Entwicklung eines Risikobewertungsverfahrens für die Informationssicherheit in der Versicherungsbranche

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M. Sc.)" im Studiengang Wirtschaftswissenschaften der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: [redacted] Buschmann [redacted] Vorname: [redacted] René [redacted]

Prüfer: Michael H. Breitner
Zweitprüfer: Davinia Rodríguez Cardona
Betreuer: Andreas Walz & Marc Burde

Hannover, den 25.09.2019

Inhaltsverzeichnis

1. Einleitung

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology." – Bruce Schneier

Dieses Zitat des US-amerikanischen Experten für Kryptografie und Computersicherheit Bruce Schneier hebt deutlich hervor, dass eine vollständige Informationssicherheit nicht ausschließlich durch Technologie gewährleistet werden kann (vgl. Schneier o. J.). Ein wesentlicher Erfolgsfaktor im Unternehmen sind die Mitarbeiter, der im Verbund mit technologischen Lösungen dazu beitragen kann, dass die Informationen im Unternehmen geschützt werden. Oftmals werden Mitarbeiter oder Kunden als Einfallstore benutzt, um Zugang zum Unternehmensnetzwerk oder zu sensiblen Daten zu erhalten. Durch die Mitarbeiter kann die Gewährleistung und Verbesserung der Informationssicherheit erfolgen.

Die Unternehmen stehen heutzutage vor zahlreichen Herausforderungen und sind durch die Digitalisierung einer sich ändernden sowie global vernetzten Umwelt ausgesetzt (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017a: 5–6). In der sogenannten Wissensgesellschaft sind Informationen in einer noch nie dagewesen Vielzahl vorhanden und können global abgerufen werden (vgl. Ahmad et al. 2014). Dadurch sind Informationen neben Arbeit, Boden und Kapital zu einem entscheidenden Produktions- und Wettbewerbsfaktor geworden. Unternehmen sammeln, verarbeiten, speichern und übertragen Informationen, die z.T. sensibel und kritisch zu behandeln sind (vgl. ISO / IEC 27000:2014 2014: 12). Daher sollten Unternehmen ihr Wissen und die Informationsassets, wie geistiges Eigentum, Geschäftsgeheimnisse, Strategien und Produktentwürfe sichern. Um einen Wettbewerbsvorteil zu generieren müssen diese Assets vor Kompromittierung, Zugriff und Nutzung durch unautorisierte Nutzer, Offenlegung und Modifikation geschützt werden (vgl. Ahmad et al. 2014; Nieles et al. 2017: 2–3). Informationen und die dazugehörigen Prozesse, Systeme und Netzwerke sind in den Unternehmen zu einem wichtigen Asset geworden und müssen demzufolge wie jeder andere Wert angemessen geschützt werden (vgl. ISO / IEC 27000:2014 2014: 12; ISO / IEC 27002:2013 o. J.: vi; Misra et al. 2007). In dem Zusammenhang kam es durch den Wettbewerb zwischen Unternehmen in vielen Organisationen zu einem Umdenken und Informationen und Daten sind in den Fokus der Führungskräfte gerückt (vgl. Borek et al. 2014). Außerdem hat die zur Informationsverarbeitung, -speicherung und -übertragung benötigte IT weiterhin an Wichtigkeit gewonnen. Unternehmen stützen sich im Tagesgeschäft zusätzlich vermehrt auf IT-Produkte und -Services (vgl. Nieles et al. 2017: ii). Sind Informationen unverändert sowie vollständig vorhanden und nur für autorisierte Personen verfügbar, stellen sie einen entscheidenden Katalysator für die Effizienz des Unternehmens dar (vgl. ISO / IEC 27000:2014 2014: 12).
Der angesprochene benötigte Schutz der Informationen muss außerdem gewährleistet werden, um die Organisationsziele zu erreichen. Dabei ist die Definition, Implementierung, Aufrechterhaltung und Verbesserung der Informationssicherheit von zentraler Bedeutung (vgl. ISO / IEC 27000:2014 2014: 12). Die Informationssicherheit kann dazu beitragen, dass der Zugriff und Fluss von Daten sowie Informationen durch die Gewährleistung von Integrität, Vertraulichkeit und Verfügbarkeit gefördert und optimiert wird (vgl. Nieles et al. 2017: 11–12).

Jedoch behindern fehlende Ressourcen und knappe Budgets zur Absicherung der komplexen Systeme und Infrastrukturen die Gewährleistung einer angemessenen Informationssicherheit. Zusammen mit den kurzen Innovations- und Entwicklungszyklen der IT sowie der steigenden Komplexität der Systeme stehen Unternehmen vor zahlreichen Problemen (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017a: 5–6). Außerdem sind die Unternehmen durch die zunehmenden Veränderungen im Geschäftsumfeld mit Risiken unterschiedlicher Art konfrontiert, die eng mit den geschäftlichen Aktivitäten verbunden sind (vgl. Hoffmann et al. 2016: 1). Da Dynamik, Vielfältigkeit und Komplexität der Bedrohungslage zunehmen, widmet das Management zahlreicher Unternehmen dem Thema Informationssicherheit mehr Aufmerksamkeit. Das Anliegen des dazugehörigen Risikomanagements ist daher immer häufiger ein wichtiges Element der strategischen Unternehmensführung (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017a: 5–6; Hoffmann et al. 2016: 1). Durch die komplexen Bedrohungen, die neuen Technologien und das zunehmende Wissen bzw. Können der Angreifer werden heutzutage zur Neutralisierung von Bedrohungen mehr Ressourcen benötigt. In der Realität ist das Risikomanagement daher ein anspruchsvoller Prozess, der sich an die ständig ändernden Risikofaktoren anpassen muss. Insbesondere in der Risikobewertung treten Probleme bei den Unternehmen auf, da in den zahlreichen Standards keine Handlungsempfehlungen bezüglich der Umsetzung gegeben sind. Die angesprochene Risikobewertung ist ein wichtiger Bestandteil des Risikomanagements und ist für die anschließende Auswahl und Umsetzung von Informationssicherheitsmaßnahmen und zur Entscheidungsunterstützung essentiell. Jedoch treten in dieser Phase in der Theorie und Praxis häufig Probleme auf und behindern den Risikomanagementprozess. Theoretisch sind in dem Zusammenhang mehrere Standards vorhanden (z.B. ISO 2700X, BSI 200-X, NIST Special Publications), die allesamt Anforderungen an die Risikobewertung stellen und den Prozess beschreiben. Jedoch werden keine Empfehlungen zur Umsetzung gegeben, sodass in der Praxis kein einheitliches Vorgehen existiert (vgl. Sendi et al. 2016: 14–15; Young 2010). Aus diesem Grund haben viele Unternehmen in der Umsetzung Probleme und erarbeiten komplizierte Risikobewertungsmethoden, die oftmals Mängel in der Vergleichbarkeit sowie Reproduzierbarkeit aufweisen und nicht förderlich für die Awareness und die Hervorhebung der Wichtigkeit des Themas sind. Außerdem ist die Bewertung von Assets und Risiken z.T. sogar innerhalb eines Unternehmens inkonsistent. Obwohl die verschiedenen Abteilungen vor der gleichen Herausforderung stehen, gibt es keine dezentrale Lösung zur Risikobewertung. Hinzu kommt die Tatsache, dass die Ergebnisse der Risikobewertung oft schlecht kommunizierbar und unanschaulich aufbereitet werden. Diese beiden Aspekte sind ebenfalls hinderlich für die Sicherung Awareness und die Entscheidungsunterstützung.

Bei der Betrachtung der Informationssicherheit und des Risikomanagements explizit für die Versicherungsbranche treten einige Besonderheiten auf, durch die das Thema von besonderer Relevanz ist. Das Risikomanagement und die Sicherheit sind bereits im Grundsatz der Versicherungsunternehmen verankert. Versicherungsunternehmen existieren grundsätzlich, um die Kunden abzusichern. Die Haupttätigkeit von Versicherungen ist außerdem das Management bzw. der Transfer von Risiken (vgl. Müller-Peters/Völler 2012: 17). Des Weitern unterscheidet sich die Versicherungsbranche im Vergleich zu anderen Branchen dahingehend, dass Versicherungsunternehmen keine Produktion besitzen und die Daten sowohl Input als auch Output sind. Daher verarbeiten, speichern und übertragen diese Unternehmen eine Vielzahl an

sensiblen, personenbezogenen und kritischen Daten (z.B. Vertragsdaten, Bankdaten, Gesundheitsdaten, Betriebsgeheimnissen) (vgl. EIOPA 2018: 1; International Association of Insurance Supervisors 2016: 4; Müller-Peters o. J.). Das besondere an Versicherungen ist nicht ausschließlich die Vielzahl an sensiblen Daten, sondern vielmehr die sehr hohe Datenqualität. Die Daten, die Versicherungsunternehmen verarbeiten, werden bei der Erfassung mehrfach geprüft und validiert, weshalb die Daten eine hohe Güte haben. Außerdem bieten die Versicherungsunternehmen im hart umkämpften Wettbewerb zunehmend Online-Portale an, um den Kunden über verschiedene Schnittstellen zu kontaktieren. Jede zusätzliche Schnittstelle muss jedoch abgesichert werden und stellt eine potentielle Schwachstelle dar (vgl. Müller-Peters o. J.; Schröder/Lohse 2018: 110). Weiterhin ist die Branche durch die Bundesanstalt für Finanzdienstleistungsaufsicht stark reguliert, wodurch ein regulatorischer Druck auf der Informationssicherheit und insbesondere auf dem Risikomanagement der Versicherungsunternehmen liegt.

1.1 Zielsetzung und Aufbau

Die Wichtigkeit des Risikomanagements für die Informationssicherheit in den Versicherungsunternehmen, die eine Vielzahl an sensiblen Daten besitzen, sowie die zahlreichen Probleme, die in der Risikobewertung auftreten, sind ausschlaggebende Gründe für die Themenwahl der Arbeit. Außerdem sind die Prozess- und Systemlandschaften in großen Unternehmen äußerst heterogen und komplex, wodurch oftmals eine einheitliche Vorgehensweise der Bestimmung der Informationswerte und Risikobewertung problematisch ist (vgl. EIOPA 2018). In dem Zusammenhang ist ein Ziel der Arbeit die Bedeutung der Risikobewertung für die Informationssicherheit in der Versicherungsbranche. Außerdem soll darauf eingegangen werden, wie eine angemessene Bewertung die Informationssicherheit verbessern und somit für die Unternehmen einen Wettbewerbsvorteil generieren kann. Zur Verbesserung der Informationssicherheit und zum Schutz der geschäftskritischen Assets durch eine angemessene und übersichtliche Risikobewertung soll in Rahmen der Arbeit ein Verfahren entwickelt werden, dass bei den zahlreichen Probleme in der Risikobewertung Abhilfe schaffen kann. Dazu soll das entwickelte Verfahren hinsichtlich Bedienbarkeit als auch Einfachheit überzeugen und Informationsassets sowie Risiken anschaulich und angemessen bewerten. Innerhalb dieses Tools sollen die Ergebnisse verständlich aufbereitet und kommuniziert werden, sodass die Ergebnisse zur Priorisierung von Risiken, zur Risikobehandlung und zur Entscheidungsunterstützung genutzt werden können. Außerdem ist das Verfahren individuell auf Unternehmen und die aktuelle Bedrohungslage, die auf Grund der Digitalisierung und hohen Entwicklungsgeschwindigkeit der IT dynamischer geworden ist, anpassbar und lässt sich dementsprechend verändern. Letztendlich soll das entwickelte Verfahren auch dazu beitragen die Divergenz der Risikobewertung, die zwischen Theorie und Praxis besteht, aufzuheben bzw. zu reduzieren. Das zuvor erwähnte Verfahren soll daher bei der Umsetzung der theoretischen Grundlagen und Anforderungen zur Risikobewertung unterstützen.

Aus den angesprochenen Zielen und Problemen in der Thematik ergibt sich die folgende Forschungsfrage dieser Mastarbeit, die es im Rahmen der Arbeit zu beantworten gilt:

> *Wie und warum kann eine angemessene Bewertung von Risiken, als wesentlicher Bestandteil des Risikomanagements, zur Verbesserung der Informationssicherheit in der Versicherungsbranche beitragen?*

Um die Forschungsfrage zu beantworten und ein Verfahren zur Risikobewertung zu entwickeln, wird zuerst auf das methodische Vorgehen eingegangen, das zur Erarbeitung verwendet wurde. Im Anschluss wird der Auftraggeber, die Talanx AG, betrachtet und es folgen theoretischen Grundlagen im Kontext der Versicherungsbranche. In dem Zusammenhang werden aktuelle Zahlen und Herausforderungen sowie gesetzliche Besonderheiten behandelt. Ferner erfolgt eine theoretische Erklärung des Begriffs Information sowie eine detaillierte Darlegung der Informationssicherheit. Bezüglich der Informationssicherheit werden Erfolgsfaktoren, Schutzziele, Aufgaben und Pflichten des Managements sowie das Managementsystem für Informationssicherheit berücksichtigt. Nachdem diese theoretischen Grundlagen abgeschlossen wurden, widmet sich das 5. Kapitel dem Risikomanagement und beginnt mit einer Einführung in die Begrifflichkeiten und Prinzipien. Darauffolgend wird der Risikomanagementprozess, der ein Hauptbestandteil der Arbeit ist, ausführlich beschrieben. Nach der Erläuterung der Grundlagen, wird im darauffolgenden Kapitel mit der Entwicklung des Verfahrens zur Risikobewertung für die Informationssicherheit in der Versicherungsbranche begonnen. Dabei orientiert sich das Kapitel stark an den Phasen der Design Science Research Methodology und beginnt mit der Definition des Problems und der Erarbeitung der Ziele des Verfahrens. Darauf folgt das Design und die Entwicklung sowie die Demonstration mit Hilfe eines Use Cases. Auf die Entwicklung und die Demonstration erfolgt die Evaluation des Verfahrens durch Experten. Als Abschluss werden die Ergebnisse des Verfahrens mit Hilfe der Masterarbeit und eventuell durch eine Präsentation im Unternehmen kommuniziert. Nach der Entwicklung des Verfahrens wird die Arbeit durch Limitationen der Thematik und die Zusammenfassung der Ergebnisse im Fazit abgeschlossen.

8. Fazit und Ausblick

Das Ziel der Arbeit ist die Beantwortung der Forschungsfrage, wie und warum die Bewertung von Risiken, als wesentlicher Bestandteil des Risikomanagements, zur Verbesserung der Informationssicherheit in der Versicherungsbranche beitragen kann. Zur Beantwortung wurde ein Verfahren zur Risikobewertung für die Informationssicherheit in der Versicherungsbranche entwickelt. Dabei hat sich das Verfahren an verbreiteten Risikomanagementprozessen der Informationssicherheit orientiert und wurde mit Hilfe der Design Science Research Methodology entwickelt. Im Anschluss wurde das Verfahren mit Hilfe eines Use Cases demonstriert und durch Experteninterviews evaluiert.

Zur Klärung des Einflusses der Risikobewertung auf die Informationssicherheit wurden zuerst Herausforderungen und Besonderheiten der Versicherungsbranche herausgearbeitet. Diese Besonderheiten wurden anschließend mit der Informationssicherheit in Verbindung gebracht, sodass Schlussfolgerungen für die Wichtigkeit des Themas gezogen werden konnten.
Versicherungsunternehmen sind dahingehend besonders, dass die Haupttätigkeit der Versicherungen das Management bzw. der Transfer von Risiken ist und sie zur Absicherung von Risiken existieren (vgl. Experteninterview, Anhang G: XVI; Müller-Peters und Völler 2012: 17).
Außerdem sind die Kunden von Versicherungen eine anspruchsvolle Interessengruppe, die durch die mit der Globalisierung einhergehende Vernetzung individuelle Produkte und Beratung über verschiedene Kanäle nachfragen. Hinzu kommt, dass die Kunden in den letzten Jahren durch Vergleichsportale preissensitiver und informierter geworden sind. Insbesondere die neuen Kanäle in der Beratung, die oftmals durch Online-Portale auf mobilen Endgeräten umgesetzt werden, stellen die Versicherungsunternehmen vor neue Herausforderungen, da Schnittstellen abgesichert werden müssen und Angriffspunkte bieten (vgl. Experteninterview, Anhang J: XXXIII; Müller-Peters o. J.; Schröder und Lohse 2018: 110).
Eine weitere Besonderheit der Versicherungsunternehmen in Bezug auf die Informationssicherheit ist die starke Regulation der Branche. Einen enormen Einfluss hat in dem Zusammenhang Solvency II, durch die Versicherungsunternehmen Schlüsselfunktionen zur Gewährleistung des Vermögens und der Leistungsansprüche der Versicherten einrichten müssen. Zu den Schlüsselfunktionen zählt u.a. das Risikomanagement, das ein wesentlicher Bestandteil der Informationssicherheit ist (vgl. Gesamtverband der Deutschen Versicherungswirtschaft 2015b). Weiterhin hat die BaFin durch die Versicherungsaufsichtlichen Anforderungen darauf hingewiesen, dass der IT-Grundschutz des BSI und die ISO Normen zum Thema Informationssicherheit und Risikomanagement zu berücksichtigen sind. In den Anforderungen wird ebenfalls festgelegt, dass das Risikomanagement sowie das Informationssicherheitsmanagement in den Unternehmen kontinuierlich und strukturiert durchgeführt werden sollte (vgl. Bundesanstalt für Finanzdienstleistungsaufsicht 2018a, 2018b: 11–14). Zusätzlich zählen Versicherungsunternehmen nach der BSI-Kritisverordnung als kritische Infrastruktur und sind dahingehend besonders zu schützen. Dieser Schutz beinhaltet u.a. die Sicherheit der Informationen (vgl. Bundesministerium der Justiz und für Verbraucherschutz 2017: 1903). Die Vielzahl an Regularien sowie der Druck der Regulatoren hat die Bedeutung und Wichtigkeit der Informationssicherheit in der Versicherungsbranche stark vorangetrieben.

Des Weiteren ist die Betrachtung der Informationssicherheit in der Versicherungsbranche von Relevanz, da durch die Digitalisierung und Vernetzung die Geschwindigkeit der Entwicklung und die Komplexität der IT gestiegen ist. In diesem dynamischen Umfeld ist die Anpassung der Prozesse und Informationssicherheitsmethoden sowie -techniken zunehmend schwieriger. Die Probleme in der Anpassung liegen z.T. auch an der hohen Komplexität der Systeme und Prozesse sowie den organisatorischen Strukturen in Versicherungsunternehmen. Versicherungen stellen in der digitalen und vernetzten Welt durch die Vielzahl an sensiblen, personenbezogenen und kritischen Daten (Vertragsdaten, Bankdaten, Gesundheitsdaten, Betriebsgeheimnisse etc.) sowie der Schnittstellen zu Dienstleistern ein attraktives Ziel dar. Hinzu kommt die Tatsache, dass die Daten der Versicherungsunternehmen durch mehrfache Validierungen eine sehr hohe Datenqualität aufweisen. Zusätzlich sind infolge der Vernetzung die Informationsverbunde gewachsen, wodurch großflächige Angriffe einfacher und lukrativer geworden sind (vgl. EIOPA 2018: 1; International Association of Insurance Supervisors 2016: 4; Müller-Peters o. J.).

Das Ziel der Informationssicherheit ist grundsätzlich der Schutz der Informationen hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit. Generell sollten diese Ziele der Informationssicherheit im Einklang mit der strategischen Ausrichtung des Unternehmens sein. In diesem Bereich ist das Management zusätzlich für den Umgang mit Risiken sowie die Verabschiedung von Richtlinien, Strategien und Zielen verantwortlich. Weiterhin sollte das Management die Wichtigkeit der Informationssicherheit deutlich kommunizieren und als Vorbild agieren (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017a: 20–22; Grant et al. 2014; ISO / IEC 27001:2013 2013: 2–3). Erfolgsfaktoren in der Informationssicherheit sind u.a. organisatorische Regelungen, geregelte Zuständigkeiten sowie Verantwortlichkeiten, Berechtigungsmanagement und die Unterstützung durch das Management. Außerdem sind zuverlässige und informierte Mitarbeiter entscheidend, wobei die Awareness eine übergeordnete Rolle spielt. Die Awareness kann durch die Einbindung der Mitarbeiter, die Aufklärung über Sinn und Zweck von Sicherheitsmechanismen sowie -maßnahmen und das Aufzeigen von Folgen der Risiken gestärkt werden. Der Mensch ist in der Informationssicherheit ein Schlüsselelement, da täglich Interaktionen zwischen Menschen und Technik stattfindet. Für die Kommunikation der Wichtigkeit ist der Wissenstransfer entscheidend, wobei das Wissen einfach und verständlich kommuniziert werden sollte. Weiterhin sollte im Bereich der komplex erscheinenden Informationssicherheit Transparenz hergestellt und die dazugehörigen Prozesse möglichst vereinfacht werden (vgl. Bundesamt für Sicherheit in der Informationstechnik 2012: 41–53, 2017a: 5–6, 27; Ernst and Young 2012; Safa et al. 2016: 70; Trček et al. 2017).
Das Risikomanagement hat als Voraussetzung für die Gewährleistung einer angemessenen Informationssicherheit das Ziel die Risiken zielgerichtet und angemessen zu steuern, sodass unerwartete negative Ergebnisse minimiert werden. Für ein angemessenes Risikomanagement ist eine Risikokultur entscheidend, in der Risiken auf allen Ebenen identifiziert, analysiert, evaluiert und kommuniziert werden. Außerdem unterstützt das Risikomanagement die Führungskräfte bei Entscheidungen, dem Festlegen von Maßnahmen und der Auswahl von Handlungsmaßnahmen im Bedrohungsfall (vgl. Bundesamt für Sicherheit in der Informationstechnik 2017c: 5; Hoffmann et al. 2016: 5; ISO / IEC 27005:redline:2018 2018: 6; Liu et al. 2009; Nieles et al. 2017: 44; Wheeler 2011). Zu dem Risikomanagement gehört der Risikomanagementprozess der in gängigen Standards, wie den BSI Standards und den ISO-Normen, darge-

stellt wird. Dieser Prozess beginnt mit der Definition von Umfang, Kontext und Kriterien. Anschließend folgt die Risikobewertung, die für den Hauptteil der Arbeit am wichtigsten ist. Die Risikobewertung setzt sich aus der Identifikation, Analyse und Evaluation von Risiken zusammen. Nachdem alle relevanten Risiken identifiziert und bewertet vorliegen, wird die Risikobehandlung durchgeführt. Dabei werden durch Risikovermeidung, -übernahme, -reduktion oder dem Transfer von Risiken die vorliegenden Risiken minimiert, sodass diese akzeptiert werden können. Auf die Bewertung folgt abschließend die Aufzeichnung und Berichterstattung, damit die Risiken beobachtet und die Ergebnisse kommuniziert werden können. Die angesprochene Kommunikation findet während des gesamten Prozesses statt, um betroffene Interessengruppen in den Prozess zu involvieren und über den aktuellen Stand zu informieren. Weiterhin wird der gesamte Prozess überwacht und geprüft, sodass das Ergebnis als valide Grundlage für weitere Entscheidungen dient (vgl. ISO / IEC 27005:redline:2018 2018: 9, 24; ISO 31000:2018 2018: 9).

Aus den vorangegangen Abschnitten geht deutlich hervor, dass die Risikobewertung ein wichtiger Bestandteil des Risikomanagements ist und somit die Informationssicherheit beeinflussen kann. Im Hinblick auf die Forschungsfrage geht hervor, dass ein angemessenes Level der Informationssicherheit hergestellt werden kann, wenn geschäftskritische Informationsassets und relevante Risiken strukturiert und adäquat identifiziert, analysiert und evaluiert werden. Werden die wichtigsten Informationssicherheitsrisiken nicht angemessen bewertet, kann das Level der Informationssicherheit nicht aufrechterhalten werden. Die Risikobewertung ist demzufolge eine wichtige Entscheidungsgrundlage für das Management im Hinblick auf die Risikobehandlung, die Priorisierung der Risiken, die dazugehörige Maßnahmenauswahl und das Erkennen von Handlungsbedarfen im Fall von Bedrohungen. Des Weiteren muss die Risikobewertung ein einheitliches Vorgehen und eine angemessene Qualität haben, damit die Risiken minimiert und gesteuert werden können. Auf diese Weise kann das Ziel des Risikomanagements erreicht werden. Zusätzlich sind Versicherungsunternehmen regulatorischen Zwängen ausgesetzt und durch Solvency II verpflichtet Risikomanagement auszuüben.
Weiterhin wird die Wichtigkeit des Risikomanagements, insbesondere des Risikomanagementprozesses, in den Standards von ISO, BSI und NIST hervorgehoben.

Im Rahmen der Risikobewertung sind Unternehmen jedoch mit zahlreichen Problemen konfrontiert. In dem Zusammenhang spielt vor allem die Divergenz zwischen Theorie und Praxis eine übergeordnete Rolle und soll mit Hilfe des Verfahrens geschlossen werden. Auf der einen Seite ist in der Theorie zahlreiches Wissen über die Einführung und Umsetzung des Managementsystems der Informationssicherheit und des Risikomanagements vorhanden. Auf der anderen Seite sind jedoch keine Details zur Implementierung verbreitet, die Vorgaben zur Umsetzung einer angemessenen Risikobewertung für die Praxis geben (vgl. Oppliger 2015b: 18; Sendi et al. 2016: 15).
In der Risikobewertung kommt es oftmals durch Fehler in der Phase der Identifikation der Assets zu Ungenauigkeiten (vgl. Siponen 2005; Webb et al. 2014; Zafar/Clark 2009). Die Identifizierung der kritischen Assets ist eine Grundvoraussetzung für die anschließende Identifikation und Evaluation der relevanten Risiken in Versicherungsunternehmen. Zu den häufigsten Defiziten in dieser Phase zählen eine zu grobe Granularität der Assets, die Vernachlässigung von Informationsassets und die fehlende Berücksichtigung von immateriellen Assets

(vgl. Ahmad et al. 2005; Röhrig/Knorr 2004; Shedden et al. 2011). Auch in der ersten Phase der Risikobewertung, der Identifikation, treten Probleme auf, da Listen von Bedrohungen und Schwachstellen unvollständig sind oder irrelevante Risiken enthalten. Auf die Identifikation folgt die Risikoanalyse, die oftmals quantitativ durchgeführt werden soll, um die Entscheidungsfindung zu verbessern sowie die Steuerung und die Priorisierung von Risiken zu unterstützen (vgl. ISO / IEC 27005:redline:2018 2018: 20; National Institute of Standards and Technology 2012: 14). Jedoch werden für den quantitativen Ansatz eine Vielzahl an Informationen zur Ermittlung der Eintrittswahrscheinlichkeit und der Auswirkungen des Risikos benötigt (vgl. Oppliger 2015b: 19–20).
Weiterhin gibt es in Unternehmen selten einheitliche Vorgehensweisen in der Informationswertbestimmung und der Risikobewertung. Die Schwierigkeit liegt dabei in der Entwicklung eines Verfahrens zur anschaulichen und adäquaten Risikobewertung.

An den angesprochenen Problemen setzt das entwickelte Verfahren zur Risikobewertung an. Dabei werden zuerst die geschäftskritischen Assets sowie die relevanten Risiken bewertet und anschließend miteinander in Verbindung gebracht. Die Entwicklung basiert auf der Motivation, dass die wichtigsten Informationsassets im Unternehmen zu schützen sind. Durch die anschauliche Darstellung sollen Mitarbeiter und Geschäftsführung für die Auswirkungen der Risiken auf die geschäftskritischen Assets sensibilisiert und die Awareness in Bezug auf Informationssicherheit gesteigert werden. Die Awareness kann sich durch die einfache Aufbereitung der technischen sowie schwer verständlichen Risiken erhöhen, wodurch die Mitarbeiter mit möglichen Risiken der täglichen Arbeit konfrontiert werden. Somit kann das Verfahren dazu beitragen, dass das Thema Informationssicherheit die benötigte Aufmerksamkeit und Sichtbarkeit im Unternehmen erhält. Das Verfahren liefert einen Wert für Versicherungsunternehmen, da ein einheitliches, standardisiertes und angemessenes Bewertungsverfahren dargestellt wird und eine gewisse Vergleichbarkeit und Reproduzierbarkeit hergestellt werden kann. Zusätzlich wird ein kombinierter Ansatz aus einer qualitativen und quantitativen Risikoanalyse verfolgt, damit die Nachteile des jeweiligen Vorgehens eliminiert werden. Durch die hergestellte Vergleichbarkeit und Reproduzierbarkeit können Risiken durch das Management gesteuert und priorisiert werden. Neben den Mitarbeitern profitiert dementsprechend das Management von dem entwickelten Verfahren. Das Verfahren liefert eine fundierte Grundlage für die Risikobehandlung, weshalb sich die Leitung auf die Ergebnisse der Risikobewertung stützen und diese für die Entscheidungsfindung und Maßnahmenauswahl nutzen kann. Weiterhin liefert das Verfahren Vorteile hinsichtlich der Anwendbarkeit und der Individualität, da die Bewertung ohne detaillierte Erklärungen individuell für einzelne Versicherungsunternehmen durchgeführt werden kann.
Durch die Steigerung der Awareness sowie die Bereitstellung von Entscheidungsgrundlagen, kann das Verfahren zur Risikobewertung dazu beitragen, dass sich die Informationssicherheit in Versicherungsunternehmen verbessert.

Obwohl das Tool zahlreiche Vorteile liefert und die Informationssicherheit unterstützt, bedarf der Bereich weiterer zukünftiger Forschung. Bezüglich des Verfahrens zur Risikobewertung sollte z.B. eine Programmierung des Tools vorgenommen werden, damit dieses als Website abrufbar ist und besser erreichbar bzw. nutzbar ist. Durch mehrere Nutzer kann das Verfahren hinsichtlich Anwendbarkeit und Funktionalität evaluiert und anschließend verbessert werden.

Um die Qualität des Verfahrens zu verbessern, wäre die Integration der Risikoidentifikation in das Tool hilfreich. Dieser Punkt ist entscheidend für die Risikobewertung, da oftmals Probleme bei der Identifikation der relevanten Informationssicherheitsrisiken auftreten. Dafür könnten z.B. CERT- oder LKRZV-Meldungen automatisch ausgewertet werden, um diese teilweise als relevante Risiken zu erfassen. Für die erste Nutzung des Verfahrens ist jedoch die Betrachtung der OWASP Top 10 Risiken sowie die Möglichkeit der Erstellung eigener Risiken ausreichend. Ein weiterer Aspekt für die zukünftige Forschung beinhaltet die Betrachtung des Einflusses von existierenden bzw. geplanten Maßnahmen auf den Schutz der Informationsassets. Die Berücksichtigung der Maßnahmen hätte zur Folge, dass Management und Unternehmen bei Entscheidungen und der Maßnahmenauswahl unterstützt werden.
Weitere Verbesserungspotentiale treten im Risikomanagement in der Praxis auf. In diesem Gebiet könnte ein präventives Risikomanagementsystem in Zukunft von Interesse sein. Die Herangehensweise könnte dahingehend geändert werden, dass bereits vor dem Auftreten von Risiken reagiert wird. Die Risikoprävention könnte durch einen Maßnahmenkatalog durchgeführt werden. Dieser Katalog enthält Maßnahmen, die standardgemäß umgesetzt werden sollen und somit eine Vielzahl an Risiken vorab eliminiert können. Hinzu kommt, dass das Prinzip der Prävention auch während der durchaus fehlerbehafteten quantitativen Risikoanalyse durchgeführt werden könnte. Auf diese Weise könnten die fehlenden Informationen ausgeglichen werden, indem keine Bewertung der Risiken vorgenommen wird, sondern Gegenmaßnahmen mit einem guten Kosten-Nutzen Verhältnis umgesetzt werden. Zu möglichen Maßnahmen zählen z.B. Virenscanner, Passwortmanagement, Patchmanagement und Firewalls. Die Umsetzung dieser Maßnahmen ist kostengünstig und hat einen positiven sowie signifikanten Effekt auf die Informationssicherheit. Ein weiterer Ansatz, um die quantitative Risikoanalyse zu umgehen, ist die Identifikation und Eliminierung von Schwachstellen. Ohne Schwachstellen können keine Risiken auftreten, weshalb dies einen automatischen bzw. semiautomatischen Weg zur Eliminierung von Risiken darstellt. Eine letzte Möglichkeit ist die Vereinfachung der Risikoanalyse hinsichtlich der Machbarkeit. Dahingehend würden keine exakten Werte für die Wahrscheinlichkeit und Schäden genutzt werden, sondern qualitative Werte durch Ordinalskalen (vgl. Oppliger 2015b: 20–21). Der Ansatz der qualitativen Risikoanalyse bzw. des kombinierten Ansatzes aus beiden Verfahren wird bereits in der Praxis angewendet. Jedoch muss ein solches Vorgehen hinsichtlich Qualität und Aussagekraft durch Erfahrungswerte im Unternehmen stetig verbessert werden.

Abschließend lässt sich sagen, dass die Informationssicherheit ein wichtiger Teil eines jeden Versicherungsunternehmens sein sollte, da bei einem unzureichenden Schutz enorme Kosten entstehen können. Hinsichtlich der Umsetzung der Informationssicherheit und des Risikomanagements gibt es jedoch große Handlungsbedarfe in vielen Unternehmen, wobei automatisierte Tools die Arbeit erleichtern können.