich ebenfalls deutliche Unterschiede. Nur einige Versicherungsunternehmen können bislang bestehende Silent Cyber-Risiken quantifizieren. Insgesamt ist eine Quantifizierung der Silent Cyber-Risiken aufgrund geringer Datenbestände und des Änderungsrisikos erschwert. Dies hat zur Konsequenz, dass bei den befragten Experten aktuell in der Modellierung von Silent Cyber-Risiken hauptsächlich mit qualitativen Annahmen gearbeitet wird. Das notwendige Know-how ist nur bedingt vorhanden, weshalb sich einige Versicherer

sich bemühen, das erforderliche Fachwissen extern über den Arbeitsmarkt zu akquirieren. Romanosky et al. (2019) konnten in diesem Kontext zum Pricing von Cyber-Risiken fünf Informationsquellen identifizieren: externe Quellen, Schätzungen, Orientierung an Wettbewerbern, Erfahrungen eigener Underwriter, Preise anderer Versicherungssparten. In der vorliegenden Studie wurden von den Befragungsteilnehmern im Rahmen des Pricings von Silent Cyber-Risiken hingegen primär Schätzungen auf Basis qualitativer Annahmen hervorgehoben. Insgesamt sind Silent Cyber-Risiken infolge der mangelhaften Datenlage zunehmend schwerer quantifizierbar als klassische Cyber-Risiken. Aufgrund der Ähnlichkeit des Kumulrisikos wird in der Praxis zur Modellierung von Silent Cyber-Risiken der befragten Versicherungsunternehmen zudem auf klassische Naturkatastrophenmodelle zurückgegriffen. Während auf Ebene des Underwritings in den befragten Unternehmen mit Leitfäden zur Risikobewertung gearbeitet wird, ist das Risiko auf Konzernebene zu bewerten, damit Risikobewältigungsmaßnahmen ergriffen werden können. Die befragten Versicherer schätzen die Silent Cyber-Risiken des eigenen Unternehmens bezüglich des unternehmensinternen Portfolios unterschiedlich ein. Risikobewältigungsmaßnahmen sind Ausschlusskriterien, präzises Pricing und weitere Maßnahmen zum Kumulmanagement. Im Kontext der Ausschlüsse werden Wiedereinschlüsse mit konkretem Versicherungsumfang oder begrenzten Sublimits tragbarer Cyber-Risiken mittels Write-back-Lösung umgesetzt. Letzteres scheint die bevorzugte Methode der Versicherer in Deutschland zu sein. Das Pricing spielt zurzeit eine untergeordnete Rolle, da aktuell nur die wenigsten Versicherer die Silent Cyber-Risiken korrekt quantifizieren können. Romanosky et al. (2019) zeigen, dass beim Pricing von Cyber-Risiken zwischen ‚Pauschalpreisen' und ‚Basispreisen' unterschieden werden kann. Im Rahmen der Pauschalpreisgestaltung erfolgt die Bepreisung des einen Tarifs für alle Antragssteller unabhängig der Unternehmensgröße oder spezifischen Sicherheitskontrollen. Die Berechnung des Basispreises umfasst hingegen diverse Modifikationen hinsichtlich der Standardversicherungskriterien sowie der Branche des Antragsstellers. Zudem bilden die Vermögenswerte bzw. die Einnahmen das wichtigste Unternehmensmerkmal zur Berechnung der Versicherungsprämie. Ferner wird in dieser Bepreisung die Verwendung von allgemeinen Sicherheitsfragen hinzugezogen. Ein ähnliches Vorgehen wäre bei dem Pricing von Silent Cyber-Risiken zukünftig denkbar. Nurse et al. (2020) zeigen darüber hinaus, dass Versicherer vor der Herausforderung stehen für das Underwriting genannter Risiken die Kundendaten in einem angemessenen Umfang zu erheben. Während die Abfrage zu vieler Informationen Kunden abschrecken könnte, führen im Rahmen des Underwritings zu wenige Kundendaten zu Quantifizierungsproblemen seitens des Versicherers. Darüber hinaus sind in diesem Kontext sicherheitsrelevante Informationen, wie zum Beispiel der Schulungsstand der

Mitarbeiter im Bereich der Cyber-Sicherheit, für Versicherer von Bedeutung (Nurse et al. 2020).

Hinsichtlich der Kumulgefahr sichern sich Erstversicherer im Wesentlichen über Rückversicherungen ab. Rückversicherer versuchen wiederum bestimmte Kumulgefahren vertraglich auszuschließen. Die Umsetzung einer Risikoüberwachung bzw. eines Monitoringsystems stellt sich als besonders schwierig dar, da u. a. Schadenbearbeiter über das dafür benötige Know-how verfügen müssten und dies zumeist nicht vollumfänglich vorhanden ist. Indessen befinden sich einige der befragten Versicherer bereits im Prozess der Implementierung solcher Systeme, wodurch die nachhaltigen Datenprobleme zukünftig gelöst werden könnten. Andere Versicherer haben dahingegen keine Maßnahmen geplant.

Auch verschiedene wissenschaftliche Studien zeigen, dass die Umsetzung des Managements von Silent Cyber-Risiken in Versicherungsunternehmen unterschiedlich weit fortgeschritten ist (EIOPA 2019; Cartagena et al. 2020; Wrede et al. 2020). Zudem verdeutlichen diese Studien, dass die Versicherer erhebliche Probleme mit der Quantifizierung des Risikos haben. Aufgrund der vorhandenen Kumulrisiken kann dies zu bedeutenden finanziellen Problemen führen (EIOPA 2019; Cartagena et al. 2020; Wrede et al. 2020). Mögliche Datenpools für Silent Cyber-Schäden werden im Schrifttum als Lösungsansatz für die Quantifizierungsprobleme angeführt (EIOPA 2019; Wrede et al. 2020). Die Untersuchungsergebnisse der vorliegenden Studie zeigen, dass der GDV in Deutschland eine Stelle zur Sammlung von Daten zu Silent Cyber-Schäden bereits eingerichtet hat. Die wettbewerbsrechtlichen Herausforderungen scheinen im abgesicherten Umfeld des Verbands gelöst zu sein (Eling und Schnell 2016). Inwieweit sich deutsche Versicherungsunternehmen zukünftig daran beteiligen, ist aktuell jedoch noch nicht absehbar. Mögliche Anreizprobleme für große Versicherer sind hier zu erwähnen, da diese einen geringen Nutzen aus einer Kollaboration ziehen (OECD 2017). Entscheidend ist allerdings, dass alle Versicherer zur Schadenmeldung über ein einheitliches Schadenserfassungssystem verfügen.

Zukünftige Entwicklung von Silent Cyber-Risiken

Die Untersuchungsergebnisse zeigen bei der Risikobewältigung zwei mögliche Trends auf. Einerseits besteht die Möglichkeit Cyber-Risiken in den traditionellen Versicherungssparten affirmativ einzubeziehen. Andererseits können explizite Ausschlüsse in den konventionellen Sparten zur Verlagerung der Risiken in die Cyber-Versicherung führen. Ein deutscher Versicherer hat bereits damit begonnen sämtliche Cyber-Risiken in traditionellen Sparten auszuschließen und verweist in diesem Zusammenhang auf die Cyber-Versicherung. Damit dieser

Ansatz zukünftig am Markt bestehen kann, sollten Versicherer sich in der Cyber-Versicherung nicht ausschließlich auf die Absicherung von Vermögensschäden beschränken, sondern auch Personen- und Sachschäden implizieren. Weniger Deckungsüberschneidungen oder die Konzentration der Cyber-Risiken in einer Sparte wären dabei vorteilhaft. Ferner ist es möglich durch Writeback-Lösungen Cyber-Risiken in den traditionellen Produktsparten zu versichern. Zudem verfügen konventionelle Versicherungssparten über ein höheres Beitragsvolumen, weshalb der Schadensausgleich somit erleichtert wäre. In diesem Fall gilt es, eine klare Abgrenzung zwischen der Cyber-Versicherung und den traditionellen Versicherungen zu finden.

Welche Möglichkeit zur Risikobeherrschung die Versicherungsunternehmen wählen sollten, ist im Hinblick auf die unternehmensinterne Ausrichtung und Struktur von den Versicherern individuell zu wählen. Zur Risikobewertung und Datensammlung ist allerdings entscheidend, dass eine Offenlegung der Silent Cyber-Risiken erfolgt. Eine verbesserte Datenlage kann langfristig potenziell zu All-Risk-Deckungen führen (Baban et al. 2017a, b), was grundsätzlich den Bedürfnissen der Versicherungsnehmer entsprechen würde. Sofern einzelne Cyber-Risiken auch zukünftig nicht versicherbar sind, sollten Versicherer diese Risiken trotz des vorherrschenden Wettbewerbsdrucks unternehmensübergreifend endgültig ausschließen (EIOPA 2019). Der aktive Umgang mit Silent Cyber-Risiken kann für Versicherer erhebliche Chancen implizieren. Eine Inkludierung dieser Risiken in die Cyber-Versicherung kann ein Qualitätsmerkmal darstellen und das Marktwachstum anregen. Sollten die Silent Cyber-Risiken hingegen affirmativ in die konventionellen Versicherungen aufgenommen werden, ist die Generierung eines erhöhten Prämienvolumens denkbar. Inwieweit sich darüber hinaus alternative Risikotransfers durchsetzen, wird die Entwicklung der nächsten Jahre zeigen. Erste Bewegungen in diesem Kontext sind im Bereich Cyber bereits zu verzeichnen (Gallin 2020). In diesem Zusammenhang ist jedoch zu beachten, dass derartige Produkte für den Kapitalmarkt profitabel sind. Ferner sollten zur Steigerung der Investitionsbereitschaft potenzielle Investoren das Risiko vollumfänglich verstehen (Lale 2013). Insbesondere genanntes Verständnis könnte allerdings eine Herausforderung darstellen.

Implikationen und Limitationen der Studie

Die Ergebnisse dieser Studie verfügen neben einer theoretischen auch über eine praktische Relevanz. Die Versicherer beschäftigen sich zurzeit hauptsächlich mit Silent Cyber-Exponierungen in denjenigen Sparten, in denen genannte Schäden oftmals bereits aufgetreten sind. Neben den akuten Gefahren gilt es auch andere Sparten vor Schadeneintritt zu adressieren (EIOPA 2019). Darüber hinaus sollten aufgrund der vorhandenen Änderungsrisiken regelmäßige Über-

prüfungen der Risikoentwicklung stattfinden. Des Weiteren sind insbesondere die Erstversicherer angehalten ein Silent Cyber-Schaden-Monitoring zu etablieren, um entsprechende Maßnahmen frühzeitig einleiten zu können. Hierbei könnten möglicherweise staatliche Eingriffe zur Entwicklung und Bereitstellung geeigneter Instrumente zum Monitoring sinnvoll sein (Wrede et al. 2020). Verfügen Versicherer über die Möglichkeit Daten zu generieren, sollte eine Beteiligung an der Datensammelstelle des GDV erfolgen. Grundsätzlich sollten Erst- und Rückversicherer weiterhin eng zusammenarbeiten, um jeweilige Erfahrungen weiterzugeben. Ferner ist die Entwicklung auf dem britischen Markt zu verfolgen, wodurch trotz eingeschränkter Übertragbarkeit relevante Erkenntnisse generiert werden können (Wrede et al. 2020). Die eingeschränkte Übertragbarkeit internationaler Erkenntnisse ist zugleich eine Limitation der vorliegenden Studie. Die Ergebnisse der Untersuchung fokussieren sich ausschließlich auf den deutschen Versicherungsmarkt. Weitere Untersuchungen mit internationalen Versicherungsexperten könnten wertvolle Erkenntnisse liefern. Weitere Restriktionen ergeben sich aufgrund des gewählten qualitativen Ansatzes. Infolge der vorliegenden Stichprobengröße ist die Generalisierbarkeit und Objektivität der Ergebnisse begrenzt, wodurch diese als Trend im Rahmen einer Ausschnittsbetrachtung anzusehen sind (Firestone 1993; Miles und Huberman 1994; Lee und Baskerville 2003; Groleau et al. 2009).

6 Fazit

Der vorliegende Beitrag befasst sich mit drei zentralen Fragestellungen im Umgang von deutschen Versicherungsunternehmen mit Silent Cyber-Risiken. In diesem Zusammenhang wurde der Status quo der Wahrnehmung etwaiger Risiken, die Einschätzung des Gefahrenpotenzials und der damit einhergehende Umgang mit Silent Cyber-Risiken im Underwriting und Pricing untersucht. Zudem ist die Frage nach der zukünftigen Entwicklung der Silent Cyber-Problematik Gegenstand des Forschungsbeitrags. Hinsichtlich der Wahrnehmung von Silent Cyber-Risiken in der deutschen Versicherungswirtschaft zeigt die vorliegende Untersuchung, dass sich die Mehrheit der befragten Versicherer in Deutschland erst seit wenigen Jahren mit dieser Problematik beschäftigen. Grundsätzlich ist die Wahrnehmung dieser Risiken zwischen den Versicherungsunternehmen äußerst unterschiedlich. Bezogen auf die Gefährdungspotenziale in den einzelnen Versicherungssparten verdeutlichen die Untersuchungsergebnisse, dass insbesondere die Sparten der technischen Versicherungen, Ertragsausfall-, Sach-, Haftpflicht-, Vertrauensschaden- und die Transportversicherungen eine hohe Exponierung durch Silent Cyber-Risiken aufweisen. In Zukunft werden mit hoher Wahrscheinlichkeit zusätzlich die Kraft- und Luftfahrtversicherung hochgradig von Silent Cyber-Exponierungen betroffen sein. Hinsichtlich des Umgangs mit Silent Cyber-Risiken zeigt sich in der Praxis kein einheitlicher Umsetzungsstand

bei den Versicherern. Beim Pricing und Underwriting sind zwei wesentliche Trends zu erkennen. Einerseits die Cyber-Risiken in die traditionellen Sparten affirmativ einzubeziehen und andererseits die Risiken aus den konventionellen Versicherungen auszuschließen und diese in Cyber-Versicherungen zu verlagern. Bezüglich der zeitlichen Entwicklung des Risikos stellt sich heraus, dass in naher Zukunft eine intensive Auseinandersetzung mit dem Thema stattfinden wird. Mittelfristig werden sich Trends zum Umgang abzeichnen, wodurch langfristig Silent Cyber-Risiken voraussichtlich an Relevanz verlieren.

Literatur

Allianz Global Corporate & Specialty SE (AGCS): Allianz Risk Barometer 2022: The most important business risks for the next 12 months and beyond, based on the insight of 2,650 risk management experts from 89 countries and territories (2022). https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/grd/AGCS-GRD-Winter-Spring-2019.pdf, Zugegriffen: 11. Nov. 2022

Amin, Z.: A Practical Road Map for Assessing Cyber Risk. Journal of Risk Research. **22**(1), 32–43 (2019)

Armbrüster, C.: New Technologies. Political, Legal, Economic and Factual Impact in Germany. Zeitschrift für die gesamte Versicherungswissenschaft. **109**(1), 9–38 (2020)

Baban, C.P., Barker, T., Gruchmann, Y., Paun, C., Peters, A.C., Stuchtey, T.H.: Cyberversicherungen als Beitrag zum IT-Risikomanagement—Eine Analyse der Märkte für Cyberversicherungen in Deutschland, der Schweiz, den USA und Großbritannien. Standpunkt zivile Sicherheit Nr. 8. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (2017a). https://www.bigs-potsdam.org/app/uploads/2020/02/Standpunkt_8_2017-Online_120218.pdf, Zugegriffen: 2. Nov. 2022

Baban, C.P., Barker, T., Gruchmann, Y., Paun, C., Peters, A.C., Stuchtey, T.H.: Cyber insurance as a contribution to IT risk management—An analysis of the market for cyber insurance in Germany. Policy Paper No. 7. Potsdam: Brandenburgisches Institut für Gesellschaft und Sicherheit gGmbH (2017b). https://www.bigs-potsdam.org/app/uploads/2020/06/PP_No7_Cyber-Insurance.pdf, Zugegriffen: 2. Nov. 2022

Baer, W.S.: Rewarding IT Security in the Marketplace. Contemporary Security Policy. **24**(1), 190–208 (2003)

Baer, W.S., Parkinson, A.: Cyberinsurance in IT Security Management. IEEE Security and Privacy. **5**(3), 50–56 (2007)

Baker, T., Shortland, A.: Insurance and Enterprise: Cyber Insurance for Ransomware. The Geneva Papers on Risk and Insurance – Issues and Practice. 2022, 1–25 (2022)

Bandyopadhyay, T., Shidore, S.: Towards a Managerial Decision Framework for Utilization of Cyber Insurance Instruments in IT security. In: Proceedings of the 17th Americas Conference on Information Systems (AMCIS), Detroit, August 4–7, 2011 (2011)

Bank of England Prudential Regulation Authority (PRA): Cyber Insurance Underwriting Risk (2017). https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417, Zugegriffen: 3. Nov. 2022

Bodin, L.D., Gordon, L.A., Loeb, M.P., Wang, A.: Cybersecurity Insurance and Risk-Sharing. Journal of Accounting and Public Policy. **37**(6), 527–544 (2018)

Böhme, R., Kataria, G.: Models and Measures for Correlation in Cyber-Insurance. In: Proceedings of the 5th Workshop on the Economics of Information Security (WEIS), Cambridge, June 26–28, 2006 (2006)

Böhme, R., Schwartz, G.: Modeling Cyber-Insurance: Towards A Unifying Framework. In: Proceedings of the 9th Workshop on the Economics of Information Security (WEIS), Cambridge, June 7–8, 2010 (2010)

Bogner, A., Littig, B., Menz, W.: Interviews mit Experten: Eine praxisorientierte Einführung. Springer VS, Wiesbaden (2014)

Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland (2020). https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1, Zugegriffen: 3. Dez. 2022

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom) (Hrsg.): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt (2020). https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf, Zugegriffen: 1. Dez. 2022

Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly. **34**(3), 523–548 (2010)

Cartagena, S., Gosrani, V., Grewal, J., Pikinska, J.: Silent Cyber Assessment Framework. British Actuarial Journal. **25**, 1–19 (2020)

Castriotta, K.: A Semantic Framework for Analyzing "Silent Cyber". Journal of Financial Transformation, **55**, 102–111 (2022)

Cavusoglu, H., Cavusoglu, H., Raghunathan, S.: Economics of IT Security Management: Four Improvements to Current Security Practices. Communications of the Association for Information Systems. **14**, 65–75 (2004)

Charalambous, M., Farao, A., Kalantzantonakis, G., Kanakakis, P., Salamanos, N., Kotsifakos, E., Froudakis, E.: Analyzing Coverages of Cyber Insurance Policies Using Ontology. In: Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES), Vienna, August 23–26, 2022 (2022)

Chertoff, M.: The cybersecurity challenge. Regulation & Governance. **2**(4), 480–484 (2008)

Chopra, A.: Cyberattack – Intangible Damages in a Virtual World: Property Insurance Companies Declare War on Cyber-Attack Insurance Claims. Ohio State Law Journal, **82**, 121–162 (2021)

Coburn, A., Ulrich, P., Savage, R., Harvey, T., Woo, G., Sarabandi, P., Arnold, S., Glennie, E., Vos, C., Rufe, S., Leverett, É., Skelton, A., Copic, J., Sweeney, S., Rais-Shaghagi, A., Kasaite, V., Kelly, S., Ralph, S., Tuveson, M., Pryor, L., Evan, T.: Managing cyber insurance accumulation risk. Cambridge, UK: Risk Management Solutions, Inc. and University of Cambridge Centre for Risk Studies (2016). https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-rms-managing-cyber-insurance-accumulation-risk.pdf, Zugegriffen: 20. Okt. 2022

Elhabashy, A.E., Wells, L.J., Camelio, J.A.: Cyber-physical Security Research Efforts in Manufacturing – A Literature Review. Procedia Manufacturing. **34**, 921–931 (2019)

Eling, M.: Cyber Risk and Cyber Risk Insurance: Status Quo and Future Research. The Geneva Papers on Risk and Insurance – Issues and Practice. **43**(2), 175–179 (2018)

Eling, M., Schnell, W.: Ten Key Questions on Cyber Risk and Cyber Risk Insurance. The Geneva Association, Zurich (2016). https://www.genevaassociation.org/sites/default/files/research-topicsdocument-type/pdf_public//cyber-risk-10_key_questions.pdf, Zugegriffen: 7. Dez. 2022

Eling, M., Wirfs, J.H.: What are the Actual Costs of Cyber Risk Events? European Journal of Operational Research. **272**(3), 1109–1119 (2019)

European Insurance and Occupational Pensions Authority (EIOPA): EU-U.S. insurance dialogue project: The cyber insurance market (2018). https://www.eiopa.europa.eu/sites/default/files/publications/other_documents/181031_eu-us_project_cyber_insurance_white_paper_publication.pdf. Zugegriffen: 5. Nov. 2022

European Insurance and Occupational Pensions Authority (EIOPA): Cyber risk for insurers – Challenges and opportunities (2019). https://www.eiopa.europa.eu/sites/default/fles/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf, Zugegriffen: 5. Nov. 2022

European Insurance and Occupational Pensions Authority (EIOPA): Supervisory Statement on Management of Non-Affirmative Cyber Exposures (2022). https://www.eiopa.europa.eu/sites/default/files/publications/supervisory_statements/supervisory_statement_on_management_of_non-affirmative_cyber_exposures.pdf, Zugegriffen: 22. Dez. 2022

Faisst, U., Prokein, O., Wegmann, N.: Ein Modell zur dynamischen Investitionsrechnung von IT-Sicherheitsmaßnahmen. Journal of Business Economics. **77**(5), 511–538 (2007)

Ferland, J.: Cyber insurance – What Coverage in Case of an Alleged Act of War? Questions raised by the Mondelez v. Zurich Case. Computer Law & Security Review. **35**(4), 369–376 (2019)

Firestone, W.A.: Alternative Arguments for Generalizing from Data as Applied to Qualitative Research. Educational Researcher. **22**(4), 16–23 (1993)

Flagmeier, W., Heidemann, J.: Sonderheft: Cyber-Versicherungen, 4. Aufl. Wolters Kluwer, Münster (2018)

Franke, U.: The Cyber Insurance Market in Sweden. Computers & Security. **68**, 130–144 (2017)

Franke, U.: Cyber Insurance against Electronic Payment Service Outages: A Document Study of Terms and Conditions from Electronic Payment Service Providers and Insurance Companies. In: Katsikas, S.K., Alcaraz, C. (Hrsg.) Security and Trust Management: 14th International Workshop, STM 2018, Barcelona, Spain, September 6–7, 2018, Proceedings, S. 73–84. Springer, Cham (2018)

French, C.C.: Five Approaches to Insuring Cyber Risks. Maryland Law Review. **81**, 103–143 (2021)

Gallin, L.: Aon & HSCM launch $70mn catastrophic cyber product (2020). https://www.reinsurancene.ws/aon-hscm-launch-70mn-catastrophic-cyber-product/, Zugegriffen: 4. Dez. 2022.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., Laplante, P.: Dimensions of Cyberattacks: Cultural, Social, Economic, and Political. IEEE Technology and Society Magazine. **30**(1), 28–38 (2011)

Gebert, Y., Klapper, S.: § 24 Cyberversicherung. In: Veith, J., Gräfe, J., Gebert, Y. (Hrsg.) Der Versicherungsprozess: Ansprüche und Verfahren – Praxishandbuch, S. 1360–1383. Nomos, Baden-Baden (2020)

Gläser, J., Laudel, G.: Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen, 4. Aufl. VS, Wiesbaden (2010)

Graneheim, U.H., Lundman, B.: Qualitative Content Analysis in Nursing Research: Concepts, Procedures and Measures to Achieve Trustworthiness. Nurse Education Today. **24**(2), 105–112 (2004)

Groleau, D., Zelkowitz, P., Cabral, I.E.: Enhancing Generalizability: Moving from an Intimate to a Political Voice. Qualitative Health Research. **19**(3), 416–426 (2009)

Guest, G., Bunce, A. Johnson, L.: How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. Field Methods. **18**(1), 59–82 (2006)

Haas, A.: Management von Cyber-Risiken und Möglichkeiten des Risikotransfers: eine ökonomische und versicherungstechnische Analyse (2016). http://opus.uni-hohenheim.de/volltexte/2016/1192/pdf/Diss_Haas_Buchdruck_Final.pdf, Zugegriffen: 6. Nov. 2022

Haas, A., Hofmann, A.: Risiken aus der Nutzung von Cloud-Computing-Diensten: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. Zeitschrift für die gesamte Versicherungswissenschaft. **103**(4), 377–407 (2014)

Hartley, J.F.: Case studies in organizational research. In: Cassell, C., Symon, G. (Hrsg.) Qualitative Methods in Organizational Research: A Practical Guide, S. 209–229. SAGE, London (1994)

Harwood, T.G., Garry, T.: An Overview of Content Analysis. The Marketing Review. **3**(4), 479–498 (2003)

Hunt, T.D.: "The Internet of Buildings": Insurance of Cyber Risks for Commercial Real Estate. Oklahoma Law Review. **71**(2), 397–452 (2019)

Hsieh, H.-F., Shannon, S.E.: Three Approaches to Qualitative Content Analysis, Qualitative Health Research. **15**(9), 1277–1288 (2005)

Järveläinen, J.: IT Incidents and Business Impacts: Validating a Framework for Continuity Management in Information Systems. International Journal of Information Management. **33**(3), 583–590 (2013)

Jerry II, R.H., Mekel, M.L.: Cybercoverage for Cyber-Risks: An Overview of Insurers' Responses to the Perils of E-Commerce. Connecticut Insurance Law Journal. **8**(1), 7–36 (2001)

Jouini, M., Rabai, L.B.A., Aissa A.B.: Classifcation of Security Threats in Information Systems. Procedia Computer Science. **32**, 489–496 (2014)

Kesan, J.P., Majuca, R.P., Yurcik, W.J.: Cyberinsurance as a market-based solution to the problem of cybersecurity – A case study. In: Proceedings of the 4th Workshop on the Economics of Information Security (WEIS), Cambridge, June 2–3, 2005 (2005)

Kuckartz, U.: Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 3. Aufl. Beltz Juventa, Weinheim, Basel (2018)

Lale, Ö.: Alternativer Risikotransfer: Vorteile und Risiken des Transfers versicherungstechnischer Risiken auf die Kapitalmärkte (2013). https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2013/fa_bj_2013_06_alternativer_risikotransfer.html, Zugegriffen: 25. Okt. 2022

Lathrop, A.J., Stanisz, J.M.: Hackers are After More Than Just Data: Will Your Company's Property Policies Respond when Cyber Attacks Cause Physical Damage and Shut Down Operations? Environmental Claims Journal. **28**(4), 286–303 (2016)

Lee, A.S., Baskerville, R.L.: Generalizing Generalizability in Information Systems Research. Information Systems Research. **14**(3), 221–243 (2003)

Marotta, A., Martinelli, F., Nanni, S., Orlando, A., Yautsiukhin, A.: Cyber-Insurance Survey. Computer Science Review. **24**, 35–61 (2017)

Marotta, A., Martinelli, F., Nanni, S., Yautsiukhin, A.: A Survey on Cyber-Insurance. Technical Report IIT TR-17/2015. Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa (2015). http://www.iit.cnr.it/sites/default/files/TR-17-2015.pdf, Zugegriffen: 8. Dez. 2022

Mayring, P.: Qualitative Inhaltsanalyse: Grundlagen und Techniken, 12. Aufl. Beltz, Weinheim, Basel (2015)

McLellan, E., MacQueen, K.M., Neidig, J.L.: Beyond the Qualitative Interview: Data Preparation and Transcription. Field Methods. 15(1), 63–84 (2003)

Meland, P.H., Tøndel, I.A., Moe, M.E.G., Seehusen, F.: Facing uncertainty in cyber insurance policies. In: Livraga, G.,Mitchell, C. (Hrsg.) Security and Trust Management: 13th International Workshop, STM 2017, Oslo, Norway, September 14–15, 2017. Proceedings, S. 89–100. Springer, Cham (2017)

Merkens, H.: Stichproben bei qualitativen Studien. In: Friebertshäuser, B., Prengel, A. (Hrsg.) Handbuch Qualitative Forschungsmethoden in der Erziehungswissenschaft, S. 97–106. Juventa, Weinheim, München (1997)

Middleton, K., Kazamia, M.: 2016. Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns. In: Marano, P., Rokas, I., Kochenburger, P. (Hrsg.) The "Dematerialized" Insurance: Distance Selling and Cyber Risks from an International Perspective, S. 185–200, Cham, Springer (2016)

Miles, M.B., Huberman, A.M.: Qualitative Data Analysis: An Expanded Sourcebook, 2. Aufl. SAGE Publications, Thousand Oaks, CA, London, New Delhi (1994)

Moore, T.: The Economics of Cybersecurity: Principles and Policy Options. International Journal of Critical Infrastructure Protection. **3**(3–4), 103–117 (2010)

Myers, M.D., Newman, M.: The Qualitative Interview in IS Research: Examining the Craft. Information and Organization. 17(1), 2–26 (2007)

Nieuwesteeg, B., de Waard, B.: The Law and Economics of Cyber Insurance Contracts: a Case Study. European Review of Private Law. **26**(3) (2018)

Nurse, J. R., Axon, L., Erola, A., Agrafiotis, I., Goldsmith, M., Creese, S.: The Data that Drives Cyber Insurance: A Study into the Underwriting and Claims Processes. In: Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, June 15–19, 2020 (2020)

Organization for Economic Cooperation and Development (OECD): Supporting an Effective Cyber Insurance Market: OECD Report for the G7 Presidency (2017). https://www.oecd.org/daf/fn/insurance/Supporting-an-efective-cyber-insurance-market.pdf, Zugegriffen: 17. Nov. 2022

Romanosky, S.: Examining the Costs and Causes of Cyber Incidents. Journal of Cybersecurity. **2**(2), 121–135 (2016)

Romanosky, S., Ablon, L., Kuehn, A., Jones, T.: Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk?. Journal of Cybersecurity. **5**(1), 1–19 (2019)

Rowley, J.: Conducting Research Interviews. Management Research Review. **35**(3/4), 260–271 (2012)

Salmela, H.: Analyzing Business Losses Caused by Information Systems Risk: A Business Process Analysis Approach. Journal of Information Technology. **23**(3), 185–202 (2008)

Schnell, R., Hill, P.B., Esser, E.: Methoden der empirischen Sozialforschung, 9. Aufl. Oldenbourg, München (2011)

Schultze, U., Avital, M.: Designing Interviews to Generate Rich Data for Information Systems Research. Information and Organization. **21**(1), 1–16 (2011)

Siegel, M., Bartol, N., Carrascosa Pulido, J.J., Madnick, S.E., Coden, M., Jalali, M.S., Bernaski, M.J.: Cyber Insurance as a Risk Mitigation Strategy. Zurich: The Geneva Association (2018). https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf, Zugegriffen: 17. Nov. 2022

Smith, G.S.: Recognizing and Preparing Loss Estimates from Cyber-Attacks. Information Systems Security. **12**(6), 46–57 (2004)

Strupczewski, G.: The Cyber Insurance Market in Poland and Determinants of its Development from the Insurance Broker's Perspective. Economics and Business Review. **3**(2), 33–50 (2017)

Strupczewski, G. P., Thlon, M.: How Do Behavioral Factors Influence the Purchase of Cyber Insurance? Empirical Evidence From Polish Companies. In: Proceedings of the 27th Americas Conference on Information Systems (AMCIS), Online, August 9–13, 2021 (2021)

Talesh, S.A.: Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act As "Compliance Managers" for Businesses. Law & Social Inquiry. **43**(2), 417–440 (2018)

Tatar, U., Nussbaum, B., Gokce, Y., Keskin, O. F.: Digital Force Majeure: the Mondelez Case, Insurance, and the (Un) Certainty of Attribution in Cyberattacks. Business Horizons. **64**(6), 775–785 (2021)

Tonn, G., Kesan, J. P., Zhang, L., Czajkowski, J.: Cyber Risk and Insurance for Transportation Infrastructure. Transport policy. **79**, 103–114 (2019)

Tosh, D.K., Shetty, S., Sengupta, S., Kesan, J.P., Kamhoua, C.A.: Risk management using cyber-threat information sharing and cyber-insurance. In: Duan, L., Sanjab, A., Li, H., Chen, X., Materassi, D., Elazouzi, R. (Hrsg.) Game Theory for Networks: 7th International EAI Conference, GameNets 2017, Knoxville, TN, USA, May 9, 2017. Proceedings, S. 154–164. Springer, Cham (2017)

Willis Towers Watson (Hrsg.): Industrieversicherungen MARKTspot 2020 – Rückblick | Ausblick (2020). https://www.wtwco.com/-/media/WTW/Insights/2020/06/Industrieversicherungen-MARKTspot-2020.pdf?modified=20200624173253. Zugegriffen am 29. Dez. 2022

Woods, D.W., Agrafotis, I., Nurse, J.R.C., Creese, S.: Mapping the Coverage of Security Controls in Cyber Insurance Proposal Forms. Journal of Internet Services and Applications. **8**(1), 1–13 (2017)

Woods, D. W., Weinkle, J.: Insurance Definitions of Cyber War. The Geneva Papers on Risk and Insurance – Issues and Practice. **45**(4), 639–656 (2020)

Wrede, D., Stegen, T., von der Schulenburg, J.-M.: Affirmative and Silent Cyber Coverage in Traditional Insurance Policies: Qualitative Content Analysis of Selected Insurance Products from the German Insurance Market. The Geneva Papers on Risk and Insurance – Issues and Practice. **45**(4), 657–689 (2020)

Yin, R.K.: Case Study Research: Design and Methods, 3. Aufl. SAGE Publications, Thousand Oaks, CA, London, New Delhi (2003)

Young, D., Lopez Jr., J., Rice, M., Ramsey, B., McTasney, R.: A Framework for Incorporating Insurance in Critical Infrastructure Cyber Risk Strategies. International Journal of Critical Infrastructure Protection. **14**, 43–57 (2016)

Zelle, A.R., Whitehead, S.M.: Cyber Liability: It's Just a Click Away. Journal of Insurance Regulation. **33**(6), 145–168 (2014)

Zhao, X., Xue, L., Whinston, A.B.: Managing Interdependent Information Security Risks: Cyberinsurance, Managed Security Services, and Risk Pooling Arrangements. Journal of Management Information Systems. **30**(1), 123–152 (2013)