Institut für Versicherungswirtschaft

Universität St.Gallen

Cyber Risk: Risikomanagement und Versicherbarkeit

Christian Biener / Martin Eling / Andreas Matt / Jan Hendrik Wirfs



I·VW HSG Schriftenreihe, Band 54

Christian Biener / Martin Eling / Andreas Matt / Jan Hendrik Wirfs

Cyber Risk:
Risikomanagement und Versicherbarkeit

Herausgeber und Verlag

Institut für Versicherungswirtschaft der Universität St. Gallen

ISBN 978-3-9523551-8-3

© Verlag Institut für Versicherungswirtschaft der Universität St. Gallen, St. Gallen 2015

(I·VW Schriftenreihe; Band 54)

Alle Rechte vorbehalten. Nachdruck oder Vervielfältigung, auch auszugsweise, in allen Formen wie Mikrofilme, Xerografie, Mikrofiche, Microcard, Offset verboten.

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Cyber Risk: Risikomanagement und Versicherbarkeit

[Hrsg. Institut für Versicherungswirtschaft der Universität St. Gallen]

Christian Biener / Martin Eling / Andreas Matt / Jan Hendrik Wirfs

St. Gallen: Institut für Versicherungswirtschaft, 2015

Inhaltsverzeichnis

Abstract V
Dank VI
Tabellenverzeichnis VII
Abbildungsverzeichnis VIII
1 Motivation 1
2 Cyber Risk: Definition und Beispiele 4
2.1 Definition und Abgrenzung von Cyber Risk 4
2.1.1 Nicht kriminelle Ursachen für Cyber Risk 10
2.1.2 Kriminelle Ursachen (Cybercrime) 11
2.2 Systematische Analyse von Cyber Risk 16
2.2.1 Datenquellen zu Cyber Risk 16
2.2.2 Fallbeispiele International 18
2.2.3 Fallbeispiele Schweiz 23
2.3 Analyse der globalen und politischen Seite von Cyber Risk 26
2.3.1 Cyberattacke auf Estland 26
2.3.2 Stuxnet-Virus 26
2.3.3 Afrikanischer Frühling: Tunesien 27
2.3.4 NSA-Spionage 28
2.3.5 Zusammenfassung der Fallbeispiele 29
2.4 Abhängigkeit vom Internet und Ausfallrisiko 30
3 Management von Cyber Risk 34
3.1 Risikomanagement nach ISO 31000:2009 34
3.2 Cyber Risk im Risikomanagement-Prozess 40
3.2.1 Zusammenhang herstellen 41
3.2.2 Cyber Risk identifizieren 42
3.2.3 Cyber Risk analysieren 45
3.2.4 Cyber Risk bewerten 46
3.2.5 Cyber Risk bewältigen 47
3.2.6 Kommunikation und Informationsaustausch 49
3.2.7 Überwachung und Überprüfung 49
3.3 Zusammenfassung: Was ist für ein erfolgreiches Management von Cyber Risk wichtig? 50
4 Cyber-Versicherung: Versicherbarkeit von Cyber Risk 51
4.1 Definition von Cyber-Versicherung 51
4.2 Marktübersicht Versicherungslösungen 55
4.2.1 Globaler Markt für Cyber-Versicherung 55
4.2.2 Schweizer Markt für Cyber-Versicherung 55
4.3 Kriterien der Versicherbarkeit 60
4.3.1 Zufälligkeit des Schadenereignisses 62
4.3.2 Maximal möglicher Schaden 64
4.3.3 Mittlere Schadenhöhe 64
4.3.4 Mittlere Schadenhäufigkeit 64
4.3.5 Informationsasymmetrien 65
4.3.6 Versicherungsprämie 65
4.3.7 Deckungsabgrenzung 66
4.3.8 Gesellschaftliche Werte 67
4.3.9 Gesetzliche Schranken 68

4.3.10 Zusammenfassung der Kernresultate zur Versicherbarkeit 69
5 Cyber Risk: Befragung aus Perspektive der Kunden 71
5.1 Befragungsdesign und Methodik 71
5.2 Definition und Bedeutung von Cyber Risk 72
5.3 Risikomanagement von Cyber Risk 74
5.4 Versicherbarkeit von Cyber Risk 78
5.5 Zusätzliche Informationen aus der Befragung 79
5.6 Befragungsergebnisse der KMUs 80
5.7 Ableitung von fünf Thesen 82
6 Cyber Risk: Befragung aus Perspektive der Anbieter 83
6.1 Befragungsdesign und Methodik 83
6.2 Definition und Bedeutung von Cyber Risk 84
6.3 Risikomanagement von Cyber Risk 85
6.4 Versicherbarkeit von Cyber Risk 88
6.5 Zusätzliche Informationen aus der Befragung 90
6.6 Ableitung von fünf Thesen 93
7 Fazit 94
Anhang 98
Teil A: Fragenkatalog für die Marktbefragung in Kapitel 5 (Kundensicht) 98
Teil B: Fragenkatalog für die Marktbefragung in Kapitel 6 (Anbietersicht) 100
Literaturverzeichnis 104
Autoren 113

Abstract

Cyber Risk stellt eines der grossen neuen Risiken des 21. Jahrhunderts dar. Wir analysieren das Management dieser neuen Risikoart und nehmen eine Einschätzung zur Versicherbarkeit vor. Zu diesem Zweck begutachten wir die bestehende Literatur und nehmen Befragungen unter Kunden und Anbietern von Cyber-Versicherungen vor. Unsere Ergebnisse zeigen, dass ein effizientes Risikomanagement die Wahrscheinlichkeit und das Ausmass eines Cyber-Risk-Schadens erheblich senken kann. Cyber-Versicherungen bieten in diesem Kontext eine gute Möglichkeit, Risiken zu transferieren und können so zu einem effizienten Risikomanagement beitragen. Die Marktbefragung unter Kunden und Anbietern der Cyber-Versicherung unterstreicht die zunehmende Bedeutung von Cyber Risk, aber auch eine gewisse Skepsis vor entsprechenden Versicherungslösungen. Wir zeigen auf, welche Faktoren die Entwicklung dieses Marktes derzeit noch behindern und unter welchen Bedingungen eine Marktentwicklung möglich erscheint. Unserer Prognose nach entsteht mit der Cyber-Versicherung derzeit ein grosser neuer Versicherungsmarkt, der in den kommenden Jahren enorm an Bedeutung gewinnen wird.

Statements aus der Studie

„Das Management von Cyber Risk ist in Unternehmen noch unterentwickelt und bedarf erheblicher Verbesserungen."

"Das Volumen des Cyber-Versicherungsmarkts wird in der Schweiz auf lediglich fünf Millionen Schweizer Franken geschätzt."

„Die Befragten gehen davon aus, dass sich der Markt für Cyber-Versicherung in der Schweiz in den kommenden fünf Jahren vervierfachen oder sogar bis zu verzehnfachen wird."

Einige Highlights der Studie

- Aktuelle Fallbeispiele – International und Schweiz (ab Seite 18)
- Sieben Leitlinien für ein erfolgreiches Cyber-Risikomanagement (Seite 50)
- Schweizer Markt für Cyber-Versicherung im Überblick (Seite 55)
- Versicherbarkeit von Cyber Risk heute nur bedingt möglich (Seite 70)
- Fünf Thesen zu Cyber Risk – Aus Kunden- (Seite 82) und Anbietersicht (Seite 93)
- Pro und Kontra der Cyber-Versicherung (Seite 96)

Dank

Wir bedanken uns sehr herzlich bei allen Teilnehmern der Befragung. Angaben der teilnehmenden Unternehmen wurden anonym behandelt und eine Weitergabe der Daten fand nicht statt. Auch bedanken wir uns bei allen Personen, die für Vorgespräche zur Verfügung standen und der Kessler & Co AG für den finanziellen und inhaltlichen Beitrag zur Umsetzung dieser Studie, insbesondere bei Martin Kessler, Christian Kessler, Christian Peters und Simon Schneiter. Des Weiteren bedanken wir uns bei Margarete Geser und Andreina Zink für die Hilfe bei der Erstellung und Umsetzung dieser Studie.

Tabellenverzeichnis

Tabelle 1: Cyber-Risk-Definitionen 5
Tabelle 2: Abgrenzung der Risikoarten 6
Tabelle 3: Cyber-Risk-Kategorien (in Anlehnung an Cebula und Young, 2010) 8
Tabelle 4: Ursachen für Cyber Risk 9
Tabelle 5: Auswirkungen von Cyber Risk 10
Tabelle 6: Hackermethoden 14
Tabelle 7: Datenquellen zu Cyber Risk 16
Tabelle 8: Ausgewählte Fallbeispiele International 23
Tabelle 9: Ausgewählte Fallbeispiele Schweiz 24
Tabelle 10: Fallbeispiele zur globalen und politischen Bedeutung von Cyber Risk 29
Tabelle 11: Wissenschaftliche Arbeiten zu Cyber-Versicherung 52
Tabelle 12: Deckungen für Cyber Risk (in Anlehnung an Peters, 2012 und Marsh, 2012) 53
Tabelle 13: Datenquellen zur Cyber-Versicherung 55
Tabelle 14: Überblick Cyber-Versicherung in der Schweiz 59
Tabelle 15: Kriterien der Versicherbarkeit (Berliner, 1982) 60
Tabelle 16: Versicherungskriterien und Erfüllungsgrad bei Cyber Risk 69
Tabelle 17: Ergebnis zur Effektivität von RM-Massnahmen 87
Tabelle 18: Ergebnis zur Erfüllung der Versicherbarkeitskriterien 88
Tabelle 19: Ergebnisse zu Pricing-Parametern 91
Tabelle 20: Einschätzung zu Risiken beim Pricing 91
Tabelle 21: Kernresultate der Marktbefragungen 95
Tabelle 22: Pro und Kontra der Cyber-Versicherung 96

Abbildungsverzeichnis

Abbildung 1: Zahlen und Fakten zu Cyber Risk 2
Abbildung 2: Abgrenzung von Cyber Risk 7
Abbildung 3: Angriffstopografien (in Anlehnung an Kizza, 2002, S. 80–81) 12
Abbildung 4: Technologische Risiken im Rahmen des Global Risk Reports (WEF, 2012) 17
Abbildung 5: Kurseinbruch S&P 500 (Yahoo Finance, 2013) 20
Abbildung 6: Aktuelle Fallbeispiele Schweiz – Phishing (MELANI, 2014) 25
Abbildung 7: Aktuelle Fallbeispiele Schweiz – E-Mail-Hacking (MELANI, 2014) 25
Abbildung 8: Tiefseekabel weltweit (TeleGeography, 2014) 31
Abbildung 9: Risikomanagement nach ISO 31000:2009 (ISO31000, 2009) 35
Abbildung 10: Marsh Cyber-Risikotest 44
Abbildung 11: Zusammenfassung Marsh Cyber-Risikotest für das I·VW 45
Abbildung 12: Risk Map (in Anlehnung an Seibold, 2006, S. 86) 47
Abbildung 13: Ergebnisse der Befragung zum Umgang und Relevanz von Cyber Risk 80
Abbildung 14: Ergebnisse der Befragung zur Konsequenz und Wahrscheinlichkeit eines beispielhaften Cyber-Risk-Vorfalls 81
Abbildung 15: Befragungsergebnis zur Risk Map 86

1 Motivation

Mit der Kommerzialisierung des Internets in den 1990er-Jahren startete eine neue Ära des Informationszeitalters. Die weltweite Vernetzung nahm rasant zu. Der enorme technologische Fortschritt brachte viele Chancen mit sich: Innert kürzester Zeit entstanden neue Weltkonzerne wie Google oder Facebook und ihre Gründer wurden zu Milliardären. Auch machte dieser Fortschritt den Datenverkehr effizienter, da er sich viel schneller abwickeln liess. Das Internet und die entstandenen sozialen Netzwerke ermöglichen den Menschen weltweit, jederzeit, einfach und kostengünstig in Kontakt zu treten.[1] Nahezu alle Aktivitäten des Alltags lassen sich heutzutage über Datennetzwerke abwickeln: Vom E-Mail-Verkehr und Telefon, über Einkäufe bis hin zu Bankgeschäften.

Neben den Chancen, die durch diesen technologischen Aufschwung entstehen, reihen sich auch neue Gefahren ein. Diese werden insbesondere unter dem Stichwort Cyber Risk zusammengefasst. Beispielsweise kann ein Unternehmen finanziell stark geschädigt werden, wenn verloren gegangene Daten zurückgewonnen werden müssen. Es können aber auch erhebliche indirekte Kosten entstehen, beispielsweise wenn der Datenverlust mit einer Reputationsschädigung einhergeht. Datennetzwerke, wie das Internet, bieten auch ausgesprochen lukrative Möglichkeiten für Kriminelle. Die Methoden, mit denen sie ihre Cyberangriffe durchführen, sind sehr vielseitig und können Privatpersonen, Unternehmen oder auch staatliche Institutionen treffen und so massiv schädigen. Zudem werden die Angriffe immer zielgerichteter, professioneller und verursachen erhebliche Schäden bei den Betroffenen (siehe Ponemon, 2013).

Es lassen sich zahlreiche aktuelle Belege für die enorme Relevanz von Cyber Risk anführen. Aus ökonomischer Sicht können etwa die jüngsten Stellungnahmen der G20 oder des World Economic Forums genannt werden.[2] Aus gesellschaftspolitischer Sicht können Themen wie der arabische Frühling oder der NSA-Datenskandal angeführt werden. Abbildung 1 zeigt einige aktuelle Zahlen und Fakten zu Cyber Risk in Deutschland und der Schweiz. Schon diese wenigen Belege verdeutlichen die hohe ökonomische, technologische und gesellschaftliche Bedeutung von Cyber Risk. Alle Studien und Experten weisen darauf hin, dass ihre Bedeutsamkeit in den kommenden Jahren erheblich zunehmen wird. Cyber Risk stellt damit eines der grossen neuen Risikothemen des 21. Jahrhunderts dar.

---

1 Die rasante technologische Entwicklung kann gut anhand des weltweit in einem Jahr generierten Datenvolumens verdeutlicht werden. IDC (2014) bestimmt das im Jahr 2013 entstandene Volumen auf rund 4,4 Zettabyte (Zahl mit 21 Stellen). Bis ins Jahr 2020 soll dieser Wert auf 44 Zettabyte anwachsen (IDC, 2014).

2 So hat die G20 Cyber Risk als eine Gefahr für die Weltwirtschaft bezeichnet; Vgl. Ackermann (2013). Das World Economic Forum (2014) führt im Global Risk Report Cyberattacken als eines der Top 5 Risiken bzgl. Eintrittswahrscheinlichkeit.



Abbildung 1: Zahlen und Fakten zu Cyber Risk

Der grossen Bedeutung von Cyber Risk steht derzeit eine relativ geringe Nachfrage nach Cyber-Versicherungsprodukten gegenüber. Eine aktuelle Umfrage der Harvard Business Review unter 152 US-amerikanischen Unternehmen des privaten und öffentlichen Sektors zeigt, dass zwar viele Unternehmen um ihre IT-Sicherheit besorgt sind, die Mehrheit (60 %) aber in näherer Zukunft keine Pläne hat, eine Cyber-Versicherung abzuschliessen. Nur 19 % der befragten Unternehmen verfügen derzeit über eine Form der Cyber-Versicherung (Harvard Business Review, 2013).

Dies führt unmittelbar zur Frage der Versicherbarkeit. Ein grosses Problem ist zum Beispiel, dass die Schäden aus Cyber Risk nicht verlässlich geschätzt werden können. Neben direkt zurechenbaren Kosten können auch erhebliche nicht direkt messbare Kosten, wie beispielsweise Reputationsverluste, anfallen. Wie kann sich ein Unternehmen genau vor Cyber Risk schützen? Welche Rolle können Versicherungslösungen als Risikotransferinstrumente spielen? Im Kern dieser Ausarbeitung steht die Analyse dieser beiden Fragen.

Diese Studie gibt eine Gesamtschau zu Cyber Risk und zeigt, wie sich ein Unternehmen mittels Risikomanagement vor diesem Risiko schützen kann. Die Arbeit stellt einen Brückenschlag zwischen Definition, Risikomanagement und Versicherbarkeit dar, veranschaulicht Vor- / Nachteile der jeweiligen Schutzmassnahmen und gibt einen Überblick über die aktuell angebotenen Versicherungslösungen. Anhand zweier Marktbefragungen – eine unter Kunden und eine unter Anbietern von Cyber-Versicherungen – wird ersichtlich, welche Bedeutung die Cyber-Versicherung heute hat und wie ein effektives Risikomanagement inklusive Cyber-Versicherung ausgestaltet werden kann. Unsere Resultate zeigen, dass derzeit ein grosser neuer Versicherungsmarkt entsteht. Wir zeigen aber auch, welche Faktoren die Entwicklung dieses Marktes derzeit noch behindern und unter welchen Bedingungen die Marktentwicklung gefördert werden kann.

Anzumerken ist, dass wir uns in dieser Studie auf das Geschäft mit Unternehmen fokussieren und Cyber Risk für Privatkunden weitgehend ausblenden.[3] Auch fokussieren wir in der Studie insbesondere die Situation in der Schweiz, so etwa beim Marktüberblick über Versicherungsprodukte.

Die Arbeit ist wie folgt aufgebaut. Kapitel 2 definiert zunächst den Begriff Cyber Risk. In Kapitel 3 wird das Risikomanagement von Cyber Risk analysiert. Anschliessend diskutieren wir in Kapitel 4 die Versicherbarkeit dieser Risiken. Die Kapitel 5 und 6 zeigen die Ergebnisse der beiden Marktbefragungen zu Cyber Risk aus Kunden- und Anbietersicht und Kapitel 7 schliesst mit einem Fazit.

[3] So hat beispielsweise jüngst die Groupe Mutuel eine neue Rechtsschutzversicherung unter dem Titel „legis digital“ lanciert, die auch Risiken im Internet und elektronische Transaktionen abdeckt. Dieses Produkt wurde mit dem Innovationspreis der Assekuranz im Jahr 2013 ausgezeichnet, was die Neuartigkeit und Relevanz derartiger Produktentwicklungen auch im Privatkundengeschäft unterstreicht.

2 Cyber Risk: Definition und Beispiele

2.1 Definition und Abgrenzung von Cyber Risk

Was ist Cyber?
Das Wort „Cyber“ ist vom englischen Cybernetics abgeleitet. Es beschreibt die Kybernetik mit ihren dazugehörigen Regel- und Steuervorgängen. Im Hinblick auf das Internet wird das Wort Cyber oftmals verwendet, um künstliche Realitäten zu beschreiben. Es wird aber auch als Präfix für verschiedene Gebiete benutzt, die einen Bezug zu Computern haben. Beispielsweise ist der Begriff Cyber Risk eng mit dem Begriff Cyberspace verbunden, der den Datenraum aller digitalen Netze beschreibt, in denen Informationen gespeichert, verändert und transferiert werden. Dieser Datenraum umfasst sämtliche IT-Systeme zur Unterstützung von Unternehmen und deren Infrastruktur (siehe GCHQ, 2012).

Was ist Risk?
Das Wort „Risiko“ ist schon seit vielen Jahrzehnten Gegenstand der Forschung. Risiko wird im Allgemeinen als eine Situation unter Unsicherheit definiert. Häufig wird darunter ein Ereignis mit der Möglichkeit negativer Auswirkungen gefasst. Eine weitergehende Definition kann neben Risiken aber auch Chancenpotenziale beinhalten. Im ersten Fall sprechen wir vom reinen Risiko, im zweiten Fall von spekulativem Risiko. Risiken können verschiedene Ursachen haben: physische Ursachen wie Naturkatastrophen, ökonomische Ursachen wie die BIP-Entwicklung, soziale Ursachen wie Änderungen von Normen und Werten oder rechtliche Ursachen wie die Einführung eines neuen Gesetzes. In Versicherungsunternehmen wird im Allgemeinen eine Einteilung der Risiken in Markt-, versicherungstechnische, Kredit- und operationelle Risiken vorgenommen.

Was ist Cyber Risk?
Der Begriff Cyber Risk bezieht sich auf eine Vielzahl potenzieller Risiken, die im Zusammenhang mit der Technologie oder mit Informationen eines Unternehmens stehen. Die US-amerikanische Versicherungsaufsichtsbehörde NAIC (2013) stuft Cyber Risk auf ihrer Internetseite als ein „key issue“ ein und gibt typische Beispiele für Cyber Risk. Dazu gehören Identitätsdiebstahl, die Weitergabe von sensiblen Informationen, Betriebsunterbruch etwa nach einem Hackerangriff, Schäden an Datensätzen durch einen Hacker, Diebstahl von wertvollen Daten, die Einführung von Malware, Würmern und anderen schädlichen Computercodes oder auch Fehler der eigenen Mitarbeiter, die zur Weitergabe vertraulicher Informationen oder der Schädigung der Reputation des Unternehmens führen.

In der Vergangenheit wurde bereits eine Vielzahl an unterschiedlichen Definitionen und Begriffen verwendet, um die Idee von Cyber Risk zu charakterisieren. Einige Definitionen sind relativ eng gefasst wie etwa in Mukhopadhyay et al. (2005, 2013), die Cyber Risk als schadhafte elektronische Ereignisse bezeichnen, die die Störung des Unternehmensbetriebs und einen monetären Verlust bewirken. Andere Arbeiten nehmen eine breitere Perspektive ein, etwa Risiken aus Informationen (siehe Ögüt, Raghunathan und Menon, 2011) oder Risiko aus dem Ausfall der Informationssysteme (siehe z. B. Böhme und Kataria, 2006). Insbesondere Hackerangriffe und kriminelle Aktionen haben in den Medien eine hohe Aufmerksamkeit; allerdings kann Cyber Risk auch aus Naturgefahren sowie menschlichem oder technischem

Versagen entstehen. Tabelle 1 gibt einen Überblick der bislang in der Literatur verwendeten Cyber-Risk-Definitionen.

Arbeit	**Definition**
Mukhopadhyay et al. (2005, 2013)	"Risk involved with malicious electronic events that cause disruption of business and monetary loss"
Ögüt, Raghunathan, and Menon (2011)	"Information security risk"
Böhme and Kataria (2006)	"Failure of information systems"
Cebula and Young (2010)	"Operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems"

Tabelle 1: Cyber-Risk-Definitionen

In der Praxis nehmen viele Studien keine explizite Definition von Cyber Risk vor. Vielmehr wird Cyber Risk anhand bestimmter Kategorien unterschieden. Beispielsweise grenzen Marsh (2011) den Begriff Cyber Risk ab, indem sie vier Unterkategorien definieren: (1) Verluste, verursacht durch Cybercrime und Cyberterrorismus, (2) Unbeabsichtigter / versehentlicher Verlust der eigenen Daten oder der Daten einer anderen Person, (3) Physischer Systemverlust und (4) Haftbarkeit für die eigenen Onlineaktivitäten oder der Aussagen in E-Mails.

In dieser Arbeit wird ein breiter Begriff für Cyber Risk verwendet, der nicht nur Gefahren aus dem Internet, sondern auch physische Gefahren mit einbezieht. Die Definition beinhaltet sowohl die von Marsh (2011) als auch Inputs aus den Marktbefragungen (Kapitel 5 und 6), die im Rahmen dieser Studie durchgeführt wurden. Unsere Definition stützt sich dabei auf die Kategorisierung der Aufsichtsbehörden für Risiken im Finanzdienstleistungssektor, insbesondere hier auf den Begriff der operationellen Risiken. Operationelle Risiken werden im Allgemeinen definiert als „Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge von externen Ereignissen eintreten".[4] Die Schnittmenge mit den obigen Beispielen für Cyber Risk ist offensichtlich, wobei Cyber Risk immer einen Bezug zu Informationen[5] haben. Dementsprechend verwenden wir folgende Definition:

„Cyber Risk sind operationelle Risiken, die von Informationen ausgehen, die auf Datenträgern und Netzwerken gespeichert sind."

[4] Diese Definition kommt aus Basel II und hat eine grosse Bedeutung im Risikomanagement von Banken und Versicherern, siehe z. B. BIS (2006). Sie schliesst Rechtsrisiken ein, beinhaltet aber keine strategischen Risiken oder Reputationsrisiken.

[5] Wir differenzieren nicht zwischen „Daten" im Sinne von maschinell verarbeitbaren Zeichen und „Informationen" als mittels Kontext interpretierten Daten und verwenden die beiden Begriffe in der Arbeit synonym.

Die Verankerung von Cyber Risk im Bereich der operationellen Risiken hat eine Reihe wichtiger Vorteile:

(a) Cyber Risk kann gegenüber anderen Risikoarten klar abgegrenzt werden.[6]
(b) In der Strukturierung von Cyber Risk kann die bekannte und etablierte Einteilung operationeller Risiken weitergeführt werden.[7]
(c) Durch die Anknüpfung von Cyber Risk an das bekannte Gebiet der operationellen Risiken können auch gezielt Daten identifiziert und analysiert werden.[8]

Cebula und Young (2010) definieren Cyber Risk ebenfalls in Anlehnung an operationelle Risiken. Sie arbeiten dabei noch den Aspekt heraus, dass Cyber Risk stets die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen oder Informationssystemen einschränken.

Abgrenzung gegenüber anderen Risikoarten
In der Folge wollen wir die Abgrenzung von Cyber Risk und anderen Risikoarten weitergehend diskutieren. Diese Abgrenzung ist auch deswegen relevant, da eine Schnittmenge zwischen Cyber Risk und anderen Risikoarten Implikationen, etwa für das Pricing, Risikomanagement oder die Versicherbarkeit dieser Risikoart, haben kann. So kann zum Beispiel durch den engen Bezug von Cyber Risk und operationellen Risiken auf bekannte Modellierungsmethoden der operationellen Risiken zurückgegriffen werden.[9]

Tabelle 2 zeigt eine mögliche Abgrenzung der Risikoarten, die typischerweise in Versicherungsunternehmen definiert wird. Wie bereits angeführt sind dies die Kategorien Markt-, versicherungstechnische, Kredit- und operationelle Risiken.

	Marktrisiko	**Versicherungs-technisches Risiko**	**Kreditrisiko**	**Operationelles Risiko**	**Cyber Risk**
Definition	Änderungen von Marktpreisen, z. B. Aktienkursen	Verluste aus dem Versicherungsgeschäft (Prämien- und Reserverisiko)	Ausfallrisiko oder Gegenparteirisiko von Vertragspartnern (Kapitalanlagen, Rückversicherung)	Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge von externen Ereignissen eintreten	Risiko, das von Informationen ausgeht, die auf Datenträgern und Netzwerken gespeichert sind
Einordnung	Spekulatives Risiko	Reines Risiko	Reines Risiko	Reines Risiko	Reines Risiko

Tabelle 2: Abgrenzung der Risikoarten

[6] In der Bankenregulierung werden Markt-, Kredit-, Liquiditäts-, Rechts- und operationelle Risiken voneinander abgegrenzt. In der Versicherungsregulierung werden dagegen Markt-, versicherungstechnische, Kredit- und operationelle Risiken betrachtet.
[7] Gemäss Basel II (siehe BIS, 2006) und Solvency II (siehe CEIOPS, 2009) werden operationelle Risiken in vier Kategorien unterteilt: (1) Menschliche Fehler, (2) Systemfehler, (3) Fehlerhafte interne Abläufe, (4) Externe Ursachen. Wir werden diese Kategorisierung auf Cyber Risk anwenden.
[8] Dies ist von besonderer Relevanz, da die Verfügbarkeit von Daten zu Cyber Risk oftmals sehr schwierig ist.
[9] Beispielhaft seien die Methoden der Extremwerttheorie genannt; Vgl. dazu etwa Hess (2011).

Abgrenzung von OpRisk

Seit etwa 15 Jahren sammeln viele Unternehmen Daten zu operationellen Risiken (OpRisk). Auch sind inzwischen einige etablierte Datenanbieter in diesem Bereich aktiv (z. B. SAS). Gegebenenfalls können Daten aus dem Bereich OpRisk – wenn diese z. B. als Verluste, die infolge des Versagens von IT-Systemen deklariert sind – zur Analyse und Bewertung von Cyber Risk herangezogen werden. Dies kann insbesondere dann hilfreich sein, wenn noch wenig Daten zu Cyber Risk zur Verfügung stehen. Des Weiteren können Überlegungen zum Risikomanagement operationeller Risiken auf Cyber Risk übertragen werden. So können beispielsweise auch Produkte zur Absicherung von OpRisk analysiert werden, um so Rückschlüsse auf das Design von Cyber-Versicherungen zu ziehen.

Die Diskussion zeigt, dass Cyber Risk in der klassischen Risikodefinition der Assekuranz grundsätzlich als eine Teilmenge von OpRisk aufzufassen ist. Ein Unterschied zwischen Cyber Risk und operationellem Risiko besteht allerdings darin, dass Reputationsrisiken bei operationellen Risiken explizit ausgeschlossen werden. Bei Cyber Risk ist das Thema Reputation dagegen von sehr grosser Bedeutung. Insofern sind Cyber Risk ein Teil der operationellen Risiken, sie gehen aber auch darüber hinaus. In diesem Zusammenhang ist auch zu beachten, dass Versicherer vermehrt Deckungen für Cyber Risk anbieten. Für diese Unternehmen stellt Cyber Risk ein OpRisk im eigenen Haus und darüber hinaus ein versicherungstechnisches Risiko in der Beziehung mit dem Versicherungsnehmer dar. Abbildung 2 verdeutlicht die Abgrenzung von Cyber Risk gegenüber den anderen Risikokategorien.

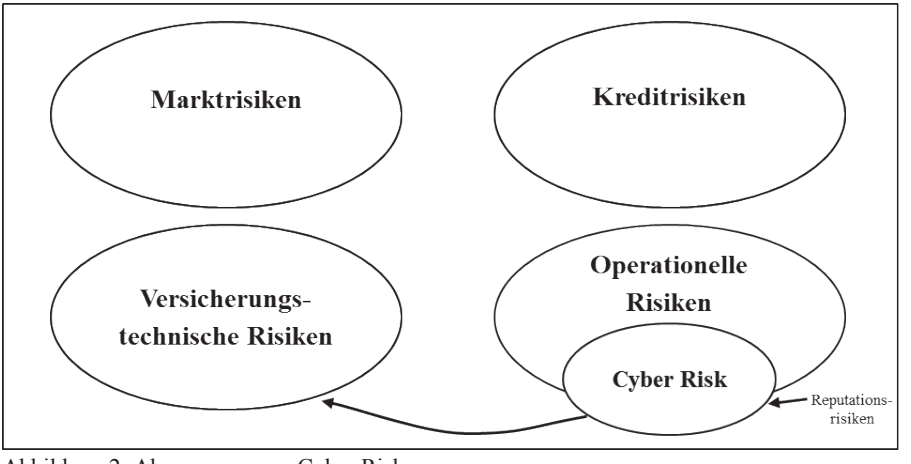


Abbildung 2: Abgrenzung von Cyber Risk

Abgrenzung von IT-Risk

Eine weitere Frage stellt sich bei der Abgrenzung von Cyber Risk und IT-Risiken. Gemäss der Information Systems Audit and Control Association (ISACA) kann IT-Risk als "business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise" definiert werden. Diese Definition umfasst also alle Risiken, die sich aus der Informationstechnologie und deren Nutzung ergeben. IT- und Cyber Risk haben folglich ebenfalls eine grosse Schnittmenge. Auffällig ist jedoch, dass IT-Risk generell das Risiko von

Informationstechnologien abdeckt, während Cyber Risk insbesondere den Datenaspekt darstellt. Aufgrund der Schnittmenge von IT- und Cyber Risk ist es wiederrum möglich, Überlegungen aus dem Risikomanagement von IT-Risiken auf den Bereich Cyber Risk anzuwenden.

Vier Kategorien

Gemäss Basel II (siehe BIS, 2006) und Solvency II (siehe CEIOPS, 2009) werden operationelle Risiken in vier Kategorien unterteilt: (1) Menschliche Fehler, (2) Systemfehler, (3) Fehlerhafte interne Abläufe, (4) Externe Ursachen. In Tabelle 3 wenden wir diese vier Kategorien auf Cyber Risk an.

Kategorie		**Beschreibung**	**Elemente**
1. Menschliche Fehler			
1.1	Unbeabsichtigt	Handlungen ohne böswillige oder schädigende Absicht	Fehler, Irrtümer, Unterlassungen
1.2	Absichtlich	Vorsätzliche Handlungen, ausgeübt mit der Absicht zu schaden	Betrug, Sabotage, Diebstahl oder Vandalismus
1.3	Untätigkeit	Untätigkeit oder Versagen, auf eine gegebene Situation zu reagieren	Mangel an geeigneten Fähigkeiten, Fachwissen, Leitung und der Verfügbarkeit von Personal, das handelt
2. Systemfehler			
2.1	Hardware	Risiken zurückzuführen auf Versagen in physischer Ausstattung	Versagen aufgrund von Kapazität, Performance, Leistungsfähigkeit, Instandhaltung, und Überalterung
2.2	Software	Risiken, die aus jeder Art von Software-Assets herrühren; umfasst Programme, Anwendungen und Betriebssysteme	Kompatibilitäts-, Konfigurierungs-, Änderungsmanagement, Sicherheitseinstellungen, Programmierpraktiken und Überprüfung
2.3	System	Versagen integrierter Systeme, Ausführung läuft anders als erwartet	Design, Spezifizierungen, Integration und Komplexität
3. Fehlerhafte interne Abläufe			
3.1	Prozess-Design und / oder Ausführung	Versagen eines Vorgangs bei der Erreichung eines erhofften Ergebnisses aufgrund von mangelhaftem Prozess-Design oder Ausführung	Ablauf, Dokumentation, Rollenverteilung und Zuständigkeiten, Benachrichtigungen und Warnmeldungen, Informationsfluss, Zuspitzung von Problemen, Vereinbarungen über Service-Levels und Weitergabe von Aufgaben
3.2	Prozessüberwachung	Unzureichende Kontrolle der Wirkungsweise von Prozessen	Statusüberwachung, Masse / Kriterien, regelmässige Überprüfung und Gesamtverantwortung
3.3	Unterstützungsprozesse	Versagen von organisationalen Unterstützungsprozessen, um die geeigneten Ressourcen zu liefern	Personalführung, Buchhaltung, Fort- und Weiterbildung sowie Beschaffung
4. Externe Ursachen			
4.1	Katastrophen	Ereignisse, sowohl natürliche als auch menschlichen Ursprungs, über die die Organisation keine Kontrolle hat und die ohne Ankündigung auftreten	Wetter, Feuer, Überschwemmung, Erdbeben, Unruhen
4.2	Rechtliche Fragen	Risiken, die aus rechtlichen Fragen entstehen	Regulatory Compliance, Gesetzgebung und Rechtsstreit
4.3	Geschäftsvorfälle	Risiken, die aus Veränderungen der Geschäftsumgebung der Unternehmen entstehen	Ausfall des Lieferanten, Marktlage und ökonomische Bedingungen
4.4	Service-Abhängigkeiten	Risiken, die aus der Abhängigkeit des Unternehmens von externen Parteien / Partnern entstehen	Versorgungswirtschaft, Notdienste, Kraftstoffe und Logistik

Tabelle 3: Cyber-Risk-Kategorien (in Anlehnung an Cebula und Young, 2010)

Ursache-Wirkungs-Modell für Cyber Risk

Eine weitergehende Kategorisierung kann in Anlehnung an Marsh (2011) vorgenommen werden und in ein Ursache-Wirkungs-Modell für Cyber Risk eingebettet werden. Die Ursachen sind dabei die Risiken, während die Wirkungen die finanziellen und nicht finanziellen Verluste sind, die etwa durch eine Versicherung getragen werden können. Tabelle 4 zeigt zunächst die Ursachen für Cyber Risk. Demnach können wir Cyber Risk in zwei Kategorien einteilen: „Datenverlust durch Naturkatastrophen, menschliches Versagen und Hardware-Versagen" und „Cybercrime". Cyber Risk lässt sich folglich auf nicht kriminelle und kriminelle Ursachen zurückführen. Im Bereich der nicht kriminellen Ursachen ist zwischen höherer Gewalt, technischem Defekt und menschlichem Versagen zu differenzieren. Kriminelle Risiken wollen wir in die Kategorien physischer Angriff, Hackerangriff und Erpressung unterteilen. In der Folge entwickeln wir ein Ursache-Wirkungs-Modell für Cyber Risk, um Risiken und deren Konsequenzen besser voneinander trennen zu können.

Ursachen	**Erläuterung und Beispiele**
I. Nicht kriminelle Ursachen für Cyber Risk	
Höhere Gewalt	Stromausfall nach Naturkatastrophe, Zerstörung von Servern oder Computern bei Überschwemmung, Brand etc.
Technisches Versagen	Hardware-Versagen, etwa Datenverlust durch Headcrash von Festplatten oder Computerabsturz, Software-Fehler
Menschliches Versagen	Versehentliches Veröffentlichen von Informationen, Falschmeldungen
II. Kriminelle Ursachen (Cybercrime)	
Physischer Angriff	Physischer Datendiebstahl, z. B. LGT Bank
Hackerangriff	Etwa um Kundendaten auszuspionieren oder Betriebe zu sabotieren, z. B. Lahmlegen von Systemen mittels Denial-of-Service- bzw. Distributed-Denial-of-Service-Attacken, Installation eines Keyloggers, Malware (z. B. Viren, Würmer, Spam-Mails, Trojanischen Pferden oder Ransomware)
Erpressung	Drohung via Internet, z. B. mexikanisches Drogenkartell etc.

Tabelle 4: Ursachen für Cyber Risk

Was sind nun also die Konsequenzen aus diesen Risiken? Welche finanziellen und nicht finanziellen Verluste können aus diesen Risiken erwachsen? Wir unterscheiden in der Folge zwischen Eigenschäden und den Ansprüchen Dritter (siehe Tabelle 5).

I. Eigenschäden (Property)
• Kosten durch Betriebsunterbruch • Erpressungszahlungen (Cyber Extortion) • Kosten durch Veruntreuung von Vermögenswerten • Kosten für Datenwiederherstellung, Ersatzbeschaffung • Kosten durch Crisis-Management-Services • Reputationsverlust
II. Ansprüche Dritter (Haftpflicht, Liability)
• Ansprüche aus Verletzung von Datenschutzbestimmungen (durch die versicherte Gesellschaft oder externe IT-Firmen) • Network Security Liability (Ansprüche aufgrund von Pflichtverletzungen, die einem Dritten einen Vermögensschaden zufügen) • Kosten für Datenwiederherstellung • Haftbarkeit für eigene Onlineaktivitäten oder Aussagen in E-Mails (Kosten aus der Verletzung oder wiederrechtlichen Verwendung von geistigem Eigentum) • Kosten aus der Beeinträchtigung oder Verwehrung des berechtigten Zugangs von Kunden • Reputationsverlust bei Kunden durch eigenes Fehlverhalten

Tabelle 5: Auswirkungen von Cyber Risk

In der Folge wollen wir die nicht kriminellen und kriminellen Ursachen für Cyber Risk noch etwas näher analysieren.

2.1.1 Nicht kriminelle Ursachen für Cyber Risk

Höhere Gewalt
Wie bereits angedeutet, können nicht kriminelle Ursachen in drei Untergruppen unterteilt werden: Das Risiko aus höherer Gewalt, menschlichem und technischem Versagen. In einigen Regionen dieser Welt kommt es des Öfteren zu Naturkatastrophen, die als Folgeschaden einen Datenverlust herbeiführen können. Als Naturkatastrophen gelten Hurrikane, Tornados, Tsunamis, Vulkanausbrüche, Erdbeben etc. Diese Katastrophen können unter Umständen ein Rechenzentrum zerstören oder zu Stromausfällen führen, bei denen dann Daten verloren gehen können.

Menschliches Versagen / Fehlverhalten
Des Weiteren kann auch ein unbeabsichtigtes, menschliches Fehlverhalten zu Datenverlusten führen. In einer vom Unternehmen Kroll Ontrack durchgeführten Erhebung denken 40 % der Befragten, dass menschliche Fehler die Hauptschuld für Datenverluste tragen (Bergler, 2010). Das versehentliche Veröffentlichen / Verbreiten von vertraulichen Informationen stellt ebenfalls ein grosses Risiko dar (z. B. versehentlich falsche Adressierung oder zu frühes Versenden von E-Mails).

Technisches Versagen
Ein weiteres Risiko geht von der Hardware aus. Es kann vorkommen, dass ein Defekt an der Hardware zu Datenverlusten führt. Beispiele hierfür sind das Überhitzen von Rechnern oder ein Headcrash von Festplatten (siehe auch Bey-Miller, Clarke und van Dyk, 2008, S. 368).

Auch stellen Sonnenwinde für die Technik eine Bedrohung dar (Spanier, 2011). Die in Sonnenwinden transportierten elektrischen Teilchen können Schaltkreise von Computerchips aufladen, dadurch Fehlfunktionen auslösen, die im schlimmsten Fall zur Veränderung oder zum Verlust von gespeicherten Daten führen.

2.1.2 Kriminelle Ursachen (Cybercrime)

Gemäss dem deutschen Bundeskriminalamt umfasst Cybercrime *„… alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden“* (Bundeskriminalamt, 2012, S. 5). Darunter fallen alle Sachverhalte, die mit einem gezielten Angriff, Spionage oder Sabotage auf digital gespeicherte Daten oder elektronische Geräte zu tun haben. Cybercrime kann dabei sowohl über Netzwerke, wie das Internet, als auch über physischen Zugang erfolgen. Zu unterscheiden sind in diesem Zusammenhang vor allem der Hackerangriff und der physische Angriff. Ferner kann Erpressung als Ursache krimineller Cyber Risk klassifiziert werden.

Die Motive für Cybercrime können im Allgemeinen sowohl persönlicher als auch finanzieller Natur sein und verursachen meist eine grosse Bandbreite an Schadensummen: Vorfälle mit (fast) keinem Schaden und Schadenfälle in Millionenhöhe sind möglich (siehe dazu auch ausgewählte Fallbeispiele in Abschnitt 2.2.2).

Hackerangriffe
Während der letzten Jahre sind weltweit immer mehr Hackerangriffe bekannt geworden. Solche Cyberattacken können von einer einzelnen Person ausgehen oder auch von bestens organisierten Hackerorganisationen durchgeführt werden. Zudem wird immer öfter vermutet, dass manche Staaten speziell eingerichtete, nach aussen getarnte Hackerzentren haben (Schweizerische Eidgenossenschaft, 2012). Ein potenzielles Ziel eines Hackerangriffs kann heutzutage jeder sein: Von Einzelpersonen über Unternehmen bis hin zu Staaten waren alle Gruppen bereits betroffen. So vielfältig die Ziele sein können, so vielfältig sind auch die Methoden, mit denen die Hacker vorgehen. Ein Hackerangriff erfolgt zumeist zur Spionage oder Sabotage. Bei der Spionage wird über ein Netzwerk in das System des Ziels eingedrungen, um von dort sensible Informationen zu beschaffen. Bei der Sabotage dringt der Angreifer ebenfalls in das System des Ziels ein, stört bzw. verändert aber Abläufe, was zu Datenverlusten und Fehlfunktionen führen soll. Hackerangriffe können nach verschiedenen Mustern erfolgen. Die Wahl der entsprechenden Angriffstopografie hängt dabei aber entscheidend von der technischen Ausstattung und dem Know-how der Angreifer und dem Ziel ab.[10] Hackerangriffe können allgemein in vier verschiedene Topografien unterschieden werden (siehe Abbildung 3):

[10] Manche Hackerangriffe benötigen erhebliche Rechenleistungen, um durchgeführt werden zu können. Ein Beispiel dafür sind Programme, die Passwörter knacken. Durch die Bereitstellung von Rechenleistung (via Internet) können so Passwörter erheblich schneller geknackt werden.

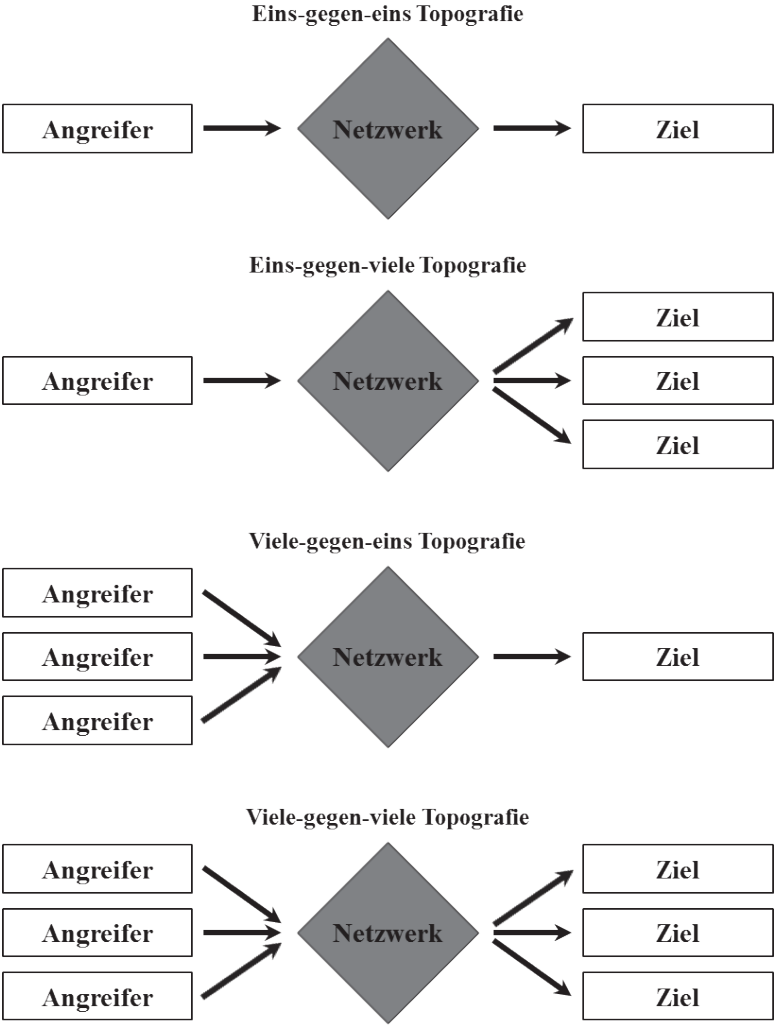


Abbildung 3: Angriffstopografien (in Anlehnung an Kizza, 2002, S. 80–81)

- Die erste der vier Topografien stellt die „Eins-gegen-eins-Topografie“ dar (Kizza, 2002, S. 80). Hierbei handelt es sich um personalisierte Attacken, bei denen dem Angreifer das Ziel bekannt ist und manchmal auch das Ziel den Angreifer kennt. Die Motive sind meistens Hass, persönliche Rache, persönliche Bereicherung oder Geschäftsspionage und -sabotage.

- Bei der zweiten Topografie („Eins-gegen-viele-Topografie“) greift ein Angreifer mehrere Ziele gleichzeitig an (Kizza, 2002, S. 80). In den meisten Fällen kennt der Angreifer die Ziele nicht. In vielen Fällen möchte der Angreifer aber auch gegenüber den Zielen anonym bleiben, sodass er hier meist unbekannt bzw. unerkannt bleibt. Oft verwendete Me-

thoden sind Viren und Trojaner. Die Motive dieses Angriffsmusters sind meist Hass, persönliche Bereicherung, Geschäftsspionage und -sabotage.

- Bei der „Viele-gegen-eins-Topografie“ greifen mehrere Angreifer ein einzelnes Ziel an (Kizza, 2002, S. 80). Hier kennen die Angreifer das Ziel, jedoch weiss das Ziel nicht von wem es angegriffen wird. Es findet ein koordinierter Angriff auf das Ziel statt, was eine durchdachte Planung und viel Know-how erfordert. Diese Art des Hackmusters ist sehr beliebt bei Denial-of-Service-Attacken (DoS-Attacken). Hierbei wird beispielsweise eine Internetseite durch einen zeitgleich koordinierten Angriff zur Überlastung gebracht. Motive für solch einen Angriff sind meist Rache, Hass, Terrorismus und Ruhm. Viele DoS-Attacken finden hierbei über automatisierte Computerprogramme, sogenannte Botnetzwerke oder Botnets, statt (Bu, Bueno, Kashyap und Wosotowsky, 2013). So kann ein einzelner Angreifer durch einen Befehl über das Botnetzwerk einen gezielten Angriff in Form einer „Viele-gegen-eins-Topografie“ ausführen.

- Die vierte Topografie stellt die „Viele-gegen-viele-Topografie“ dar (Kizza, 2002, S. 81ff.). Hier attackieren viele Angreifer viele Ziele. Die Ziele werden hier sorgfältig ausgewählt und gesammelt. Wie in der Topografie zuvor findet ein koordinierter Angriff statt. Wie schon bei der „Viele-gegen-eins-Topografie“ werden auch hier oft Denial-of-Service-Attacken angewendet. Die Motive sind meist Hass, Terrorismus und Ruhm.

Wie in der Beschreibung der Topografien gesehen, können die Angriffe dabei auf viele verschiedene Arten erfolgen. Tabelle 6 zeigt die populärsten Arten von Hackermethoden auf.

Social Engineering	Bei Social Engineering wird die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit des Ziels vom Angreifer ausgenutzt (Schweizerische Eidgenossenschaft, 2013). Das Ziel wird oftmals via E-Mail darum gebeten, auf etwas zu reagieren, was ihm einen Nutzen bringt, z. B. Lotteriegewinn (Gradigo und Pirc, 2011, S. 68). So wird es meist dazu aufgefordert, sensible Daten wie Benutzername, Kennwort oder Kreditkartendaten preiszugeben. Immer wieder findet Social Engineering auch über soziale Netzwerke statt. Diese Art von Computer- und E-Mail-Betrug ist auch als „Phishing“ bekannt (KPMG, 2013, S. 25).
Trojanisches Pferd	Ein Trojanisches Pferd – oder auch Trojaner – ist ein Programm, das zuerst völlig harmlos erscheint (Kendrick, 2010, S. 40). Erst nach dem Herunterladen und Installieren stellt es sich als bösartig codiertes Programm heraus und kann dann verschiedenste Funktionen ausführen (Spionage, Sabotage).
Denial-of-Service-Attacken (DoS)	DoS-Attacken sind Angriffe, die die Funktionsweise eines Systems stören und so zum Absturz bringen sollen (Kizza, 2002, S. 76). Dabei gehen meist keine Daten verloren, das System wird lediglich überlastet.
Vulnerability Scanner	Vulnerability Scanner sind Programme, die die Hard- und Software des Ziels auf ihre Verletzlichkeit prüfen (Kizza, 2002, S. 73). Der Hacker kann durch die so gewonnenen Informationen einen gezielten Angriff auf die Schwachstellen des Ziels vorbereiten.
Keylogger	Ein Keylogger (dt. „Tastenrekorder“) ist eine Hard- oder Software, die verwendet wird, um die Eingaben des Benutzers an einem Computer mit zu protokollieren. So können alle Eingaben überwacht und rekonstruiert werden (Gabler, 2014a). Der Keylogger wird von Hackern verwendet, um an Passwörter, Benutzernamen oder PINs zu gelangen.
Virus	Ein Virus ist ein Computerstörprogramm, das sich unkontrolliert in andere Programme einschleust, sich reproduziert und sich in das bestehende Programm einpflanzt (infiziert), sobald es einmal ausgeführt wird (Gabler, 2014b). Getreu seinem biologischen Vorbild ist der Virus auf den Wirt (in diesem Fall bestehende Programme) angewiesen, um seinen Maschinencode ausführen zu können und kann auch nur durch die Weitergabe eines infizierten Programms / Files übertragen werden.
Wurm	Ein Wurm ist ein Computerprogramm mit der Eigenschaft sich selbst zu vervielfältigen, nachdem es ausgeführt wurde (Gabler, 2014c). Im Gegensatz zu einem Virus wartet ein Wurm nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versucht, aktiv in neue Systeme einzudringen (Gabler, 2014c), wobei er meist Netzwerke, wie das Internet, nutzt.

Tabelle 6: Hackermethoden

Die Unterscheidung in Virus und Wurm sind nicht immer trennscharf. Viele Quellen verwenden den Begriff Virus und Wurm, ohne eine eindeutige Abgrenzung vorzunehmen. In manchen Fällen werden Würmer auch als Spezialfälle von Viren angesehen (siehe z. B. Symantec, 2014).

Physischer Angriff
Der physische Angriff umfasst das physische Eindringen, Spionieren und Sabotieren des Ziels. In den frühen 2000er-Jahren verschafften sich Kriminelle oft physischen Zugang zu ihren Zielen, um an sensible Daten zu gelangen oder Prozesse zu sabotieren. Dabei kamen die Kriminellen oft aus dem eigenen Unternehmen. In den meisten Fällen stahlen Mitarbeiter, die Zugang zu vertraulichen Informationen hatten, Kopien der Daten, die sie dann an Interessierte weiterverkauften. Berühmte Fälle sind die Datendiebstähle bei der LGT Bank (siehe auch Fallbeispiele in 2.2).

Erpressung
Erpressungen sind eine häufig in den Medien diskutierte Form des kriminellen Cyber Risk. Ein Beispiel ist etwa der Erpressungsversuch beim mexikanischen Drogenkartell „Los Zetas". Im Oktober 2011 wurde ein Mitglied der Hackergruppe „Anonymous" vom mexikanischen Drogenkartell „Los Zetas" entführt, woraufhin die Hackergruppe drohte „Zetas"-Unterstützer zu enttarnen, was für diese ein fast sicheres Todesurteil bedeutet hätte (Vgl. Polansky, 2011).

In der Folge wollen wir ausgewählte Risiken aus Cyber Risk einer systematischen Analyse unterziehen und mögliche Datenquellen zu Cyber Risk aufführen.

2.2 Systematische Analyse von Cyber Risk

Daten zu Cyber Risk sind in der Regel schwer verfügbar. Zum einen, da es sich um eine relativ neuartige Risikoart handelt. Zum anderen, da betroffene Institutionen im Allgemeinen ungern Informationen zu derartigen Vorfällen preisgeben. Um etwas Licht in diese Situation zu bringen, werden wir in der Folge alle Datenquellen, die wir im Rahmen unserer Recherche gefunden haben, auflisten. Dann werden wir einige populäre Fallbeispiele zu Cyber Risk aus den letzten 15 Jahren systematisch auswerten.[11] Schliesslich werden die Resultate der Fallbeispiele tabellarisch zusammengefasst. Diese Zusammenstellung unterstreicht die grosse Heterogenität und ihre grosse ökonomische sowie gesellschaftliche Relevanz.

2.2.1 Datenquellen zu Cyber Risk

Tabelle 7 listet alle im Rahmen unserer Recherche gefundenen Datenquellen auf.

Arbeit	Daten
Ponemon Institute	• Global Cost of a Data Breach Study • U.S. Cost of a Data Breach Study (jährlich und für verschiedene Länder, z. B. Deutschland, Italien etc., veröffentlicht) • U.S. Cost of Cyber Crime Study (jährlich und für verschiedene Länder veröffentlicht, z. B. UK) • Aussagen der Studien: - Vorfälle mit Verletzung der Datensicherheit kosten, die US-Unternehmen in 2009, 204 US$ pro betroffenem Kundendatensatz (Vergleich: 202 US$ im Jahr 2008). - Ungeachtet eines allgemeinen Rückgangs in der Zahl der gemeldeten Vorfälle (498 in 2009 gegenüber 657 in 2008, Information laut dem Identity Theft Resource Center), betrugen die durchschnittlichen Gesamtkosten pro Vorfall 2009 6,76 Millionen US$, verglichen mit den durchschnittlichen Gesamtkosten pro Vorfall von 6,65 Millionen US$ in 2008.
CSI/FBI	Computer Crime and Security Survey (jährlich veröffentlicht)
Hackmageddon	Cyber Attacks Timeline Master Index (jährliche und monatliche Veröffentlichung)
Symantec	Internet Security Threat Report (jährliche und monatliche Veröffentlichung)
McAfee	• The Economic Impact of Cyber Crime and Cyber Espionage • Aussagen der Studie: - Globale Cyber-Aktivitäten verursachen Kosten im Wert von 300 Milliarden US$ bis 1 Billion US$ (0,4 % bis 1,4 % des GDP) - US-Cyber-Aktivitäten verursachen Kosten in Höhe von 24 bis 120 Milliarden US$ (0,2 % bis 0,8 % des GDP)
World Economic Forum	9th Global Risk Report: Cyberattacken gehören zu den Top 5 der grössten globalen Risiken im Jahr 2014 (in Bezug auf Eintrittswahrscheinlichkeit), dies ebenfalls bereits im Report für 2012
NetDiligence	• Cyber Claims Study (erscheint auf jährlicher Basis) trägt echte Schäden aus Cyber-Liability-Versicherungen zusammen, um die realen Kosten eines Data Breach zu bestimmen • Aussagen der Studie: - Die Anzahl an Daten, die im Durchschnitt verloren gehen, beträgt etwa 2,4 Mio. US$ - Schadenzahlen in Bericht von 2014 schwanken zwischen 30‘000–400‘000 US$ - Der Durchschnittsschaden pro verlorenem Datensatz beträgt 956,21 US$
KPMG	KPMG Forensic Services (Studien zu verschiedenen Ländern, z. B. USA, Schweiz etc.)

Tabelle 7: Datenquellen zu Cyber Risk

[11] Die Fälle wurden aufgrund ihrer unterschiedlichen Methodik der Täter ausgewählt und werden jeweils auf Ziel, Angreifer, Methode, entstandener Schaden sowie Konsequenzen analysiert und verglichen.

Ein Beispiel für eine Datenquelle sind die vom World Economic Forum (WEF) im Rahmen seines Global Risk Reports ausführlich diskutierten Erkenntnisse. Abbildung 4 zeigt die Befragungsergebnisse des WEF-Reports im Bereich der technologischen Risiken aus dem Jahr 2012 (World Economic Forum, 2012). Befragt wurden 469 Experten aus Industrie, staatlichen Organisationen, Wissenschaft und Zivilgesellschaft zu den Themen Auswirkung und Eintrittswahrscheinlichkeit verschiedener technologischer Risiken. Die Bewertungsskala reichte von 1 bis 5, wobei Abbildung 4 nur einen Ausschnitt im Bereich 2.5 bis 4.5 darstellt. Die verschiedenen Grössen der Punkte zeigen die Anzahl Szenarien je Kategorie an.



Abbildung 4: Technologische Risiken im Rahmen des Global Risk Reports (WEF, 2012)

Die grösste Bedeutung weisen hier die sogenannten Cyberattacken (Cyber attacks) auf. Hierbei handelt es sich um einen gezielten Angriff auf grössere, für eine spezielle Infrastruktur wichtige Computernetzwerke. Noch bedeutsamer bezüglich der möglichen Auswirkungen, allerdings weniger wahrscheinlich, ist der Bereich „Critical systems failure". Es handelt sich hierbei um Schwachstellen in einem System, die zu Ausfällen in Informations- und Infrastrukturnetzwerken führen können. Des Weiteren werden Vorfälle aus Datenbetrug und Datendiebstahl („Massive incident of data fraud and theft") genannt. All diese Risiken haben gemeinsam, dass sie von gespeicherten Informationen auf Datenträgern oder in Netzwerken ausgehen und so, nach unserer Definition in Abschnitt 2.1, zu Cyber Risk gehören.[12]

Es lassen sich zahlreiche weitere Belege für die hohe Bedeutung von Cyber Risk anführen. Beispielsweise hat die britische Regierung die Kosten von Cybercrime in Grossbritannien auf 27 Milliarden Pfund pro Jahr geschätzt. Die Nationale Sicherheitsstrategie (National Security Strategy) platziert Cyberattacken als eins der fünf Toprisiken für Grossbritannien (Vgl. Marsh, 2011). Mittlerweile haben auch verschiedene Regierungen Meldestellen und Zentren für Cyberangriffe eingerichtet, die das Internet auf Schadsoftware hin untersuchen (Amoroso,

[12] Neben den technologischen Risiken betrachtet WEF (2012) wirtschaftliche Risiken, Umweltrisiken, geopolitische Risiken und gesellschaftliche Risiken. In der Gesamtschau aller Risiken nehmen Cyberattacken Rang 7 ein. „Massive incident of data fraud or theft" belegt den 27. Platz und „Critical systems failure" ist auf dem 28. Platz zu finden.

2013, S. 30; als Beispiel für die Schweiz sei MELANI genannt). Diese Belege zeigen, dass Cyber Risk bereits heute eine grosse ökonomische, technologische und gesellschaftliche Bedeutung haben und dass ihre Bedeutung in den kommenden Jahren deutlich zunehmen wird.

2.2.2 Fallbeispiele International

In diesem Abschnitt fassen wir einige populäre Fallbeispiele der letzten 15 Jahre zusammen. Die Fälle wurden aufgrund ihrer unterschiedlichen Methodik der Täter ausgewählt und werden jeweils auf Ziel, Angreifer, Methode, entstandener Schaden sowie Konsequenzen analysiert und verglichen.

Loveletter Computerwurm

Am 4. Mai des Jahres 2000 breitete sich der Loveletter-Wurm[13] via E-Mail mit dem Betreff „I Love You" auf der ganzen Welt aus (Nazario, 2004, S. 54). Sobald ein Benutzer die angehängte Datei öffnete, nistete sich der Wurm im System ein, löschte Daten und versendete sich selbständig an alle im Adressbuch gespeicherten Kontakte weiter. Betroffen war praktisch jeder – vom einzelnen privaten PC-Nutzer bis zur staatlichen Einrichtung. Durch den Computerwurm gingen sehr viele Daten verloren. Das Ziel des Programmierers war offenbar, möglichst viele Computer auf der Welt von seinem Wurm befallen zu lassen und somit möglichst viel Schaden zu verursachen. Ein Motiv für die Tat ist nicht bekannt. Bei der Angriffsmethode handelt es sich um einen Computerwurm, der sich nach der Ausführung durch einen Benutzer selbständig an weitere Opfer weitersendetet. In Netzwerkumgebungen ersetzte der Wurm einige Microsoft-Programme durch sich selbst und sorgte so dafür, dass die Computer anderer durch das Ausführen dieser Programme ebenfalls von dem Wurm betroffen waren. Um sich zu verbreiten, verwendete er das E-Mail-Programm von Microsoft (Microsoft Outlook).

Die Konsequenzen waren sowohl für Unternehmen als auch private Nutzer fatal. Da der Wurm Dokumente löschte, entstanden erhebliche Wiederherstellungskosten. Der Rückversicherer Swiss Re schätzte den Schaden weltweit auf 2,6 Milliarden US-Dollar und deklarierte diesen Vorfall als grösste von Menschen verursachte Katastrophe im Jahr 2000; angeblich stammte der Wurm von einem 24-jährigen Mann von den Philippinen, jedoch konnte dieser aufgrund mangelnder Rechtsgrundlage nicht angeklagt werden (Habegger, 2001). Bis zum Schluss konnte also der Täter nicht eindeutig ermittelt, geschweige denn zur Rechenschaft gezogen werden. Die Konsequenzen, die aus diesem Vorfall resultierten sind: Medien weltweit berichteten über den Vorfall, sodass der Wurm ein gewisses Risikobewusstsein bei den Menschen vor Cyber Risk schaffte, da er zeigte, was für ein Schadenpotenzial in einem bösartigen Computerprogramm stecken kann (Nazario, 2004, S. 55).

Ziel:	Unternehmen und private Nutzer weltweit
Angreifer:	(vermutlich) 24-jähriger Philippiner
Methode:	Computerwurm (-virus)
Schaden:	ca. 2,6 Milliarden US-Dollar

[13] Sehr oft wird dieser auch als Loveletter-Virus bezeichnet, siehe z. B. Hayes (2005).

Konsequenzen:	Schaffung von Risikobewusstsein und generelle Erhöhung der Sicherheitsmassnahmen

LGT Bank

Im Jahr 2006 kam es zu einem der grössten Steuerskandale in Liechtenstein (Teevs, 2010). Der im Jahr 1999 bei der LGT Bank in Liechtenstein eingestellte Heinrich Kieber verkaufte die von ihm im Jahr 2002 gestohlenen Kundendaten an Geheim- und Nachrichtendienste aus 13 verschiedenen Ländern. Kieber hatte bei der LGT Bank die Aufgabe, Kundendaten zu digitalisieren und demzufolge leichten Zugang zu hochsensiblen (Kunden-)Daten. Durch seine Tat schadete er nicht nur der LGT Bank, sondern auch dem ganzen Finanzplatz und dem Land Liechtenstein. Plötzlich war das Land in vielen Staaten im Fokus der Medien und erhielt schlechte Publicity, was zu Geldabflüssen führte. Der Finanzplatz musste sich daraufhin neu orientieren. Kieber floh ins Ausland und wandte sich an die Medien. Sein Motiv war nach seiner eigenen Aussage, dem Land Liechtenstein und dessen Fürstenhaus zu schaden. Allerdings wird vermutet, dass er eher finanzielle Ziele verfolgte: Schätzungen zufolge verdiente er durch den Verkauf der gestohlenen Daten einen hohen zweistelligen Millionenbetrag.

Ziel:	LGT Bank
Angreifer:	Interner Mitarbeiter
Methode:	Physischer Angriff, Datendiebstahl
Schaden:	Nicht schätzbar
Konsequenzen:	Etablierung einer neuen kriminellen Branche (Datenklau), verbesserte Sicherheitsvorkehrungen bei Banken, Liechtenstein musste sich neu orientieren und seinen Ruf wieder herstellen

Sony

Der japanische Elektronikkonzern Sony ist seit April 2011 mehrfach Opfer von Hackerangriffen geworden (Spiegel, 2011). Betroffen war das Onlinenetzwerk der Spielekonsole Playstation 3. Über dieses Netzwerk werden Onlinespiele abgewickelt. Des Weiteren dient es dazu, mittels Gutscheincodes oder Kreditkarteneinsatz, Spiele oder Filme zu kaufen, die Sony über dieses Netzwerk zum Kauf anbietet. Jeder Playstation-Besitzer, der den Onlinedienst nutzt, muss sich hier einen Account erstellen und Daten wie Name, Adresse, Land, E-Mail-Adresse und Geburtsdatum angeben. Wer Einkäufe im Playstation-Store mit seiner Kreditkarte abwickelt, speichert auch seine Kreditkartendaten im Playstation-Netzwerk. Der erste Angriff auf das Netzwerk fand vom 17. bis 19. April 2011 statt. Bei dieser Attacke drangen Hacker in das Playstation-Netzwerk und den Video- und Musikdienst Qriocity ein und stahlen über 70 Millionen Kundendaten. Als Folge musste Sony seine Onlinedienste für mehrere Wochen einstellen.

Das Ziel der / des Hacker(s) war es offenbar, zum einen den Elektronikkonzern Sony zu schädigen und zum anderen durch die gestohlenen Kreditkartendaten selbst einen finanziellen Nutzen zu erzielen. Das Motiv der Täter ist in diesem Fall aber nicht ganz klar: Es wurde berichtet, dass es einerseits ein Racheakt für das Vorgehen von Sony gegen einen bisherigen Playstation-Hacker sein könnte, andererseits der Angriff auch nur aus rein finanziellem Interesse durchgeführt wurde. Die Angriffsmethode ist bis heute unklar. Der finanzielle Schaden

(Verkaufsausfälle in den Netzwerken, Wartungskosten, Kosten für Schadensersatz, Prozess- und Anwaltskosten) beläuft sich nach Schätzungen des in Michigan angesiedelten Ponemon Instituts auf ca. 1,4 Milliarden US-Dollar (Reppesgaard, 2011). Zusätzlich zum finanziellen Schaden kommt aber noch der Image- und Vertrauensverlust von Sony hinzu. Während Sony für Wartungs- und Sicherheitsarbeiten die Netzwerke abschaltete, wechselten viele Nutzer zu anderen Spielekonsolen oder Video- und Musikdiensten. Der hier entstandene Schaden ist nur sehr schwer zu schätzen. Als Konsequenz überarbeitete Sony seine IT-Infrastruktur, um resistenter vor weiteren Angriffen zu sein.

Ziel:	Sony
Angreifer:	Unbekannt
Methode:	Unbekannt
Schaden:	ca. 1,4 Milliarden US-Dollar
Konsequenzen:	Erhöhung der Sicherheitsmassnahmen bei Sony, Darstellung der Verwundbarkeit von Grosskonzernen vor Hackerangriffen

Associated Press (AP)

Am Dienstag, den 23. April 2013, war der Twitter-Account von Associated Press (AP) von einem Hackerangriff befallen (Steier, 2013). Unbekannte hackten sich in das Konto ein und twitterten die Falschmeldung, dass es zwei Explosionen im Weissen Haus gegeben habe und Präsident Obama verletzt wurde. Unmittelbar nachdem die Meldung gepostet wurde, begannen die Kurse an den Börsen ihre Talfahrt. Der Marktwert der im S&P 500-Index enthaltenen Unternehmen sank innerhalb von drei Minuten um rund 136 Milliarden US-Dollar. Als sich herausstellte, dass es sich um eine Falschmeldung handelte, bewegten sich die Aktienmärkte wieder unmittelbar auf den Ausgangspunkt vor der Meldung zurück. Allerdings richtete diese Meldung ein grosses Chaos an. Vor allem Investoren, die einen Stop-Loss in ihren Produkten eingetragen hatten, verloren viel Geld. Nachträglich bekannte sich die syrische Hackergruppe „Syrian Electronic Army“ zu der Tat. Das Motiv ist bislang noch unbekannt. In diesem Zuge wurde kritisiert, dass manche Onlineplattformen, wie etwa Twitter, nicht über einen ausreichenden Schutz vor Cyberkriminalität verfügen.

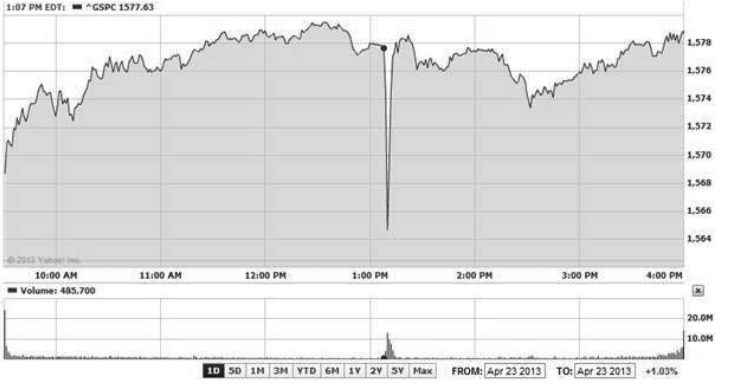


Abbildung 5: Kurseinbruch S&P 500 (Yahoo Finance, 2013)

Abbildung 5 macht deutlich, wie sensibel Finanzmärkte auf derartige Falschmeldungen reagieren. Dennoch gibt es bislang keine konkreten Schadenschätzungen.

Ziel:	AP (via Twitter)
Angreifer:	Hackergruppe Syrian Electronic Army (SEA)
Methode:	Social Engineering: Phishing
Schaden:	Nicht schätzbar
Konsequenzen:	Fokus auf soziale Netzwerke wird verstärkt, da viele nicht über die nötigen Sicherheitsvorkehrungen verfügen

Target Corporation

Ende des Jahres 2013 wurde die Target Corporation, einer der grössten Einzelhändler der USA, von einem massiven Hackerangriff auf seine Kundendaten getroffen. Hacker erlangten Zugriff auf 40 Millionen Kredit- und Girokontoinformationen sowie 70 Millionen weitere Informationen zu Kundenadressen und Telefonnummern. Dies führte dazu, dass die Target-Aktie um elf Prozent einbrach und der Nettoprofit im entsprechenden Quartal um 46 Prozent fiel. Zudem wurde der Ruf des Unternehmens massiv geschädigt, sodass der Umsatz im vierten Quartal 2013 um 3,8 Prozent einbrach. Neben diesen Verlusten entstanden weitere finanzielle Schäden, die direkt mit dem Data Breach in Verbindung standen in Höhe von 61 Mio. US-Dollar. Target gibt an, dass von diesem Schaden 44 Mio. US-Dollar durch eine Versicherung abgedeckt werden konnten (Skariachan und Finkle, 2014) und sich so der momentane Schaden, den das Unternehmen selbst zu tragen hat, auf 17 Mio. US-Dollar reduziert. Dennoch wird erwartet, dass weitere Kosten entstehen und der Gesamtschaden noch nicht genau quantifiziert ist (Skariachan und Finkle, 2014). Das Beispiel zeigt aber auch, welche Bedeutung eine Versicherung haben kann, wenn damit bis zu zwei Drittel eines Schadens transferiert werden können.

Wer genau hinter dem Hackerangriff steht und mit welchem Ziel er ausgeführt wurde, ist bislang nicht bekannt. Es kann aber vermutet werden, dass ein finanzielles Motiv am wahrscheinlichsten ist.

Ziel:	Target Corportation (US-Einzelhändler)
Angreifer:	Nicht bekannt
Methode:	Hackerangriff
Schaden:	Zurzeit 61 Millionen US-Dollar, es werden aber noch weitere Kosten erwartet
Konsequenzen:	Reputationsverlust, es wird aufgezeigt, welche Bedeutung Cyber-Versicherung haben kann.

Zusammenfassung der Fallbeispiele

Die vorgestellten Fallbeispiele zeigen, welch immensen Schaden Cyberangriffe verursachen können. Breit gefächerte Angriffe, wie der Computerwurm, der im Jahr 2000 ins Netz gesetzt wurde, richteten eine hohe Anzahl von kleinen Einzelschäden (in Summe ca. 2,6 Milliarden US-Dollar) an, während gezielte Hackerangriffe immens hohe Einzelschäden (Fall Sony, ca. 1,4 Milliarden US-Dollar, oder Target, 61 Mio. US-Dollar) verursachen konnten. In vielen

Fällen ist aber auch der entstandene Schaden nicht mess- bzw. schätzbar, da viele Kosten, wie beispielsweise Reputationsverlust, Kundenabgang etc., nicht präzise zu bestimmen sind.

Problematisch ist auch, dass in vielen Fällen die Täter nicht bekannt sind und über das Motiv nur spekuliert werden kann. Die Beweggründe sind meist Rache, finanzielle Motive sowie Wirtschaftsspionage. Bei den Tätern gibt es sowohl Einzeltäter als auch organisierte Hackergruppen, wie es bei AP der Fall war. Des Weiteren lässt sich feststellen, welch grosse Auswirkungen ein physischer Datendiebstahl sowohl auf ein Unternehmen als auch auf das Umfeld haben kann. Der Fall von Target zeigt hingegen, wie wertvoll eine Versicherung gegen Cyber-Schäden sein kann und wie essenziell dies auch für ein Unternehmen, das nicht primär mit Daten arbeitet, wie z. B. ein Dienstleistungsunternehmen, ist.

Aus der Analyse dieser Fälle lässt sich schliessen:

- Würmer, Viren und Trojaner sowie andere Malware verursachen hohe kumulative Schäden auf der ganzen Welt, hingegen gezielte Hackerangriffe sehr hohe Einzelschäden
- Entstandene Gesamtkosten sind teilweise schwer bzw. nicht schätzbar
- Täter und deren Motive bleiben in vielen Fällen unbekannt
- Täter können sowohl Einzeltäter als auch kriminelle Gruppierungen sein
- Methoden der Täter nehmen an Komplexität zu
- Versicherungen können einen erheblichen Teil des Schadens abdecken.

Tabelle 8 fasst die diskutierten Fallbeispiele zusammen. Die einzelnen Fälle werden nach Ziel, Angreifer, Schaden und Motiv aufgelistet. Diese Zusammenstellung unterstreicht nochmals grosse Heterogenität (z. B. bezüglich der Ziele und Motive) sowie die grosse ökonomische Relevanz.

Jahr	Fall / Methode	Ziel	Angreifer	Schaden	Motiv
2000	Loveletter-Computerwurm	Ganze Welt, alle PC-User	(Vermutlich) 24-jähriger Philippiner	Ca. 2,6 Mrd. US$	Unbekannt
2006	Datendiebstahl LGT Bank	LGT Bank	IT-Mitarbeiter	Nicht schätzbar	Rache, monetäre Gründe
2011	Hackerangriff Playstation-Netzwerk (Methode unbekannt)	Sony	Nicht bekannt	Ca. 1,4 Mrd. US$	Rache, monetäre Gründe
2013	Hackerangriff AP Twitter-Account (durch Phising)	AP (Twitter)	Hackergruppe „Syrian Electronic Army“	Nicht schätzbar	Unbekannt
2013/ 2014	Hackerangriff auf Kredit- und Girokontodaten, bzw. Kundeninformationen bei Target (wie Adressen und Telefonnummern)	Target Corporation (US-Einzelhändler)	Nicht bekannt	Bis jetzt 61 Mio. US$, es wird aber noch deutlich mehr erwartet[14]	Unbekannt, aber wahrscheinlich monetäre Gründe

Tabelle 8: Ausgewählte Fallbeispiele International

2.2.3 Fallbeispiele Schweiz

In diesem Abschnitt werden einige aktuelle Fallbeispiele aus der Schweiz dargestellt (Tabelle 9). Wieder werden die Fälle aufgrund ihrer unterschiedlichen Methodik der Täter ausgewählt und auf Ziel, Angreifer, Methode, entstandener Schaden sowie Motiv hin analysiert. Wie bei den internationalen Fallbeispielen zeigt sich eine grosse Vielfalt in den unterschiedlichen Fallbeispielen. Bei den kriminellen Ereignissen bleiben die Angreifer in den meisten Fällen wieder unerkannt.

[14] Laut Target sind aber 44 Millionen US-Dollar des jetzigen Schadens durch eine Versicherung abgedeckt.

Jahr	Fall / Methode	Ziel	Angreifer	Schaden	Motiv
2007, 2009, und 2012	Hackerangriffe (z. B. in 2007 Virusattacke getarnt als Fotowettbewerb)	Eidgenössisches Departement für auswärtige Angelegenheiten (EDA), Bern	Unbekannt; mittels besonderer Software wurde in die Informatik-Infrastruktur des EDA eingedrungen	IT-Netz muss kurzzeitig vom Internet getrennt werden, Gefahr wird bewusst und erste Diskussionen zur Behebung des Problems werden auch in der Schweiz unternommen.	Vermutlich Spionage
2012	Softwarefehler nach Update	Coop Genossenschaft, Basel	Nicht kriminell	Aufgrund einer fehlerhaften Softwareanpassung fällt das Kassensystem aus und alle Deutschschweizer Filialen müssen vorübergehend geschlossen bleiben.	--
2013	Distributed Denial-of-Service-Attacke (DDoS) + unsachgemässe Behebung	Spamhaus Project, Genf	Anti-Spamhaus-Aktivisten unter dem Namen 'Stophaus'	Unbekannte versenden eine DDoS und legen die Unternehmensseite lahm. Bei der Behebung des Problems wird die Funktionsweise eines Internetknotens eingeschränkt und so zusätzlich Schaden verursacht.	Vermutlich Rache
2014	Softwarefehler (fehlerhafte Software versendet 43'000 Kontoauszüge an die falschen Kunden)	Bank Coop AG	Nicht kriminell	Staatsanwaltschaft leitet Ermittlungsverfahren ein, erheblicher Reputationsschaden und Wiedergutmachungsaktion (SBB Gutscheine) nötig.	--
2014	Phishing bei Kunden von 12 Schweizer Banken	Schweizer Banken und deren Kunden	Unbekannt	Bankkunden werden von Fremden per E-Mail (unter dem Deckmantel eines offiziellen Bankschreibens) aufgefordert, Bankdaten preiszugeben; Schaden nicht bekannt.	Vermutlich monetäre Gründe

Tabelle 9: Ausgewählte Fallbeispiele Schweiz

Aktuelle Schweizer Fallbeispiele gehen insbesondere auf das Thema Phishing und das Hacken von Internetkonten ein. Abbildungen 6 und 7 zeigen zwei aktuelle Fallbeispiele, die aus dem jüngsten Report der Melde- und Analysestelle Informationssicherung (MELANI, 2014) entnommen sind. In Abbildung 6 sehen wir exakte Kopien der Internetseiten von Läderach, dem Bundesamt für Energie, der Swisscom und PayPal, jeweils mit dem Ziel an Kreditkarteninformationen zu gelangen (Phishing). Abbildung 7 zeigt Informationen zu zwei aktuellen E-Mail-Hackerattacken, bei denen zwei Kantonsräte betroffen waren. In beiden Fällen wurden Bettelbriefe im Namen der Kantonsräte versandt.

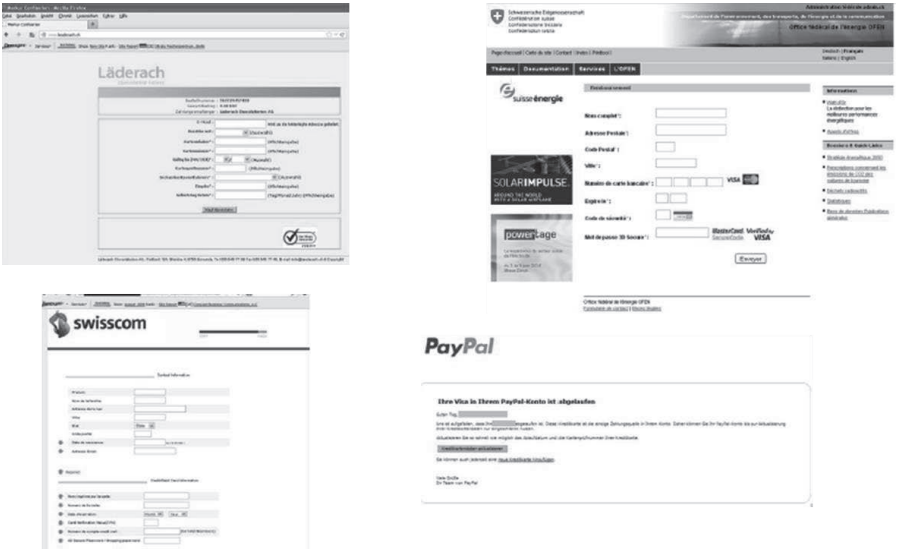


Abbildung 6: Aktuelle Fallbeispiele Schweiz – Phishing (MELANI, 2014)



Abbildung 7: Aktuelle Fallbeispiele Schweiz – E-Mail-Hacking (MELANI, 2014)

2.3 Analyse der globalen und politischen Seite von Cyber Risk

Immer häufiger wird auch die globale und politische Seite von Cyber Risk hervorgehoben. Das prominenteste Beispiel des Jahres 2013 ist der NSA-Spionageskandal, der von Edward Snowden enthüllt wurde. Analog zum Abschnitt 2.2 beleuchten wir die globale und politische Bedeutung von Cyber Risk ebenfalls anhand ausgewählter Fallbeispiele.

2.3.1 Cyberattacke auf Estland

Am 27. April 2007 startete ein Cyberangriff auf wichtige estländische Internetseiten. Betroffen waren Regierungswebseiten sowie für die Öffentlichkeit wichtige private Seiten von Zeitungen, Banken, Parteien oder Handynetzbetreibern (Spiegel, 2007). Mittels Distributed-Denial-of-Service-Attacken wurden die Webseiten überlastet und waren für mehrere Wochen nicht abrufbar oder deren Inhalte waren mit russischer Propaganda ersetzt worden (The Economist, 2007). Der massive Angriff war die erste Attacke, die auf die gesamte Informationsinfrastruktur eines Landes abzielte.

Anders als bei den meisten Cyberattacken blieben die Angreifer hier nicht anonym. Schon längst wurde vermutet, dass der Angriff seinen Ursprung in Russland hatte, doch erst im Mai 2009 bekannte sich die russische Jugendorganisation „Nashe“, die eng mit dem Kreml zusammenarbeitet, zu der Tat (Clover, 2009). Der Auslöser für den Angriff liegt in einem historischen Konflikt zwischen Estland und Russland, der sich in der Entfernung eines russischen Kriegsopferdenkmals aus dem Zentrum von Tallinn entfachte. Während die Esten diese ständige Erinnerung an die russische Besetzung auf einen militärischen Friedhof umsetzen wollten, sahen die russischen Teile der Bevölkerung darin eine Beleidigung und protestierten heftig (The Economist, 2007). Konsequenz aus dem Konflikt war, dass NATO und EU durch die Vorfälle alarmiert wurden und daraufhin in Tallinn einen Think-Tank einrichteten, der sich mit Fragen rund um diese neue Angriffsart auf Staaten beschäftigen sollte (Diggelmann, 2013).

Ziel:	Homepages staatlicher Einrichtungen, Zeitungen, Banken, Parteien oder Handynetzbetreibern
Angreifer:	Russische Jugendorganisation Nashe
Methoden:	DDoS mit Botnetzwerken
Schaden:	Nicht bekannt
Konsequenzen:	Einrichtung eines NATO-finanzierten Think-Tanks

2.3.2 Stuxnet-Virus

Der Stuxnet-Virus gilt als einer der professionellsten Computerviren, die es bisher gab (FAZ, 2010). Im Juni 2010 befiel der Virus mehrere Industrieanlagen, die durch das SCADA-System von Siemens gesteuert wurden. Durch die Infizierung der Systeme war es möglich, Zugriff auf die Industrieanlagen zu bekommen, Daten abzugreifen und die Systeme zu sabotieren. Entdeckt wurde der Computervirus zuerst im Iran bei einem Atomkraftwerk, das kurz nach der Infizierung in Betrieb genommen werden sollte. Der Virus verursachte Störungen in der iranischen Atomanlage. Kurze Zeit später wurde der Virus auch bei anderen Kraftwerken, Ölraffinerien und Militäranlagen entdeckt. Die iranische Regierung vermutete, dass der

Stuxnet-Virus von einer anderen Regierung entwickelt wurde, um ihr Atomprogramm auszuspionieren und zu sabotieren. Das Besondere an diesem Virus ist, dass er speziell für Industrieanlagen von Siemens (SCADA) entwickelt wurde. Aufgrund der Professionalität, die grosses Know-how verlangt, wird davon ausgegangen, dass die Entwicklung dieses Virus mit hohen finanziellen Kosten verbunden war. Gesicherte Erkenntnisse zum entstandenen Schaden, zum Entwickler und dessen Motiv gibt es bislang nicht.

Ziel:	Industrieanlagen mit SCADA-System der Firma Siemens
Angreifer:	Unbekannt
Methode:	Spezifischer, professionell entwickelter Virus
Schaden:	Nicht schätzbar
Konsequenzen:	Politische Instabilität: Iran beschuldigte andere Länder, den Angriff durchgeführt zu haben

2.3.3 Afrikanischer Frühling: Tunesien

Soziale Netzwerke spielten bei der tunesischen Jasmin-Revolution 2011 eine ausserordentlich wichtige Rolle (de Roquefeuil, 2011). Demonstrationen und weitere Aktionen der oppositionellen Bewegung wurden grösstenteils über Facebook und Twitter organisiert und koordiniert. Daraufhin verschärfte die machthabende Regierung die bereits vorhandenen Zensurmassnahmen erheblich, um so die Möglichkeiten zur Organisation zu beschneiden. Möglich war dies vor allem, weil sich die tunesische Internetbehörde, also der nationale Internet-Service-Provider (ISP), im Staatsbesitz befand.

Es sollen Facebook-, Google- und Yahoo-Passwörter ausspioniert, Accounts von Kritikern gelöscht und sogar Informationen bezüglich deren Aufenthaltsorte genutzt worden sein (Forbes, 2011). Solche Eingriffe in die Freiheit des Internets alarmierten die Organisation Anonymous, die daraufhin DDoS-Attacken gegen offizielle Regierungsseiten lancierte. Diese sollten von der tunesischen Regierung als Warnung verstanden werden, dass, wenn sie den Ruf des tunesischen Volkes nach Freiheit nicht anhöre, sie weiterhin Ziele von Cyberangriffen werden würde.

Ausserdem hackte Anonymous 2‘725 E-Mails von Mitgliedern der tunesischen Regierungspartei „Ennahda“, um Informationen über die Ermordung des Oppositionsführers Chokri Belaid zu gewinnen (Amara, 2012). Bei diesem Fallbeispiel muss bei der Kategorisierung zwischen den Handlungen der tunesischen Regierung und der Anonymous-Gruppierung unterschieden werden.

Angreifer:	Tunesische Regierung
Ziel:	Tunesische Oppositionsbewegung
Motiv:	Unterdrückung einer Revolution
Methoden:	Spionage, Manipulation
Schaden:	Nicht schätzbar
Konsequenzen:	Verschärfung des Konflikts, Involvierung der Anonymous-Gruppierung

Angreifer:	Anonymous
Ziel:	Tunesische Regierung
Motiv:	Wahrung der Meinungsfreiheit, Unterstützung der tunesischen Revolutionsbewegung
Methoden:	DDoS-Attacke, Hacking
Schaden:	Nicht schätzbar
Konsequenzen:	Stärkung der Oppositionsbewegung, Schwächung der Regierungspräsenz im WWW

2.3.4 NSA-Spionage

Edward Snowden löste im Juni des Jahres 2013 einen der grössten Datenskandale überhaupt aus (Pham und Wefing, 2013). Der US-amerikanische Whistleblower arbeitete zunächst als Computerfachmann für die Central Intelligence Agency (CIA) und war zuletzt als Systemadministrator des Beratungsunternehmens Booz Allen Hamilton für die National Security Agency (NSA) in Hawaii tätig. Durch seine berufliche Tätigkeit hatte er Zugang zu sehr vielen vertraulichen Daten der Organisation. So konnte er beispielsweise Informationen über die Praktiken der Geheimdienste sammeln, mit denen nicht nur Verdächtige, sondern auch befreundete Staaten ausspioniert wurden. Der Whistleblower kopierte Dokumente aus dem NSA-Büro und leitete sie an die Washington Post und den Guardian weiter.

Am 20. Mai beginnt die Flucht Snowdens (Reissmann, 2013). Er meldete bei seinem Arbeitgeber Urlaub an mit der Begründung, seine im vorherigen Jahr festgestellte Epilepsie behandeln lassen zu müssen. Er reist von Hawaii nach Hongkong. Am 6. Juni begannen die Washington Post und der Guardian mit der Veröffentlichung der von ihm gelieferten Dokumente. Diese teils als streng geheim klassifizierten Informationen erschütterten Menschen auf der ganzen Welt, da sich viele in ihrer Privatsphäre verletzt fühlten. Auch schlug die Veröffentlichung grosse Wellen in der Politik, da klar wurde, wie befreundete Staaten einander überwachen.

Zu den brisantesten Veröffentlichungen gehörten die Informationen über die Spionageprogramme „Prism“, „Boundless Informant“ und „XKeyscore“ der NSA sowie „Tempora“ der Govenment Communications Headquarters (GCHQ) aus Grossbritannien (Spiegel, 2013). Der nach Hongkong geflüchtete Snowden wurde von einem amerikanischen Gericht wegen Diebstahls von Regierungseigentum angeklagt (Zeit Online, 2013). Laut Wikileaks hat der Whistleblower in 21 Staaten Asyl beantragt, jedoch lehnten ihn die meisten Staaten aufgrund des grossen Drucks der USA ab. Schliesslich erklärte sich Russland dazu bereit, Snowden Asyl zu gewähren. Die USA reagierten auf die Handlung Moskaus zutiefst empört (Tagesanzeiger, 2013). Auch weiterhin hält sich Snowden in Russland versteckt.

Angreifer:	Systemadministrator Edward Snowden
Ziel:	NSA
Motiv:	Veröffentlichung von Geheimdienstpraktiken
Methoden:	Physischer Datendiebstahl
Schaden:	Nicht schätzbar

Konsequenzen: Aufklärung der Welt über Geheimdienstpraktiken, politische Dissonanzen, Sensibilisierung betreffend Datensicherheit

2.3.5 Zusammenfassung der Fallbeispiele

Tabelle 10 fasst die Fallbeispiele anhand der Kriterien Ziel, Angreifer, Schaden und Motiv zusammen. Wiederum unterstreicht die Zusammenstellung die ausserordentliche Heterogenität und ökonomische Relevanz von Cyber Risk. Was hier noch hinzukommt ist die grosse gesellschaftliche Relevanz, etwa im Beispiel der tunesischen Revolution.

Jahr	Fall / Methode	Ziel	Angreifer	Schaden	Motiv
2007	Cyberattacke auf Estland (mittels DDoS)	Staatliche Einrichtungen	Russische Jugendorganisation Nashe	Nicht schätzbar	Rache
2010	Stuxnet-Virus	Industrieanlagen mit SCADA-System	Nicht bekannt	Nicht schätzbar	Schädigung von Irans Atomprogramm
2011	Afrikanischer Frühling: Tunesien (mittels Spionage, Manipulation und DDoS)	Tunesische Revolutionsbewegung	Tunesische Regierung	Nicht schätzbar	Unterdrückung der Revolution
		Tunesische Regierung	Hackergruppe Anonymous	Nicht schätzbar	Unterstützung der tunesischen Revolutionsbewegung
2013	NSA-Spionage Snowden (Datendiebstahl)	NSA	Ehemaliger NSA-Mitarbeiter Edward Snowden	Nicht schätzbar	Enthüllung von NSA-Praktiken

Tabelle 10: Fallbeispiele zur globalen und politischen Bedeutung von Cyber Risk

2.4 Abhängigkeit vom Internet und Ausfallrisiko

Wir wollen hier die Abhängigkeit vom Internet und die Gefahr eines totalen Ausfalls des Internets analysieren. Dieses Szenario wird häufig als totaler Blackout bezeichnet und als Beleg für die grosse Abhängigkeit von neuen Technologien angesehen. Die Gefahr eines globalen Totalausfalls des Internets wird allerdings von den meisten Experten als eher gering eingeschätzt. Um dies weiter zu erläutern, wollen wir genauer auf das Internet selbst und das Risiko eines Totalausfalls eingehen. Später wollen wir noch mögliche Auswirkungen eines solchen Ausfalls bestimmen. Dabei wird dann schnell klar, wie abhängig wir mittlerweile vom Internet und der damit verbundenen Infrastruktur sind.

Geschichte des Internets
In den 1960er-Jahren war die technologische Entwicklung so weit, mittels technischer Netzwerke Daten übermitteln zu können (Bleicher, 2010). Das US-amerikanische Militär nutzte diese Technologie für die Kommunikation innerhalb des Militärs und den Universitäten, die für das Militär forschten. So entstand das Arpanet (Advanced Research Projects Agency Network), das eine erste Version des Internets darstellte. In den 1980er-Jahren trennte sich das Arpanet von seinem bisher nur für militärische Zwecke genutzten Netzwerk und wurde nun für die zivile Nutzung bereitgestellt. Während dieser Zeit entwickelte sich das Internet zu einem Informationsmedium und neue Kommunikationsformen, wie beispielsweise das E-Mail-System, wurden entwickelt. Anfang der 1990er-Jahre wurde mit dem World Wide Web das Internet für die breite Öffentlichkeit zugänglich gemacht, was zu einem regelrechten Boom führte.

Funktionsweise des Internets
Der Begriff „Internet“ steht für „Interconnected Net“ (Bleicher, 2010). Das bedeutet, dass das Internet einen Zusammenschluss verschiedener Netzwerke darstellt. Die Daten werden über Telekommunikationsleitungen (via Unterseekabel) und Satelliten übertragen und die verschiedenen Netzwerke werden mit Computern, Routern oder Gateways, die Knotenpunkte darstellen, miteinander verbunden. Innerhalb der Netzwerke verständigen sich die Computer mit gemeinsamen Sprachen (Protokollen). Die sogenannten Backbones sind Garant für das einwandfreie Funktionieren des Internets. Hierbei handelt es sich um leistungsstarke Netze, die für das Internet zentrale Datenleitungen bereitstellen. Die zu übertragenden Daten werden mittels Transfer Control Protocol (TCP) übertragen. Bei diesem Übertragungsvorgang werden die Daten beim Sender in kleinere Datenpakete aufgeteilt, nummeriert und beim Empfänger wieder zusammengesetzt. Mit Hilfe eines Internetprotokolls (IP) leiten die Router an den Knotenpunkten die jeweiligen Daten an die richtigen Empfänger weiter. Beim Verlust von Daten fordert das TCP die Daten erneut an. Das Internet selbst ist in verschiedene Schichten aufgeteilt, bei dem die Anwendungsschicht die für die Nutzer sichtbare Ebene darstellt. Die anderen Schichten dienen zur reibungslosen technischen Abwicklung des Datenaustauschs.

Totalausfall des Internets

Auf die Frage, ob ein totaler Kollaps des Internets möglich ist, antworten die meisten Experten mit einem „Nein“.[15] Diese Einschätzung wird zumeist durch die Topologie bzw. die allgemeine Architektur des Internets begründet; es ist hoch dezentralisiert, verteilt auf viele Server und Geräte an verschiedenen Orten und ist so sehr robust und belastbar (Vgl. z. B. Ahamad, 2012 oder Beckstrom, 2012). Zudem können die Daten über verschiedene Wege (überwiegend Kabel, jedoch auch Satelliten) übertragen werden.

Teilausfall des Internets

Obwohl viele Experten davon überzeugt sind, dass ein (globaler) Totalausfall unwahrscheinlich ist, hat die Vergangenheit gezeigt, dass grosse (regional begrenzte) Teilausvorfälle möglich sind. So kann es durchaus vorkommen, dass einzelne Gebiete vom Internet abgeschottet werden. Beispielsweise kam es im März 2013 zu einem Vorfall, bei dem fast ganz Afrika kurzzeitig vom Internet abgetrennt wurde (T-Online, 2013). Grund dafür waren mehrere durchtrennte Tiefseekabel. Die genaue Ursache ist immer noch unklar. Dennoch wird vermutet, dass der Vorfall auf Fischernetze zurückzuführen ist, die sich im Kabel verfangen hatten. In den meisten Teilen Afrikas war nicht nur das Internet ausser Kraft gesetzt, sondern auch der ganze Transaktionsverkehr war lahmgelegt. Es war während dieser Zeit beispielsweise unmöglich, mit ausländischen Kredit- oder Bankomatkarten Transaktionen durchzuführen. Bis alle Systeme wieder fehlerfrei zur Verfügung standen, dauerte es einige Tage (Hochstätter und Masiero, 2009). Abbildung 8 zeigt die verlegten Tiefseekabel (Stand: Februar 2014).

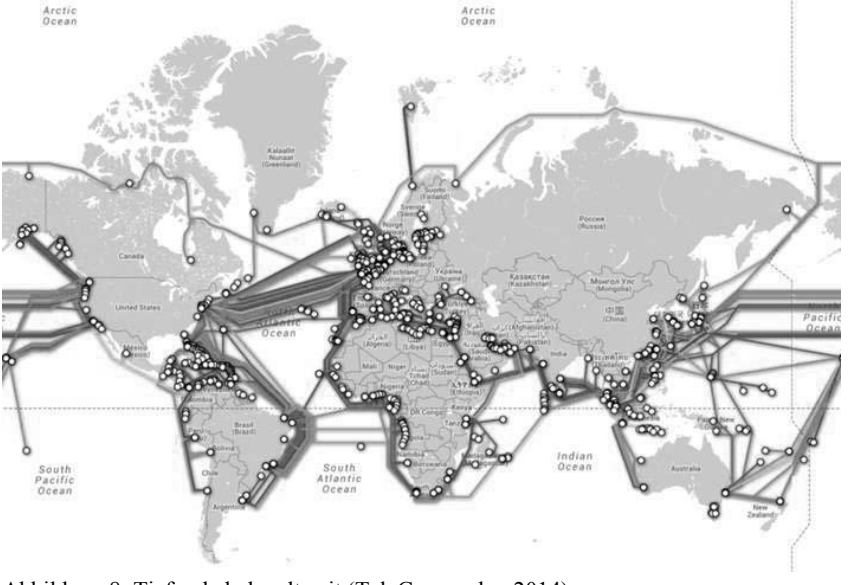


Abbildung 8: Tiefseekabel weltweit (TeleGeography, 2014)

[15] Dies deckt sich auch mit der Einschätzung des WEF im Rahmen ihres Global Risk Reports bzgl. eines „Critical Information Infrastructure Breakdowns“, der mit einer vergleichsweise geringen Eintrittswahrscheinlichkeit bewertet wird (siehe WEF, 2014, Abbildung 1.1). Im Jahr 2007 (siehe WEF, 2014, Abbildung 1.3) wurde dies noch für das Toprisiko nach Eintrittswahrscheinlichkeit gehalten.

Es ist zu erkennen, dass es sehr viele parallel verlegte Tiefseeleitungen gibt, die für einen Datenaustausch zwischen den Kontinenten verantwortlich sind. Einzelne Gebiete vom Internet zu trennen mag daher zwar möglich sein, dass aber die weltweite Datenübertragung kollabiert, scheint in der Realität eher sehr unwahrscheinlich.

Nach Strickland (2010) könnten aber auch solare Superstürme (Sonnenstürme) Beschädigungen an Satelliten verursachen, was wiederrum „nur" zu einem Teilausfall führen würde. Würden sich diese Stürme aber auch weitläufiger auswirken (z. B. Internetverbindungen auf der Erde betreffen), wären die Auswirkungen wohl generell viel schwerwiegender als der globale Kollaps des Internets.

Gegenmeinungen zum Totalausfall

Wenngleich die Mehrheit der Experten die Gefahr des Totalausfalls als gering erachtet, gibt es auch Gegenmeinungen. Neuere Facharbeiten bezweifeln die gängige Meinung, dass das Internet aufgrund seiner Topologie robust ist. Bashan et al. (2013) zeigen in einem Netzwerkmodell, dass ein Ausfall des Internets sehr wohl möglich ist. Hochstätter und Masiero (2009) führen an, dass vor allem IXPs (Internet Exchange Points; Internetknoten, die Schnittstellen zwischen verschiedenen Rechnernetzwerken bilden) für Angriffe von Cyberterroristen sehr gefährdet sind. Aufgrund der marktbeherrschenden Stellung des Routerherstellers für diese IXPs,[16] könnte durch Angriffe auf diese das Internet in einer grösseren Region oder gar weltweit zum Erliegen kommen. Eine weitere Gefahr sehen Hochstätter und Masiero (2009) in Angriffen auf DNS-Servern (Domain Name System). Bei DNS handelt es sich um das System, mit dessen Hilfe die Adressierung von Internetadressen umgesetzt wird. Gezielte Angriffe könnten dazu führen, dass zwar der Datentransport über das Internet weiterhin gewährleistet ist, jedoch Domainnamen nicht richtig aufgelöst werden können und so das Internet unbrauchbar wird.

Zusammenfassung Total- / Teilausfall des Internets

Zusammenfassend lässt sich sagen, dass ein längerer globaler Ausfall des Internets von den meisten Experten als eher unwahrscheinlich erachtet wird. Es gibt aber sowohl theoretische als auch empirische Belege, dass zumindest Teilausfälle des Internets gut möglich sind. Dies ist auch vor allem vor dem Hintergrund bedenklich, dass es bis heute nur relativ wenig Notfallplanungen für ein derartiges Szenario gibt. Zwar haben inzwischen viele Staaten erste nationale Strategien zum Schutz kritischer Infrastrukturen definiert, einen echten Plan B im Fall eines globalen Ausfalls gibt es aber nicht (P.M. Magazin, 2012). Unternehmen wie auch Staaten sollten folglich ein derartiges Szenario in ihrer Notfallplanung tiefergehend diskutieren.

Auswirkungen

Schlussendlich wollen wir noch mögliche Auswirkungen diskutieren, mit denen zu rechnen ist, falls es dennoch zu einem Totalausfall kommen sollte bzw. zu einem regionalen Ausfall kommt. Die finanziellen Konsequenzen eines flächendeckenden und nur wenige Tage dauernden Ausfalls werden vom WEF auf bereits rund 250 Milliarden US-Dollar geschätzt (siehe WEF, 2010). Dies zeigt bereits, welche weitreichenden wirtschaftlichen Folgen ein solcher

[16] Cisco Systems, Inc. ist die ungebrochene Grösse im Enterprise Networking Markt (Vgl. Synergy Research Group, 2013). So besass Cisco im Jahre 2012 einen Marktanteil von 54 % in diesem Segment, wobei die Marktanteile bei Ethernet Switches (Netzwerkweichen) und Routern mit bis zu 68 % noch deutlich höher lagen.

Totalausfall des Internets haben kann. Dabei würde ein solches Szenario zuerst einmal die allgemeinen Kommunikationsmöglichkeiten einschränken. Kommunikation über Textmessaging-Dienste oder E-Mails ist nicht mehr möglich. Cloud-Systeme sind nicht mehr verfügbar und die darauf gespeicherten Daten nicht mehr zugänglich. Auch Dienste wie Onlinebanking und PayPal sind nicht mehr verfügbar (Vgl. Strickland, 2010). Ist ein Ausfall nur temporär bedingt – wie im Fall des getrennten Verbindungskabels in Afrika bereits geschehen –, kann es zu um Tage verzögerten Überweisungen und Onlinesteuererklärungen kommen (Vgl. auch Hochstätter und Masiero, 2009). Zudem sind alle Webseiten offline, was vor allem für Unternehmen, deren Geschäftsbetrieb auf das Internet angewiesen ist, essenzielle Folgen haben kann (z. B. Google oder Amazon). Im schlimmsten Fall gehen diese Unternehmen Bankrott und die Mitarbeiter können nicht weiterbeschäftigt werden. Zudem kann der Ausfall des Internets zu weitreichenden Versorgungsproblemen in der Industrie führen. Produzierende Unternehmen stehen mittlerweile immer öfter mit ihren Zulieferern und Abnehmern über Internet in Verbindung, um so eine effiziente Just-in-time-Produktion zu ermöglichen (Vgl. Hochstätter und Masiero, 2009). Auch dies würde mit Wegfall des Internets erschwert. Zudem wird der Handel an Börsen behindert, da Orders nicht mehr ausgeführt werden können (Vgl. Hochstätter und Masiero, 2009).

Neben den Versorgungsengpässen in der Wirtschaft kann der Ausfall des Internets auch Auswirkung auf die privaten Haushalte haben. Fällt das Internet aus, können die sogenannten Smart Grids nicht mehr kommunizieren und ihrer Aufgabe nicht mehr adäquat nachgehen. Dabei handelt es sich um intelligente Systeme, die Versorgungsengpässe und -überschüsse, z. B. bei Strom oder Wasser, erkennen und diese automatisch ausgleichen (Strickland, 2010). Die nötige Kommunikation basiert meist auf dem Internet. Stromausfälle und Unterversorgung sind möglich. Ahamad (2012) gibt zusätzlich noch das Beispiel, dass durch fehlendes Internet elektronische Arztberichte nicht verfügbar sein könnten, und so im schlimmsten Fall Menschen sterben.

Alle Beispiele beschreiben Worst-Case-Szenarien, zu denen es so vielleicht nie kommen wird. Dennoch wird an der Vielzahl und Vielfalt der Beispiele deutlich, welche weitreichenden Folgen ein Ausfall dieses mittlerweile so wichtigen Mediums – des Internets – auf den verschiedensten Ebenen haben kann. Es unterstreicht aber auch, wie gross unsere Abhängigkeit vom Internet mittlerweile ist. Diese Abhängigkeit wird voraussichtlich in Zukunft weiter zunehmen und so die Gefahren, die mit einem Ausfall des Mediums Internet einhergehen können, weiter verschlimmern.

3 Management von Cyber Risk

3.1 Risikomanagement nach ISO 31000:2009

Definition von Risikomanagement
Mit der ISO Norm 31000:2009 „Risk Management – Principles and Guidelines“, wurde im Jahr 2009 ein weltweit abgestützter und branchenübergreifender Standard zum Risikomanagement (RM) geschaffen (Vgl. ISO31000, 2009). Darin wird das RM definiert als

„… alle koordinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiko“.

Aufgaben des Risikomanagements
Das RM eines Unternehmens muss die wesentlichen Risiken identifizieren und diese systematisch mit geeigneten Instrumenten steuern. Des Weiteren sollen unter Berücksichtigung der vorhandenen Strukturen und Prozesse die organisatorischen Massnahmen zur Integration des Risikomanagements in die Unternehmensführung getroffen werden. Dazu gehört, dass die Risiken eines Unternehmens identifiziert, analysiert und bewertet werden (sogenannter Risikobeurteilungsprozess; Vgl. ISO31000, 2009).

Bedeutung des Risikomanagements
Die Bedeutung des RM hat in den vergangenen Jahren deutlich zugenommen. So wird beispielsweise RM im Corporate Governance als eine der wichtigsten Führungsaufgaben der obersten Leitung einer Organisation oder eines Unternehmens gesehen (Vgl. Romeike und Brühwiler, 2010, S. 106). So wird auch im “Swiss Code of Best Practice for Corporate Governance“ ein für das Unternehmen angepasstes RM gefordert. In einigen Unternehmen wird RM noch primär als ein Instrument des internen Kontrollsystems verstanden, das sich vordringlich mit den Fragen der finanziellen Berichterstattung und Gesetzeskonformität (Reporting und Compliance) befasst. Viele Unternehmen verknüpfen das RM aber auch immer stärker mit dem strategischen Management und definieren RM als Aufgabe auf Vorstandsebene (z. B. durch die Definition eines Chief Risk Officers).

Risikomanagement-System
Wurde beim RM in der Vergangenheit nur der Prozess der Risikobeurteilung (also Identifizierung, Analyse und Bearbeitung von Risiken) als wichtig angesehen, wird durch die Definition im ISO 31000:2009 auch die Betrachtung des organisatorischen Rahmens für das RM als wichtiger Bestandteil vermerkt. Dafür definiert der Standard das RM-System, das in Abbildung 9 grafisch veranschaulicht wird. Dieses besteht grundsätzlich aus drei Teilen. Neben der Definition von Grundsätzen für das RM, wird das RM durch das RM-Framework und den RM-Prozess beschrieben.

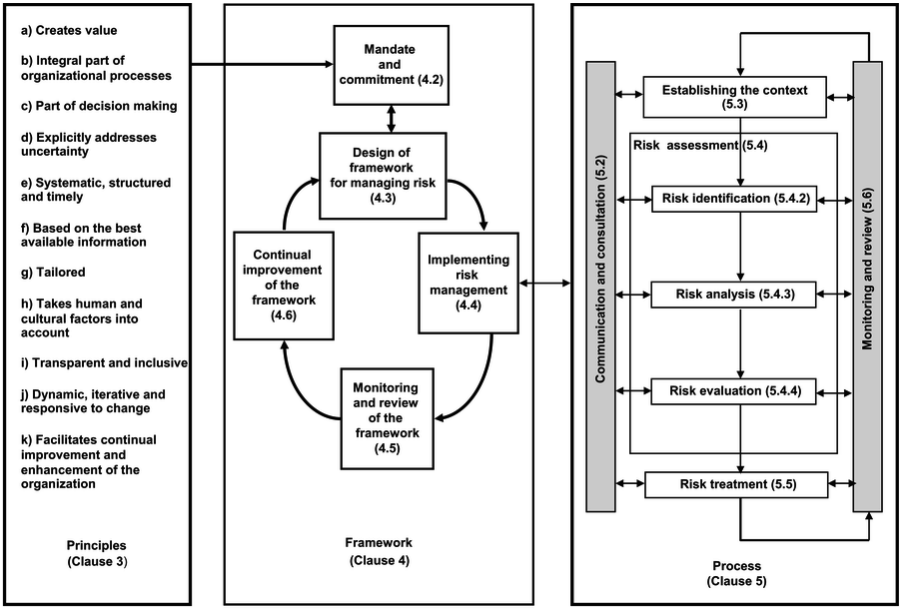


Abbildung 9: Risikomanagement nach ISO 31000:2009 (ISO31000, 2009)

Risikomanagement – Grundsätze
Die ISO Norm 31000:2009 definiert elf Grundsätze für das RM (Vgl. ISO31000, 2009):

(1) Es schafft Wert
(2) Ist integrierter Bestandteil des Organisationsprozesses
(3) Ist Teil der Entscheidungsfindung
(4) Befasst sich ausdrücklich mit der Unsicherheit
(5) Ist systematisch, strukturiert und zeitgerecht
(6) Es stützt sich auf die besten verfügbaren Informationen
(7) Ist massgeschneidert
(8) Berücksichtigt Human- und Kulturfaktoren
(9) Ist transparent und umfassend
(10) Es ist dynamisch, iterativ und reagiert auf Veränderungen
(11) Erleichtert kontinuierliche Verbesserung und Verstärkung der Organisation.

Speziell aus den Punkten (2), (3) und (11) wird deutlich, dass das RM einen Unterstützungsprozess für die Unternehmensführung darstellt und im Gegensatz zur reinen Risikobetrachtung immer handlungsbezogen ist. Somit ist der Einsatz systematischer Vorgehensweisen und passender Instrumente (beschrieben im RM-Prozess) für ein effektives RM ebenso wichtige Voraussetzung wie die Integration in die Unternehmensführung (beschrieben im RM-Framework).

Risikomanagement-Framework
Das RM-Framework beschreibt die Aufgaben der Führung einer Organisation und somit auch die Einordnung des RM in der Unternehmensleitung. Zum Framework gehören im Wesentlichen die Managementaufgaben Planung, Umsetzung, Bewertung und Verbesserung (auch als Deming-Kreis mit P-D-C-A-Zyklus bzw. Plan-Do-Check-Act-Zyklus bekannt, Vgl. in der Folge Romeike und Brühwiler, 2010, S. 113ff.).

Den Anfang des RM-Frameworks bildet die RM-Politik. Sie beschreibt die allgemeinen Ziele und die Ausrichtung der Organisation in Bezug zum RM. Zudem sind hier die Verpflichtungen der obersten Leitung für die Einführung, Aufrechterhaltung, Bewertung und Verbesserung des RM-Frameworks zu definieren. Wichtige Vorgaben dazu können sich auch aus den Grundsätzen für das RM ergeben.

Sind diese Grundlagenentscheidungen getroffen, kann mit der Planung (*Plan*) und dem Design des Frameworks begonnen werden. Hierbei soll die RM-Politik formal umgesetzt werden. In der Planung wird insbesondere das „Was" und das „Wie" im Umgang mit Risiken, die dazu erforderlichen Ressourcen und Fähigkeiten, die Rollen, die Verantwortlichkeiten und Kompetenzen sowie die Integration des RM-Prozesses und die Kommunikation im RM spezifiziert.

Die eigentliche Umsetzung (*Do*) wird dann durch den RM-Prozess beschrieben, der auch den zuvor genannten Risikobeurteilungsprozess enthält. Zusätzlich müssen Entscheidungen über den Gebrauch von Notfall-, Krisen- und Kontinuitätsmanagement sowie über die allgemeine Integration ins Managementsystem getroffen werden. Des Weiteren soll / muss auch hier die Dokumentation des RM stattfinden.

Der Umsetzung soll dann die Überwachung (*Check*) folgen, bei der festgestellt werden soll, ob das RM wirksam ist bzw. die gewünschten Änderungen auch wirklich eintreten. Durch qualitative und quantitative Leistungsbewertung oder ein Audit des RM kann dies bewerkstelligt werden.

Werden bei der Überwachung Defizite festgestellt, können diese im letzten Handlungsschritt (*Act*) behoben werden. Defizite können dabei Anforderungen darstellen, die noch nicht umgesetzt oder Anforderungen, die falsch oder mehrfach umgesetzt wurden. Nachdem Verbesserungen umgesetzt wurden, beginnt der Prozess im RM-Framework erneut, da durch etwaige Änderungen wieder neue Risiken entstanden bzw. im Laufe der Zeit andere Risiken hinzugekommen sein können.

Risikomanagement-Prozess
Wie bereits angedeutet nimmt der RM-Prozess einen essenziellen Teil in der Umsetzung des RM ein. Laut der Norm ISO 31000 (Vgl. ISO31000, 2009, Definition 2.8) versteht man unter dem RM-Prozess die

„… systematische Anwendung von Managementstrategien, Verfahren und Praktiken zur Bearbeitung / Koordination der Aktivitäten der Kommunikation, der Beratung, der Gründung eines Kontexts und der Identifikation, der Analyse, der Bewertung, der Behandlung, der Überwachung und Überprüfen von Risiken".

Konkret schliesst dies die eigentliche Risikobeurteilung, die Anwendung der RM-Instrumente, die Überwachung / Überprüfung der Massnahmen und die Kommunikation mit ein. Der Prozess lässt sich grundsätzlich in fünf Schritte aufteilen, die zeitlich aufeinander folgen. Die Schritte 2 bis 4 werden auch unter dem Namen Risikobeurteilung zusammengefasst. Eine grafische Darstellung des RM-Prozesses ist im rechten Teil der Abbildung 9 zu finden.

Schritt 1: Zusammenhang herstellen
Im ersten Schritt soll ein Zusammenhang zum RM-Framework und damit zur Unternehmensführung hergestellt werden. Dazu müssen externe und interne Parameter definiert werden, die bei der Behandlung von Risiken zu beachten sind (Vgl. ISO31000, 2009, Definition 2.9). Extern beschreibt in diesem Zusammenhang Kenngrössen, die durch das Umfeld des Unternehmens bestimmt werden, z. B. kulturelle, soziale, politische, regulatorische, finanzielle Rahmenbedingungen (Vgl. Definition 2.10). Intern beschreibt hingegen Parameter, die durch Eigenschaften der Organisation vorgegeben werden, z. B. Unternehmensstruktur, firmenspezifische Standards und Politiken, Unternehmenskultur, Informationssysteme oder Entscheidungsprozesse (Vgl. Definition 2.11). Zusätzlich zu den Parametern sollten der Anwendungsbereich und die Risikokriterien für die RM-Politik erarbeitet werden (Vgl. Definition 2.9). Die Risikokriterien stellen dabei Zielvorgaben dar, anhand derer sich die Bedeutung des Risikos in einem späteren Schritt einstufen lässt (Vgl. Definition 2.22). Gemeint sind hierbei Vorgaben zur Risikotragfähigkeit des Unternehmens (etwa Höhe des vorhandenen Eigenkapitals) und zum Risikoappetit der Eigentümer.

Schritt 2: Risiken identifizieren
Nachdem der Zusammenhang mit der Unternehmensführung hergestellt wurde, müssen nun die Risiken identifiziert werden. Die Identifizierung erklärt den Prozess des Findens, Erkennens und Beschreibens von Risiken (Vgl. ISO31000, 2009, Definition 2.15). Zum einen müssen die Ursachen für Risiken bestimmt werden (Vgl. Definition 2.16). Zum anderen sollten Events (Ereignisse bzw. bestimmte Zustandsveränderungen) definiert werden, bei denen man vom Eintritt eines Risikos spricht (Vgl. Definition 2.17). Schlussendlich müssen auch zu den Events mögliche Konsequenzen erarbeitet werden (Vgl. Definition 2.18). Darüber hinaus lassen sich die zu identifizierenden Risiken in vier verschiedene Erscheinungsformen einordnen (Vgl. VBV, 2003, S. 46): Offenkundige Gefahren, die sofort erfasst werden können (z. B. Aktienkurse); versteckte Gefahren, die nicht gleich ersichtlich sind (z. B. Liquiditätsrisiken in der Zeit vor der Finanzkrise); verdrängte Gefahren (z. B. Immobilienblase) sowie unbekannte Gefahren (z. B. Asbest in den 1960er-Jahren).

Schritt 3: Risiken analysieren
Die Analyse von Risiken ist geprägt durch das Verstehen der identifizierten Risiken und der Bestimmung des Risikolevels (Vgl. ISO31000, 2009, Definition 2.21), die die Grössenordnung eines Risikos beschreiben sollen. Diese Grössenordnung wird zum einen gemessen durch das Ausmass des Risikos, also die Konsequenzen (Gewinn- / Verlustpotenziale), die bereits identifiziert wurden und zum anderen durch deren Eintrittswahrscheinlichkeiten (Vgl. Definition 2.23). Für beide Parameter müssen also in diesem Schritt Werte definiert bzw. falls möglich (auf historischen Daten), approximiert werden.

Schritt 4: Risiken bewerten
Dieser Schritt beschäftigt sich mit dem Vergleich der Resultate aus Schritt 3 (Risiken analysieren) mit den Definitionen aus Schritt 1 (Risikokriterien). Dadurch soll entschieden werden, ob ein Risiko akzeptabel oder tolerierbar ist (Vgl. ISO31000, 2009, Definition 2.24). Dieser Schritt bildet damit zugleich die Grundlage für den nächsten Schritt der Risikobewältigung. Wird beispielsweise ein Risiko als für das Unternehmen „nicht tragbar" erklärt, kommen andere Risikomanagement-Strategien zum Einsatz als im Fall, in dem ein Risiko als „akzeptierbar" erachtet wird. Ein effizientes Mittel, um die Risiken in „akzeptierbare" und „nicht tragbare" Risiken zu klassifizieren, ist die sogenannte Risk Map, die wir später auch auf Cyber Risk anwenden werden.

Schritt 5: Risiken bewältigen
Wurden Risiken als „nicht tragbar" erklärt, müssen sie bewältigt werden. Die ISO Norm 31000 definiert diesen Schritt als den Prozess der Risikoumwandlung (Vgl. Definition 2.25). Die Wahl des entsprechenden Instruments zur Umwandlung ist dabei durch die Risikobereitschaft des Unternehmens bestimmt, denn spezielle Massnahmen eliminieren das Risiko nicht vollständig, sondern schwächen es nur ab. Die Risikoumwandlung kann durch die folgenden Alternativen erfolgen:

- Risiko vermeiden: Entschluss, die Tätigkeiten, bei denen das Risiko auftreten kann, nicht aufzunehmen bzw. nicht mehr fortzusetzen
- Verminderung / Begrenzung: alle Massnahmen zur Gefahrenverhütung (Verminderung der Eintrittswahrscheinlichkeit) und Schadenbegrenzung (Abschwächung der Konsequenzen)
- Risikotransfer: Risiko wird mit einer oder mehreren Parteien geteilt (z. B. Versicherung)
- Selbsttragung des Risikos: Entscheidung, sich bewusst dem Risiko auszusetzen. Für diesen Fall sollte allerdings Vorsorge getroffen werden (z. B. Eigenkapital bilden). Das Risiko muss weiter überwacht und später erneut überprüft werden.

In unserer Risikodefinition haben wir auch über Chancen gesprochen. In diesem Zusammenhang kann es also nützlich sein, Risiko bewusst einzugehen bzw. sich verstärkt Risiko auszusetzen, um die daraus resultierenden Vorteile auch ausnutzen zu können. Wie bereits beschrieben hängen diese Entscheidungen aber von der individuellen Risikobeurteilung des Unternehmens ab und können nur schwer auf einem objektiven Niveau definiert werden.

Kommunikation und Informationsaustausch
Begleitet werden diese fünf Schritte durch die Kommunikation und den Informationsaustausch. Dies soll die Bedeutung betonen, den RM-Prozess mit den internen und externen Stakeholdern abzustimmen (Vgl. ISO31000, 2009, Definition 2.12). Die Informationen, die dabei ausgetauscht werden können, beziehen sich auf die Existenz, Natur, Ausgestaltung, Wahrscheinlichkeit, Bedeutung, Bewertung, Annehmbarkeit und Bewältigung von Risiken.

Überwachung und Überprüfung

Da sich das Unternehmen in einem dynamischen Umfeld befindet, sind regelmässige Anpassungen notwendig. Die Überwachung und die Überprüfung der Risiken stellen einen essenziellen Bestandteil des RM-Prozesses dar und sorgen so dafür, dass bei Bedarf Anpassungen an den fünf Schritten vorgenommen werden. Nur so ist das RM eines Unternehmens effektiv und sichert das Unternehmen vor den bestehenden Risiken adäquat ab. Im Einzelnen besteht die Überwachung in kontinuierlichem Kontrollieren, Beaufsichtigen, kritischem Beleuchten und der Bestimmung von Abweichungen vom Soll (Vgl. ISO31000, 2009, Definition 2.28). Die Überprüfung stellt die Tätigkeit dar, mit der die Eignung, Angemessenheit und Wirksamkeit der Zielerreichung gemessen werden soll (Vgl. Definition 2.29). Sowohl Überwachung als auch Überprüfung sind auch im RM-Framework im Bereich „Handeln“ anzutreffen und erfüllen dort eine ähnliche Aufgabe wie im RM-Prozess.

3.2 Cyber Risk im Risikomanagement-Prozess

Der im vorangegangenen Abschnitt vorgestellte Standard zum RM ist sehr allgemein und nicht an einer bestimmten Problemstellung des RM ausgerichtet. In diesem Abschnitt wenden wir den allgemeinen RM-Prozess auf das Fallbeispiel Cyber Risk an.

Standards für Informationssicherheitsmanagement
Es handelt sich bei Cyber Risk um ein Thema, das in der wissenschaftlichen Literatur bisher noch nicht viel Aufmerksamkeit genossen hat. Allerdings lassen sich inzwischen eine Reihe von Industriestandards, insbesondere auch aus dem Bereich IT, aufzählen, die als Vorlage und Unterstützung für das RM von Cyber Risk dienen können. So sind etwa eigens für das RM von Informationssicherheitsrisiken spezialisierte Standards definiert worden. Zu den wichtigsten Standards in diesem Bereich gehören etwa:[17]

- ISO/IEC 2700x-Familie (Information technology – Security techniques): Dieser Standard beschäftigt sich mit dem Information-Security-Management und dem dazugehörigen Information-Security-Management-System (ISMS). Eine ausführliche Zusammenstellung des Standards kann in Klipper (2011) oder direkt im Standard (Vgl. neuste Version des Standards: ISO27000, 2012) gefunden werden.
- BSI-IT-Grundschutz (BSI-Standard 100-x Familie): Für Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) 2006 den BSI-IT-Grundschutz veröffentlicht. Dabei handelt es sich um eine Sammlung von Informationen, die dazu dienen, mögliche sicherheitsrelevante Schwachstellen im IT-Verbund eines Unternehmens zu erkennen und zu beheben.
- Control Objectives for Information and Related Technology (COBIT): Im Jahr 2012 veröffentlichte die Information Systems Audit and Control Association (ISACA) COBIT 5 ein übergeordnetes Rahmenwerk für die Governance und das Management der unternehmensweiten IT (Vgl. ISACA, 2012).
- ISACA Risk IT: IT-Risk-Management-Framework
- Cyber Security Best Practices des Communications Security, Reliability and Interoperability Council

Zertifizierung
Ein wichtiger Aspekt in diesem Zusammenhang sind auch Bestimmungen, um eine Zertifizierung nach den entsprechenden Standards zu erhalten. Eine solche Zertifizierung weist nach, dass in einem Unternehmen ein gewisses Sicherheitsniveau vorhanden ist. Dies wird immer häufiger von Geschäftspartnern und Kunden als Nachweis der eigenen Vorkehrungen gegen IT-Sicherheitsvorfälle verlangt (Vgl. BSI, 2012). Eine Zertifizierung nach bestimmten IT-Standards kann auch ein wichtiges Signal an einen Versicherer sein, um die Versicherbarkeit bestimmter Risiken zu erhöhen.

[17] Neben den IT-Standards ist zu berücksichtigen, dass aufgrund der inhaltlichen Schnittmenge mit operationellen Risiken auch das Management operationeller Risiken nützliche Hinweise für das Management des Cyber Risk liefern kann.

In den Standards werden viele Informationen zu einem angemessenen Management für Informationsrisiken gegeben. Leider sind diese Informationen meist sehr allgemein und nur bedingt auf Cyber Risk anwendbar. Um einen noch besseren Einblick in das Management von Cyber Risk zu bekommen, wird in der Folge der RM-Prozess für Cyber Risk analysiert. Dazu werden wir aus den bekannten Standards und weiteren wissenschaftlichen Quellen die aus unserer Sicht relevanten Aspekte für ein Management von Cyber Risk herausfiltern. Auch aus dem Cyber-Risk-Self-Assessment, das Versicherer im Rahmen einer Antragsprüfung verlangen (siehe etwa Drouin, 2004, für ein Beispiel), können wertvolle Hinweise zum RM abgeleitet werden.

3.2.1 Zusammenhang herstellen

Als Erstes muss das Ziel des Risikomanagements vor dem Hintergrund des Unternehmensziels festgelegt werden. Zudem muss insbesondere die organisatorische Verankerung des RM festgelegt werden und es müssen Kriterien zur Risikobewertung definiert werden.

Zielsetzung
Typischerweise wird im RM ein Sicherheitsniveau (sogenanntes Konfidenzniveau) festgelegt. So setzen etwa Solvenzmodelle im Versicherungsbereich ein Konfidenzniveau von 99 % oder 99,5 % voraus, das bedeutet, eine Insolvenz erfolgt im statistischen Durchschnitt in 1 % bzw. 0,5 % der Fälle (1-mal in 100 Jahren oder 1-mal in 200 Jahren). Für die Zielfestlegung spielen die (internen und externen) Rahmenbedingungen eine wichtige Rolle. So ist dem Cyber Risk in einer Bank und einem Krankenhaus aufgrund der hohen Datensensibilität eine andere Priorisierung beizumessen als in weniger sensiblen Geschäftsbereichen. Dies könnte sich etwa in einem höheren Konfidenzniveau widerspiegeln. Dabei ist weiter zu differenzieren in verschiedene Vorfälle, die einer unterschiedlichen Behandlung bedürfen (etwa Verstoss gegen Gesetze, gegen Verträge mit Kunden etc.). Konsequenterweise ist in einer Bank oder einem Krankenhaus also ein höheres Sicherheitsniveau für kritische Ereignisse zu definieren als in weniger sensiblen Branchen.

Institutionelle Verankerung
Es gibt empirische Belege, dass bereits die institutionelle Verankerung des Themas Cyber Risk für ein erfolgreiches Management dieser neuen Risikoart zentral ist. So weisen Firmen, die einen Chief Information Security Officer (CISO) oder eine ähnliche Funktion installiert haben, im Falle eines Datenverlusts signifikant niedrigere Kosten auf (157 US-Dollar versus 236 US-Dollar pro Vorfall; siehe Shackelford, 2012).[18] Dieses empirische Resultat belegt auch direkt zu Beginn der Diskussion, dass durch ein effizientes RM (die Wahrscheinlichkeit und) das Ausmass eines Cyber-Risk-Schadens signifikant gesenkt werden kann.[19]

[18] Dieses Resultat entspricht allgemeinen Resultaten zur institutionellen Verankerung eines Chief Risk Officers (CRO). Vgl. etwa Grace et al. (2014).

[19] Es sei angemerkt, dass eine der weltweit grössten IT-Firmen (Sony) beim grossen Hackerangriff im April 2011 keinen Chief Information Security Officer oder eine ähnliche Funktion installiert hatte. Vor dem Hintergrund der empirischen Resultate erscheint die Definition einer derartigen Funktion bereits für Unternehmen mittlerer Grösse sehr relevant und empfehlenswert, insbesondere wenn das Unternehmen in einer datensensiblen Branche (z. B. Bank, Krankenhaus) tätig ist.

Anwendungsbereiche und Grenzen
Zur Festlegung des Kontextes gehört auch, den Anwendungsbereich und seine Grenzen klar zu definieren. Hierbei ist im Speziellen zu klären, für wen und was Cyber-Risk-Management überhaupt bindend sein soll. Da Cyber Risk sehr breit definiert ist, ist auch der Anwendungsbereich grundsätzlich sehr breit.[20] Zudem müssen Nebenbedingungen beachtet werden. So können beispielsweise Informationssicherheitsrichtlinien und datenschutzrechtliche Rahmenbedingungen den Anwendungsbereich einschränken.[21]

Kriterien zur Risikobewertung
Eine weitere Aufgabe des ersten Schrittes ist, dass Kriterien festgelegt werden müssen, anhand derer später eine Risikobewertung vorgenommen wird. Insbesondere ist hier die Risikotragfähigkeit des Unternehmens zu definieren, sowohl bezüglich möglicher Verlusthöhen als auch möglicher Verlustwahrscheinlichkeiten. Dies ist insbesondere mit dem Risikoappetit der Stakeholder abzustimmen. Cyber Risk hat hier eine besondere Relevanz, da sie mitunter neben direkten Kosteneffekten auch indirekte Wirkungen entfalten können, etwa hinsichtlich der Reputation des Unternehmens. Die Definition der Kriterien ist sehr bedeutsam, da hier die Richtung für den gesamten RM-Prozess vorgegeben wird. Wichtig ist hier auch, dass bei jedem erneuten Durchlauf des RM-Prozesses die Kriterien auf die aktuellen Gegebenheiten angepasst werden.

3.2.2 Cyber Risk identifizieren

Die Risikoidentifikation stellt den ersten Teil der Risikobeurteilung dar. Die Risikoidentifikation gliedert sich in der Informationssicherheit in fünf Teile, auf die wir nachfolgend nacheinander eingehen (Vgl. Klipper, 2011, S. 72).

Assets identifizieren
Zuerst sollen Assets mit den dazugehörigen Geschäftsprozessen identifiziert werden, die für das RM relevant sind (Vgl. Klipper, 2011, S. 72). Dabei unterscheidet der ISO-Standard 27001 zwei Asset-Gruppen: Primary Assets und solche, die zur Unterstützung von Primary Assets dienen.

- Zu den Primary Assets gehören alle Geschäftsprozesse, die unerlässlich bei der Erreichung der Geschäftsziele sind, unerlässlich bei der Einhaltung gesetzlicher und vertraglicher Verpflichtungen sind oder geheimhaltungsbedürftige Prozesse oder Prozessbestandteile. Zudem werden alle Informationen, die unerlässlich bei der Erreichung der Geschäftsziele sind, dem Datenschutz unterliegen, den strategischen Geschäftszielen dienen

[20] Grundsätzlich ist jeder im Unternehmen vom Management des Cyber Risk betroffen, insbesondere aber solche Personen, die Zugang zu sensiblen Informationen haben. Letztere bedürfen einer speziellen Aufmerksamkeit im Management des Cyber Risk. Auch gibt es spezielle Aspekte des Cyber Risk, die nur durch Spezialisten zu organisieren sind, etwa das Risiko eines Datenverlusts durch Naturkatastrophen. Demgegenüber gibt es aber auch viele Themen, die für alle Mitarbeiter im Unternehmen relevant sind, etwa der vertrauliche Umgang mit Kundendaten. Dieser breite Anwendungsbereich ist ein Unterschied etwa zum Management von Markt-, versicherungstechnischen und Kreditrisiken. Bei operationellen Risiken ist der Anwendungsbereich allerdings grundsätzlich auch sehr breit.

[21] Auch dies steht wieder im Unterschied zum Management anderer Risikoarten, wo derartige Einschränkungen in der Regel nicht bestehen. Eine derartige Einschränkung ist aber für das Management operationeller Risiken sehr typisch, etwa die Persönlichkeitsrechte der Mitarbeiter etc.

oder bei ihrer Beschaffung, Speicherung, Verarbeitung oder Ähnlichem hohe Kosten verursacht haben und nicht öffentlich zugänglich sind, gezählt.
- Unterstützende Assets zeichnen sich dadurch aus, dass sie dazu geeignet sind, durch die Kombination einer Schwachstelle und einer Bedrohung zum Problem für eines der Primary Assets zu werden (z. B. Hardware, Software, Netzwerk, Mitarbeiter; Vgl. auch Klipper, 2011, S. 73).

Bedrohungen identifizieren
In einem zweiten Schritt müssen mögliche Bedrohungen, deren Typ und mögliche Quelle bestimmt werden. Eine ausführliche Liste gängiger Bedrohungen kann im Annex C des ISO-Standards 27005 gefunden werden (Vgl. Klipper, 2011, S. 74). Dabei können verschiedene Erscheinungsformen von Cyberrisiken beispielhaft zugeordnet werden:[22]

- Offenkundige Gefahren: Unternehmen könnte von einem Hackerangriff oder einem Stromausfall betroffen sein
- Versteckte Gefahren: Ein installierter Keylogger kann über lange Zeit Eingaben des Benutzers an einem Computer mitprotokollieren, ohne dass dieser sich einer Gefahr bewusst ist
- Verdrängte Gefahren: Beispielsweise wird die Gefahr eines Datenverlusts und damit verbunden die Notwendigkeit einer regelmässigen Datensicherung häufig aus Bequemlichkeit verdrängt
- Unbekannte / unerkannte Gefahren: Gerade im dynamischen Umfeld des Internets können schnell neue Gefahren auftreten; beispielsweise war vor zehn Jahren die Gefahr eines vollständigen und systematischen Abbildens von Personenprofilen noch unvorstellbar, da entsprechende Daten nicht zur Verfügung standen oder nicht effizient verarbeitet werden konnten.[23]

Bestehende Massnahmen identifizieren
Des Weiteren sollten bereits umgesetzte Massnahmen bzw. geplante Massnahmen zum Management der identifizierten Bedrohungen und deren Status aufgelistet werden (Vgl. Klipper, 2011, S. 74). So kann später überprüft werden, ob bestehende Massnahmen funktionieren und ob durch neue Massnahmen neue Schwachstellen entstanden sein könnten.

Schwachstellen identifizieren
Im vierten Teil sollten Schwachstellen, mit jeweils ihrem Bezug zu den Assets, den Bedrohungen und den bereits umgesetzten Massnahmen zusammengetragen werden. Zusätzlich sollten auch mögliche Schwachstellen aufgelistet werden, für die derzeit keine Bedrohung gesehen wird (Vgl. Klipper, 2011, S. 74). Vor allem der letzte Punkt sollte bei Cyber Risk Gewicht haben. Mit fortschreitender Technologieentwicklung werden immer neue Schwachstellen möglich und immer innovativere Angriffsmethoden entwickelt. So können Schwach-

[22] Diese Auflistung verdeutlicht, dass Cyber Risk die ganze Bandbreite der möglichen Erscheinungsformen abdecken. Die grosse Bandbreite der versteckten, verdrängten und unbekannten / unerkannten Gefahren erschweren auch die Identifikation von Cyber Risk.

[23] Big Data (Analyse sehr grosser Datenmengen, unstrukturierte Daten, Data-Mining) bietet insofern viele Chancen. Zugleich kann es aber auch eine Gefahr darstellen, wenn dadurch eine totale Überwachung möglich wird (Beispiele: Totale Überwachung à la George Orwell 1984, Präkognition à la Minority Report).

stellen, die bisher keine Gefahr darstellten, schnell zu einer werden. Ging beispielsweise von Computern zu Zeiten ohne Internet keine erhöhte Gefahr von Systemzusammenbrüchen aus, hat sich dies mit der Einführung des Internets und somit der Möglichkeit für Denial-of-Service-Attacken stark verändert. Dieser Aspekt unterstreicht nochmals die Bedeutung des Begleitschrittes „Überwachung und Überprüfung".

Schadenauswirkungen identifizieren
Im letzten Schritt gilt es, mit den Informationen aus den ersten vier Punkten, Szenarien für mögliche Vorfälle zu entwickeln und speziell für diese Schadenauswirkungen zu bestimmen (Vgl. Klipper, 2011, S. 75). Diese Schadenauswirkungen können bei Cyber Risk sehr unterschiedlich ausfallen (z. B. dauerhaft – zeitlich begrenzt, direkt – indirekt etc.).

Methoden zur Risikoidentifizierung
Eine Reihe von Techniken, die im Schritt der Risikoidentifizierung behilflich sein können, stellt Klipper (2011) in seinem fünften Kapitel vor. Dazu zählen z. B. Brainstorming (S. 114), (un-)strukturierte Interviews (S. 116), Delphi-Methode (S. 118), Checklisten (S. 120), vorläufige Sicherheitsanalysen (S. 122) oder HAZOP-Studien (S. 124).

Cyber-Risk-Self-Assessment
Mögliche erste Anhaltspunkte zur Risikoidentifizierung können dabei auch Cyber-Risk-Self-Assessment-Tools liefern, die beispielsweise von Marsh (Marsh Cyber-Risikotest)[24] oder dem Office of the Superintendent of Financial Institutions Canada (Cyber Security Self-Assessment Guidance for Federally Regulated Financial Institutions)[25] zur Verfügung gestellt werden. Ziel dieser Tools ist es, die Risikoexponierung eines Unternehmens zu ermitteln, ein Risikobewusstsein zu schaffen und Anhaltspunkte zu liefern, welche Risiken noch nicht identifiziert / berücksichtigt wurden. Abbildung 10 zeigt die Startseite des Marsh Cyber-Risikotests.



Abbildung 10: Marsh Cyber-Risikotest

[24] http://www.marsh-stresstest.eu/groups/1/surveys/49; Letzter Zugriff: 16.12.2014.
[25] http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx; Letzter Zugriff: 16.12.2014.

Der Test kann anonym ausgefüllt werden und nimmt nur knapp 15 Minuten Zeit in Anspruch, sodass dieses Tool sehr einfach erste Erkenntnisse für das eigene RM liefert. Dabei soll der Test bei der Einschätzung der folgenden Punkte helfen: (a) Welche Folgen kann ein Cyber-Schaden für das Unternehmen haben? (b) Welche Schäden können durch eine Cyber-Versicherung abgedeckt werden? (c) Ist ein Bewusstsein und ein Bewertungssystem für die komplexen Cyber-Risk-Szenarien im Unternehmen vorhanden? Dazu kann das Unternehmen 31 Fragen beantworten und erhält anschliessend einen Cyberrisikobericht zugesandt. Hauptbestandteil des Berichts ist die Zuordnung eines Unternehmens zu einem von vier Risikoprofilen („A1 – stark gefährdet“, „A2 – gefährdet“, „A3 – weniger angreifbar“, „A4 – angreifbar“), für das jeweils bestimmte Handlungsalternativen diskutiert werden. Eine beispielhafte Zusammenfassung für das I·VW wird in Abbildung 11 gezeigt.

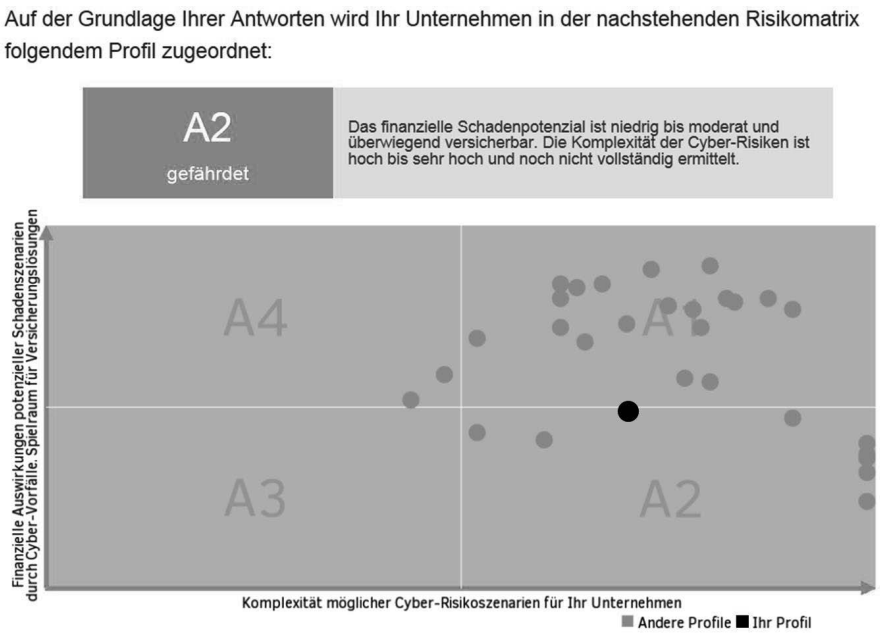


Abbildung 11: Zusammenfassung Marsh Cyber-Risikotest für das I·VW

Die beiden dargestellten Tools sollen nur beispielhaft zeigen, dass Cyber-Risk-Self-Assessment-Tools verfügbar sind und erheben keinen Anspruch auf Vollständigkeit. Es sollte hier deutlich geworden sein, dass ein solches Self-Assessment nicht sehr aufwendig sein muss, aber bereits wichtige Informationen zu Risikoidentifizierung liefern kann.

3.2.3 Cyber Risk analysieren

In diesem Schritt müssen die identifizierten Risiken analysiert werden. Analysieren bedeutet, dass Auswirkungen, Eintrittswahrscheinlichkeiten und Risikolevels für die Risiken geschätzt werden (Vgl. Klipper, 2011, S. 77).

Auswirkungen schätzen
Als Erstes sollten die Auswirkungen auf die Geschäftstätigkeit geschätzt werden (Vgl. Klipper, 2011, S. 77). Ein Tool für diese Aufgabe stellt die Business Impact Analyse (BIA) dar. Bei dieser Methode wird zuerst versucht, die direkten Kosten einzelner Szenarios zu ermitteln. Über die Abhängigkeiten verschiedener Szenarien soll dann der erwartete Gesamtschaden eines Vorfalls berechnet werden, also neben den direkten auch die indirekten Kosten (Vgl. dazu auch Klipper, 2011, S. 134). Letzterer Aspekt ist für Cyber Risk von besonderer Relevanz, da die Auswirkungen vielfältig sein können und sich nicht etwa auf reine Wiederherstellungskosten beschränken.

Wahrscheinlichkeiten schätzen
Die Schätzung der Eintrittswahrscheinlichkeiten stellt eines der grössten Probleme im Management von Cyber Risk dar. Da es sich bei Cyber Risk um eine relativ neue Risikoart handelt, könnten noch nicht genug (historische) Daten für eine adäquate Schätzung der Wahrscheinlichkeiten vorhanden sein (Vgl. Klipper, 2011, S. 77). Zudem ist Vorsicht geboten, wenn mittels (evtl. weniger) statistischer Erhebungen eine Aussage für die Zukunft getroffen werden soll. Das aber vor allem auch unter dem Aspekt, dass es sich bei Cyber Risk um ein sehr schnelllebiges Risiko handelt, dass gewissen Änderungsrisiken unterliegt (Vgl. etwa Haas und Hofmann, 2013). Historische Daten können folglich die Schnelllebigkeit von Cyber Risk gegebenenfalls nicht adäquat abbilden. Zudem kann es bei Cyber Risk vorkommen, dass ein identifiziertes Szenario von vielen verschiedenen Punkten abhängen kann, die alle Unsicherheiten mit in die Berechnung einbringen. Komplexität und Abhängigkeiten sind damit ein weiteres Spezifika, die die Einschätzung von Cyber Risk erheblich erschwert (Vgl. etwa Hofmann und Ramaj, 2011).

Risikolevels bestimmen
Risikolevels bestehen im Wesentlichen aus einer Kombination von Auswirkungen und Eintrittswahrscheinlichkeiten. Dieser Punkt entspricht für Cyber Risk weitgehend dem für andere Risiken. Dennoch werden einige Methoden für die Risikoanalyse in ISO/IEC 27005 Annex E bereitgestellt. Wurden die Risikolevels definiert, kann auf deren Basis im nächsten Schritt leicht eine Risikobewertung vorgenommen werden.

Methoden zur Risikoanalyse
Auch für die Risikoanalyse beschreibt Klipper (2011) Methoden, die allgemein in diesem Schritt Anwendung finden, z. B. Delphi-Methode (S. 118), SWIFT-Technik (S. 130) oder Szenario-Analysen (S. 132).

3.2.4 Cyber Risk bewerten

Die zuvor geschätzten Risiken (voriger Abschnitt) müssen nun mit den definierten Risikokriterien aus Abschnitt 3.2.1 in Verbindung gebracht werden. Dann muss entschieden werden, ob die Risiken „akzeptierbar“ oder „nicht tragbar“ sind. Die daraus abzuleitenden Ergebnisse bilden die Grundlage für den letzten Schritt der Risikobewältigung.

Die Risk Map stellt eine effiziente Methodik für diese Kategorisierung dar. Abbildung 12 zeigt ein Beispiel einer solchen Darstellung.

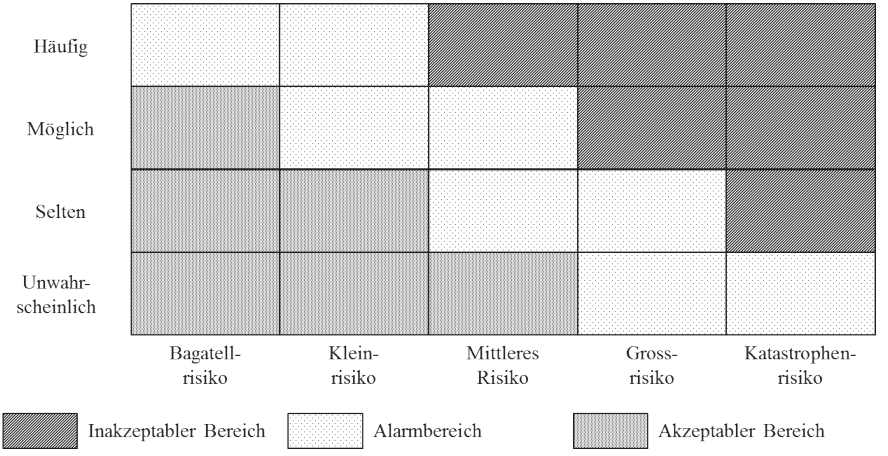


Abbildung 12: Risk Map (in Anlehnung an Seibold, 2006, S. 86)

Auf einer Risk Map wird üblicherweise auf der Abszisse das Gewinn- / Verlustpotenzial und auf der Ordinate die Eintrittswahrscheinlichkeit des Risikos abgetragen. Diese Parameter wurden im vorherigen Schritt mit Werten versehen und konnten so in die verschiedenen Level aufgeteilt werden. Durch die in Schritt 1 (Zusammenhang herstellen) definierten Risikokriterien kann die Risk Map dann entsprechend eingefärbt werden. Liegt ein Risiko aufgrund von geringer Eintrittswahrscheinlichkeit und / oder geringem Verlustpotenzial im akzeptablen Bereich (siehe Abbildung 12), wird es in den meisten Fällen als nicht so essenziell angesehen und im Normalfall nicht stärker problematisiert. Liegt es allerdings im inakzeptablen Bereich, weist es entweder ein hohes Verlustpotenzial (mit mittelhoher bis hoher Eintrittswahrscheinlichkeit) oder eine hohe Eintrittswahrscheinlichkeit (mit mittelhohem bis hohem Verlustpotenzial) auf. In diesem Fall wäre das Risiko „nicht (mehr) tragbar“ (inakzeptabel) und sollte zügig behoben werden. Der mittlere Bereich – der Alarmbereich wie in Abbildung 12 dargestellt – kann eine Zwischenstufe bilden, für den dann speziell zu definieren ist, was das Unternehmen unternimmt bzw. nicht unternimmt. Hier ist auch im Speziellen über das Kosten-Nutzen-Verhältnis von RM-Massnahmen zu diskutieren.

3.2.5 Cyber Risk bewältigen

Cyber Risk hat zahlreiche Ursachen und weist ein breites Spektrum an potenziellen Schäden auf. Dementsprechend ist die Liste der möglichen Instrumente, mittels derer sich ein Unternehmen vor Cyber Risk schützen kann, sehr vielseitig. Als RM-Instrumente kommen die Risikoverminderung, Risikovermeidung, Risikotransfer oder Selbsttragung in Betracht. Für die Auswahl des geeigneten Instruments sollte primär die Absicherung des bestimmenden Risikos im Vordergrund stehen. Dennoch sollte bei der Wahl auch immer eine Kosten-Nutzen-Überlegung mit einbezogen werden (Vgl. etwa Kapitel 7 in Klipper, 2011, zur Wirtschaftlichkeitsbetrachtung). Bei der Auswahl der entsprechenden Instrumente ist allerdings weiter zu beachten, dass sich die Nutzungen untereinander nicht ausschliessen. Die optimale Auswahl mag vielleicht in einer Kombination aus mehreren Massnahmen liegen. Zudem sollten Wech-

selwirkungen zwischen verschiedenen Risiken beachtet werden. Eine Massnahme kann beispielsweise dazu führen, dass mehrere Risiken gleichzeitig behandelt werden.

Vermeidung
Die erste Möglichkeit zum Schutz vor Cyber Risk ist, sich nicht dem Risiko auszusetzen. Ausgehend von unserer Definition von Cyber Risk könnte dies etwa bedeuten, dass das elektronische Speichern von Informationen und die Verwendung von Informationssystemen eingeschränkt werden. Dies dürfte in der heutigen Zeit, in der man auf effiziente Informationsverarbeitung angewiesen ist, kaum denkbar sein. Insofern sind die Möglichkeiten der Risikovermeidung eingeschränkt. So kann eine Vermeidung auch im Konflikt mit den Unternehmenszielen stehen. Wenn eine Bank beispielsweise ihren Kunden kein Onlinebanking mehr anbietet, bietet sie zweifelsohne keine Angriffsfläche für Cyber Risk, hat aber auch einen (essenziellen) Wettbewerbsnachteil. Allerdings ist zu überlegen, ob bestimmte Aktivitäten zu unterlassen sind, etwa die Einbindung externer Partner in der Informationsverarbeitung (Outsourcing), insbesondere bei Unternehmen mit sensiblen Daten.

Verminderung und Begrenzung
Es gibt eine Vielzahl an Möglichkeiten, um sich durch Risikoverminderung bzw. -begrenzung vor Cyber Risk zu schützen. Diese Art der Risikobewältigung erfordert gegebenenfalls hohen Implementierungsaufwand und hat grosse Auswirkungen auf die beteiligten Mitarbeiter (Vgl. auch Klipper, 2011, S. 83). Die Instrumente dieser Kategorie sind meist in zwei Bereiche eingeteilt: Instrumente, um Eintrittswahrscheinlichkeiten zu verringern (Schadenverhütung, z. B. etwa Anti-Viren-Software, Firewalls etc.) und um die Konsequenzen, die ein Risiko verursachen kann, abzumildern (Schadenbegrenzung).[26] Es gibt allerdings auch Instrumente, die beide Bereiche abdecken.[27] Es gibt viele IT-spezifische Tests, um allfällige Sicherheitslücken aufzudecken, so wie etwa Penetrationstests.[28]

Transfer
Ein Transfer von Risiken wird grundsätzlich durch den Abschluss einer Versicherung ermöglicht. Die Versicherbarkeit von Cyber Risk und die momentan verfügbaren Versicherungslösungen im Schweizer Markt diskutieren wir ausführlich in Kapitel 4. Hier zeigt sich eine breite Auswahl an vorhandenen Deckungen, es werden aber auch die Herausforderungen in der Bereitstellung von Versicherungsschutz aufgezeigt. Ein besonders wichtiger Punkt ist in diesem Zusammenhang auch im Zusammenspiel der RM-Massnahmen zu sehen. Ein Versicherer wird nur dann eine Police abschliessen, wenn er sich vorab über die Wirksamkeit der Schadenprävention vergewissert hat.

Selbstbehalt
Die Selbsttragung oder auch Risikoübernahme genannt, beschreibt den Fall, indem sich das Unternehmen dazu entschliesst, verbleibende Schäden selbst zu bezahlen. Für einen solchen

[26] So reduziert beispielsweise eine Löschanlage im Serverraum nicht die Gefahr eines Feuers; aber falls ein Feuer ausbricht, kann dieses schnell gelöscht und so die Auswirkungen des Feuers reduziert werden.
[27] So reduzieren Schulungen der Mitarbeiter die Eintrittswahrscheinlichkeit, allerdings können geschulte Mitarbeiter, die im Schadenfall mit Prozessen vertraut sind, auch helfen, den möglichen Schadenumfang zu reduzieren.
[28] Dies sind umfassende Sicherheitstests, um Fehlkonfigurationen oder Schwachstellen auf einzelnen Rechnern / Netzwerken aufzuspüren; Vgl. Klipper (2011, S. 163).

Fall steht üblicherweise das Eigenkapital des Unternehmens als Sicherheitspuffer zur Verfügung. Bei Cyber Risk können die anfallenden Kosten allerdings sehr hoch sein, sodass unter Umständen extrem viel Eigenkapital gebildet werden müsste. Ein weiteres Problem bei Cyber Risk könnte eine schlechte Datenlage darstellen, durch die die adäquate Berechnung des notwendigen Risikokapitals erschwert wird. Deshalb könnte das Kriterium Selbsttragung von Cyber Risk nicht praktikabel erscheinen. Neben der Eigenkapitalbildung sind auch Notfallplanungen bei Cyber Risk von grosser Bedeutung. Beispielsweise können Notfallpläne entwickelt werden für den Fall, dass ein Serverraum durch Naturkatastrophen unbrauchbar wird. So kann schneller und koordinierter im Ernstfall gehandelt werden. Ein effektives Krisenmanagement ist damit eine wichtige Voraussetzung für einen effizienten Umgang mit Cyber Risk.

3.2.6 Kommunikation und Informationsaustausch

Die Kommunikation und der Informationsaustausch haben bei Cyber Risk eine hohe Bedeutung. So dient eine ausgiebige Kommunikation der Reduzierung bzw. Verhinderung von Sicherheitsvorfällen. Zudem hilft es Security-Know-how aufzubauen und die Security-Awareness zu stärken (Vgl. Klipper, 2011, S. 92).

3.2.7 Überwachung und Überprüfung

Um als Unternehmen angemessen auf Entwicklungen reagieren zu können, muss es seinen RM-Prozess stets neu anpassen und neu starten. Nur so ist es angemessen vor Bedrohungen geschützt. Dies ist bei Cyber Risk aufgrund der hohen Veränderungsdynamik – die vor allem durch die technologische Entwicklung und den Fortschritt entsteht – sehr bedeutsam.

3.3 Zusammenfassung: Was ist für ein erfolgreiches Management von Cyber Risk wichtig?

Durch ein effizientes RM kann die Wahrscheinlichkeit und das Ausmass eines Cyber-Risk-Schadens signifikant gesenkt werden. Wir wollen einige wesentliche Resultate der Diskussion zum RM in übersichtlicher Form zusammenstellen und auf dieser Basis sieben Leitlinien für ein erfolgreiches Management von Cyber Risk definieren.

Sieben Leitlinien für ein erfolgreiches Cyber-Risk-Management

1. Die institutionelle Verankerung der Thematik ist zentral („Jemand muss verantwortlich sein"). Z. B. senkt die Implementierung eines Chief Information Security Officers die Durchschnittskosten bei Cybervorfällen um über 30 % (Shackelford, 2012).

2. Ein effektives Krisenmanagement ist eine zentrale Voraussetzung für einen effizienten Umgang mit Cyber Risk. Für bestimmte Szenarien sollten klar definierte Ablaufpläne und Zuständigkeiten vorhanden sein (z. B. wenn es zu einem Datenverlust kommt).

3. Cyber Risk ist nicht Aufgabe einer Fachabteilung, sondern erfordert einen unternehmensübergreifenden Risikodialog (Sensibilisierung, Schulung etc.).

4. Cyber Risk erfordert auch einen kontinuierlichen Dialog mit Kunden und Lieferanten (wie ist deren Sicherheitslevel?).

5. Durch die rasante technologische Entwicklung muss auch der RM-Prozess fortlaufend angepasst werden, da immer neue Gefahrenquellen entstehen. Ein wirksamer Überwachungs- und Überprüfungsprozess ist unerlässlich.

6. Gegebenenfalls ist eine Zertifizierung nach Informationssicherheitsmanagement-Standards ein wichtiges Signal gegenüber Kunden und Lieferanten.

7. Gegebenenfalls stellt auch Risikotransfer mittels Versicherung ein probates Mittel dar.

4 Cyber-Versicherung: Versicherbarkeit von Cyber Risk

Der Abschluss einer Cyber-Versicherung kann für die Versicherten einen grossen Nutzen darstellen (Betterley, 2013). So profitiert das versicherte Unternehmen neben dem Risikotransfer von weiteren Services, insbesondere im Bereich der Prävention. Beispielsweise werden vielfach Penetrationstests durchgeführt, um allfällige Sicherheitslücken aufzudecken. Die Behebung solcher Mängel wird sich dann sowohl auf die Prämienhöhe als auch auf die Wahrscheinlichkeit, Opfer von Cyber Risk zu werden, auswirken. Die extensiven Vorabuntersuchungen können aber auch eine Hemmschwelle für das Abschliessen einer Cyber-Versicherung sein.

4.1 Definition von Cyber-Versicherung

Definition
Farny (2006) definiert Versicherung als:

> *„Deckung eines im Einzelnen ungewissen, insgesamt geschätzten Mittelbedarfs auf der Grundlage des Risikoausgleichs im Kollektiv und in der Zeit."*

Eine Cyber-Versicherung hat also die Aufgabe, den Versicherungsnehmer durch die von Cyber Risk entstandenen Schäden finanziell zu schützen und dazu einen Ausgleich im Kollektiv und über die Zeit zu realisieren. Fraglich ist, inwieweit ein Ausgleich im Kollektiv und über die Zeit bei Cyber Risk hergestellt werden kann, etwa vor dem Hintergrund noch sehr kleiner Versichertenkollektive und eines sich stark wandelnden Risikoumfelds. Es gibt nur sehr wenige Publikationen, die eine explizite Definition der Cyber-Versicherung vornehmen.[29]

Literatur
Generell gibt es bislang sehr wenig wissenschaftliche Literatur zur Cyber-Versicherung. Tabelle 11 gibt einen Überblick über bislang publizierte Arbeiten, die einige Hinweise auf die nachfolgende Diskussion zur Versicherbarkeit von Cyber Risk vermitteln. So sind beispielsweise die Komplexität und die Abhängigkeiten der Cyber Risk ein Aspekt, der sowohl in ökonomischen als auch in stärker technisch orientierten Publikationen problematisiert wird (etwa Hofmann and Ramaj, 2011; Ögüt, Raghunathan und Menon, 2011). Auf dieser Grundlage wurden dann auch bereits Pricing-Ansätze entwickelt, die diese komplexen Abhängigkeiten mit Hilfe von Copulas abbilden (siehe Herath und Herath, 2011). Generell ist auch auffällig, dass die bisherige wissenschaftliche Diskussion zur Cyber-Versicherung weniger in ökonomischen als vielmehr in technisch orientierten Journalen stattfindet. Insofern lässt sich hier ein weitergehender Forschungsbedarf gerade aus ökonomischer Sicht identifizieren.

[29] Gordon et al. (2003) definieren die Cyber-Versicherung als "insurance policies that cover losses from cyber attacks and data breaches".

	Arbeit	Inhalt
1	Biener, Eling und Wirfs (2015)	Diskutieren die Eignung der Cyer-Versicherung für das Management von Cyber Risk. Sie verwenden einen Operational-Risk-Datensatz und identifizieren Cyber-Risk-Vorfälle, die dann zur Analyse der Versicherbarkeit herangezogen werden.
2	Haas und Hofmann (2013)	Risikomanagement und Versicherbarkeit von Cloud Computing aus der Sicht eines unternehmensinternen Risikomanagements.
3	Mukhopadhyay et al. (2013)	Verwenden Nutzenmodelle, um Unternehmen bei der Entscheidung zu unterstützen, ob und in welchem Mass eine Cyber-Versicherungspolice nützlich ist. Dies basiert auf einem Copula-unterstützten Bayesian Belief Network.
4	Shackelford (2012)	Untersucht den Einfluss von Cyberattacken auf Unternehmen, diskutiert einige U.S.-Gesetze zu diesem Thema und inwiefern Cyber-Versicherung Bedrohungen durch Cyber Risk mildern kann.
5	Herath und Herath (2011)	Entwickeln ein Modell mit Copulas, um Cyber-Versicherungspolicen zu pricen.
6	Hofmann und Ramaj (2011)	Aufstellung eines ökonomischen Modells, das die genauen Wechselbeziehungen in einem Cyber-Netzwerk widerspiegeln soll.
7	Ögüt, Raghunathan, und Menon (2011)	Behandeln den Nutzen von Versicherung und Selbstschutzmassnahmen im Zusammenhang mit korreliertem Cyber Risk und dem Problem, dass Verluste schwer verifizierbar sind.
8	Cebula und Young (2010)	Beschreiben eine Klassifizierung für operationelles Cyber Risk und identifizieren und organisieren Quellen dafür (Ergebnis: vier Klassen).
9	Shetty, Felegyhazi, und Walrand (2010)	Netzwerk-Security ist eventuell geringer mit Versicherung wegen Moral Hazard.
10	Bandyopadhyay, Vijay, und Rao (2009)	Zeigen, dass Versicherer auf die hohe Unsicherheit bezüglich Durchschnittsverlusten durch Cyber-Risk-Vorfälle, mit hohen Selbstbehalten und niedrigen Maximal-Deckungslimiten reagieren.
11	Bolot und Lelarge (2009)	Kombinieren Ansätze der Risikotheorie und der Netzwerkmodellierung, um den Einfluss von Cyber-Versicherungen auf die allgemeine Internetsicherheit zu analysieren.
12	Wang und Kim (2009a)	Untersuchen Wechselbeziehungen in Cyberattacken über nationale Grenzen hinweg durch die Auswertung von Spatial-Autocorrelations dieser Cyberattacken.
13	Wang und Kim (2009b)	Charakterisieren empirisch die Wechselbeziehungen in Cyberattacken und untersuchen den Einfluss eines internationalen Vertrags gegen Cyberkriminalität.
14	Baer und Parkinson (2007)	Untersuchen Grenzen für den Cyber-Versicherungsmarkt, wie Informationsasymmetrien und Korrelationen von Cyber Risk, vor allem aber auch im Zusammenhang mit dem Public-Good-Charakter von Selbstschutzmassnahmen.
15	Böhme und Kataria (2006)	Analysieren Korrelationseigenschaften verschiedener Cyber Risk und entwickeln eine neuartige Einteilung von Cyber Risk, basierend auf deren Korrelationseigenschaften; die Unterteilung unterscheidet zwischen „internal“ und „global“ Korrelationen und deren Wechselbeziehungen, ein Beispiel für ein Cyber Risk mit hoher internal und geringer global Korrelation ist eine interne Hackerattacke (oder auch physischer Datendiebstahl).
16	Majuca et al. (2006)	Untersuchen die Entwicklung des Cyber-Versicherungsmarktes und finden heraus, dass die Entwicklung von Internetsicherheitsrisiken und steigende Compliance-Anforderungen die Nachfrage signifikant fördern.
17	Mukhopadhyay et al. (2006)	Entwickeln einen Ansatz, um Wahrscheinlichkeiten für Cyber Risk (aufbauend auf einem Bayesian Belief Network) zu schätzen. Dies soll eine Grundlage für die Bestimmung von Cyber-Versicherungsprämien schaffen.
18	Böhme (2005)	Diskutiert die Entstehung eines richtigen Cyber-Versicherungsmarkts und Probleme durch korrelierte Verluste; zudem werden Bedingungen unter denen Deckung von Cyber Risk möglich ist untersucht.
19	Mukhopadhyay et al. (2005)	Entwickeln ein Nutzenmodell, um die Vorteile für das Cyber-Risk-Management durch eine Versicherung zu beurteilen.
20	Gordon, Loeb und Sohail (2003)	Bieten eine qualitative Diskussion über Versicherung als ein Mittel, um Cyber Risk zu managen, auch unter dem Aspekt von Informationsasymmetrien (Adverse Selektion, Moral Hazard) und einem Überblick der Cyber-Versicherungsprodukte in den USA.

Tabelle 11: Wissenschaftliche Arbeiten zu Cyber-Versicherung

Deckung

Um einen Überblick zu bekommen, welche Kosten durch ein Cyberprodukt abgedeckt werden können, haben wir in Tabelle 12 mögliche Deckungsbausteine einer Cyber-Versicherung aufgelistet. Die Auflistung erfolgt in Anlehnung an Peters (2012) und Marsh (2012).[30]

Deckungs-baustein	**Ursache**	**Versicherte Kosten**
Haftpflichtversicherung		
Privacy Liability	• Verlust von vertraulichen Informationen, die durch das Unternehmen gesammelt oder verwaltet werden oder unter dessen Obhut / Aufsicht stehen (z. B. durch Unterlassung, Verlust oder Diebstahl durch Mitarbeiter)	• Gesetzliche Haftung (auch Verteidigungs- und Schadenzahlungen, Strafen) • Vicarious Liability (falls Informationskontrolle outgesourct ist) • Crisis Control (z. B. Benachrichtigungskosten für Stakeholder, Untersuchungskosten, Ausgaben für PR)
Network Security Liability	• (Unbewusstes) Einschleusen eines Virus, der Daten eines Drittsystems beschädigt • Schädigung an Drittsystemen oder unberechtigter Zugang zu ihnen durch ein System des Versicherten • Beeinträchtigung oder Verwehrung des berechtigten Zugangs von Kunden • Verletzung oder widerrechtliche Verwendung von geistigem Eigentum	• Befriedigung von Berechtigten und Abwehr Unberechtigter • Kosten im Zusammenhang mit Verfahren (Straf-, Auslieferungs-, Verwaltungs- und Aufsichtsverfahren)
Intellectual Property and Media breaches	• Software-Lücken sowie PR-Schäden (z. B. Verleumdung etc.)	• Gesetzliche Haftung (auch Verteidigungs- und Schadenzahlungen, Strafen)
Eigenschadenversicherung		
Cyber Extortion	• Drohung, über die Systeme der versicherten Gesellschaft Vermögenswerte zu überweisen • Drohung auf Herausgabe oder Veröffentlichung personenbezogener Daten • Drohung, Daten der versicherten Gesellschaft durch eine Computerattacke zu verändern, zu beschädigen oder zu zerstören • Drohung, die Dienstleistungen der versicherten Gesellschaft zu beeinträchtigen / zu unterbrechen	• Erpressungszahlungen • Kosten in Zusammenhang mit der Vermeidung von Erpressung (Kosten für Untersuchung)
Business Interruption	• Denial-of-Service-Attacke • Hacking	• Alle daraus entstehenden Kosten, die zur Fortführung der Geschäftsaktivitäten angewendet werden • Entgangener Gewinn • Mehrkosten, Wiederherstellungskosten
Data Asset Protection	• Informationsassets werden durch eine Hackerattacke beschädigt, vernichtet oder gelöscht • Beschädigung oder Zerstörung anderer immaterieller Vermögensgegenstände (z. B. Software)	• Kosten für die Wiederherstellung und das Zurückholen von Daten • Ersatzbeschaffung gleichwertiger Daten • Kosten für Ersatz immaterieller Vermögenswerte (z. B. Software)
Crisis Management	• Alle vorgenannten Computerattacken auf Informationen und Informationssysteme	• Krisenmanagement durch eine spezialisierte Drittgesellschaft, die nach einem Cybervorfall entstehen, um die Reputation wiederherzustellen • Kosten für die Notifizierung von betroffenen Kunden (auch Behörden) • Kosten für Monitoring (z. B. Verwendung Kreditkartendaten, Ausweisdaten)

Tabelle 12: Deckungen für Cyber Risk (in Anlehnung an Peters, 2012 und Marsh, 2012)

[30] Eine alternative Auflistung der Deckung bietet ENISA (2012). Zufolge dieser Auflistung können Cyber-Versicherungsprodukte folgende Punkte abdecken: Haftungsfragen, Eigentumsverlust und Diebstahl, Datenbeschädigung sowie Einkommensausfälle durch Netzwerk- und Computerausfälle oder Website-Manipulationen.

Direkt zurechenbare Kosten
Ein schwieriger Aspekt in der Definition der Deckung ist die Abgrenzung der Kosten. Generell kann hier zwischen direkten und indirekten Kosten unterschieden werden. Mit direkt zurechenbaren Kosten sind diejenigen Kosten gemeint, die direkt dem eingetretenen Ereignis zugerechnet werden können. Beispiele dafür sind:

- Das Wiederherstellen der Website im Falle einer Denial-of-Service-Attacke
- Wiederherstellungskosten bei Datenverlust (beispielsweise durch einen Hackerangriff)
- Kosten der Geschäftsunterbrechung (wenn die Produktionsanlagen sabotiert wurden)
- Kosten für Rechtsstreitigkeiten, die Folgeschaden eines Cyber-Ereignisses sind

Diese Art von Kosten ist gut ermittelbar, messbar und lässt sich gut in einer Versicherung definieren.

Indirekt zurechenbare Kosten
Unter indirekt zurechenbaren Kosten sind jene Kosten zu verstehen, die nicht in direktem Zusammenhang mit dem jeweiligen Ereignis stehen, sondern eher als Folge auftreten. Beispiele hierfür sind (Vgl. Mukhopadhyay et al., 2005):

- Verluste, die durch Reputationsschäden entstehen
- Marktwertverlust nach einem Negativereignis
- Unbeabsichtigte Verletzung der Privatsphäre des Kunden durch Offenlegung von persönlichen Informationen
- Nichteinhaltung von gesetzlichen Vorschriften zum Datenschutz und damit einhergehende Klagen und Haftpflichtansprüche

Indirekte Kosten sind schwer messbar. Es lässt sich beispielsweise kaum sagen, ob ein bestimmter Kundenabgang durch ein spezielles Cyber-Risk-Ereignis hervorgerufen wurde. Eine entsprechende Kausalität kann daher oft nicht etabliert werden, wenngleich solche indirekten Kosten mitunter für das versicherte Unternehmen eine viel grössere Relevanz haben können als direkte Kosten (z. B. Kosten für Datenwiederherstellung). Diese Problematik kann ein weiterer Hinweis auf die Grenzen der Versicherbarkeit sein.

4.2 Marktübersicht Versicherungslösungen

4.2.1 Globaler Markt für Cyber-Versicherung

In den USA ist der Markt für Cyber-Versicherungen wesentlich etablierter als in Europa (Allianz, 2013). Laut dem Betterley Report (2013) beträgt das Prämienvolumen in den USA derzeit 1,3 Milliarden US-Dollar (ca. 990 Mio. Euro).[31] Für den europäischen Markt liegen derzeit noch keine detaillierten Schätzungen vor (Böhme und Schwartz, 2010); es wird vermutet, dass das Marktvolumen in Kontinentaleuropa aber bei etwa 150 Millionen Euro liegt (Vgl. Gould, 2013). Nach Berechnungen der Allianz (Allianz, 2013) könnte der Markt für Cyber-Versicherungen bis zum Jahr 2018 ein Marktvolumen von 700–900 Millionen Euro erreichen. In Tabelle 13 haben wir weitere Datenquellen zur Cyber-Versicherung zusammengetragen.

Betterley (2013)	Global: Jährlich gebuchte Bruttoprämien für Cyber-Versicherungen in den USA betragen 1,3 Milliarden US-Dollar, weitere Zunahme mit 10 bis 25 % im Durchschnitt erwartet.
Harvard Business Review (2013)	Umfrage unter 152 US-amerikanischen Unternehmen des privaten und öffentlichen Sektors: Viele Unternehmen sind um ihre IT-Sicherheit besorgt, die Mehrheit (60 %) hat aber in näherer Zukunft keine Pläne, eine Cyber-Versicherung abzuschliessen. 19 % der befragten Unternehmen verfügen derzeit über eine Form der Cyber-Versicherung.
Marsh (2013)	Europa: 25 % der Unternehmen wissen nichts von Versicherungslösungen gegen Cyber Risk und nur 10 % haben bereits Versicherungsschutz gekauft.
Willis (2013a, b)	USA: Deckung bei etwa 6 % der Fortune 1‘000 Unternehmen, aber grosse Unterschiede zwischen den Industrien.
Betterley (2010)	Global: Der Cyber-Versicherungsmarkt wuchs von 100 Millionen US-Dollar im Jahr 2003 auf mindestens 600 Millionen US-Dollar in 2009.

Tabelle 13: Datenquellen zur Cyber-Versicherung

Sowohl in der Schweiz als auch in anderen europäischen Ländern ist der Cyber-Versicherungsmarkt heute noch relativ klein, entwickelt sich aber dynamisch. Wir stellen im nachfolgenden Teilkapitel die Situation in der Schweiz ausführlich dar. Für eine detaillierte Analyse des deutschen Markts verweisen wir auf Choudhry (2014).[32]

4.2.2 Schweizer Markt für Cyber-Versicherung

Viele Versicherer in der Schweiz bieten in ihren Produkten Deckungen für Betriebsunterbrechung, menschliches Versagen oder auch die Wiederherstellung von Daten bei Datenverlusten an. Auf den Websites werden allerdings aktuell keine spezifischen Cyber-Versicherungen

[31] In Relation zum Volumen des US-amerikanischen Non-Life-Markts (703,1 Milliarden US-Dollar in 2012; siehe Swiss Re, 2013) beträgt dies nur 0,18 %.

[32] Gemäss Choudhry (2014), S. 33, gibt es im deutschen Markt per Mitte 2014 zwölf Produkte von zwölf Gesellschaften. Der Markt wird dabei von grossen angloamerikanischen Industrieversicherern dominiert (Choudhry, 2014, S. 1).

angeboten. Jedoch wird vermerkt, dass die Möglichkeit besteht, sich auch in Rücksprache mit der Versicherung individuell versichern zu lassen.[33]

Die wesentlichen Versicherer in der Schweiz, die explizit Produkte anbieten, die Cyber Risk abdecken, sind die AIG Europe Limited, die Allianz Global Corporate & Specialty AG (AGCS), die Chubb Insurance Company of Europe SE und die Zürich Versicherungs-Gesellschaft AG. Die Produkte werden wir im weiteren Verlauf dieses Abschnitts mit ihren wichtigsten Eigenschaften vorstellen (siehe Tabelle 14). Eine Einteilung wurde dabei vorgenommen nach versichertem Risiko, Deckung, Deckungsgrenzen, nicht versicherten Objekten, Produkttyp, Selbstbehalt und etwaigen Zusatzleistungen.[34]

AIG Europe Limited

Der Versicherer AIG Europe Limited bietet in der Schweiz in seinem Produkt *CyberEdge* ein reines Cyber-Versicherungsprodukt an (AIG, 2014).[35] Darin enthalten ist eine Daten-Haftpflicht-Komponente (Schutz gegen finanzielle Folgen bei Verlust von Daten), die Deckung von Krisenmanagementmassnahmen nach einer Datensicherheitsverletzung, die Deckung von Kosten im Zusammenhang mit behördlichen Ermittlungen und Datenwiederherstellungskosten. Zusätzlich können optional Zusatzbausteine hinzugebucht werden, die die Kosten aus Netzwerkunterbrechungen, Kosten im Zusammenhang mit Verletzungen geistigen Eigentums Dritter oder elektronischen Inhalten, Kosten, entstanden aus Cyber-Erpressung (forensische Untersuchungen, Erpressungsgelder etc.), für notwendige Goodwill-Aktionen oder für Cloud-Ausfälle abdecken (Vgl. AIG, 2014).

Allianz Global Corporate & Specialty (AGCS)

Der Industrie- und Spezialversicherer AGCS der Allianz Gruppe bietet ebenfalls Versicherungslösungen zum Schutz vor Cyber Risk an (AGCS, 2013). So wurden bereits seit knapp zehn Jahren im deutschsprachigen Raum Cyber-Versicherungsprodukte unter dem Namen Global Net bzw. ESI Net vertrieben. Im Sommer 2013 wurde das Versicherungsprodukt *Allianz Cyber Protect* lanciert, das in drei verschiedenen Deckungsvarianten (Basis, Premium und Premium plus) erhältlich ist und unter anderem die Kosten für Wiederherstellung von beschädigten oder zerstörten Daten, Kosten für Ertragsausfälle durch Betriebsstörungen, Krisenkommunikationskosten zum Reputationsschutz, Kosten für Datenschutzverletzungen, fehlerhafte digitale Kommunikation sowie dem entstandenen Schaden eines Hackerangriffs abdeckt (Vgl. Allianz, 2013). Bei den Premium-Varianten handelt es sich um individuell angepasste Versicherungslösungen, die über einen erweiterten Deckungsumfang (wie z. B. selbst verschuldete Prozessschwächen oder Mitarbeiterfehler) verfügen, die aber zudem eine ausführli-

[33] Der nachfolgende Marktüberblick stellt die Situation im Mai 2014 dar. Wie oben beschrieben, entwickelt sich der Markt dynamisch, sodass die dargestellten Aussagen nicht zwingend aktuell und vollständig sein müssen.

[34] Anzumerken ist, dass wir uns hier auf Geschäft mit Unternehmen, nicht dagegen auf Privatkunden fokussieren. So hat beispielsweise jüngst die Groupe Mutuel eine neue Rechtsschutzversicherung unter dem Titel „legis digital“ lanciert, die auch Risiken im Internet und von elektronischen Transaktionen bei Privatpersonen abdeckt. Dieses Produkt wurde mit dem Innovationspreis der Assekuranz im Jahr 2013 ausgezeichnet, was die Neuartigkeit und Relevanz derartiger Produktentwicklungen auch im Privatkundengeschäft unterstreicht.

[35] Zusätzlich bietet AIG in der Schweiz ein Produkt namens Vertrauensschaden-Versicherung E-Crime für KMU (bzw. Fidelity Insurance E-Crime) an, das den Schutz von diversen Cyber-Risk-Risiken abdeckt (AIG, 2013). Dabei handelt es sich aber um kein reines Cyberprodukt. Das Produkt besteht aus einer Grunddeckung und einer Deckungserweiterung, die der Kunde frei wählen kann. Die Grunddeckung (Option A) schützt das Unternehmen vor externen Bedrohungen (Computerkriminalität, Schutz vor Schäden durch Dritte).

che Vorabprüfung der IT-Prozesse des Unternehmens durch spezialisierte Risikoingenieure von AGCS voraussetzen. Letztere Risikoprüfung wird in der Standard-Variante nur sehr schlank durchgeführt (AGCS, 2013). Die Cyber-Versicherungsprodukte wurden vorerst nur in Deutschland, aber seit Kurzem auch in Österreich, der Schweiz, Grossbritannien, Frankreich, Spanien, Australien und Neuseeland angeboten. Zudem soll dieses Produkt auch in asiatischen Märkten eingeführt werden (Vgl. AGCS, 2013).

Chubb Insurance Company of Europe SE

Die Chubb Insurance Company of Europe SE, Direktion für die Schweiz, bietet ihren Kunden ebenfalls Versicherungslösungen zum Schutz vor Cyber Risk an (Chubb, 2014). Das Versicherungsprodukt *CyberSecurity by CHUBB* kann individuell auf die Bedürfnisse der Versicherungsnehmer zugeschnitten werden, indem verschiedene Deckungsbausteine zur Verfügung stehen, die gewählt werden können. Diese beinhalten neben einem Cyber-Haftpflichtschutz auch einen Schutz bei Beeinträchtigung oder Unterbrechung des Geschäftsbetriebs, Cyber-Erpressung, Cyber-Vandalismus, Cyber-Diebstahl,[36] Zahlung von Benachrichtigungskosten sowie Kosten für Krisenmanagementaktivitäten wie z. B. die Einbeziehung externen Rechtsanwälte, forensischer Sicherheitsberater, PR-Berater oder für PR-Aktionen. CyberSecurity-Kunden der Chubb erhalten ausserdem exklusiven Zugriff auf das Chubb *eRisk HUB Portal*, das wertvolle Informationen rund um das Thema IT-Sicherheit und Risikoprävention bietet. Diese Informationen beinhalten unter anderem Coaching-Services für den Fall eines Datenverlusts, Incident Road Maps, Incident Response Planning Templates und Best-Practice-Guides, Risk-Manager-Tools sowie ein weltweites Verzeichnis von Kooperationspartnern im Bereich IT-Sicherheit.

Zürich Versicherungs-Gesellschaft AG

Die Zürich Versicherungs-Gesellschaft AG bietet das Produkt *Cyber Security and Privacy* als eigenständige Cyber-Versicherungslösung an.[37] Dieses Produkt besitzt eine modulare Versicherungsstruktur, bei der, je nach Bedarf des Kunden, diverse Versicherungsbausteine gewählt werden können. Die folgenden fünf Deckungsbausteine sind verfügbar: (1) Cyber-Haftpflichtversicherung, um Ansprüche Dritter sowie Verfahrenskosten zu decken, (2) die „Privacy Breach Cost"-Deckung, bei der Kosten gedeckt werden, die durch einen Verstoss gegen eine Datenschutzregelung entstehen, (3) eine Datenrekonstruktionsversicherung, die Kosten für Datenwiederherstellung übernimmt, (4) die Komponente „Business income loss" entschädigt für Verluste aus Betriebsunterbruch, die durch Hackerangriffe verursacht worden sind, und (5) eine Versicherung gegen die finanziellen Folgen einer Cyber-Erpressung (Vgl. Zurich, 2014).

[36] Nur für Finanzdienstleister, da dieser Baustein bereits in marktüblichen Vertrauensschadenversicherungen für Industrierisiken enthalten ist.

[37] Zusätzlich wird ein Produkt namens *Vertrauensschaden und Cyber-Crime* angeboten, das Teile einer üblichen Cyber-Versicherung enthält, aber kein Stand-alone-Cyberprodukt darstellt (Zurich, 2013).

	Produkt 1	**Produkt 2**
Versicherer	**AIG Europe Limited**	**Allianz Global Corporate & Specialty AG**
Versicherungsprodukt	**CyberEdge**	**Allianz Cyber Protect (Basis, Premium, Premium plus)**
Versicherte Risiken (siehe auch Ursachen Tabelle 4)	• Menschliche Fehler • Hackerangriff • Erpressung	• Menschliche Fehler (Premium-Produkt) • Technische Fehler (Premium-Produkt) • Hackerangriff • Erpressung
Deckung (kleingedruckt sind detaillierte Angaben)	• Kosten bzgl. Datendiebstahl und Datenverlust • Zahlungen für Betriebsunterbrechungen • Wiederherstellungskosten • Übernahme von Strafzahlungen • Ermittlungskosten • Verfahrenskosten • Kosten im Zusammenhang mit dem Krisenmanagement • Lösegeldzahlungen bei Cyber-Erpressung • Abwehrkosten und Haftung bei Verstössen gegen Schutz von Personen- und Unternehmensdaten (unabhängig von wem sie verursacht werden) • Infizierung Daten Dritter durch Virus, physischer Diebstahl von Zugangscodes, Diebstahl von Hardware mit persönlichen Daten, Offenlegung von Daten • Lösegeldzahlungen • Kosten im Zusammenhang mit der Verletzung von geschützten Inhalten • Deckt Nettogewinneinbussen, die als Folge von Störungen des Netzwerks eines Versicherten entstehen • Honorare und Aufwendungen für unabhängige Berater und Dienste, um Image (Unternehmen und Einzelpersonen) wiederherzustellen oder im Voraus zu schützen • Benachrichtigungskosten bei Datenschutzverstössen • Deckt Kosten von Cyber-Krisenreaktionsspezialisten • Deckt Kosten für Gebühren und Honorare ab, die bei der Feststellung anfallen, ob Daten wiederhergestellt, gesammelt oder neu angelegt werden müssen	• Zahlungen für Datenschutz- und Datenvertraulichkeitsverletzungen • Zahlungen für Netzwerksicherheitsverletzungen • Wiederherstellungskosten • Übernahme von Strafzahlungen • Schadenzahlung für Betriebsunterbrechung • Kosten für Computerbetrug • Kosten im Zusammenhang mit Cyber-Erpressung (optional) • Verfahrenskosten • Kosten für forensische Dienstleistungen • Krisenkommunikationskosten und Informationskosten („Notification costs“) • In den Premium-Produkten erweiterter Deckungsumfang für Eigen- und Drittschäden, der auch durch technische Störungen oder Bedienungsfehler von Mitarbeitern verursachte Betriebsunterbrechungsschäden einschliesst
Deckungsgrenze	Keine Angabe	Bis zu CHF 50 Mio. (Premium-Variante); bis CHF 10 Mio. im Basismodell
Nicht versicherbare Objekte / Ausschlüsse	Keine Angabe	Keine Angabe
Produkttyp (und deren Deckungssumme)	Keine Angabe	Standardisiert: bis CHF 10 Mio. Individuell: bis CHF 50 Mio.
Selbstbehalt	Keine Angabe	Keine Angabe
Zusatzleistungen		Risikomanagement-Services

	Produkt 3	**Produkt 4**
Versicherer	**Chubb Insurance of Europe SE**	**Zürich Versicherungs-Gesellschaft AG**
Versicherungsprodukt	**CyberSecurity by CHUBB**	**Cyber Security and Privacy**
Versicherte Risiken (siehe auch Ursachen Tabelle 4)	• Menschliche Fehler • Technische Fehler • Hackerangriff • Erpressung	• Menschliche Fehler • Hackerangriff • Erpressung
Deckung (kleingedruckt sind detaillierte Angaben)	• Cyber-Haftpflichtschäden aufgrund von Pflichtverletzungen seitens der Versicherten • Benachrichtigungskosten beim Verlust sensibler, personenbezogener Daten • Krisenmanagementkosten • Entgangener Gewinn und Wiederherstellungskosten bei Unterbrechung des elektronischen Geschäftsbetriebs • Bedrohungsabwehrkosten bei Cyber-Erpressung (z. B. Drohungen, sensible, personenbezogene Daten öffentlich zu stellen oder herauszugeben oder auch bei der Androhung sog. Denial-of-Service-Attacken) Cyber-Haftpflichtschäden: • Pflichtverletzungen können beispielsweise bei der Schädigung von Drittsystemen, der Verletzung fremder Rechte, dem Verlust sensibler, personenbezogener Daten, einer Zugangsbeschränkung oder einer Rufschädigung von Personen, Produkten oder Dienstleitungen als Folge von Cyberaktivitäten seitens des Versicherungsnehmers vorliegen • Versicherungsschutz besteht in der Abwehr unberechtigter sowie der Befriedigung berechtigter Schadenersatzansprüche Benachrichtigungskosten: • Versichert sind u. a. Kosten, um betroffene Personen zu benachrichtigen und zu informieren, Kontodaten oder Sicherheitscodes zu ändern oder Überwachungsdienstleistungen zu gewähren (sog. „credit monitoring expenses“) Krisenmanagementkosten: • Versichert sind u. a. die Kosten für die Einbeziehung externer Rechtsanwälte, forensischer IT-Sicherheitsberater, PR-Berater oder PR-Aktivitäten Bedrohungsabwehrkosten: • Versichert sind u. a. Geld- oder Vermögenswerte, die aufgrund einer Cyber-Erpressung gezahlt werden oder auch Kosten für externe Verhandlungsführer	• Kosten bzgl. Datendiebstahl und Datenverlust • Datenwiederherstellungskosten • Schadenzahlungen für Betriebsunterbrechungskosten inkl. Gewinnausfall • Kosten im Zusammenhang mit Cyber-Erpressung • Verfahrens- und Verteidigungskosten • Übernahme von Bussen und Geldstrafen, sofern versicherbar unter anwendbarem Recht • Schutz bei Schadenersatzansprüchen Dritter, wenn persönliche Daten oder Unternehmensdaten verloren gehen oder veröffentlicht werden • Absicherung gegen unfreiwillige Verletzung von Datenschutzbestimmungen • Übernahme von Verfahrens- und Verteidigungskosten • Die Haftpflichtdeckung schliesst externe Dienstleister und Lieferanten ein, für die das Unternehmen verantwortlich ist • Optional versicherbar ist die Haftpflicht von Fällen mit Bezug zu Internetmedien • Mehrkosten nach Datendiebstahl oder Datenverlust für juristische Analysen, Rechtsanwälte und PR-Beratung zwecks Wiederherstellung des Vertrauens • Kosten für vorgeschriebene Benachrichtigung von Kunden • Aufwand für die Rekonstruktion von abhanden gekommenen oder beschädigten Daten sowie Wiederherstellung und Reparatur von beschädigter Software • Umsatzverluste, die sich aus Cyberangriffen oder Datenverlusten ergeben • Cyber-Erpressungskosten
Deckungsgrenze	Keine Angabe	Bis zu CHF 25 Mio. In Einzelfällen kann eine Deckung bis zu CHF 50 Mio. gewährt werden
Nicht versicherbare Objekte / Ausschlüsse	Keine Angabe	Online-Trading, Online-Gambling, Adult Content und reine Kreditkarten-Herausgeber-Firmen
Produkttyp (und deren Deckungssumme)	Keine Angabe	Keine Angabe
Selbstbehalt	Keine Angabe	Keine Angabe
Zusatzleistungen	Chubb eRisk HUB sowie Kooperation mit IT-Sicherheitsberatern sowohl lokal als auch international	Risikomanagement-Services durch spezialisiertes Partnerunternehmen, Unterstützung durch Juristen und IT-Fachleute vor, während und nach Schadenereignissen

Tabelle 14: Überblick Cyber-Versicherung in der Schweiz

4.3 Kriterien der Versicherbarkeit

Welche Risiken können versichert werden? Die Antwort darauf ist häufig sehr subjektiv (Vgl. Berliner, 1982). So kann es sein, dass ein Versicherer A ein gegebenes Risiko absichert, Versicherer B dies aber ablehnt. Die Versicherbarkeit eines Risikos hängt also immer sehr stark von den individuellen Entscheidungen und Kapazitäten des Versicherers bzw. des Versicherungsnehmers ab.[38] Folglich existieren keine allgemeinen Grenzen und Definitionen für Versicherbarkeit. Um die Versicherbarkeit von Risiken systematisch zu analysieren, hat Berliner (1982) neun Kriterien definiert, die eine Einteilung in versicherbare und nichtversicherbare Risiken ermöglicht. Tabelle 15 zeigt die neun Kriterien mit den Anforderungen, die erfüllt sein sollten. Wir führen die neun Kriterien kurz ein und wenden diese dann auf Cyber Risk an.

Versicherbarkeitskriterien	**Anforderungen**
Versicherungsmathematisch:	
Zufälligkeit des Schadenereignisses	Unabhängigkeit und Schätzbarkeit des Verlustrisikos
Maximal möglicher Schaden	Muss für Versicherungsunternehmen handhabbar sein
Mittlere Schadenhöhe (severity)	Moderat (relativ geringes Schadenausmass)
Mittlere Schadenhäufigkeit (frequency)	Relativ gross
Informationsasymmetrien	Adverse Selektion und Moral Hazard dürfen nicht zu grossen Einfluss haben
Marktbezogen:	
Versicherungsprämie	Kostendeckend und bezahlbar
Deckungsabgrenzung	Akzeptierbar
Gesellschaftsbezogen:	
Gesellschaftliche Werte	Im Einklang mit gesellschaftlichen Werten
Gesetzliche Schranken	Erlauben die Deckung

Tabelle 15: Kriterien der Versicherbarkeit (Berliner, 1982)

Zufälligkeit des Schadenereignisses

Das Kriterium der Zufälligkeit des Schadenereignisses wird von Berliner (1982) in zwei Teile unterteilt. Zur Erfüllung des Kriteriums muss zum einen die Unabhängigkeit der Verlustrisiken gewährleistet sein (Vgl. Berliner, 1982, S. 32). Unabhängigkeit bedeutet, dass ein Schadenereignis nicht Folge eines anderen Schadenereignisses ist (Vgl. Berliner, 1982, S. 30). Etwas ausführlicher beschreibt dies Farny (2006, S. 39): „Es soll möglichst keinen systematischen Zusammenhang derart geben, dass durch ein Ereignis zufällig die Schadenrealisation bei mehreren, vielen oder allen versicherungstechnischen Einheiten ausgelöst wird, sei es gleichzeitig (Kumulrisiko, z. B. Hagelschaden) oder nacheinander (Ansteckungsrisiko, z. B. ansteckende Krankheiten)“. Zur Messung der Unabhängigkeit bietet sich der Korrelationskoeffizient an, der auf Basis historischer Daten bestimmt werden kann (Vgl. Berliner, 1982,

[38] Zu nennen sind etwa die Risikofreudigkeit des Versicherers oder die Zahlungsbereitschaft des Versicherungsnehmers; Vgl. dazu auch Farny (2006).

S. 30). Der zweite Teil, der für die Erfüllung des Kriteriums gegeben sein sollte, ist die Schätzbarkeit des Verlustrisikos. Damit ist gemeint, dass Einflussfaktoren, die die Schadenhöhe bzw. den Eintrittszeitpunkt eines Risikos bestimmen, bekannt oder bestimmt werden können.

Maximal möglicher Schaden
Für dieses Versicherbarkeitskriterium muss gelten, dass der grösstmögliche Schaden (Maximum Possible Loss) bestimmbar ist. So kann ermittelt werden, welchen Betrag ein Risikoträger zur gesamten bzw. teilweisen Abdeckung eines bestimmten Risikos zur Entschädigung im Maximum bereitstellen muss (Vgl. Berliner, 1982, S. 37). In diesem Zusammenhang ist nicht nur wichtig, dass dieser Schaden identifizierbar ist, sondern auch handhabbar bleibt (Vgl. Biener und Eling, 2012). Ein Versicherer muss also auch die Möglichkeit haben, einen solchen Schaden zu bewältigen. Ist dies nicht alleine möglich, kann das Risiko immer noch auf mehrere Träger verteilt werden.

Mittlere Schadenhöhe
Während das Kriterium des grösstmöglichen Schadens problematische Einzelschäden identifiziert, setzt sich das Kriterium der mittleren Schadenhöhe bei Schadeneintritt mit der Durchschnittshöhe von Schäden auseinander (Farny, 2006, S. 38). Damit dieses Versicherbarkeitskriterium erfüllt ist, muss dieses moderat ausfallen, damit eine Versicherung möglich wird. Die Schätzung stellt eine Voraussetzung für die Versicherbarkeit dar: Geschätzt wird hierbei die Schadenverteilung. Allerdings kann die Qualität der Schätzung stark variieren, da sie auf Grundlage der verfügbaren Daten gemacht wird. Im Falle neuer Risiken, über die man noch keine statistischen Daten hat, sind mitunter nur subjektive Schätzungen möglich.

Mittlere Schadenhäufigkeit
Das Verlustrisiko muss entsprechend hoch sein, damit der Versicherer einen Ausgleich im Kollektiv herstellen kann.

Informationsasymmetrien
Das Risiko von Adverser Selektion und Moral Hazard darf nicht zu gross sein (Berliner, 1982). Adverse Selektion bezeichnet die Gefahr, dass nur relativ schlechte Risiken sich versichern wollen, während für gute Risiken der Abschluss einer Versicherung teuer und unattraktiv ist. Moral Hazard bezeichnet dagegen eine Verhaltensänderung nach Vertragsabschluss, beispielsweise den Anreiz zur Reduktion von Präventionsmassnahmen bei einer Vollversicherung.

Versicherungsprämie
Die Versicherungsprämie muss für das Unternehmen kostendeckend und für die Versicherungsnehmer bezahlbar sein (Berliner, 1982). Aus Sicht des Versicherers geht es hier darum, für das eingesetzte Eigenkapital eine risikoadäquate Verzinsung zu erzielen, das bedeutet, neben den erwarteten Kosten muss die Prämie auch ein Loading für das bereitgestellte Risikokapital enthalten.

Deckungsabgrenzung
Hierbei geht es darum, die Schäden, die versichert werden sollen, zu definieren und so auch die Grenzen der Deckung zu bestimmen (Farny, 2006, S. 39). Die Definition der Schäden wird im Versicherungsvertrag materiell und formalrechtlich festgehalten. Je genauer die Definition ist, desto besser kann die Versicherung die Schadenverteilungen bestimmen. Pauschale Versicherungen sind theoretisch auch möglich, jedoch scheitern diese Versicherungslösungen meist an ihrer Eindeutigkeit, da es in solch einem Fall sehr schwierig ist, den erwarteten Schaden genau zu schätzen. Ein Beispiel für eine pauschale Versicherungslösung stellt das unternehmerische Risiko dar. Ein derartiges Risiko wird kaum pauschal versichert, jedoch lassen sich gewisse Teile dieses Risikos absichern.

Gesellschaftliche Werte
Bei diesem Kriterium wird untersucht, ob das Versicherungsprodukt im Einklang mit gesellschaftlichen Werten steht (Biener und Eling, 2012, S. 81). Biener und Eling (2012) gehen bei diesem Kriterium ausserdem auf die Verfügbarkeit von Diensten ein (etwa Verfügbarkeit von Dienstleistungen im Gesundheitswesen).

Gesetzliche Schranken
Hier geht es darum, zu prüfen, ob das Versicherungsprodukt aus rechtlicher Perspektive überhaupt angeboten werden darf (Biener und Eling, 2012, S. 81). Dieses Kriterium ist relativ einfach zu bestimmen, da nur zwei Ausprägungen möglich sind (entspricht gesetzlichen Auflagen oder nicht). Anzumerken ist aber, dass dieses Kriterium essenziell von der Stabilität der rechtlichen Rahmenbedingungen abhängt. Diese können sich ändern und so unter Umständen ein noch versicherbares Risiko unversicherbar machen.

4.3.1 Zufälligkeit des Schadenereignisses

Eine zentrale Anforderung für die Bereitstellung von Versicherung für ein spezielles Risiko ist Unabhängigkeit der Risiken. Das Gesetz der grossen Zahlen besagt, dass, je mehr unabhängige Risiken sich in einem Versicherungsportfolio befinden, desto wahrscheinlicher ist es, dass die durchschnittlichen Gesamtschäden gegen den erwarteten Schaden tendieren und so Sicherheitszuschläge verringert werden können (siehe z. B. Böhme, 2005; Biener, 2013). Die Unabhängigkeitsbedingung stellt also eine wichtige Vorbedingung für einen Versicherer dar, um Prämienschätzungen für bestimmte Risiken zu erstellen, die das Insolvenzrisiko des Versicherers beschränken.

Für Cyber Risk stellen einige Autoren fest, dass diese grundsätzliche Voraussetzung verletzt wird. Baer und Parkinson (2007) führen an, dass die existierenden IT-Systeme in einer ähnlichen Weise aufgebaut und so gegen die gleichen Vorfälle anfällig sind. Dies rechtfertigt die Hypothese, dass Vorfälle zwischen Firmen sehr stark korreliert sind (z. B. DDoS). Einige weitere Arbeiten bestätigen die Korrelationen bei Cyber Risk (siehe z. B. Hofmann und Ramaj, 2011; Ögüt, Raghunathan und Menon, 2011; Bolot and Lelarge, 2009). Wichtig ist allerdings anzumerken, dass die Korrelation nicht unbedingt bei allen Kategorien von Cyber Risk auftreten und somit Zufälligkeit auch immer in Bezug zum aktuellen Vorfall gesehen werden muss (z. B. physische Datendiebstähle). Neben den Problemen durch Korrelation sollte zu-

dem die Frage gestellt werden, ob Cyber-Risk-Portfolios zum heutigen Stand gross genug sind, um eine effektive Bündelung der Risiken vornehmen zu können.

Nur wenig Literatur setzt den Fokus auf die Modellierung von Korrelationscharakteristiken bei Cyber Risk. Unter den wenigen Studien befinden sich Böhme (2005) und Böhme und Kataria (2006). Die erste Arbeit befasst sich mit der Modellierung globaler Korrelationen, während sich die zweite Arbeit auf Korrelationen innerhalb einer Firma als auch den Korrelationen zwischen Firmen fokussiert. Dies ist wichtig, da es eine Verknüpfung zwischen internen und externen Korrelationen geben kann. Während die globale Korrelation zwischen Firmen das Pricing von Cyber-Versicherungen beeinflusst (z. B. Pricing-Perspektive des Versicherers), ist die interne Korrelation das, was Unternehmen betrifft, wenn sie über das Versichern von Cyber Risk entscheiden (z. B. Unternehmensperspektive zum Risikomanagement). Böhme und Kataria (2006) stellen einen empirischen Ansatz für die Modellierung beider Korrelationen bereit und analysieren mögliche Einflüsse auf den Cyber-Versicherungsmarkt. Sie finden heraus, dass Cyber-Versicherungen optimal für Cyber Risk mit hoher interner und geringer globaler Korrelation sind. Wang und Kim (2009a, b) ferner beziehen sich auf globale Korrelationsaspekte durch die Analyse von räumlichen Korrelationen (spatial correlations), d. h. die Wechselbeziehungen auf Länderebene.

Herath und Herath (2011) erklären einen Copula-basierten Cyber-Risk-Pricing-Ansatz, um die nicht lineare Art der Abhängigkeiten zwischen Cyber-Risk-Pricing-Variablen zu erfassen. Ihre Methode ermöglicht die Einbindung von nicht normalverteilten Schadenhäufigkeits- und Schadenausmassverteilungen, die die Eigenschaften von Cyberverlusten geeigneter abbilden als die Annahme einer Normalverteilung. Herath und Herath (2011) führen deshalb einen neuartigen Aspekt bezüglich Korrelationsproblemen bei Cyber Risk ein, indem sie nicht lineare Abhängigkeiten zwischen Schadenhäufigkeit und Schadenausmass beachten, um so eine robustere Schätzung für die multivariate Schadenverteilung für Cyber Risk zu erhalten.

Neben den Korrelationen bei Cyber Risk, besteht ein grundsätzliches Problem beim Pricing von Cyber Risk im Mangel an Daten (siehe ENISA, 2012; Herath und Herath, 2011; Baer und Parkinson, 2007; Gordon et al., 2003). Ungeachtet dessen, wie genau und durchdacht die Modellierungen für Cyber Risk sind, werden die Modelle von geringem Nutzen sein, falls keine Daten zum Testen der Modelle vorhanden sind.[39] Des Weiteren führen Bandyopadhyay, Vijay und Rao (2009) an, dass Versicherer auch nur wenig bis gar keine Informationsvorteile gegenüber den einzelnen Firmen wahrnehmen können. Darauf reagieren sie mit hohen Selbstbehalten und niedriger Maximaldeckung, was zu Versicherungspolicen führt, die nur geringen Wert für das RM haben.

Ein weiteres Problem ist das Änderungsrisiko, das heisst, aufgrund von dynamischen Veränderungen wandelt sich das Risiko (siehe z. B. Haas und Hofmann, 2013; ENISA, 2012). In diesem Fall kann eine Analyse historischer Cyber-Risk-Daten irreführend sein. Ein weiteres Änderungsrisiko, das auch eine Herausforderung für die Zufälligkeitsvoraussetzung darstellt, sind regulatorische Interventionen, die die Spielregeln der Cyber-Versicherung verändern. Änderungen in Gesetzen, Regulierung und Corporate-Risk-Management-Strategien können

[39] Weitere Autoren sehen in dem Problem der Datenknappheit in Cyber-Versicherungen ein mögliches Hindernis für die Entwicklung des Marktes (siehe z. B. Shackelford, 2012; Betterley, 2010).

die Bedeutung von Cyber Risk signifikant verändern und so die in Cyber-Policen versicherten Verluste beeinflussen (siehe z. B. Haas und Hofmann, 2013; Gatzlaff und McCullough, 2012).

Somit sind die Kriterien der Zufälligkeit (und der Unabhängigkeit) als problematisch einzustufen.

4.3.2 Maximal möglicher Schaden

Dieses Kriterium ist erfüllt, falls der maximal mögliche Schaden pro Ereignis kontrollierbar, im Sinne von Solvenz des Versicherers, ist. Maximale historische Verluste halten sich bei Cyber Risk im Allgemeinen in überschaubaren Grenzen. Dies auch, weil Versicherer sich mit Deckungslimiten schützen. Im Beispiel von Sony (Vgl. Abschnitt 2.2.2) betrug der Schätzwert für einen Cyberangriff ca. 1,4 Milliarden US-Dollar und stellt damit schon ein sehr extremes Beispiel dar.

Allerdings sollte sich Cyber Risk auch gut poolen und rückversichern lassen. Der maximal mögliche Schaden durch Cyber Risk ist damit gut kontrollierbar.

4.3.3 Mittlere Schadenhöhe

Bezüglich des durchschnittlichen Verlustes durch Cyber Risk zeigt Ponemon (2013), dass Schwachstellen in der Datensicherheit durchschnittlich finanzielle Verluste von 9,4 Millionen US-Dollar erzeugen. Durchschnittliche Verluste durch Datendiebstähle werden, laut KPMG (2013), auf 2,1 Millionen US-Dollar geschätzt.[40] Ein Vergleich dieser Zahlen mit anderen operationellen Risiken (siehe etwa Hess, 2011) zeigt, dass diese einen relativ überschaubaren Umfang haben – sie sind niedriger als andere operationelle Risiken. Die durchschnittlichen Verluste hängen dabei von der Unternehmensgrösse, den vorhandenen Sicherungsmassnahmen oder auch von der institutionellen Verankerung der Informationssicherheit ab. So weisen Unternehmen mit einem Chief Information Security Officer (CISO) oder einer gleichwertigen Position bei einem Vorfall geringere Durchschnittsverluste auf (siehe Shackelford, 2012). Zusammenfassend sehen wir dieses Kriterium aber nicht als ein Hindernis für die Versicherbarkeit von Cyber Risk.

4.3.4 Mittlere Schadenhäufigkeit

Viele Studien zeigen, dass die Anzahl der Cyber-Risk-Ereignisse im Zeitablauf zunimmt. Dennoch hängt die Schadenhäufigkeit sehr stark von den Cyber-Risk-Ereigniskategorien ab. Die Kategorien mit einer menschlichen Komponente sind deutlich relevanter als andere Kategorien, z. B. externe Ereignisse wie etwa Naturkatastrophen, die viel seltener Quelle von Cyber Risk sind. Im Allgemeinen ist dieses Kriterium unserer Meinung nach nicht problematisch.

[40] Laut einer Studie des Unternehmens Symantec fallen pro verlorenen Kundendatensatz bei einem Datendiebstahl in den USA durchschnittliche Kosten von 191 US-Dollar an (Symantec, 2013). In der Studie NetDiligence (2014) werden die Kosten allerdings auf knapp 956 US-Dollar pro verlorenen Datensatz beziffert.

4.3.5 Informationsasymmetrien

Moral Hazard und Adverse Selektion werden oft als grundlegende Hindernisse in der Marktentwicklung diskutiert. Moral Hazard entsteht aus dem Mangel an Anreizen beim Versicherten, Selbstschutzmassnahmen zu ergreifen, die die Schadenwahrscheinlichkeit drastisch verringern, falls eine Versicherung gekauft wurde (siehe Gordon, Loeb und Sohail, 2003). Ferner haben, aufgrund der komplexen Verflechtungen der modernen Informationssysteme, Investitionen in die Informationssicherheit den Charakter eines öffentlichen Gutes mit positiven Externalitäten (siehe Baer und Parkinson, 2007; Cylinder, 2008). Daraus ergibt sich ein Koordinationsproblem; der Nutzen von Investitionen in Cyber-Sicherheit für ein Unternehmen hängt also von den Investitionen in Cyber-Sicherheit der anderen Unternehmen ab. Die Eigenschaften eines Informationssystems erzeugen auch Probleme für das Nachweisen von Verlusten und der Feststellung von Tätern, die die Abneigung eines Unternehmens, in Selbstschutzmassnahmen zu investieren, weiter erhöht (siehe Ögüt, Raghunathan und Menon, 2011).[41]

In der bestehenden Literatur wird dargestellt, dass Unternehmen, die bereits Erfahrung mit Cyberattacken haben, viel wahrscheinlicher eine Versicherung kaufen werden, was zu dem klassischen Problem der Adversen Selektion führt (siehe Shackelford, 2012). Zudem führt der Mangel an Cyberverlustdaten dazu, dass Unternehmen nur schwer in Risikogruppen eingeteilt werden können, was das Adverse Selektionsproblem noch verstärkt. Die Arbeiten von Majuca, Yurcik und Kesan (2006) und Ögüt, Raghunathan und Menon (2011) deuten ebenfalls erhebliche Probleme durch Informationsasymmetrien in Cyber-Versicherungen an.[42]

Die Erfüllung des Versicherbarkeitskriterium zu Informationsasymmetrien ist problematisch.

4.3.6 Versicherungsprämie

Cyber-Versicherungspolicen werden oft als sehr teuer und weit entfernt von einem fairen Preis beschrieben.[43] Es existieren mindestens vier Gründe dafür: (1) die Neuartigkeit und daher die geringe Grösse der Risikokollektive; (2) die Neuartigkeit und daher die geringe Anzahl an Marktteilnehmern (beschränkte Verfügbarkeit, wenig Wettbewerb); (3) die Neuartig-

[41] Es gibt viele Mechanismen, um derartige moralische Risiken abzumildern: Um potenzielle Probleme durch Moral Hazard abzuschwächen, nennen Gordon, Loeb und Sohail (2003) die klassischen Lösungen wie Selbstbehalt und die Einführung eines Prämienreduktionssystems. Zudem empfehlen Bear und Parkinson (2007) regelmässige Risikobeurteilungen durchzuführen, die die Verknüpfung von Deckung und bestimmten Minimalstandards für Cyber-Sicherheit ermöglichen. Shackelford (2012) weist zudem auf ein finanzielles Anreizsystem für Selbstschutzmassnahmen hin, analog zu einem „save driver discount“ in der Kraftfahrzeugversicherung.

[42] Um Probleme der Adversen Selektion zu mildern, kann Screening, Self-selection und Signaling verwendet werden. Gordon, Loeb und Sohail (2003) schlagen Informationssicherheits-Audits und Prämiendifferenzierung für richtige Risikotypselektion vor. Ähnlich dazu empfehlen Baer und Parkinson (2007) eine intensive Prüfung der Firmen-IT und deren Sicherheitsprozesse. Majuca, Yurcik und Kesan (2006) erörtern mögliche Fragen für das Underwriting (d. h. Selbstselektion), die gestellt werden sollen, um Probleme durch Adverse Selektion abzumildern, bevor ein ausführlicher Überprüfungsprozess durchgeführt wird. Eine Zertifizierung nach bestimmten IT-Standards kann auch ein wichtiges Signal an einen Versicherer sein, um die Versicherbarkeit bestimmter Risiken zu erhöhen.

[43] Mukhopadhyay et al. (2005, 2006, 2013) wenden ein kollektives Risikomodell in Verbindung mit Erwartungsnutzen-Theorie an, um eine Beurteilung über den theoretischen Nutzen von Cyber-Versicherung für Unternehmen mit verschiedenen Risikoaversionslevel geben zu können. Sie finden heraus, dass mit steigender Risikoaversion Unternehmen eher eine fair kalkulierte Cyber-Versicherung wählen als gar keine Versicherung. Diese Erkenntnis ist ein fundamentales Resultat in der Versicherungsökonomie; daher stellt es in unserem Kontext den Ausgangspunkt für die Diskussion über Prämien dar.

keit und mangelnde Datenverfügbarkeit, die hohe Risikozuschläge notwendig machen, und (4) erhebliche Informationsasymmetrien, die aufwendige Prüfungen und vorhergehende Risikobeurteilungen nötig machen und so die Prämien treiben.

Nach Betterley (2013) sind Prämien für Cyber-Versicherungen zurzeit vor allem für kleine und mittelgrosse Unternehmen hoch, aber relativ moderat, wenn die grossen Unsicherheiten, die damit verbunden sind, mit einbezogen werden. Shackelford (2012) erwartet, dass die Prämien mit weiterem Ausbau und konkurrenzfähigeren Märkten schrumpfen.[44] Diese Erwartung wird verstärkt durch aktuelle Marktentwicklungen in den USA, wo neue Player in den Markt eintreten (siehe Betterley, 2013). Laut einer Studie von Ponemon (2013) bestätigen Konsumenten von Cyber-Versicherungen, dass Cyber-Versicherungsprämien nicht aussergewöhnlich hoch sind. In der Studie mit 638 Cyber-Risk-Spezialisten in den USA halten 62 % der Unternehmen die Prämien für „fair"; nur 29 % sagen, dass die Prämien zu hoch seien.

Verglichen mit den traditionellen Sach- / Haftpflichtversicherungen, existieren noch zusätzliche Kosten, die von Cyber-Versicherungen abgedeckt werden müssen. So können beispielsweise hohe Kosten im Voraus für eine Beurteilung von Unternehmensrisiken entstehen (z. B. Netzwerksicherheit). Versicherer erwarten eine solche Beurteilung und oft auch zusätzliche Informationen über Vorfälle in der Vergangenheit, um überhaupt Versicherungsschutz anzubieten. Die Beschaffung dieser Informationen kann eine sehr aufwendige Aufgabe darstellen und wird so die Prämie in die Höhe treiben.[45]

Die im Voraus durchgeführten Beurteilungen haben allerdings einen positiven Impuls, da sie das Bewusstsein des Unternehmens für Cyber Risk stärken und so möglicherweise zu steigenden Investitionen in Prävention und einer besseren Implementierung von Präventionsmassnahmen führen. Die wichtigsten ökonomischen Funktionen einer Versicherung sind, einen Preis für ein Risiko zu bestimmen und Anreize für risikoadäquates Verhalten zu setzen.

Unter dem Strich ist aber festzuhalten, dass in allen Studien, die die Angemessenheit der Versicherungsprämie für Cyber Risk begutachten, die Prämie im Allgemeinen als moderat eingestuft wird. Die Trends der letzten Jahre deuten aber auch an, dass sich Prämien verringern, sobald der Markt sich ausweitet und Erfahrungen mit Cyber Risk gewonnen wurden.

Das Kriterium ist deshalb (mit starkem Blick auf die Zukunft) zunehmend unproblematisch.

4.3.7 Deckungsabgrenzung

Cyber-Risk-Policen decken typischerweise ein Maximum, z. B. Verluste bis zu maximal 50 Millionen US-Dollar, ab. Diese Deckungsgrenzen variieren in der Praxis, aber wenn etwa 50 Millionen das Limit wäre, sollten mehr als 90 % aller Cybervorfälle komplett durch eine Police

[44] Shackelford (2012) berichtet allerdings auch über grosse geografische und industrielle Abweichungen. Zum Beispiel sind in den USA mehr Policen verfügbar als in Europa oder Kanada.

[45] Um das Versicherungsprodukt auf den Kunden abzustimmen, muss der Versicherer ein vollumfängliches Profil des Kunden erstellen. Hierbei handelt es sich um einen umfangreichen Prozess, der den Rahmen eines Fragebogens oder Telefongesprächs übersteigt. Das zu versichernde Unternehmen muss über einen längeren Zeitraum überwacht werden, damit dessen Sicherheitsstrategie analysiert werden kann. Ausserdem sollte ein Risk-Assessment durchgeführt werden, um Schwächen aufzuzeigen und eine konkrete Schätzung des potenziell möglichen Schadens durch Cyber Risk erstellen zu können. Für ein Beispiel eines Fragebogens zur Risikobeurteilung, siehe Drouin (2004).

abgedeckt sein (siehe Analysen in Biener, Eling und Wirfs, 2015). Ob dieser Wert akzeptierbar ist, hängt von den Risikopräferenzen des Versicherungsnehmers ab. Eine Erhöhung in der Deckung ist meist verhandelbar, wird aber zu einer erhöhten Prämie führen.

Neben den Deckungsgrenzen schliessen Versicherungspolicen typischerweise bestimmte weitere Aspekte mit aus, z. B. selbstverschuldete Verluste, Zugriff auf ungesicherte Webseiten oder Terrorismus (siehe Mukhopadhyay et al., 2005). Neben diesen Ausschlüssen können weitere indirekte Effekte von Cyber Risk ausgeschlossen werden, die nicht gemessen und somit nicht abgedeckt werden können. Ein Beispiel könnten Reputationsverluste darstellen, obwohl einige Policen versuchen, diese mit in die Deckung aufzunehmen. Gaztlaff und McCullough (2012) beispielsweise merken an, dass Versicherungen oft einen grossen Teil an Kosten für Datenverstösse nicht abdecken, wie das bei Verlusten durch Reputation und dem Einfluss von Aktienpreisen der Fall ist; zudem werden Verluste, die im Zusammenhang mit Handelsgeheimnissen und „propriety information“ stehen, nicht abgedeckt (siehe auch Wojcik, 2012).

Ein weiteres ernstes Problem bezüglich Deckungsgrenzen ist die Komplexität der Police. Es existieren viele Ausschlüsse und die Eigenschaften von Cyber Risk sind so dynamisch, dass sowohl für den Verkäufer einer Versicherung als auch den Käufer Unsicherheit bezüglich der wirklichen Deckung besteht. ENISA (2012) merkt an, dass diese Unklarheiten ein Grund dafür sind, dass Unternehmen keine Cyber-Versicherung kaufen. Des Weiteren wird angemerkt, dass viele Unternehmen glauben, ihre Sach- / Haftpflichtversicherung sei ausreichend, um Risiken aus Cyber Risk abzudecken.

Somit ist dieses Versicherbarkeitskriterium aus unserer Sicht etwas problematisch.

4.3.8 Gesellschaftliche Werte

Die Verfügbarkeit von Versicherung gegen Cyber Risk, speziell gegen Hackerattacken und physische Attacken, lassen Bedenken aufkommen, ob dadurch Hürden für Cybercrime gesenkt oder sogar Anreiz dazu geschaffen werden. So könnte eine Motivation für Versicherungsbetrug geschaffen werden, da Hackerattacken oder physische Attacken schwer zu erkennen und nachzuverfolgen sind. Des Weiteren könnten Anreize für Firmen geschaffen werden, weniger Anstrengungen in Selbstschutz zu investieren.[46] In Kombination mit den hohen Korrelationen von Cyber Risk, könnte dies die Schadenlast in der Industrie erhöhen und zu gesellschaftlichen Wohlfahrtsverlusten führen.

In diesem Zusammenhang zeigen Ögüt, Raghunathan und Menon (2011), dass Unternehmen, wenn Risiken korreliert sind und die Überprüfbarkeit von Verlusten nicht perfekt ist, weniger in Selbstschutz investieren als sozial optimal wäre. Daher agieren Versicherung und Selbstschutz als Substitute. Im Gegensatz dazu zeigen Kesan, Majuca und Yurcik (2004), dass der Abschluss einer Cyber-Versicherung auch mit mehr Investitionen in die Cyber-Sicherheit einhergeht und so positive Externalitäten erzeugt. Dies kann gegebenenfalls mit der Unterstützung der Versicherer im Bereich der Prävention erklärt werden; Versicherer beurteilen die

[46] Eine genaue und in allen Einzelheiten im Vertrag festgelegte Definition solcher Fälle kann das Risiko etwas minimieren (siehe Biener und Eling, 2012).

Deckung und stellen beratende Dienstleistungen zur Verfügung. Gemäss Bolot und Lelarge (2009) erhöht der umfassende Gebrauch von Cyber-Versicherungen die Internetsicherheit allgemein.

Somit ist dieses Kriterium – aus unserer Sicht – nur wenig problematisch.

4.3.9 Gesetzliche Schranken

Rechtliche Rahmenbedingungen können ebenfalls Einschränkungen für die Versicherbarkeit mit sich bringen. So ist an erster Stelle zu nennen, dass in manchen Ländern das Versichern von Geldbussen verboten ist (eine internationaler Überblick: siehe Barlow Lyde & Gilbert, 2007).

Des Weiteren hat die Europäische Kommission kürzlich eine regulatorische Vorlage für neue Datenschutzrichtlinien erlassen (siehe European Commission, 2012), die 2014/2015 eingeführt werden soll. In diesem Zusammenhang wird etwa über mögliche regelmässige Meldepflichten für Cyberattacken diskutiert. Zudem könnten solche Vorlagen dazu führen, dass zusätzliche Risiken aber auch zusätzliche Beschränkungen aufkommen, die mittels Versicherung abgedeckt werden können. Deshalb stellt das Änderungsrisiko in Verordnungen und Gesetzen einen wichtigen Gegenstand für Versicherer dar. Ausserdem müssen allgemeine Versicherungsbedingungen angepasst werden, falls Änderungen in Kraft treten. Dennoch können Änderungen auch eine Chance darstellen, wenn durch neue regulatorische Vorgaben die Nachfrage nach Cyber-Versicherung beflügelt wird.

Die Neuheit, Komplexität und Dynamik von Cyber Risk kann dennoch auch rechtliche Unsicherheiten mit sich bringen, etwa im Versicherungsvertrieb. Ein erfahrener Versicherungsbroker weiss, dass eine genaue Vorhersage der Deckung für Cyber Risk sehr schwierig ist; dies könnte die Bereitschaft, entsprechende Produkte anzubieten, einschränken. Dies führt dann dazu, dass im Allgemeinen nur wenige Spezialisten bereit und in der Lage sind, Cyber-Versicherungen zu verkaufen. Es kommt zu einem Mangel an diesen Fachkräften (siehe Chabrow, 2012).

Schliesslich könnte auch die zum Abschluss einer Versicherung notwendige Offenlegung von Informationen aus Datenschutzsicht problematisch sein. Beispielsweise diskutiert Ouellette (2012), dass Krankenhäuser nicht bereit sein könnten, Patientendaten an einen Drittanbieter (z. B. Cyber-Versicherungsanbieter) weiterzugeben.

Dieses Versicherbarkeitskriterium ist dennoch nur wenig problematisch.

4.3.10 Zusammenfassung der Kernresultate zur Versicherbarkeit

In Tabelle 16 fassen wir die Kriterien der Versicherbarkeit und deren Erfüllungsgrad in Bezug auf Cyber Risk zusammen.

Kriterium / Bewertung	**Begründung**
Versicherungsmathematisch:	
• Zufälligkeit des Schadenereignisses *problematisch*	• Risiken sind nicht unabhängig (Ausgleich im Kollektiv) • Risikokollektive sind noch relativ klein • Schwer messbares Schadenpotenzial; Mangel an Daten • Erhebliche Änderungsrisiken
• Maximal möglicher Schaden *nicht problematisch*	• Maximale Schäden gut beherrschbar • Versicherer schützen sich zudem durch Deckungsgrenzen
• Mittlere Schadenhöhe (severity) *nicht problematisch*	• Relativ geringe Durchschnittsschäden, etwa im Vergleich zu anderen operationellen Risiken • Durchschnittsschäden hängen ab von der Grösse, den vorhandenen Schutzmassnahmen und der institutionellen Verankerung der Informationssicherheit
• Mittlere Schadenhäufigkeit (frequency) *nicht problematisch*	• Zunehmende Frequenz im Zeitablauf • Hängt stark von der Event-Kategorie ab (human action sehr dominant)
• Informationsasymmetrien *problematisch*	• Moral Hazard, d. h. Verhaltensänderung nach Vertragsabschluss; Screening (Audits) und Selbstbehalte helfen, Moral Hazard zu verringern • Adverse Selektion (Firmen, die bereits Cyberattacken erlebt haben, kaufen eher eine Versicherung); Screening (up-front Audits), Selbstselektion (Underwriting Fragen) und Signaling (Zertifikate) helfen, um Adverse Selektion zu mildern
Marktbezogen:	
• Versicherungsprämie *(noch) ein wenig problematisch*	• Hohe Risikoaufschläge führen zu relativ hohen Prämien, es wird erwartet, dass diese in den kommenden Jahren sinken • Grosse Unterschiede in der Verfügbarkeit hinsichtlich Regionen und Industrien • Relativ geringe Anzahl an Wettbewerbern (es wird erwartet, dass diese zunimmt) • Signifikante zusätzliche Kosten (etwa „up-front assessments“)
• Deckungsabgrenzung *problematisch*	• Typischerweise gibt es ein Maximum (z. B. 50 Millionen US-Dollar) • Policen enthalten viele Ausschlüsse (z. B. grobe Fahrlässigkeit, Terror); indirekte Kosten können nicht gemessen und häufig auch nicht gedeckt werden (z. B. Reputationseffekte). • Komplexität der Produkte (Ausschlüsse, dynamische Natur der Risiken, für Käufer besteht Unsicherheit über die tatsächliche Abdeckung)
Gesellschaftsbezogen:	
• Gesellschaftliche Werte *ein wenig problematisch*	• Anreize zur Reduktion von Schutzmassnahmen kann Industry Exposure und damit gesellschaftliches Risiko erhöhen • Anreize für Versicherungsbetrug, da Verursacher häufig nicht identifizierbar sind
• Gesetzliche Schranken *ein wenig problematisch*	• Änderungsrisiken (neue Gesetze / Regulierungen) • Rechtliche Unsicherheit im Vertrieb der Cyber-Versicherung; nur wenige Spezialisten sind willens und in der Lage, die Produkte zu vertreiben; es herrscht ein Mangel an Spezialisten • Offenlegung sensibler Informationen kann datenschutzrechtlich problematisch sein

Tabelle 16: Versicherungskriterien und Erfüllungsgrad bei Cyber Risk

Fazit: Cyber Risk ist bedingt versicherbar

Insgesamt fällt die Bewertung durchmischt aus. Wesentliche Probleme lassen sich in den Bereichen Zufälligkeit des Schadenereignisses, Informationsasymmetrien und Deckungsabgrenzungen identifizieren. Des Weiteren erscheinen die Prämienhöhe und die gesetzliche Lage zumindest ein wenig problematisch. Vor dem Hintergrund dieser Resultate sind Cyberrisken nur bedingt versicherbar, was teilweise den noch recht geringen Marktumfang erklären kann.[47]

Aber: Positiver Ausblick auf Marktentwicklung

Dennoch lässt sich ein positiver Ausblick für die Marktentwicklung geben. Mit zunehmender Marktentwicklung werden die Risikopools stetig grösser und es stehen mehr Daten zur Verfügung. Eine Reihe von neuen Wettbewerbern ist in den Markt eingestiegen oder plant, dies zu tun. So werden die Verfügbarkeit und der Wettbewerb erhöht und die Preise reduzieren sich. Vor dem Hintergrund unserer Resultate erscheint es ferner wichtig, gewisse Standards für Deckungsgrenzen oder Vorabprüfungen zu etablieren; dies könnte helfen, weitere Probleme der Versicherbarkeit zu verringern.

[47] Die Einteilung in „nicht problematisch“, „ein wenig problematisch“ und „problematisch“ ist sicherlich etwas pauschal und bedarf grundsätzlich einer weiteren Differenzierung. Allerdings ermöglicht sie das Herausarbeiten der Kernaspekte zur Versicherbarkeit.

5 Cyber Risk: Befragung aus Perspektive der Kunden

5.1 Befragungsdesign und Methodik

Dieses Kapitel stellt die Ergebnisse zweier Marktbefragungen zu Cyber Risk aus der Perspektive von (potenziellen) Kunden zusammen. Im Zentrum der nachfolgenden Diskussion steht eine Befragung von Mitarbeitern aus 16 Unternehmen der Finanzbranche (Abschnitte 5.2 bis 5.4). Des Weiteren werden wir in Abschnitt 5.5 auch die Ergebnisse einer weiteren Befragung unter 22 Mitarbeitern von kleinen und mittelgrossen Unternehmen (KMUs) einbinden.

Befragung in der Finanzbranche
Um die Einschätzung von potenziellen Kunden von Cyber-Versicherungen zu analysieren, wurden in einem ersten Schritt 16 Interviews zu verschiedenen Cyber-Risk-Themen durchgeführt. Die Interviews fanden im Frühjahr 2013 statt.[48] Die Befragung gliedert sich in vier Teile: Als Erstes wurde die jeweils interviewte Person nach einer Definition von Cyber Risk gefragt. Zusätzlich sollte sie eine Einschätzung zur Bedeutung von Cyber Risk für das Unternehmen abgeben. Im zweiten Teil folgten Fragen zum aktuellen Schutz des Unternehmens vor Cyber Risk. In Teil drei wurden dann Erfahrungen der Unternehmen mit Cyber-Risk-Vorfällen angesprochen. Zum Schluss folgten Fragen zum Risikotransfer mit Hilfe einer Versicherung. In der Analyse werden wir die Ergebnisse nach Unternehmensgrösse (gemessen an der Anzahl der Angestellten) und Branche differenziert. Die Unternehmen werden hierbei in zwei Kategorien unterteilt. Die Kategorie „grosse Unternehmen“ umfasst Unternehmen mit mehr als 200 Angestellten, die Kategorie „kleine Unternehmen“ enthält Unternehmen mit weniger als 200 Angestellten. Neun Unternehmen zählen zu den grossen, sieben zählen zur Gruppe der kleinen Unternehmen. Es sind Vertreter von Banken, Versicherungen, Asset-Management-Firmen, Risk-Management-Firmen und Beratungsfirmen vertreten. Insofern liegt der Fokus der Befragung auf Unternehmen der Finanzdienstleistungsindustrie. Die Befragten nehmen im entsprechenden Unternehmen verschiedenste Positionen ein (z. B. Systemadministrator, CEO etc.).

Befragung bei KMUs
Die zweite Befragung (Abschnitt 5.5) erfolgt im Rahmen eines Workshops mit Vertretern von 22 kleinen und mittelgrossen Unternehmen (KMUs) im November 2014. Hier wurde die Relevanz von und der Umgang mit Cyber Risk diskutiert und im Rahmen einer anonymisierten Befragung aufbereitet, die wir ebenfalls in die nachfolgende Diskussion einbinden.

[48] Die Befragung ist Teil der Masterarbeit von Andreas Matt (siehe Matt, 2013), aus der wir einige Kernresultate wiedergeben.

5.2 Definition und Bedeutung von Cyber Risk

Definition von Cyber Risk
Auf die Frage, wie Cyber Risk zu definieren ist, hat keiner der 16 Befragten eine konkrete Definition nennen können. Vielmehr zählten die Befragungsteilnehmer konkrete Beispiele auf, die für sie Bestandteil von Cyber Risk darstellen und versuchten so Cyber Risk einzugrenzen, etwa:

- Onlinespionage
- Datenmanipulation
- Datenzerstörung
- Illegale Datenbeschaffung
- Datendiebstahl
- Datenverlust
- E-Mail-Hacking
- Phishing
- Viren
- Kreditkartenbetrug
- Cyberwar

Alle angegebenen Beispiele sind im Einklang mit unserer Definition in Abschnitt 2.1. Dennoch vermerkte keiner der Befragten den Zusammenhang von Cyber Risk mit den operationellen Risiken. Ein Befragter stellte allerdings den Zusammenhang mit Informationssicherheitsrisiken her. 44 % der Befragten gaben dabei an, dass Cyber Risk ausschliesslich Gefahren beinhalte, die in Zusammenhang mit Datennetzwerken (z. B. dem Internet) entstehen, wobei die restlichen 56 % erklärten, dass es sich um alle Risiken handle, die von Daten auf Datenträgern und Datennetzwerken ausgehen. Aus der Sicht der Kunden existiert folglich (noch) kein einheitlicher Cyber-Risk-Begriff.

Bedeutung von Cyber Risk
Bei der Bedeutung von Cyber Risk für das Unternehmen liegen die Einschätzungen der Befragten sehr nah beieinander. Fast alle Befragten der grossen Unternehmen (sieben von neun) gaben an, dass die Bedeutung von Cyber Risk in den jeweiligen Unternehmen als sehr hoch einzuschätzen ist. Nur einer sah die Bedeutung als gering an, während der letzte Befragte der Gruppe „grosse Unternehmen“ die Frage mit stetig steigender Bedeutung beantwortete. Ein Befragter meinte zudem, dass der Schutz von Daten, insbesondere von Kundendaten, eines der obersten Güter darstelle und auch viel Geld für diesen Zweck investiert würde. Auch die Befragten in der Kategorie „kleine Unternehmen“ haben die Bedeutung von Cyber Risk sehr hoch eingeschätzt (fünf von sieben Befragten). Nur zwei Teilnehmer stellten dar, dass für sie Cyber Risk von geringer Bedeutung sei.

Auf die Frage. wie die Bedeutung von Cyber Risk für die Zukunft einzuschätzen wäre, waren sich wieder nahezu alle Befragten einig: 15 von 16 antworteten, dass die Bedeutung von Cyber Risk innerhalb der nächsten fünf Jahre zunehmen werde. Nur einer stufte die Bedeutung mit gleichbleibend bis leicht abnehmend ein. Ein Befragter hat in diesem Zusammenhang

angegeben, dass „man sich immer mehr auf die funktionierende Technologie verlässt“ und „auch immer mehr Daten abrufbar sind“ und so die Bedeutung von Cyber Risk stetig zunehme. Dies wird unterstrichen durch die Antwort eines weiteren Befragten, der anführt, dass mit der „globalen Vernetzung / Tätigkeit man immer offener und angreifbarer wird“. Lediglich ein Befragter der Bankenbranche meinte, dass die Gefahr vor Cyber Risk eher gleichbleibe, wenn nicht sogar leicht abnehme.

Im Folgenden sind die in den Interviews genannten Begründungen für die Einschätzungen der zukünftigen Bedeutung von Cyber Risk aufgelistet. Mit einem „+“ versehene Punkte stellen Argumente für eine Zunahme der Bedeutung dar, während die mit einem „–“ gekennzeichneten eine Abnahme bzw. Stagnation bestimmen:

+ Globale Vernetzung nimmt zu
+ Technologische Abhängigkeiten nehmen zu
+ Starkes technologisches Wachstum (auch Wachstum der Risiken)
+ Zunahme des Datenverkehrs / Datenvolumens
– Änderungen im Geschäftsmodell der Banken

Zusammenfassung
Offensichtlich existiert keine einheitliche Definition aus Sicht der Kunden. Nahezu alle Befragten nehmen Cyber Risk sehr ernst und messen diesem Risiko eine grosse Bedeutung für das eigene Unternehmen bei. Die Tendenz der Antworten zur zukünftigen Bedeutung von Cyber Risk ist ebenfalls eindeutig. Fast alle Befragten (94 %) sehen eine erhöhte Gefahr durch Cyber Risk in den nächsten fünf Jahren. Diese Einschätzung deckt sich mit allen uns bekannten Studien zu dieser Thematik.

5.3 Risikomanagement von Cyber Risk

Derzeitiges Schutzempfinden
Auf die Frage, ob die eigenen Unternehmen gut vor Cyber Risk geschützt sind, antworteten 14 von 16 (88 %) mit „Ja“ und nur eine Person (6 %) mit „Nein“. Ein weiterer Befragter konnte dies nicht beurteilen (6 %). Eine Differenzierung nach Grösse zeigt dabei, dass alle Befragten der grossen Unternehmen sich vor Cyber Risk gut geschützt fühlen (N=8) bzw. keine Aussage treffen können (N=1). Bei den Befragten der kleinen Unternehmen sagen dies sechs von sieben Befragten (86 %). Bei der Unterteilung nach Branche können alle Befragten aus den Kategorien „Banken“ und „Versicherungen“ angeben, dass sie gut geschützt sind bzw. keine Angaben machen können (bei Versicherungen). Dieses Ergebnis (in Kombination mit den letzten Punkten aus Abschnitt 5.2) verdeutlicht, dass Unternehmen aus der Finanzbranche sich offensichtlich über die durch Cyber Risk entstehenden Gefahren bewusst sind, aber sich auch dementsprechend vorsichtig verhalten und aktiv Schutz suchen.

Das Schutzempfinden vor Cyber Risk ist bei den meisten befragten Unternehmen sehr gut (88 %). Dies lässt sich wahrscheinlich damit begründen, dass, wie wir später sehen werden, vor allem grosse Unternehmen einen immensen Aufwand zum Schutz vor Cyber Risk betreiben, während sich kleine Unternehmen der Gefahr eines Cyberangriffs, aufgrund ihrer Grösse, nicht so stark ausgesetzt fühlen.

Im weiteren Teil der Befragung wurden die Befragten zu möglichen Schutzmassnahmen, die die Unternehmen zum Schutz vor Cyber Risk anwenden, befragt. Dies wurde in drei Kategorien unterteilt, die wir im Folgenden einzeln besprechen werden: „Schutz vor Naturkatastrophen“, „Schutz vor physischer Spionage / Sabotage“ und „Schutz vor Gefahren aus dem Internet“. In einem weiteren Schritt wollen wir dann noch auf Fragen zur Sensibilisierung der Angestellten eingehen.

Schutz vor Naturkatastrophen
Auf die Frage, wie Unternehmen ihre Daten vor Naturkatastrophen schützen, nannten die Befragten die folgenden Massnahmen:

- Mehrere analoge Rechenzentren
- Löschanlagen
- Wasserpumpen
- Notstromaggregate
- NEMP-Schutz (Schutz vor nuklearen elektromagnetischen Impulsen)
- Tresore
- Geografische Wahl der Standorte
- Bauliche Massnahmen

Ein Befragter sagte, dass das Unternehmen zwei identisch ausgestattete Rechenzentren habe, die mehrere Kilometer voneinander getrennt aufgebaut wären. Wenn eines davon ausfalle, bestehe die Möglichkeit, auf das andere umzuschalten, um weiterhin betriebsfähig zu sein. Zusätzlich hätten die Rechenzentren eine Löschanlage installiert und durch bauliche Massnahmen sei Schutz vor Hochwasser gewährleistet. Die Standorte seien zudem so gewählt

worden, dass sie sich nicht in der Nähe von Flüssen befänden und dass die Gebiete um den Standort erdbebensicher seien. Die Gebäude seien zusätzlich auch durch bauliche Massnahmen vor Flugkörpern geschützt. Alle anderen Befragten der Gruppe „grosse Unternehmen" gaben sehr vergleichbare Antworten. Auch die kleineren Unternehmen machten ähnliche Angaben. Ein Befragter merkte allerdings an, dass sich sein Unternehmen vor Naturkatastrophen nur durch regelmässig durchgeführte Backups schütze. Ein weiterer Befragter gab dieselbe Antwort, meinte allerdings, dass bei ihnen jeder Mitarbeiter für seine Daten selbst verantwortlich sei und sie nur die Buchhaltung an ein anderes Unternehmen ausgelagert hätten.

Es ist folglich zu erkennen, dass grosse Unternehmen ihre Rechenzentren sehr gut vor Naturkatastrophen schützen, damit sie nicht einen Datenverlust erleiden müssen. Es werden enorme bauliche (z. B. Schutz vor Flugkörpern) wie auch sicherheitstechnische Massnahmen (z. B. Löschanlagen) ergriffen. Hingegen sind kleine Unternehmen verstärkt Gefahren ausgesetzt, da nicht in vergleichbarem Umfang Schutzmassnahmen betrieben werden können. Dies dürfte vor allem mit dem vorhandenen Budget zu tun haben, das das jeweilige Unternehmen überhaupt zum adäquaten Schutz zur Verfügung hat.

Schutz vor physischer Spionage / Sabotage
Auf die Frage, wie sich das Unternehmen vor physischer Spionage und Sabotage (dazu wollen wir auch Datendiebstahl zählen) schützt, gaben die Befragten eine Reihe von Massnahmen an. Diese listen wir im Folgenden auf:

- Einschränkung des Zutritts zu wichtigen Informationsquellen (z. B. spezielle Freigabebewilligungen für Serverräume, Passwörter, Smartcards)
- Alarmanlagen
- Videoüberwachung
- IT-Überwachung
- Bewegungsmelder
- Sperren an USB-Ports oder allgemein Computer ohne USB-Anschlüsse
- Surfstations
- Keine CD-Laufwerke
- Compliance Officer
- Verschlüsselungen
- Protokollierung von Zugriffen
- Sensibilisierung / Schulung der Mitarbeiter und geeignete Rekrutierung für systemwichtige Arbeitsstellen

Ein Befragter erklärte, dass in seinem Unternehmen die Räume, in denen vertrauliche Daten aufbewahrt würden, durch Zykluskontrollen und Objektüberwachungen (Kameras) gesichert seien. Ausserdem werde jeder Zugriff auf Daten aufgezeichnet und die USB-Ports an allen Computern seien gesperrt, damit keine Daten auf externe Festplatten kopiert werden könnten. Ansonsten seien die Computer mit Passwörtern, die in regelmässigen Abständen geändert würden, gesichert. Des Weiteren verfüge das Unternehmen über einen Compliance Officer. Dieser beobachte und schule die Mitarbeiter, damit die Daten sicher seien und nicht gefährdet würden. Ein weiterer Befragter bestätigte, dass auch bei ihnen jeder Zugriff protokolliert wür-

de. Zudem führt ein Befragter an, dass die Computer über kein CD-Laufwerk verfügten. Ausserdem würden die USB-Schnittstellen ständig von der IT-Abteilung überwacht. So könne die Überprüfbarkeit durch die IT für diesen Bereich gewährleistet werden. Bei den kleinen Unternehmen sieht es grundsätzlich ähnlich aus. Eine Ausnahme stellt die Antwort eines Befragten dar, der meint, dass sein Unternehmen in Bezug auf physische Spionage / Sabotage relativ machtlos sei.

Wie schon im vorhergehenden Punkt zeichnet sich auch hier ab, dass sich vor allem grosse Unternehmen mit enormem Aufwand vor Spionage und Sabotage schützen, während kleinere Unternehmen einer erhöhten Gefahr durch solche Risiken ausgesetzt sind.

Schutz vor Gefahren aus dem Internet
Im Folgenden sind die in den Interviews erwähnten Massnahmen zum Schutz vor Gefahren aus dem Internet aufgelistet:

- Firewalls
- Anti-Viren-Programme
- Von aussen abgeschottete Infrastruktur
- Isolierung besonders sensitiver IT-Anwendungen auf nicht vernetzten, geschlossenen IT-Systemen
- Dedizierte Internetinfrastruktur (kein direkter Zugriff von intern nach extern)
- Monitoring
- Penetrationstests
- Outsourcing
- Einkauf von Expertenwissen von externen Dienstleistern

Ein Befragter sagte, dass ein maximaler Aufwand betrieben werde, um sich vor Gefahren aus dem Internet zu schützen. Dies geschehe mittels Firewalls, Anti-Viren-Programmen etc. Er führte aber auch an, dass der maximale Aufwand für solche Massnahmen im Rahmen bleiben müsse und erklärte dies anhand der 80:20-Regel: Vor 80 % der vorhandenen Risiken könne man sich mittels 20 % des Aufwandes schützen. Jedoch müsse man für die restlichen 20 % der Risiken einen Aufwand von 80 % betreiben. Ein Befragter gab an, dass sich sein Unternehmen vor allem mittels State-of-the-Art-Firewalls vor Risiken aus dem Internet schütze. Ein weiterer Befragter sagte, dass sich das Unternehmen ausschliesslich durch Virenprogramme vor Hackerangriffen schützen würde. Er meinte aber auch, dass es wahrscheinlich einfach sei, sein Unternehmen zu attackieren, da sie momentan kein richtiges Konzept zum Schutz vor Cyber Risk hätten und auch viel Open-Source-Software verwenden würden.

Insgesamt lässt sich feststellen, dass sich jedes der befragten Unternehmen mittels Software vor Gefahren aus dem Internet zu schützen sucht. Während sich kleine Unternehmen „nur“ mittels Software schützen, betreiben grosse Unternehmen einen weitaus grösseren Aufwand (Sicherungsmassnahmen in der Netzwerk- und Infrastruktur).

Sensibilisierung der Angestellten
Wie bereits im RM-Prozess (Kapitel 3) angesprochen, ist ein wesentlicher Punkt im Umgang mit Cyber Risk die Kommunikation. Ein Instrument zum Schutz vor Cyber Risk kann also auch die Sensibilisierung und das Aufmerksam-Machen der Angestellten über entsprechende Risiken sein. Diesem Punkt wollten wir uns mit der Frage nach Methoden, mit denen die jeweiligen Unternehmen die Mitarbeiter betreffend Cyber Risk sensibilisieren, widmen. Im Folgenden sind die verschiedenen Massnahmen der Unternehmen zur Sensibilisierung der Angestellten zusammengefasst:

- Web-based Trainings
- Kampagnen (Phishing, soziale Netzwerke)
- Richtlinien zum Umgang mit sensiblen Daten
- Mitarbeiterschulungen
- Onlinetests

In der Kategorie der grossen Unternehmen antwortete ein Befragter, dass jeder neue Mitarbeiter betreffend Informationssicherheit instruiert würde. Des Weiteren gäbe es noch Web-based Trainings für Informationssicherheit und Datenschutz im Unternehmen. Ausserdem werde im Unternehmen auch der (richtige) Umgang mit sozialen Netzwerken geschult. Ein weiterer Befragter gab an, dass in seinem Unternehmen verschiedene Sensibilisierungskampagnen durch Stabstellen, z. B. zu Phishing oder sozialen Netzwerken, durchgeführt würden. Im Unternehmen eines weiteren Befragten werden Mitarbeiter regelmässig durch verpflichtende Schulungen instruiert und laufend per E-Mail über etwaige Risiken informiert. Bei einigen der kleinen Unternehmen gibt es keine spezifischen Strategien zur Sensibilisierung von Mitarbeitern; dennoch wird versucht, die Mitarbeiter auf Gefahren aufmerksam zu machen.

Während es den Anschein macht, dass grosse Unternehmen mit erheblichem Aufwand die Sensibilisierung der Mitarbeiter, zum Teil sogar mit verantwortlichen Stabstellen, vorantreiben, setzen die kleinen Unternehmen auf „einfachere“ bis gar keine Methoden zur Sensibilisierung.

5.4 Versicherbarkeit von Cyber Risk

Schutz durch Versicherung
In den Interviews gaben fünf von 16 Befragten an, Versicherungsschutz für Cyber Risk zu besitzen, wobei sich dies in der Regel auf Versicherungen allein für Wiederherstellung oder die Versicherung technischer Einrichtung im Rahmen anderer Versicherung (z. B. Sach- / Haftpflichtversicherung) beschränkt. Ob die betroffenen Unternehmen allerdings Stand-alone-Cyber-Versicherungen besitzen, konnte im Detail von den Befragten nicht beantwortet werden. Sieben der Befragten geben an, dass keine Versicherung besteht (ca. 44 %). Der Rest der Befragten kann zu dieser Frage keine Angabe machen (4 von 16).

Eine Aufschlüsselung nach Unternehmensgrösse zeigt, dass vor allem grosse Unternehmen (drei von fünf) Versicherungen abschliessen. Auffällig ist auch, dass vor allem Banken keine Versicherung kaufen. Dies ist vor allem vor dem Hintergrund interessant, dass im Abschnitt 5.5 Banken als die Unternehmen identifiziert werden, die verstärkt Cyber Risk ausgesetzt sind. Einer der befragten Bankmitarbeiter antwortet auf die Frage mit einer möglichen Erklärung: Das Datengeschäft gehöre zu ihrem Kerngeschäft und es würde das falsche Signal an den Kunden senden, wenn man sich mit einer Versicherung vor solchen Risiken schütze.

Schutz durch Versicherung in fünf Jahren
Falls die Befragten nicht mit „Ja“ geantwortet haben (11 Beobachtungen), wurden sie gefragt, ob sie sich vorstellen könnten, dass ihr Unternehmen innerhalb der nächsten fünf Jahre eine Cyber-Versicherung abschliesst. Es antworteten zwei der elf Personen mit „Ja“, fünf von elf mit „Nein“ und der Rest (4 von 11) konnte keine genaue Auskunft geben. Zu erwähnen ist, dass es bei der Entwicklung über die nächsten fünf Jahre auch darauf ankomme, wie schnell sich die Risiken verändern (Antwort eines Befragten). Ausserdem käme es auch auf das Angebot der Versicherer an und auch, wie viele Informationen vom Unternehmen preisgeben werden müsste (Antwort eines Befragten).

Bislang ist von den befragten Unternehmen nur ein Bruchteil mittels einer Versicherung vor bestimmten Cyber Risk geschützt. Dies bezieht sich aber in der Regel nicht auf eine reine Cyber-Versicherung, sondern enthält auch Versicherungsschutz, der im Rahmen anderer Sach- / Haftpflichtversicherungen abgedeckt wird (z. B. Schutz technischer Einrichtungen). Die Nachfrage nach Cyber-Versicherungen wird für die nächsten fünf Jahre in unserer Befragung nur als sehr mässig eingeschätzt (nur zwei von elf Befragten würden Versicherung erwerben). Dies lässt sich vielleicht dadurch erklären, dass sich viele Unternehmen bereits für gut geschützt halten (siehe Schutzempfinden in Abschnitt 5.3). Manche Unternehmen sehen es aber auch als ihre Pflicht an, die Daten der Kunden selbst zu schützen und schliessen deshalb keine Cyber-Versicherung ab. Dieses Argument scheint vor allem in der Bankenbranche bedeutsam, da hier die Arbeit mit Kundendaten und Informationsverarbeitung die wichtigsten Güter im Unternehmen darstellen. Eine letzte Erklärung könnte aber auch sein, dass wir Personen befragt haben, in deren Entscheidungsgewalt die Entscheidung für oder gegen eine Versicherung gar nicht liegt und wir hier so ungewollt eine Verzerrung erhalten.

5.5 Zusätzliche Informationen aus der Befragung

Nachdem wir einen Einblick bekommen haben, was Unternehmen unter Cyber Risk verstehen, welche Bedeutung sie ihnen beimessen und, was alles bereits zum Schutz unternommen wird, wollen wir nun allgemein klären, ob die Unternehmen überhaupt schon einmal Schäden durch Cyber Risk gegenüberstanden.

Auf die Frage, ob die Unternehmen bereits Datenausfälle zu beklagen hatten oder bereits Opfer eines Hackerangriffs oder eines Datendiebstahls wurden, bejahten dies drei der 16 Befragten. Dabei gehören zwei der Branche Banken an und sind grosse Unternehmen. Bei den Ergebnissen der nicht betroffenen Unternehmen gab ein Befragter an, dass ein Keylogger an einem PC installiert wurde, was der Befragte aber nicht zu Cyber Risk zählen wollte. Dies würden wir aber nach unserer Definition in Kapitel 2 dennoch tun.

In den Fällen, in denen Unternehmen bereits Opfer von Cyber Risk geworden sind, haben wir explizit nach den Vorfällen gefragt und beschreiben diese in der folgenden Liste:

- Viren
- Trojaner
- Würmer
- Spam-Mails
- Keylogger

Etwas spezieller gab ein Befragter an, dass das Unternehmen, in dem er arbeitet, vom „ILOVEYOU-Virus“ betroffen war. Dieser habe dann das E-Mail-System für zwei Tage lahmgelegt und hätte dadurch erheblichen Schaden verursacht. Was aber allgemein auch deutlich wird ist, dass alle Befragten hier im Wesentlichen Gefahren aus dem Internet ansprechen. Keiner der Befragten geht auf Datenverluste oder ähnliche Vorfälle ein. Dies könnte den Rückschluss zulassen, dass Unternehmen in der Finanzbranche sich gut vor solchen Gefahren zu schützen wissen. Sowohl kleine als auch grosse Unternehmen sehen sich insbesondere mit Gefahren aus dem Internet (Viren, Trojaner, Spam-Mail, Wurm) konfrontiert. Jedoch hat, abgesehen vom Fall des Loveletter-Virus, keiner der Vorfälle grössere Schäden verursacht. In Bezug auf die Branchen gehören die Banken bei dieser Befragung zu den gefährdetsten Unternehmen.

5.6 Befragungsergebnisse der KMUs

Wie bereits angesprochen, haben wir zur Abrundung im Rahmen eines Workshops eine Gruppe von Vertretern von kleinen und mittelgrossen Unternehmen zu ihrer Einschätzung bezüglich der Relevanz von und dem Umgang mit Cyber Risk befragt. Konkret wurden die 22 Teilnehmer des Workshops gebeten, ihre Einschätzung im Hinblick auf die nachfolgenden zwei Dimensionen abzugeben:

- Bewerten Sie die *Relevanz* von Cyber Risk für Ihr Unternehmen auf einer Skala von 1 (nicht relevant) bis 10 (hoch relevant)
- Bewerten Sie den *Umgang* mit Cyber Risk in Ihrem Unternehmen auf einer Skala von 1 (wenig professionell, verbesserungsfähig) bis 10 (sehr professionell, optimaler Umgang)

Das Ergebnis kann im Rahmen eines zweidimensionalen Schaubilds dargestellt werden (siehe Abbildung 13). Auffällig ist die grosse Streuung der Resultate über die 22 Antworten. Manche sehen in Cyber Risk derzeit noch eine geringe Relevanz und messen auch dem heutigen Umgang noch wenig Professionalität bei. Andere sehen den Umgang mit der Thematik hingegen als durchaus gut an. Besonderer Handlungsbedarf besteht bei denen, die die Relevanz als überdurchschnittlich hoch und den heutigen Umgang als unterdurchschnittlich erachten (Quadrant unten rechts). Insgesamt ergibt sich aber ein sehr heterogenes Bild für das Zusammenspiel von Relevanz und Umgang mit Cyber Risk.

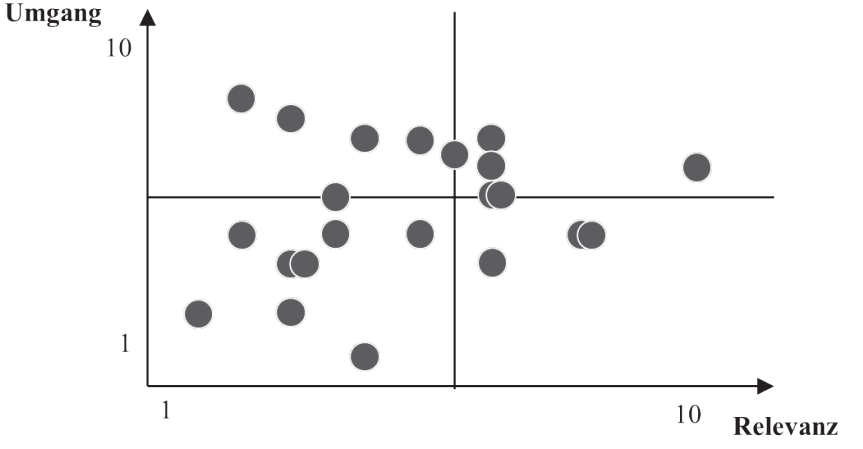


Abbildung 13: Ergebnisse der Befragung zum Umgang und Relevanz von Cyber Risk

In einem weiteren Teil haben wir den Befragten noch ein konkretes Szenario vorgestellt und eine Einschätzung bezüglich der Wahrscheinlichkeit und möglicher Konsequenzen vornehmen lassen. Konkret wurde von einem Szenario ausgegangen, indem in einer E-Mail behauptet wurde, dass die gesamten Kundendaten inklusive der Sicherungskopie vom Computersystem entfernt wurden und nur gegen eine Geldzahlung von 1 Million Schweizer Franken zu-

rückgegeben werden (siehe Anhang Teil A.2 für die Beschreibung des Szenarios). Darauf aufbauend wurden die Teilnehmer gefragt:

- Für wie wahrscheinlich halten Sie dieses Szenario? Auf einer Skala von 1 (unwahrscheinlich) bis 10 (kommt häufig vor)
- Wie schätzen Sie die möglichen finanziellen Konsequenzen dieses Szenarios ein? Auf einer Skala von 1 (Bagatellrisiko) bis 10 (Katastrophe)

Das Ergebnis kann wieder im Rahmen eines zweidimensionalen Plots dargestellt werden (siehe Abbildung 14). In diesem Fall entspricht dies der Risk Map (siehe Abschnitt 3.2.4). Wiederum erhalten wir eine sehr grosse Streuung der Antworten. Manche halten das Szenario für sehr unwahrscheinlich und messen diesem eine geringe Relevanz bei. Andere Vertreter halten dies durchaus für möglich und sehen darin ein erhebliches Risiko für die Fortführung der Unternehmenstätigkeit. Die Einschätzung ist dabei sehr kontextabhängig: Für manche Unternehmen sind die Kundendaten das A und O (z. B. im Gesundheitswesen), während diese in anderen Bereichen keine derart essenzielle Rolle einnehmen (z. B. bei einer Pensionskasse). Insgesamt bestätigt damit auch die zweite Frage die sehr heterogene Einschätzung der KMU-Vertreter zu Umgang und Relevanz von Cyber Risk.

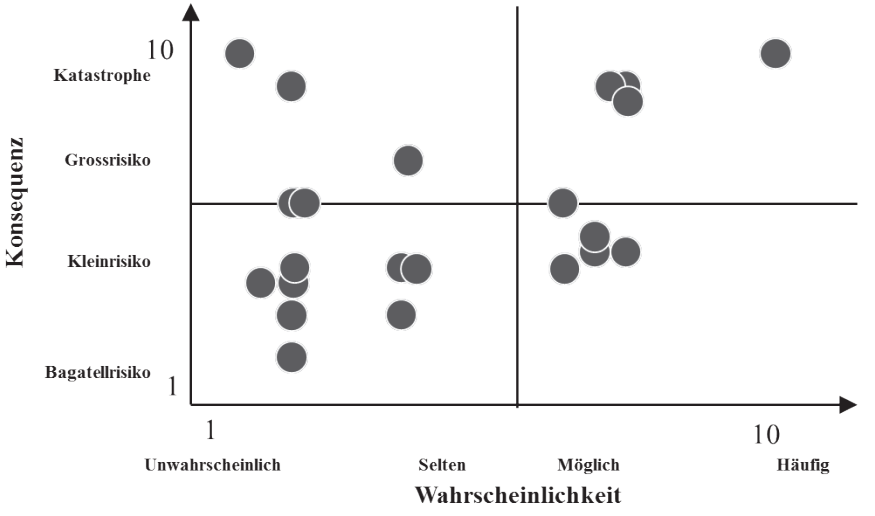


Abbildung 14: Ergebnisse der Befragung zur Konsequenz und Wahrscheinlichkeit eines beispielhaften Cyber-Risk-Vorfalls

5.7 Ableitung von fünf Thesen

Das Feedback potenzieller Kunden spiegelt viele Aspekte der obigen Diskussion zum Risikomanagement und zur Versicherbarkeit wider. So bestätigt sich etwa, dass die Preisgabe sensibler Daten ein echtes Hindernis bezüglich des Abschlusses einer Versicherung ist.

Auf Basis der Befragungsergebnisse wollen wir fünf zentrale Resultate in Thesenform ableiten:

1. Cyber Risk wird von Unternehmen als ernst zu nehmende Gefahr angesehen, deren Bedeutung in den kommenden Jahren weiter zunimmt.

2. Je grösser das Unternehmen, desto höher ist die Wahrscheinlichkeit, Ziel eines Cyberangriffs zu werden.

3. Banken sind häufiger Ziel von Cyberangriffen als andere Unternehmen des Finanzdienstleistungssektors.

4. Die meisten Unternehmen fühlen sich vor Cyber Risk gut geschützt und sehen noch nicht die unbedingte Notwendigkeit einer Cyber-Versicherung.

5. Sowohl die Nachfrage als auch das Angebot nach Versicherungslösungen zu Cyber Risk ist im deutschsprachigen Raum eher mässig.

6 Cyber Risk: Befragung aus Perspektive der Anbieter

6.1 Befragungsdesign und Methodik

Befragungsprozess
Nachdem wir in Kapitel 5 Cyber Risk aus der Sicht potenzieller Kunden analysiert haben, wollen wir nun auf die Sichtweise der Angebotsseite eingehen. Dazu haben wir in einer zweiten Marktbefragung die vier Versicherungsunternehmen angeschrieben, die Cyber-Versicherungen in der Schweiz anbieten. Alle vier Unternehmen haben an der Befragung teilgenommen, wobei, wie zuvor, sämtliche Daten anonymisiert behandelt werden.

Gliederung des Fragebogens
Die Befragung besteht aus vier Frageblöcken (siehe Anhang Teil B). In einem ersten Teil sollten die Befragten Cyber Risk definieren und die Bedeutung von Cyber Risk für sich selbst und den Kunden schätzen. Eine Einschätzung zur Marktentwicklung war Bestandteil von Abschnitt zwei. Die Cyber-Versicherungsprodukte des jeweiligen Unternehmens stehen in Teil drei im Fokus. Im letzten Teil des Fragebogens sollten Aussagen zum RM beim Kunden und zur Versicherbarkeit von Cyber Risk gegeben werden. Dafür wurden allgemeine Fragen zum Underwriting, zum Pricing und zur Risikoselektion bei Cyber-Versicherungen gestellt. Wir wollten speziell in diesem Bereich den Bezug zu den Diskussionen in Kapitel 3 und 4 dieser Studie herstellen.

Daten
Wie bereits beschrieben, umfassen unsere Befragungsergebnisse vier Antworten von Ansprechpartnern aus Unternehmen des schweizerischen Cyber-Versicherungsmarktes. Weitere Unternehmen, die zu dem Zeitpunkt der Befragung in der Schweiz spezielle Versicherungen gegen Cyber Risk angeboten haben, sind uns nicht bekannt gewesen.

Analyse
Bei der Analyse der Fragebögen in den folgenden Abschnitten werden wir wie in Kapitel 5 versuchen, die Gemeinsamkeiten der Aussagen bestmöglich zusammenzufassen und nur die markantesten Antworten ausführlich und individuell darzustellen. Besondere Aufmerksamkeit bei der Auswertung wollen wir aber auf die Antworten richten, die wichtige Hinweise zu unseren Themen in den zuvor diskutierten Kapiteln zum Risikomanagement und zur Versicherbarkeit liefern.

Wir beginnen mit den Ergebnissen zur Definition und der Bedeutung von Cyber Risk. Im zweiten Schritt wollen wir alle Informationen aus den Fragebögen zusammentragen, die sich auf das RM und den RM-Prozess beziehen und für Kapitel 3 zusätzlich wichtige Inhalte liefern. Darauf aufbauend wollen wir dann alle Antworten zu Versicherbarkeit von Cyber Risk besprechen und uns so auf Inhalte des Kapitels 4 beziehen. Abschliessend präsentieren wir noch Ergänzungen, die nicht direkt in einen der vorigen drei Bereiche passen.

6.2 Definition und Bedeutung von Cyber Risk

Definition Cyber Risk

Wie wir bereits in unserer ersten Befragung gesehen haben, liegt keine allgemeingültige Definition für Cyber Risk vor. In Kapitel 2 hatten wir aber auch schon gesehen, dass in der Literatur eine Vielzahl an Definitionen existiert. Dies bestätigt sich auch, wenn die Anbieter gefragt werden. Drei der vier Versicherer geben an, dass sie keine offizielle Definition für Cyber Risk hätten, darunter aber allgemein alle Risiken, die im Zusammenhang mit Daten, die auf Netzwerken, Datenträgern und Clouds gespeichert würden und vor unerlaubten / unerwünschten Zugriffen geschützt werden müssten, verstehen. Dazu zählten sie auch alle Risiken, die im Zusammenhang dazu und der zunehmenden Digitalisierung, dem Einsatz komplexer Technologien und der Vernetzung von Geschäftsprozessen entstehen könnten. Die genannten Aspekte sind wieder sehr nah an der Definition, die wir in Kapitel 2 in Anlehnung an Cebula und Young (2010) eingeführt haben.

Bedeutung von Cyber Risk

Wie in der Kundenbefragung haben wir auch die Versicherer nach der Bedeutung des Themas Cyber Risk befragt. Zum einen wollten wir wissen, wie sie Cyber Risk aus eigener Sicht bewerten und zum anderen wie aus ihrer Sicht die Kunden Cyber Risk wahrnehmen. Dazu sollten sie auf einer Skala von „sehr gering“ (Score 1) bis „sehr hoch“ (Score 5) je eine Einschätzung zum Zeitpunkt „vor 5 Jahren“, „heute“ und „in 5 Jahren“ vornehmen. Auf die Frage nach der Bedeutung für den Versicherer selbst waren sich alle Befragten einig. Alle schätzten die Bedeutung von Cyber Risk vor fünf Jahren als „mittel“, heute als „hoch“ und in fünf Jahren als „sehr hoch“ ein. Auch wenn sie eine Aussage über die Bedeutung für den Kunden geben sollten, gaben sie sehr ähnliche Antworten wie für sich selbst. Einziger Unterschied besteht darin, dass sie die Bedeutung „vor 5 Jahren“ und „heute“ etwas weniger hoch einschätzten.

Zusammenfassung

Die Marktbefragung unter den Versicherern ergibt, dass auch diese keine offizielle Definition für Cyber Risk verwenden, sich die Antworten aber wieder sehr gut mit den bisherigen Ausführungen decken. Für die Bedeutung des Risikos für den Kunden und für sich selbst schätzen sie Cyber Risk als sehr hoch ein und gehen davon aus, dass es in Zukunft auch noch steigen wird. Dies unterstreicht ein weiteres Mal die Bedeutung von Cyber Risk für die Zukunft.

6.3 Risikomanagement von Cyber Risk

Herausforderungen im Risikomanagement des Kunden
Wir haben konkret nach besonderen Herausforderungen im RM von Cyber Risk für die Kunden gefragt. Ein Problem, das die Versicherer im RM der Kunden sehen, hat im allgemeinen RM-Framework mit dem Thema „Kontext herstellen" zu tun. So sei bei vielen Kunden Cyber Risk noch nicht im Bewusstsein verankert. Dazu sei Cyber Risk „oftmals noch nicht richtig im RM eingebettet" und „noch nicht auf der Geschäftsleitungsstufe angekommen". Zudem fehle meist die „Verlinkung von IT-, Legal-, Risk- und Senior-Managementfunktionen". Zusätzlich wäre es wichtig, Verantwortlichkeiten zu schaffen.

Eine weitere Herausforderung sehen die Befragten im RM-Prozess selbst. Cyber Risk zu „identifizieren und [zu] quantifizieren" könnte für den Kunden ein Problem darstellen. Dies sei anders als bei den meisten anderen Unternehmensrisiken. Schliesslich wäre es wichtig, „Schutzmassnahmen kritisch und regelmässig [zu] hinterfragen". Die „ständige Evolution der (IT-)Risiken" stelle zudem ein Problem dar und erschwere es, „mit den neuesten Sicherheitsvorkehrungen immer up to date" zu bleiben. Ein Befragter wies auch explizit auf „Schwächen im Risikomanagement" hin, da „insbesondere die Bedrohungsmodellierung nur rudimentär vorhanden" sei.

Risk Map
Wie in Abschnitt 3.2.4 angedeutet, haben wir im Rahmen unserer Marktbefragung eine Risk Map ausfüllen lassen. Dazu hatten wir die Befragten gebeten, Cyber Risk aufgeteilt in:

1. Risiken durch höhere Gewalt
2. Risiken durch technisches Versagen
3. Risiken durch menschliches Versagen
4. Risiken durch physische Angriffe
5. Risiken durch gezielte Hackerangriffe
6. Risiken durch Erpressung
7. Risiken durch im Internet kursierende Malware

in eine Risk Map einzutragen. Eine genaue Beschreibung der Frage und der Kategorisierung kann im Anhang (Teil B) gefunden werden. Drei von unseren vier Versicherern haben eine solche Einteilung vorgenommen. Die Aggregation der Ergebnisse (geografische Mittelwerte der individuellen Antworten) wird in Abbildung 15 gezeigt.

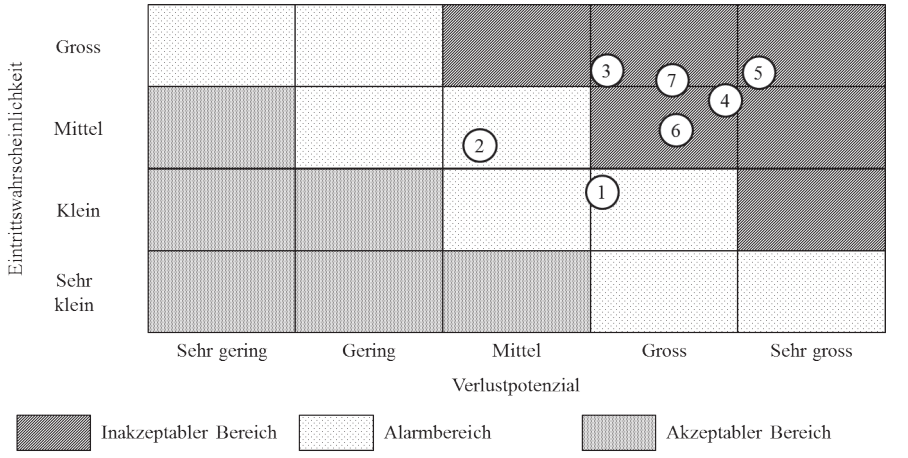


Abbildung 15: Befragungsergebnis zur Risk Map

Der Befragte, der keine Beurteilung zu dieser Frage abgab, hatte sich dennoch zu dem Thema geäussert und angegeben, dass Cyber Risk sich in den „Bereichen ‚mittel' bis ‚sehr gross' (Alarm- / Inakzeptabler Bereich der Risk Map)" befände. Diese Einschätzung deckt sich mit der Einschätzung der anderen Befragungsteilnehmer. Abbildung 15 zeigt, dass vor allem die Risiken, die einen kriminellen Hintergrund haben (Risikogruppen 4–7), als sehr schwerwiegend bezüglich Verlustpotenzial und Eintrittswahrscheinlichkeit eingeschätzt werden. Abbildung 15 zeigt aber auch, dass ein grosser Teil der Risiken in den Bereich fallen, der als „inakzeptabel" angesehen wird. Folglich sind Risikomanagementmassnahmen zur Beeinflussung der potenziellen Schadenwahrscheinlichkeit und Schadenhöhe erforderlich. Des Weiteren zählen unsere Befragten auch die Cyber Risk, die durch menschliches Versagen entstehen zum inakzeptablen Bereich.

Nur bei den Risiken „aus höherer Gewalt" (unter denen wir vor allem Naturkatastrophen zusammenfassen) und „aus technischem Versagen" fallen bei unseren Befragten in den „Alarmbereich". Dennoch zeigen sie mittel bis grosse Verlustpotenziale und kleine bis mittel hohe Eintrittswahrscheinlichkeiten und sollten somit nicht unterschätzt werden. Allgemein lässt sich aber aus der Befragung ableiten, dass unsere Befragten Cyber Risk für sehr wichtig halten und für die meisten Fälle Bedarf für eine Bewältigung besteht.

Effektivität von Risikomanagementmassnahmen

In einer weiteren Frage sind wir auf die Effektivität von möglichen RM-Massnahmen eingegangen. Dazu wollten wir von den Versicherern wissen, wie sie die Effektivität (Relation von Kosten und Nutzen) von drei möglichen RM-Massnahmen beim Kunden einschätzen. Dazu baten wir die Befragten, die Effektivität der jeweiligen Massnahme auf einer Skala von 1 („Sehr gering") bis 5 („Sehr hoch") abzuschätzen. Tabelle 17 zeigt die Resultate.

Massnahme	Durchschnittlicher Effektivitätsgrad
Schutz- und Sicherungsmassnahmen	4,25
Risikotransfer (Cyber-Versicherung)	4,25
Cyber Risk selbst tragen	2,00

Tabelle 17: Ergebnis zur Effektivität von RM-Massnahmen

Aus Sicht der Versicherer werden allgemeine Schutz- / Sicherungsmassnahmen und Risikotransfer durch Cyber-Versicherung als für den Kunden sehr effektiv angesehen (4,25 von 5 Punkten). Interessant ist, dass Selbsttragungsmassnahmen als relativ uneffektiv eingeschätzt werden (nur 2 von 5 Punkten). Dies dürfte vor allem mit den sehr hohen Verlusten zu tun haben, die bei Cyber Risk entstehen können und es so nicht rentabel sein kann, alle Verluste selbst zu tragen. Insofern ist davon auszugehen, dass eine Kombination aus Prävention (Schutz- und Sicherungsmassnahmen) und Risikotransfer die effektivste Form des Managements von Cyber Risk darstellt. Sicherlich ist in der Beurteilung der Effektivität die Tatsache zu berücksichtigen, dass hier Anbieter von Versicherungen befragt wurden. Insofern wäre ein deutlich schlechteres Urteil sehr überraschend gewesen. Dennoch erscheint die bezüglich Effektivität anvisierte Kombination aus Prävention und Risikotransfer auch aus theoretischer Sicht sinnvoll.

Zusammenfassung

Aus Sicht der Versicherer sind im RM der Kunden die institutionelle Verankerung und die Definition von Verantwortlichkeiten noch verbesserungsfähig. Weitere Schwachstellen werden in der Risikoidentifizierung und der adäquaten Überwachung von Cyber Risk genannt. Im Rahmen einer Risk Map werden nahezu alle Risiken aus Cyber Risk als „nicht akzeptierbar" bezeichnet, was die Notwendigkeit des RM unterstreicht. Zur Risikobewältigung wird dann eine Kombination aus Schutz- / Sicherungsmassnahmen und Risikotransfer empfohlen.

6.4 Versicherbarkeit von Cyber Risk

Einschätzung der Kriterien
Wir zeigen die Einschätzung der Versicherer zu den einzelnen Versicherbarkeitskriterien. Dazu wollten wir von den Befragten wissen, für wie problematisch sie die Erfüllung eines jeden Kriteriums einschätzen. Die Erfüllung des jeweiligen Versicherbarkeitskriteriums wurde auf einer Skala von 1 („Kein Problem“) bis 5 („Grosses Problem“) abgefragt. Die Ergebnisse der Antworten sind in Tabelle 18 zusammengefasst.

Versicherbarkeitskriterien	**Mittelwert** (Standardabweichung)
Versicherungsmathematisch:	
Zufälligkeit des Schadenereignisses	3,50 (1,00)
Maximal möglicher Schaden	3,50 (1,29)
Mittlere Schadenhöhe (severity)	3,75 (0,96)
Mittlere Schadenhäufigkeit (frequency)	2,75 (0,96)
Informationsasymmetrien	3,25 (0,50)
Marktbezogen:	
Versicherungsprämie	3,50 (0,58)
Deckungsabgrenzungen	3,00 (0,82)
Gesellschaftsbezogen:	
Gesellschaftliche Werte	1,50 (0,58)
Gesetzliche Schranken	1,75 (0,50)

Tabelle 18: Ergebnis zur Erfüllung der Versicherbarkeitskriterien

Die wenigsten Probleme sehen die Befragten bei den gesellschaftsbezogenen Kriterien. Hier zeigt sich auch ein relativ grosser Konsens zwischen den Befragten, gemessen an einer relativ geringen Standardabweichung der Befragungsresultate. Die grössten Probleme sehen die Befragten (im Unterschied zu unserer Evaluation in Kapitel 4) bei der mittleren Schadenhöhe bei Schadeneintritt. Ferner erachten die Befragten die Kriterien der Zufälligkeit des Schadenereignisses, des maximal möglichen Verlusts und der Versicherungsprämie als sehr problematisch.

Deckungsgrenzen
Wie bereits in Abschnitt 4.3.7 angesprochen, führen sehr komplexe Vertragsdetails bei Cyber-Versicherungen – zu denen auch die Deckungsgrenzen zählen – dazu, dass Unternehmen sehr zurückhaltend sind beim Kauf von Cyberprodukten, aber auch denken, dass sie bereits gut durch ihre Sach- / Haftpflichtversicherung abgedeckt sind (siehe ENISA, 2012). Diesem Problem begegnen unsere Befragten damit, dass sie ein Produkt mit modularer Struktur anbieten, bei dem die Deckung vom Kunden gewählt werden kann, die Intensität der Risikobeurteilung dann aber von der gewählten Deckung abhängt. Diese Beurteilung hat wiederum Einfluss auf mögliche Deckungslimiten.

Im Zusammenhang mit möglichen Deckungsgrenzen haben wir bereits viele Informationen beim Überblick über Versicherungsprodukte in der Schweiz erläutert (Abschnitt 4.2.2). Dennoch wollen wir hier nochmals die Antworten der Befragten aufzeigen. Bei den Deckungslimiten werden im Allgemeinen Werte von 10–25 Millionen Schweizer Franken als Obergrenzen genannt, obwohl auch darauf hingewiesen wird, dass die Deckungsgrenzen je nach Risi-

ko, Produktvariante und je nach Grösse des zu versichernden Unternehmens variieren können. Somit können auch in Ausnahmefällen höhere Limiten vergeben werden, was aber nicht der Standard ist. Zudem werden Sub-Limiten für bestimmte Kosten vorgegeben, z. B. Verteidigungskosten.

Deckungsausschlüsse kommen vor allem zum Zuge bei:

- Vorsätzlicher Pflichtverletzung / Schadenverursachung
- Schäden aus der Verwendung von ungetesteten Programmen
- Schäden aus einer Netzwerkunterbrechung ausserhalb der Kontrolle des Versicherten.

Versicherbarkeit bestimmter Kundengruppen
Alle Versicherer nennen auch Einschränkungen bezüglich der Kundengruppen, die sie nicht versichern. Beispiele sind:

- Online-Trading, Online-Gambling
- Credit Card Companies, Credit Card Payment Processors
- Data Aggregators, Data Warehouses, Web / Cloud Hoster
- Technology Service Providers
- Unternehmen der Luftraumüberwachung

Diese Beispiele beschreiben Kundengruppen, bei denen Cyber-Risk-Vorfälle sehr schnell hohe Verluste verursachen könnten.

Selbstbehalt
Neben Deckungsgrenzen und Ausschlüssen werden normalerweise zur Erfüllung des Versicherbarkeitskriteriums der Deckungsabgrenzung in den Verträgen Selbstbehalte definiert. Es wird darauf verwiesen, dass die vereinbarte Franchise sehr stark von der gewählten Deckungssumme und dem Risikoprofil sowie der Grösse und dem Umsatz des Versicherungsnehmers abhängt und so keine allgemeinen Aussagen zur Höhe getroffen werden können. Dennoch werden Mindestselbstbehalte in Höhe von 5‘000–25‘000 Schweizer Franken angegeben, die aber dann zusätzliche Wartefristen enthalten können. Ein prozentualer Selbstbehalt ist allerdings nicht üblich, kann aber dennoch in Einzelfällen vereinbart werden.

Zusätzliche Richtlinien und Anforderungen
In unserer Marktbefragung haben wir nach Richtlinien und Anforderungen an die Produkte gefragt, die für die Zulassung am Markt erfüllt sein müssen. Ein Befragter deutete an, dass es speziell für den US-amerikanischen Markt Besonderheiten gibt, ging aber nicht auf Details ein. Ein weiterer Teilnehmer führte an, dass in „nicht allen Ländern Bussen und Geldstrafen“ versichert werden dürften. Für diesen Punkt hätten sie in ihren Allgemeinen Vertragsbedingungen aber vorgesorgt.

Zusammenfassung
Hinsichtlich der Versicherbarkeit erachten die Marktteilnehmer neben den mittleren Schadenhöhen bei Schadeneintritt das Kriterium der Zufälligkeit, des maximal möglichen Verlusts und der Versicherungsprämie als problematisch. Versicherer schützen sich durch bestimmte Risikoausschlüsse etwa hinsichtlich der Kundengruppen.

6.5 Zusätzliche Informationen aus der Befragung

Marktentwicklung
Es sind nur relativ wenige Fakten zur Entwicklung der Cyber-Versicherung verfügbar. Um diese Lücke zu schliessen, haben wir versucht, weitere Informationen zur Marktentwicklung zu erheben. Leider konnten uns hier nur zwei von vier Befragten Informationen zur Verfügung stellen. Dies bestätigt erneut die Schwierigkeit, entsprechende Marktdaten zu erhalten. Die zwei verbleibenden Versicherer schätzen das Marktvolumen weltweit aktuell auf 0,9–1,5 Milliarden Schweizer Franken und für Europa aktuell auf 140–350 Millionen Schweizer Franken. Diese Einschätzungen decken sich in etwa mit der Einschätzung für Europa und weltweit, die wir in Kapitel 4 aufgezeigt haben. Zudem war es möglich, Marktvolumina für die Schweiz zu erhalten. So wird das Marktvolumen für Cyber-Versicherungen in der Schweiz aktuell auf lediglich fünf Millionen Schweizer Franken geschätzt.

Gefragt nach dem geschätzten Volumen der Cyber-Versicherung in fünf Jahren gaben die Befragten an, dass sich das Volumen weltweit und auch in Europa vermutlich verdoppeln bis verdreifachen wird. Für die Schweiz gehen die Befragten sogar davon aus, dass sich das Marktvolumen in den nächsten fünf Jahren vervierfacht bzw. sogar verzehnfachen wird. Dies offenbart sowohl weltweit und in Europa – und vor allem für die Schweiz – enorme Wachstumsmöglichkeiten. Zu einer Einschätzung, welches Volumen Cyber-Risk-Geschäft im eignen Unternehmen einnimmt, war keiner der Befragten bereit, Auskunft zu geben. In diesem Zusammenhang gab ein Versicherer[49] an: „Da es sich in Europa und besonders in der Schweiz um einen noch sehr jungen Markt handelt, werden in Zukunft sicherlich noch einige Anpassungen an den Cyber-Versicherungsprodukten vorgenommen werden müssen. Als einer der Hauptdriver für den Verkauf von Cyber-Versicherungen sehen wir die neue EU-Datenschutzverordnung, durch die ein grösseres Schadenpotenzial für die Unternehmen, die geschützte Personendaten verarbeiten und speichern, entsteht. Wir erwarten, dass diese Entwicklung analog zum amerikanischen Markt verlaufen wird. Dort wurden die Cyber-Versicherungen ab Einführung von sog. Notification Rules in div. Staaten in grosser Anzahl verkauft.“ Auch diese Aussage deutet für die Schweizer Versicherungsbranche einen Wachstumsschub an und zeigt, dass Cyber Risk ein Versicherungsmarkt der Zukunft ist.

Pricing
Auch zum Pricing von Cyber Risk haben wir spezifische Fragen gestellt. So gaben drei der vier Befragten auf die Frage „Was für ein Pricing-Verfahren angewendet wird“ an, dass sie ein aktuarielles Standardverfahren, wie z. B. das Erwartungswertprinzip oder das Varianzprinzip, verwenden. Einer der Befragten erklärte, dass sie mit einem anderen Verfahren, das je nach Produktvariante unterschiedlich ist, arbeiten.

Zudem wollten wir von den Befragten wissen, von welchen Parametern und in welchem Masse ihr Pricing abhängt. Dazu sollte eine vorgegebene Palette von Merkmalen von 1 („Sehr gering“) bis 5 („Sehr hoch“) eingestuft werden. Das zusammengefasste Ergebnis findet sich in Tabelle 19:

[49] Auf Wunsch der Befragten heben wir hier die Anonymisierung auf und bedanken uns nochmals bei Frau Marie-Fleur Auf der Maur (Zürich Versicherungs-Gesellschaft AG) für diese Anmerkung.

Pricing-Parameter	**Mittelwert** (Standardabweichung)
Versicherungssumme	4,50 (0,50)
Deckungsgrenzen (Selbstbehalt und Limiten)	4,25 (0,83)
Grösse des Unternehmens	4,25 (0,43)
Branche	4,50 (0,87)
Vorhandene Sicherheitsmassnahmen	4,75 (0,43)
Historie	4,00 (0,71)
Geschäftsmodell (z. B. E-Commerce)	5,00 (0,00)
Geografische Gegebenheiten / Lage	2,75 (0,83)
Qualität der bestehenden IT	4,75 (0,43)

Tabelle 19: Ergebnisse zu Pricing-Parametern

Bei den Parametern in Tabelle 19 wird das Geschäftsmodell als der wichtigste Parameter für das Pricing genannt. Dies spiegelt sich auch in der Einheitlichkeit der Meinung wider (Standardabweichung von Null). Geografische Lage / Gegebenheiten sind dagegen nicht ganz so wichtig. Es sollte aber bei diesem Punkt angemerkt werden, dass wir die Befragten nach ihrer Einschätzung für die Schweiz befragt haben. Wenn man geografische Lage global versteht, könnte durchaus ein anderes Ergebnis auftreten (z. B. der Abschluss einer Versicherung in den USA hat eventuell eine höhere Prämie zur Folge als in Europa, da Rechtsprechung unterschiedlich hart sein kann). Alle weiteren angegebenen Parameter werden zwischen „Hoch" bis „Sehr hoch" eingeschätzt. Interessant ist, dass in dieser Gruppe der Parameter „Historie" noch am wenigsten wichtig erscheint. Dies ist überraschend, da doch vergangene Cyber-Risk-Vorfälle einen guten Indikator für Anfälligkeit bieten sollten. Des Weiteren war die Möglichkeit gegeben, zusätzliche Punkte zu nennen, bei denen die „Länge der Wartefrist bei Betriebsunterbruch" und der „Umfang sensitiver Daten" als sehr wichtig mit angegeben wurden.

Final sollten dann noch Einschätzungen zu Risiken, die beim Pricing von Cyber-Versicherungen Einfluss haben könnten, abgegeben werden (Ergebnisse siehe Tabelle 20; Einstufung von 1 bis 5 entspricht „Sehr gering" bis „Sehr hoch"):

Risiko	**Erklärung**	**Mittelwert** (Standardabweichung)
Zufallsrisiko	Volatilität der historischen Schadenquoten	4,00 (0,00)
Änderungsrisiko	Natur der versicherten Risiken ändert sich; verläuft anders als auf Basis historischer Daten erwartet	4,33 (0,94)
Irrtumsrisiko	Risiko einer falschen Kalkulation, z. B. aufgrund falsch oder mangelhafter historischer Daten	3,33 (0,94)
Risiko aus Informationsasymmetrien	Schaden verläuft anders, da die Kunden ihr Verhalten ändern	3,00 (0,00)

Tabelle 20: Einschätzung zu Risiken beim Pricing

Die Beurteilung in Tabelle 20 beruht auf den Ergebnissen von nur drei Befragten, da ein Befragter keine Angaben machen konnte mit der Begründung, dass sie noch Erfahrungen sammeln müssten. Alle vier Risiken werden von den Befragten als mittel bis hoch eingeschätzt.

Aus diesem Ergebnis lassen sich aber vor allem wichtige Implikationen für die zuvor besprochenen Punkte in Kapitel 4 ableiten. So stellt das Änderungsrisiko, vor allem bei den Versicherbarkeitskriterien der Zufälligkeit der Schadenereignisse und der gesetzlichen Schranken, ein grosses Problem dar, was auch von den Versicherern hier so gesehen wird. Das Ergebnis für Risiken aus Informationsasymmetrien hingegen spiegelt in gewisser Weise das Ergebnis aus Tabelle 18 wider.

6.6 Ableitung von fünf Thesen

Auf Basis der Befragungsergebnisse wollen wir wiederum fünf zentrale Resultate in Thesenform ableiten:

1. Das Management von Cyber Risk ist in Unternehmen noch unterentwickelt und bedarf erheblicher Verbesserungen.

2. Auf einer Risk Map werden nahezu alle Risiken aus Cyber Risk als „nicht akzeptierbar“ bezeichnet, was die Notwendigkeit des RM unterstreicht.

3. Eine Kombination aus Prävention (Schutz- und Sicherungsmassnahmen) und Risikotransfer (Versicherung) wird als effektivste Form des Managements von Cyber Risk angesehen.

4. Das Volumen des Cyber-Versicherungsmarkts wird in der Schweiz lediglich auf fünf Millionen Schweizer Franken geschätzt.

5. Die Befragten gehen davon aus, dass sich der Cyber-Versicherungsmarkt in der Schweiz in den kommenden fünf Jahren vervierfachen bis sogar verzehnfachen wird.

Folglich ist zu erwarten, dass der Cyber-Versicherungsmarkt in den kommenden fünf Jahren deutlich wachsen wird.

7 Fazit

Noch nie war Cyber Risk so präsent wie heute. Mittlerweile ist Cyber Risk ein bedeutsames ökonomisches und gesellschaftspolitisches Thema. Trotz der enormen medialen Präsenz, die das Thema momentan hat, fühlen sich viele Unternehmen dennoch relativ gut vor Cyber Risk geschützt. Bei der Befragung, die im Rahmen dieser Studie durchgeführt wurde, waren es sogar 88 % der Unternehmen. Bei der Hälfte der befragten Unternehmen handelt es sich um mittlere bis grosse Betriebe, die einen erheblichen Aufwand zum Schutz vor Cyber Risk betreiben. Doch reicht dieser Aufwand, um vor Cyber Risk ausreichend geschützt zu sein? Die Vorfälle der letzten Jahre beweisen das Gegenteil, etwa wenn ein multinationaler Elektronikkonzern wie Sony, ein mit massivsten Mitteln und unter grösster Geheimhaltung geführtes Atomkraftwerk oder auch das FBI Opfer von Cyberangriffen waren.

Durch die rasante technologische Entwicklung muss auch der Risikomanagement-Prozess fortlaufend angepasst werden. Dabei reicht es nicht, sich ausschliesslich mit Software vor Cyber Risk zu schützen. Von besonderer Bedeutung ist die Schulung und Sensibilisierung der Mitarbeiter betreffend Cyber Risk, denn menschliches Fehlverhalten ist die Hauptquelle von Cyber Risk. Auch ein effektives Krisenmanagement ist eine wichtige Voraussetzung für einen guten Umgang mit Cyber Risk. Eine weitere wichtige Erkenntnis der Arbeit ist, dass für ein erfolgreiches Risikomanagement bereits die institutionelle Verankerung des Themas Informationssicherheit zentral ist. Denn Unternehmen, die einen Chief Information Security Officer (CISO) oder eine ähnliche Funktion installiert haben, weisen im Falle eines Datenverlusts signifikant niedrigere Kosten auf. Folglich sollten Unternehmen entsprechende Verantwortlichkeiten für Informationssicherheit definieren. Weitere empirische Belege zeigen, dass durch ein effizientes Risikomanagement die Wahrscheinlichkeit und das Ausmass eines Cyber-Risk-Schadens signifikant gesenkt werden kann. Der Aufwand für Risikomanagement lohnt sich also.

Eine Möglichkeit, sich vor Cyber Risk zu schützen, ist der Risikotransfer mittels Versicherung. In der Schweiz ist das Angebot zurzeit noch vergleichsweise gering und teilweise auf gewisse Unternehmensgrössen und Branchen beschränkt. Allerdings sind die Versicherer bereit, auch massgeschneiderte Produkte zum Schutz vor Cyber Risk zu entwickeln. Dennoch gibt es erhebliche Probleme der Versicherbarkeit, die die Marktentwicklung hemmen: Während Datenwiederherstellungs-, Prozess-, Strafverfolgungskosten etc. von vielen Versicherungen gedeckt sind, werden nicht direkt zurechenbare Kosten, die zum Beispiel durch Reputationsschäden verursacht werden, bislang kaum versichert. Da Cyber Risk ein relativ neues Risiko darstellt, stehen noch nicht viele historische Daten zur Verfügung. Des Weiteren sind bei Cyber Risk auch nicht immer Zufälligkeit und Unabhängigkeit gegeben, sodass der Ausgleich im Kollektiv eventuell nicht gut funktioniert. Für das Versicherungsunternehmen ist es wichtig, Grenzen in der Deckung zu ziehen, um sich vor unkalkulierbar hohen Schadenzahlungen abzusichern. Dies führt zu grossen Unklarheiten bezüglich der tatsächlichen Deckung im Schadenfall. Auch treten versicherungsspezifische Probleme wie Adverse Selektion und Moral Hazard auf. Diese Probleme können nur mittels genauer Prüfung des Versicherungsnehmers und über Selbstbehalte entschärft werden.

Betreffend der Nachfrage nach Cyber-Risk-Produkten ergab sich bei der Befragung ein gemischtes Ergebnis: Knapp 31 % der Befragten gaben an, eine Cyber-Versicherung zu besitzen.[50] Die Preisgabe sensibler Informationen scheint ein wichtiges Argument gegen den Abschluss einer Cyber-Versicherung zu sein. Tabelle 21 fasst die Kernresultate unserer Befragung unter (potenziellen) Kunden und Anbietern der Cyber-Versicherung zusammen.

Kundensicht	**Anbietersicht**
• Cyber Risk wird von Unternehmen als ernst zu nehmende Gefahr angesehen, deren Bedeutung in den kommenden Jahren weiter zunimmt. • Je grösser das Unternehmen, desto höher ist die Wahrscheinlichkeit, Ziel eines Cyberangriffs zu werden. • Banken sind häufiger Ziel von Cyberangriffen als andere Unternehmen des Finanzdienstleistungssektors. • Die meisten Unternehmen fühlen sich vor Cyber Risk gut geschützt und sehen noch nicht die unbedingte Notwendigkeit einer Cyber-Versicherung. • Sowohl die Nachfrage als auch das Angebot nach Versicherungslösungen zu Cyber Risk ist im deutschsprachigen Raum eher mässig.	• Das Management von Cyber Risk ist in Unternehmen noch unterentwickelt und bedarf erheblicher Verbesserungen. • Auf einer Risk Map werden nahezu alle Risiken aus Cyber Risk als "nicht akzeptierbar" bezeichnet, was die Notwendigkeit des RM unterstreicht. • Eine Kombination aus Prävention (Schutz- und Sicherungsmassnahmen) und Risikotransfer (Versicherung) wird als effektivste Form des Managements von Cyber Risk angesehen. • Das Volumen des Cyber-Versicherungsmarkts wird in der Schweiz lediglich auf fünf Millionen Schweizer Franken geschätzt. • Die Befragten sagen, dass sich der Cyber-Versicherungsmarkt in der Schweiz in den nächsten fünf Jahren vervierfachen oder sogar verzehnfachen wird.

Tabelle 21: Kernresultate der Marktbefragungen

Abschliessend wollen wir in Tabelle 22 die Argumente für und gegen den Abschluss einer Cyber-Versicherung überblicksartig darstellen.

[50] Dies beinhaltet aber nicht zwingend Stand-alone-Cyber-Versicherungen, sondern enthält auch Verträge die durch bestehende Sach- / Haftpflichtversicherungen abgedeckt sind (z. B. Schutz vor Schäden an technischen Einrichtungen).

Pro Cyber-Versicherung	**Kontra** (= Grenzen der Versicherbarkeit)
Allgemein	
• Hohe ökonomische Relevanz und hohe Aufmerksamkeit der Medien macht Cyber-Risk-Management und damit auch die Prüfung der Cyber-Versicherung unabdinglich. • Gesetzliche Vorgaben zur Auseinandersetzung mit Cyber Risk (etwa regulatorische Offenlegungspflichten) können einen Druck zum Abschluss der Cyber-Versicherung bewirken.	• Hohes, schwer messbares Schadenpotenzial mit erheblichen Änderungsrisiken treibt Preise der Policen in die Höhe. • Hoher Aufwand schon vor Vertragsabschluss (Vorabprüfungen). • Die Deckung ist häufig sowohl für Käufer wie auch für Verkäufer nicht ganz klar definiert; dies führt zu Unsicherheiten, ob im Schadenfall eine Zahlung erfolgt.
Aus Kundensicht	
• Cyber-Versicherung stellt grundsätzlich eine sinnvolle Ergänzung im bestehenden RM-Mix dar. • Schutz vor unvorhersehbaren Risiken und Zugang zu weiteren Services (insbesondere im Bereich der Prävention). • Sensibilisierung der eigenen Mitarbeiter für Cyber Risk (schon durch Vorabprüfungen).	• Preisgabe sensibler Informationen notwendig. • Indirekte Kosten können zumeist nicht gedeckt werden (z. B. Reputationseffekte). • Noch relativ wenige Produkte sind verfügbar und werden als relativ teuer erachtet. • Relativ geringe Zahl von Anbietern, wenig Wettbewerb.
Aus Anbietersicht	
• Relativ geringe Zahl von Anbietern, wenig Wettbewerb.	• Abhängigkeiten bei Cyber Risk erschweren den Ausgleich im Kollektiv. • Adverse Selektion treibt Prämien in die Höhe (nur Unternehmen mit einem hohen Risiko schliessen Versicherung ab). • Moral Hazard treibt Prämien in die Höhe (mit Versicherung Anreize zu weniger Prävention). • Unsicherheit bzgl. der Einschätzung der Risikoart kann Hemmschwelle sein, z. B. im Vertrieb. • Produkte können nur durch wenige Spezialisten vertrieben werden; hier herrscht ein Mangel.

Tabelle 22: Pro und Kontra der Cyber-Versicherung

Bei einer reinen Gegenüberstellung der Pro- und Kontra-Argumente scheint heute noch das Kontra zu überwiegen. Dennoch darf nicht übersehen werden, dass Faktoren, die heute die Marktentwicklung hemmen, morgen schon ganz anders aussehen können. So werden mit zunehmender Marktentwicklung die Risikokollektive grösser; der Ausgleich im Kollektiv gelingt besser und es stehen zugleich mehr Daten zur Verfügung. Eine Reihe von neuen Wettbewerbern ist in den Markt eingestiegen oder plant, dies zu tun. Dies wird die Verfügbarkeit

und den Wettbewerb erhöhen und die Preise reduzieren. Vor dem Hintergrund unserer Resultate erscheint es ferner wichtig, gewisse Standards in Bezug auf Deckungsgrenzen oder Vorabprüfungen zu etablieren; dies könnte helfen, weitere Probleme der Versicherbarkeit zu verringern. Insofern lässt sich ein positiver Ausblick für die Entwicklung der Cyber-Versicherung geben.

Anhang

Teil A: Fragenkatalog für die Marktbefragung in Kapitel 5 (Kundensicht)

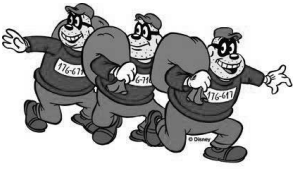
A.1. Interviews mit 16 Unternehmen der Finanzdienstleistungsindustrie (Interview-Leitfaden)

Zur Befragung von Cyber Risk und Cyber-Versicherung aus Perspektive der Kunden haben wir Interviews durchgeführt und den folgenden Fragenkatalog zugrunde gelegt. Die einzelnen Interviews sind entlang dieser Guideline durchgeführt worden und mögen in bestimmten Bereichen vom tatsächlichen Ablauf abweichen. Dennoch wurde darauf geachtet, dass möglichst alle Fragen im Fragenkatalog beantwortet wurden.

1. Grundangaben zur befragten Person: Funktion, Branche des Unternehmens, Anzahl Mitarbeiter im Unternehmen
2. Wie würden Sie Cyber Risk definieren?
3. Welche Bedeutung hat das Thema Cyber Risk für das Unternehmen, in dem Sie arbeiten?
4. Wie würden Sie die Bedeutung von Cyber Risk in der Zukunft schätzen?
5. Wie schützt Ihr Unternehmen Daten?
    a. Vor Naturkatastrophen (Gebäude)?
    b. Vor physischer Spionage / Sabotage (vor eigenen Mitarbeitern oder Externen)?
    c. Vor Hackerangriffen?
6. Ist das Unternehmen Ihrer Meinung nach gut vor Cyber Risk geschützt?
7. Welches Risikobewusstsein in Bezug zu Cyber Risk vermittelt Ihr Unternehmen den Angestellten?
8. Hatte das Unternehmen in der Vergangenheit schon Datenausfälle oder wurde es bereits Opfer eines Hackerangriffes oder Datendiebstahls?
    a. Falls Ja, in welcher Form und in welchem Ausmass?
9. Ist Ihr Unternehmen in irgendeiner Form gegen Cyber Risk versichert?
    a. Falls Ja, in welchem Umfang?
    b. Falls Nein, denken Sie, dass Ihr Unternehmen innerhalb der nächsten 5 Jahre eine Versicherung abschliesst, die Ihr Unternehmen vor Cyber Risk schützt?

A.2. Szenario im Rahmen des Workshops mit 22 Vertretern von KMUs

Sie erhalten folgende E-Mail



Sehr geehrte Damen und Herren

Wir haben Ihre gesamten Kundendaten inkl. der Sicherungskopie von Ihrem Computersystem entfernt. Gegen eine Geldzahlung von 1 Million Schweizer Franken erhalten Sie diese umgehend zurück. Wenn Sie die Polizei einschalten, veröffentlichen wir die Daten im Internet.

Mit freundlichen Grüssen

Ihre Panzerknacker

A. Relevanz des Szenarios für Ihr Unternehmen:

Für wie wahrscheinlich halten Sie dieses Szenario?

1 10

(unwahrscheinlich) (selten) (möglich) (häufig)

Wie schätzen Sie die möglichen finanziellen Konsequenzen dieses Szenarios ein?

1 10

(Bagatellrisiko) (Kleinrisiko) (Grossrisiko) (Katastrophe)

B. Umgang mit dem Szenario in Ihrem Unternehmen

1 10

(wenig professionell, verbesserungsfähig) (sehr professionell, optimaler Umgang)

Mögliche Fragen in diesem Zusammenhang:

- Haben Sie einen klar definierten Ablaufplan für ein solches Szenario? Haben Sie Zuständigkeiten eindeutig definiert?
- Haben Sie bereits in Ihrem Unternehmen die möglichen finanziellen Konsequenzen eines solchen Szenarios eingeschätzt?

Teil B: Fragenkatalog für die Marktbefragung in Kapitel 6 (Anbietersicht)

Die Marktbefragung, die wir im Rahmen dieser Studie durchgeführt haben, enthielt den folgenden Fragebogen. Der Fragebogen umfasste vier Fragenblöcke die im Folgenden kurz dargestellt werden.

Block I: Definition und Bedeutung von Cyber Risk

a. Was verstehen Sie unter Cyber Risk? Welche Definition verwenden Sie?

b. Welche Bedeutung messen Sie als Versicherer dem Thema Cyber Risk bei?

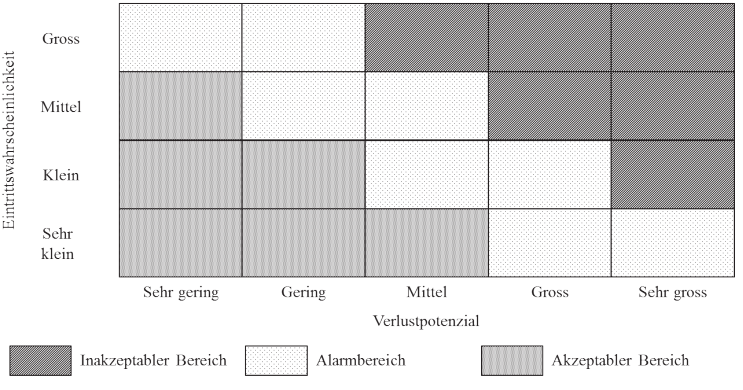
	Bedeutung für Sie als Versicherer				
Zeitpunkt	Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Vor 5 Jahren	☐	☐	☐	☐	☐
Heute	☐	☐	☐	☐	☐
In 5 Jahren	☐	☐	☐	☐	☐

c. Wie wird Cyber Risk von Ihren Kunden wahrgenommen?

	Bedeutung für den Kunden				
Zeitpunkt	Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Vor 5 Jahren	☐	☐	☐	☐	☐
Heute	☐	☐	☐	☐	☐
In 5 Jahren	☐	☐	☐	☐	☐

d. Wir definieren Cyber Risk als: „Risiko, das von Informationen ausgeht, die auf Datenträgern und Netzwerken gespeichert sind“ und teilen diese in kriminelle und nicht kriminelle Kategorien ein. Die folgende Abbildung zeigt eine Risk Map, mit deren Hilfe Risiken bewertet werden (die X-Achse zeigt das Verlustpotenzial und die Y-Achse die jeweilige Eintrittswahrscheinlichkeit). Wie beurteilen Sie die nachfolgenden Risiken in der Risk Map?

1	**Cyber Risk durch höhere Gewalt** (z. B. Stromausfall nach Naturkatastrophen, Zerstörung von Servern oder Computern bei Überschwemmung etc.)	5	**Cybercrime durch gezielten Hackerangriff** (z. B. Kundendaten spionieren oder Betriebe sabotieren, Lahmlegen von Systemen mittels DoS- bzw. DDoS-Attacken; Installation eines Keyloggers)
2	**Cyber Risk durch technisches Versagen** (z. B. Hardwareversagen, Datenverlust durch Headcrash von Festplatten oder Computerabsturz, Softwarefehler)	6	**Cybercrime durch Erpressung** (z. B. Drohung via Internet, z. B. Anonymous vs. Sony, mexikanisches Drogenkartell)
3	**Cyber Risk durch menschliches Versagen** (Versehentliches Veröffentlichen von Informationen, Falschmeldungen)	7	**Cyber Risk / -crime durch im Internet kursierende Malware** (Virus, Wurm, Spam-Mails, Trojanisches Pferd, Ransomware)
4	**Cybercrime durch physischen Angriff** (physischer Datendiebstahl, z. B. LGT Bank)	8	_____



Nehmen Sie bitte eine Einschätzung zu Verlustpotenzial und Wahrscheinlichkeit vor und ordnen Sie dazu die in der Tabelle genannten Bedrohungen der Risk Map zu (bitte die Zahlen in die Grafik einzeichnen). Ergänzen Sie ggfs. weitere Risiken oder Bedrohungen (Punkt 8, gerne auch weitere Punkte ergänzen).

Block II: Marktentwicklung

a. Auf welches Volumen schätzen Sie den Markt für Cyber-Versicherungen aktuell und in 5 Jahren (in CHF)?

Zeitpunkt	Heute (CHF)	In 5 Jahren (CHF)
Schweiz		
Europa (inklusive Schweiz)		
Weltweit (inklusive Europa)		

b. Welches Volumen hat das Geschäft mit Cyber Risk aktuell in Ihrem Haus (in CHF)? Wie sieht Ihre Prognose für in 5 Jahren aus?

Zeitpunkt	Heute (CHF)	In 5 Jahren (CHF)
Schweiz		
Europa (inklusive Schweiz)		
Weltweit (inklusive Europa)		

Block III: Cyber-Versicherungsprodukte

a. Bieten Sie ein oder mehrere Cyber-Versicherungsprodukte an? ☐ eins ☐ mehrere (Anzahl ___)

b. Werden in den Produkten ein oder mehrere Risiken abgesichert? ☐ eins ☐ mehrere

c. Welche Risiken werden in Ihren Produkten versichert?

Eigenschäden

☐ Kosten durch Betriebsunterbruch
☐ Cyber Extortion
☐ Veruntreuung von Vermögenswerten
☐ Kosten für Datenwiederherstellung
☐ Crisis Management Services
☐ Reputationsverlust
☐ Zahlung von Bussgeldern
☐ Andere:_____

Ansprüche Dritter (Haftpflicht)

☐ Ansprüche aus Verletzung von Datenschutzbestimmungen
☐ Kosten für Datenwiederherstellung
☐ Kosten für Vermögensschäden (z. B. Virus, der versehentlich an Drittsystem weitergegeben wird)
☐ Andere:_____

a. Bieten Sie standardisierte Produkte oder individuelle Versicherungslösungen an?
☐ Standardisiert ☐ Individuell ☐ Beides

b. Bieten Sie Versicherungen speziell für Cyber Risk oder nur in Verbindung mit bestehenden Sach- / Haftversicherungen an?
☐ Speziell ☐ Im Verbund ☐ Beides

c. Bieten Sie ausschliesslich Produkte in commercial lines (Firmen) oder auch in private lines (Privatkunden) an?

☐ Commercial ☐ Private ☐ Beides

d. Worin unterscheiden sich Ihre Produkte von denen der Konkurrenz?

e. Gibt es Richtlinien / Anforderungen an die Produkte, die (evtl. auch länderspezifisch) erfüllt sein müssen?

f. Aus welchen Branchen kommen Ihre Kunden typischerweise? Gibt es Schwerpunkte?

g. Welche Grösse haben Ihre Kunden typischerweise? Eher global tätige oder auch regional operierende Kunden?

Block IV: Risk Management und Versicherbarkeit von Cyber Risk (Underwriting, Pricing, Risikoselektion)

a. Wie funktioniert das Pricing von Cyber Risk?

b. Von welchen Parametern hängt das Pricing ab und wie stark?

	Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Versicherungssumme	☐	☐	☐	☐	☐
Deckungsgrenzen (Selbstbehalte und Limiten)	☐	☐	☐	☐	☐
Grösse des Unternehmens	☐	☐	☐	☐	☐
Branche	☐	☐	☐	☐	☐
Vorhandene Sicherungsmassnahme	☐	☐	☐	☐	☐
Historie	☐	☐	☐	☐	☐
Geschäftsmodell (z. B. E-Commerce)	☐	☐	☐	☐	☐
Geografische Gegebenheiten / Lage	☐	☐	☐	☐	☐
Qualität der bestehenden IT	☐	☐	☐	☐	☐
Weitere:_____	☐	☐	☐	☐	☐

c. Was ist das verwendete Pricing-Verfahren?

	Ja	Nein
Die Anwendung eines aktuariellen Standardverfahrens (EW-Prinzip, Varianz-Prinzip, …)	☐	☐
Wir arbeiten mit einer Daumenregel (%-Satz von…)	☐	☐
Wir arbeiten mit einem anderen Verfahren:_____	☐	☐

d. Fragen zur Produktgestaltung?
- Wie sieht die Definition der Deckung (covered loss) typischerweise aus?
- Was sind die üblichen Deckungsgrenzen (limits)? Variieren die Deckungsgrenzen bei verschiedenen Risiken?
- Welche Franchise (Deductibles, absoluter Selbstbehalt) verwenden Sie üblicherweise?
- Gibt es üblicherweise einen prozentualen Selbstbehalt? Wenn Ja, in welcher Höhe?
- Gibt es wichtige Ausschlüsse (Exclusions)? Wenn Ja, welche?

e. Wie schätzen Sie die nachfolgenden Risiken im Pricing der Cyber-Versicherung ein?

	Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Zufallsrisiko (Volatilität der historischen Schadenquoten)	☐	☐	☐	☐	☐
Änderungsrisiko (Natur der versicherten Risiken ändert sich; verläuft anders als auf Basis historischer Daten erwartet)	☐	☐	☐	☐	☐
Irrtumsrisiko (Risiko einer falschen Kalkulation, z. B. aufgrund falscher oder mangelhafter historischer Daten)	☐	☐	☐	☐	☐
Risiken aus asymmetrischer Information (Schaden verläuft anders, da die Kunden ihr Verhalten ändern)	☐	☐	☐	☐	☐

f. Hat Ihr Unternehmen bereits ausreichend historische Daten für ein adäquates Pricing von Cyber Risk?

☐ Ja ☐ Nein

g. Gibt es Kundengruppen, die nicht versichert werden? Falls Ja, welche?

☐ Ja ☐ Nein

h. Wie lukrativ ist das Cyber-Geschäft? Schätzen Sie die durchschnittliche Combined Ratio.

	Combined Ratio				
	<70 %	70–80 %	80–90 %	90–100 %	>100 %
Cyber-Versicherung	☐	☐	☐	☐	☐

i. Wo geht die Cyber-Versicherung im Solvenztest (SST, Solvency I/II) ein?

j. Wo sehen Sie für Ihre Kunden besondere Herausforderungen im Risk Management von Cyber Risk?

k. Durch welche Massnahmen sind Ihre Kunden bereits geschützt? Welche Schutzmassnahmen für die Ausstellung einer Versicherung werden von Ihnen vorausgesetzt?

l. Gibt es weitergehende Schutzmassnahmen, die Sie Ihren Kunden nach Abschluss der Versicherung aktiv empfehlen?

m. Wie beurteilen Sie die Effektivität von Risikomanagementmassnahmen bezüglich Cyber Risk (mit Effektivität bezeichnen wir die Relation von Nutzen zu Kosten)?

	Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Schutz- und Sicherungsmassnahmen (z. B. IT-Sicherheit)	☐	☐	☐	☐	☐
Risikotransfer (Cyber-Versicherung)	☐	☐	☐	☐	☐
Cyber Risk selbst tragen (Eigenkapital als Puffer)	☐	☐	☐	☐	☐

n. Wo sehen Sie besondere Herausforderungen in der Versicherbarkeit von Cyber Risk?

Versicherungskriterien	Kein Problem	Geringes Problem	Mittleres Problem	Grösseres Problem	Grosses Problem
Zufälligkeit des Schadenereignisses (Treten die Schadenereignisse zufällig und unabhängig voneinander auf?)	☐	☐	☐	☐	☐
Maximal möglicher Schaden (Ist der Höchstschaden kontrollierbar?)	☐	☐	☐	☐	☐
Durchschnittlicher Verlust pro Ereignis (Sind genügend historische Daten vorhanden, um einen durchschnittlichen Verlust pro Ereignis zu eruieren und fällt dieser moderat aus?)	☐	☐	☐	☐	☐
Verlustrisiko (Tritt das Risiko ausreichend häufig auf, sodass sich für den Versicherer ein Angebot lohnt?)	☐	☐	☐	☐	☐
Informationsasymmetrie (Wie gross ist das Problem der Informationsasymmetrie bei diesen Versicherungsprodukten? Insb. in Bezug auf Moral Hazard und Adverse Selektion)	☐	☐	☐	☐	☐
Versicherungsprämie (Ist ein risikoadäquates Pricing möglich?)	☐	☐	☐	☐	☐
Grenzen in der Deckung (Werden Limiten und Selbstbehalte vom Kunden akzeptiert?)	☐	☐	☐	☐	☐
Gesellschaftliche Werte (Ist die Versicherung im Einklang mit gesellschaftlichen Werten?)	☐	☐	☐	☐	☐
Rechtliche Rahmenbedingungen (Ist die Versicherung rechtlich durchsetzbar?)	☐	☐	☐	☐	☐

o. Gibt es weitere Themen und Aspekte in Bezug auf Cyber Risk und Cyber-Versicherung, die Ihnen wichtig erscheinen? Haben Sie weitere Anmerkungen?

Literaturverzeichnis

Ackermann, G. (2013): G-20 Urged to Treat Cyber-Attacks as Threat to Global Economy. http://www.bloomberg.com/news/2013-06-13/g-20-urged-to-treat-cyber-attacks-as-threat-to-economy.html. Letzter Zugriff: 03.02.2014.

Ahamad, M. (2012): What if there was a large-scale Internet failure? http://forumblog.org/2012/10/what-if-there-was-a-large-scale-internet-failure/. Letzter Zugriff: 12.03.2014.

AIG (2013): Fidelty Insurance E-Crime. http://www.aig.ch/ch-fidelity-insurance-ecrime_608_182665.html. Letzter Zugriff: 10.10.2013.

AIG (2014): Versicherung für Cyber-Risiken. http://www.aig.de/cyberedge_3194_435521.html. Letzter Zugriff: 19.02.2014.

Allianz (2013): Mit Allianz Cyber Protect sicher in die digitale Unternehmenszukunft. Medienmitteilung – Allianz vom 10.07.2013, München.

Allianz Global Corporate & Specialty AG (AGCS) (2013): "Allianz Cyber Protect" – Schutz gegen Gefahren aus dem Netz. Medienmitteilungen – Allianz Suisse vom 05.09.2013, Zürich, verschickt im Auftrag von AGCS.

Amara, T. (2012): Anonymous says hacks Tunisia prime minister's emails. Chicago Tribune. http://articles.chicagotribune.com/2012-04-08/news/sns-rt-tunisia-hackingl6e8f80ot-20120408_1_ben-ali-ennahda-lulzsec. Letzter Zugriff: 03.02.2014.

Amoroso, E. (2013): Cyber Attacks: Protecting National Infrastructure. Burlington: Elsevier.

Baer, W. S. und Parkinson, A. (2007): Cyberinsurance in IT Security Management. In: IEEE Security and Privacy 5(3), 50–56.

Bandyopadhyay, T. M., Vijay, S. und Rao, R. C. (2009): Why IT Managers Don't Go for Cyber-Insurance Products. In: Communications of the ACM 52(11), 68–73.

Bank for International Settlements (BIS) (2006): International Convergence of Capital Measurement and Capital Standards: A Revised Framework Comprehensive Version. http://www.bis.org/publ/bcbs128.pdf. Letzter Zugriff: 10.12.2013.

Barlow Lyde & Gilbert (2007): International Comparative Review of Liability Insurance Law. Insurance Day May.

Bashan, A., Berezin, Y., Buldyrev, S. V. und Havlin, S. (2013): The extreme vulnerability of interdependent spatially embedded networks. Nature Physics, veröffentlicht 25.08.2013, Macmillian Publishers Limited.

Beckstrom, R. (2012): What if a hacker caused a large-scale Internet outage? http://forumblog.org/2012/06/what-if-a-hacker-caused-a-large-scale-internet-outage/. Letzter Zugriff: 12.03.2014.

Bergler, A. (2010): Kroll Ontrack identifiziert die Ursachen für Datenverlust. http://www.it-business.de/security/bedrohungen/articles/275165/. Letzter Zugriff: 03.02.2014.

Berliner, B. (1982): Limits of Insurability of Risks. Englewood Cliffs, NJ: Prentice-Hall.

Betterley, R. (2010): Understanding the Cyber Risk Insurance and Remediation Services Marketplace: A Report on the Experiences and Opinions of Middle Market CFOs. http://www.casact.org/community/affiliates/CANE/0412/Betterley2.pdf. Letzter Zugriff: 16.12.2013.

Betterley, R. (2013): The Betterley Report – Cyber/Privacy Insurance Market Survey 2013. http://betterley.com/samples/cpims13_nt.pdf. Letzter Zugriff: 05.01.2015.

Bey-Miller, R., Clarke, R. und van Dyk, V. (2008): Introduction to Information Systems. Cape Town, Pearson South Africa (Pty) Ltd.

Biener, C. (2013): Pricing in Microinsurance Markets. In: World Development 41(1), 132–144.

Biener, C. und Eling, M. (2012): Insurability in Microinsurance Markets: An Analysis of Problems and Potential Solutions. In: Geneva Papers on Risk and Insurance 37(1), 77–107.

Biener, C., Eling, M., und Wirfs, J. H. (2015): Insurability of Cyber Risk: An Empirical Analysis. In: Geneva Papers on Risk and Insurance 40(1), 131–158.

Bleicher, J. (2010): Internet. Konstanz: UVK Verlagsgesellschaft mbH.

Böhme, R. und Kataria, G. (2006): Models and Measures for Correlation in Cyber-Insurance. Working Paper. In: Workshop on the Economics of Information Security (WEIS) University of Cambridge, UK.

Böhme, R. und Schwartz, G. (2010): Modeling Cyber-Insurance: Towards A Unifying Framework. In: Workshop on the Economics of Information Security (WEIS), Harvard.

Böhme, R. (2005): Cyber-insurance revisited. In: Workshop on the Economics of Information Security (WEIS), Harvard University, Cambridge, MA.

Bolot, J. und Lelarge, M. (2009): Cyber Insurance as an Incentive for Internet Security. In: M. E. Johnson – Managing Information Risk and the Economics of Security, New York: Springer, S. 169–290.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2012): Überblick IT-Grundschutz: Entscheidungshilfe für Manager. Broschüre des BSI zur Öffentlichkeitsarbeit. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/UberblickGrundschutz.pdf?__blob=publicationFile. Letzter Zugriff: 07.01.2014.

Bu, Z., Bueno, P., Kashyap, R. und Wosotowsky, A. (2013): McAfee Labs – Das neue Zeitalter der Botnets. http://www.mcafee.com/de/resources/white-papers/wp-new-era-of-botnets.pdf. Letzter Zugriff: 03.02.2014.

Bundeskriminalamt (2012): Bundeslagebericht Cybercrime 2012. http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true. Letzter Zugriff: 16.12.2013.

Cebula, J. J. und Young, L. R. (2010): A Taxonomy of Operational Cyber Security Risks. In: Technical Note CMU/SEI-2010-TN-028, CERT Carnegie Mellon University.

Committee of European Insurance and Occupational Pensions Supervisors (CEIOPS) (2009): CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula – Article 111 (f): Operational Risk. CEIOPS-DOC-45/09.

Chabrow, E. (2012): 10 Concerns When Buying Cyber Insurance. http://www.bankinfosecurity.com/10-concerns-when-buying-cyber-insurance-a-4859/op-1. Letzter Zugriff: 03.02.2014.

Choudhry, U. (2014): Der Cyber-Versicherungsmarkt in Deutschland, Wiesbaden: Springer,

Chubb (2014): CyberSecurity by Chubb. http://www.chubb.com/international/switzerland/chubb15150.pdf. Letzter Zugriff: 10.01.2014.

Clover, C. (2009): Kremlin-backed group behind Estonia cyber blitz. http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz2bGiQmaod. Letzter Zugriff: 03.02.2014.

Cyber Summit (2014): Beitrag in der ZDF-heute-Sendung vom 03.11.2014 zum Thema Cyber Security Summit in Bonn. Bericht von Ariane Gübel, ZDF-Studio Düsseldorf.

Cylinder, H. (2008): Evaluating Cyber Insurance. In: CPCU eJournal 61(14), 1–19.

De Roquefeuil, C. (2011): Wie Facebook und Twitter die Proteste vorantreiben. http://www.stern.de/politik/ausland/revolution-20-in-aegypten-und-tunesien-wie-facebook-und-twitter-die-proteste-vorantreiben-1647849.html. Letzter Zugriff: 03.02.2014.

Diggelmann, O. (2013): Militärische Gewalt bei Cyberattacken? http://www.nzz.ch/aktuell/international/uebersicht/militaerische-gewalt-bei-cyberattacken-1.18089666. Letzter Zugriff: 03.02.2014.

Drouin, D. (2004): Cyber risk insurance: A discourse and preparatory guide. Bethesda, MD: SANS Institute. http://www.sans.org/reading-room/whitepapers/legal/cyber-risk-insurance-1412. Letzter Zugriff: 19.12.2013.

European Network and Information Security Agency (ENISA) (2012): Incentives and barriers of the cyber insurance market in Europe. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/incentives-and-barriers-of-the-cyber-insurance-market-in-europe. Letzter Zugriff: 02.12.2013.

European Commission (2012): Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Farny, D. (2006): Versicherungsbetriebslehre. Karlsruhe: Verlag Versicherungswirtschaft GmbH.

FAZ (2010): Iran bestätigt Hacker-Angriff durch „stuxnet“. http://www.faz.net/aktuell/politik/ausland/computervirus-in-industrieanlagen-iran-bestaetigt-hacker-angriff-durch-stuxnet-11037937.html. Letzter Zugriff: 03.02.2014.

Forbes (2011): In Tunisia, Cyberwar Precedes Revolution. http://www.forbes.com/sites/jeffreycarr/2011/01/15/in-tunisia-cyberwar-precedes-revolution/. Letzter Zugriff: 03.02.2014.

Gabler (2014a): Gabler Wirtschaftslexikon – Das Wissen der Experten: Keylogger. http://wirtschaftslexikon.gabler.de/Definition/keylogger.html. Letzter Zugriff: 19.02.2014.

Gabler (2014b): Gabler Wirtschaftslexikon – Das Wissen der Experten: Virus. http://wirtschaftslexikon.gabler.de/Definition/virus.html. Letzter Zugriff: 19.02.2014.

Gabler (2014c): Gabler Wirtschaftslexikon – Das Wissen der Experten: Wurm. http://wirtschaftslexikon.gabler.de/Archiv/1408510/wurm-v2.html. Letzter Zugriff: 18.02.2014.

Gatzlaff, K. und McCullough, K. A. (2012): Implications of Privacy Breaches for Insurers. In: Journal of Insurance Regulation 31, 195–214.

Gordon, L. A., Loeb, M. P. und Sohail, T. (2003): A framework for using insurance for cyber-risk management. In: Communications of the ACM 44(9), 70–75.

Gould, J. (2013): Allianz eyes growth in computer hacking insurance. http://www.reuters.com/article/2013/07/10/net-us-allianz-hacking-cover-idUSBRE9690O120130710. Letzter Zugriff: 16.12.2013.

Government Communications Headquarters (GCHQ) (2012): 10 Steps to Cyber Security. In: White Paper of the Information Security Arm of GCHG, London.

Grace, M. F., Leverty, J. T., Phillips, R. D. und Shimpi, P. (2014): The Value of Investing in Enterprise Risk Management. In: Journal of Risk and Insurance (Early View – Online Version) 9999(9999), 1-28. Letzer Zugriff: 08.02.2014 (DOI: 10.1111/jori.12022).

Gradigo, W. und Pirc, J. (2011): Cybercrime and Espionage: An Analysis of Subversive Multivector Threats. Burlington: Elsevier.

Haas, A. und Hofmann, A. (2013): Risiken aus Cloud-Computing-Services: Fragen des Risikomanagements und Aspekte der Versicherbarkeit. In: FZID Discussion Paper, Nr. 74-2013.

Habegger, B. (2001): Swiss Re: Loveletter kostete 2.6 Mrd. Dollar. http://www.pctipp.ch/news/sicherheit/18048/swiss_re_loveletter_kostete_2_6_mrd_dollar.html. Letzter Zugriff: 16.12.2013.

Hackmageddon (2014): Cyber Attack Statistics. http://hackmageddon.com/. Letzter Zugriff: 18.01.2014.

Harvard Business Review (2013): Meeting the Cyber Risk Challenge. Boston: Harvard Business School Publishing.

Hayes, P. (2005): No ‘sorry’ from Love Bug author. http://www.theregister.co.uk/2005/05/11/love_bug_author/. Letzter Zugriff: 21.02.2014.

Herath, H. und Herath, T. (2011). Copula Based Actuarial Model for Pricing Cyber. In: Insurance Policies Insurance Markets and Companies – Analyses and Actuarial Computations 2(1), 7–20.

Hess, C. (2011): The Impact of financial crisis on operational risk in financial services industry: empirical evidence. In: The Journal of Operational Risk 6(1), 23–35.

Hochstätter, C. H. und Masiero, M. (2009): Angriffe auf das Internet: Wie realistisch ist der Totalausfall? http://www.zdnet.de/41005661/angriffe-auf-das-internet-wie-realistisch-ist-der-totalausfall/4/. Letzter Zugriff: 12.03.2014.

Hofmann, A. und Ramaj, H. (2011): Interdependent Risk Network: The Threat of Cyber Attack. In: International Journal of Management and Decision Making 11(5/6), 312–323.

Information Systems Audit and Control Association (ISACA) (2012): ISACA Issues COBIT 5 Governance Framework. http://www.isaca.org/About-ISACA/Press-room/News-Releases/2012/Pages/ISACA-Issues-COBIT-5-Governance-Framework.aspx. Letzter Zugriff : 07.01.2014.

ISO27000 (2012): ISO/IEC 27000:2012(en) – Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-2:v1:en. Letzter Zugriff : 07.01.2014.

ISO31000 (2009) : ISO/IEC 31000:2009(en) Risk management – Principles and guidelines. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en. Letzer Zugriff: 18.11.2013.

International Data Corporation (IDC) (2014): The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things – Executive Summary. http://germany.emc.com/leadership/digital-universe/2014iview/executive-summary.htm. Letzter Zugriff: 15.12.2014.

Kendrick, R. (2010): Cyber Risk Strategies for Business Professionals. Cambridgeshire: IT Governance Publishing.

Kesan, J. P., Majuca, R. P. und Yurcik, W. J. (2004): The Economic Case for Cyberinsurance. In: University of Illinois Law and Economics Working Papers.

Kizza, J. M. (2002): Computer Network Security and Cyber Ethics. Jefferson: McFarland & Company, Inc., Publishers.

Klipper, S. (2011): Information Security Risk Management: Risikomanagement mit IOS/IEC 27001, 27005 und 31010. Vieweg+Teubner Verlag | Springer Fachmedien Wiesbaden GmbH.

KPMG (2013): KPMG Forensic Services. http://www.kpmg.com/CH/de/Library/Articles-Publications/Seiten/e-crime-survey-2013.aspx. Letzter Zugriff: 18.01.2014.

Majuca, R. P., Yurcik, W. und Kesan, J. P. (2006): The Evolution of Cyberinsurance. Working Paper.

Marsh (2011): Cyber Risks Explained. http://www.marsh.com.tr/documents/CyberRisks.pdf. Letzter Zugriff: 03.02.2014.

Marsh (2012): Cyber Inurance. http://www.iod.org.nz/Portals/0/Branches%20and%20events/Canterbury/Marsh%20Cyber%20Insurance.pdf. Letzer Zugriff: 17.01.2014.

Marsh (2013): Cyber Risk Survey 2013. https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/risikomanagement/partner/Partnerbeitrag_Marsh_Cyber-Risk_Survey.pdf?__blob=publicationFile. Letzter Zugriff: 16.12.2013.

Matt, A. (2013): Cyber Risk – Risikomanagement und Versicherbarkeit, Masterarbeit, Universität St. Gallen.

McAfee (2013): The Economic Impact of Cybercrime and Cyber Espionage. http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf. Letzter Zugriff: 09.01.2014.

McAfee (2014): Net Losses: Estimating the Global Cost of Cybercrime – Economic impact of cybercrime II. http://www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf. Letzter Zugriff: 12.11.2014.

Melde- und Analysestelle Informationssicherung (MELANI) (2014): Lage in der Schweiz und international – Halbjahresbericht 2014/I (Januar – Juni). http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=de. Letzter Zugriff: 12.11.2014.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. und Sadhukan, S. K. (2006): e-Risk Management with Insurance: A Framework Using Copula Aided Bayesian Belief Networks. Hawaii International Conference on System Sciences, Hawaii.

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. und Sadhukan, S. K. (2013): Cyber-risk decision models: To insure IT or not? In: Decision Support Systems 56(1), 11–26.

Mukhopadhyay, A., Saha, D., Mahanti, A. und Chakrabarti, B. B. (2005): Insurance for Cyber-Risk: A Utility Model. Decision 32(1), 153–169.

National Association of Insurance Commissioners (NAIC) (2013): Cyber Risk. http://www.naic.org/cipr_topics/topic_cyber_risk.htm. Letzter Zugriff: 07.12.2013.

Nazario, J. (2004): Defense and Detection Strategies against Internet Worms. Norwood: Artech House.

NetDiligence (2014): Cyber Claim Study 2014. http://www.netdiligence.com/NetDiligence_2014CyberClaimsStudy.pdf. Letzter Zugriff: 16.12.2014.

Ögüt, H., Raghunathan, S. und Menon, N. (2011): Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. In: Risk Analysis 31(3), 497–512.

Ouellette, P. (2012): Pros and cons of cyber insurance for health data breaches. http://healthitsecurity.com/2012/10/29/pros-and-cons-of-cyber-insurance-for-health-data-breaches/. Letzter Zugriff: 18.01.2014.

P.M. Magazin (2012): Was passiert, wenn wir plötzlich offline wären?. P.M. Magazin – Welt des Wissens, Ausgabe 03/2012.

Peters, C. (2012): Versicherungskonzepte für Cyber Risks. Präsentation, Zürich.

Pham, K. und Wefing, H. (2013): Edward Snowden – Sein geheimes Leben. http://www.zeit.de/2013/27/edward-snowden-leben. Letzter Zugriff: 03.02.2014.

Polansky, M. (2011): "Anonymous" droht mexikanischem Drogenkartell. http://www.globalecho.org/25269/anonymous-droht-mexikanischem-drogenkartell/. Letzter Zugriff: 03.02.2014.

Ponemon Institute (2013): Ponemon Cost of Data Breach 2013. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon-2013. Letzter Zugriff: 18.01.2014.

Reissmann, O. (2013): Edward Snowdens Flucht: Rekonstruktion. http://www.spiegel.de/netzwelt/netzpolitik/edward-snowdens-flucht-rekonstruktion-a-907709.html. Letzter Zugriff: 03.02.2014.

Reppesgaard, L. (2011): Datenklau könnte für Sony teuer werden. http://www.zeit.de/wirtschaft/unternehmen/2011-04/sony-datenklau-playstation. Letzter Zugriff: 03.02.2014.

Romeike, F. und Brühwiler, B. (2010): Praxisleitfaden Risikomanagement: IOS 31000 und ONR 49000 sicher anwenden. Erich Schmidt Verlage GmbH & Co. KG, Berlin.

Schweizerische Eidgenossenschaft (2012): Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. http://www.admin.ch/ch/d/ff/2013/563.pdf. Letzter Zugriff: 03.02.2014.

Schweizerische Eidgenossenschaft (2013): Social Engineering. http://www.melani.admin.ch/themen/00103/00202/. Letzter Zugriff: 03.02.2014.

Seibold, H. (2006): IT-Risikomanagement. München: Oldenburg Wissenschaftsverlag.

Shackelford, S. J. (2012): Should your firm invest in cyber risk insurance? In: Business Horizon 55, 349–356.

Shetty, N. S. G., Felegyhazi, M. und Walrand, J. (2010): Competitive Cyber-Insurance and Internet Security. In: Moore, T., Pim, D. und Ioannidis, D. (Eds.): Economics of Information Security and Privacy, S. 229–247, Springer Verlag.

Skariachan, D. und Finkle, J. (2014): Target shares recover after reassurance on data breach impact. http://www.reuters.com/article/2014/02/26/us-target-results-idUSBREA1P0WC20140226. Letzter Zugriff: 12.05.2014.

Spanier, F. (2011): Der Einfluss des Sonnenwinds auf die Erde. http://www.weltderphysik.de/gebiet/planeten/erde/sonnenwind/. Letzter Zugriff: 03.02.2014.

Spiegel (2007): Russland unter Verdacht: Cyber-Angriffe auf Estland alarmieren EU und NATO. http://www.spiegel.de/netzwelt/web/russland-unter-verdacht-cyber-angriffe-auf-estland-alarmieren-eu-und-nato-a-483416.html. Letzter Zugriff: 03.02.2014.

Spiegel (2011): Attacke auf Playstation-Netzwerk: Hacker stehlen Millionen Sony-Kundendaten. http://www.spiegel.de/netzwelt/gadgets/attacke-auf-playstation-netzwerk-hacker-stehlen-millionen-sony-kundendaten-a-759161.html. Letzter Zugriff: 03.02.2014.

Spiegel (2013): Neue Snowden-Enthüllung: NSA-Verbindung bringt deutsche Dienste in Erklärungsnot. http://www.spiegel.de/politik/deutschland/snowden-enthuellung-verbindung-zur-nsa-bringt-bnd-in-erklaerungsnot-a-909884.html. Letzter Zugriff: 03.20.2014.

Steier, H. (2013): Pro-Asad-Hacker bekennen sich zu falschem AP-Tweet. http://www.nzz.ch/aktuell/panorama/pro-asad-hacker-bekennen-sich-zu-angriffen-auf-ap-1.18070267. Letzter Zugriff: 03.02.2014.

Strickland, R. (2010): What would happen if the Internet collapsed? http://computer.howstuffworks.com/internet/basics/internet-collapse.htm. Letzter Zugriff: 12.03.2014.

Swiss Re (2013): Assekuranz Global 2012 – Auf dem langen, beschwerlichen Weg zur Erholung. http://media.swissre.com/documents/sigma3_2013_de.pdf. Letzter Zugriff: 20.05.2014.

Symantec (2013): Internet Security Threat Report 2013. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf. Letzter Zugriff: 03.02.2014.

Symantec (2014): Glossary – worm. http://us.norton.com/security_response/glossary/define.jsp?letter=w&word=worm. Letzter Zugriff: 21.02.2014.

Synergy Research Group (2013): Cisco Dominance of Enterprise Networking Undiminished in 2012. https://www.srgresearch.com/articles/cisco-dominance-enterprise-networking-undiminished-2012. Letzter Zugriff: 13.05.2014.

Tagesanzeiger (2011): Wie viel Schaden Cyberkriminelle in der Schweiz anrichten. http://www.tagesanzeiger.ch/digital/internet/Wie-viel-Schaden-Cyberkriminelle-in-der-Schweiz-anrichten/story/20148889. Letzter Zugriff: 15.12.2014.

Tagesanzeiger (2013): Hier geht Snowden lachend ins russische Asyl. http://www.tagesanzeiger.ch/ausland/europa/Hier-geht-Snowden-lachend-ins-russische-Asyl/story/13490350. Letzter Zugriff: 16.12.2013.

Teevs, C. (2010): Bankdaten-Dieb Kieber: Staatsfeind Nummer eins rächt sich. http://www.spiegel.de/wirtschaft/soziales/bankdaten-dieb-kieber-staatsfeind-nummer-eins-raecht-sich-a-711069.html. Letzter Zugriff: 03.02.2014.

TeleGeography (2014): Submarine Cable Map. http://www.submarinecablemap.com/. Letzter Zugriff: 03.02.2014.

The Economist (2007): A cyber-riot. http://www.economist.com/node/9163598. Letzter Zugriff: 03.02.2014.

T-Online (2013): Internet-Totalausfall in Afrika. http://www.t-online.de/computer/internet/id_62686956/internet-totalausfall-in-afrika-tiefseekabel-durchtrennt.html. Letzter Zugriff: 03.02.2014.

VBV – Berufsbildungsverband der Versicherungswirtschaft (2003): Idee Versicherung – insurance@work. Verlag SKV, Zürich.

Wang, Q.-H. und Kim, S. H. (2009a): Cyberattacks: Does Physical Boundary Matter? In: ICIS 2009 Proceedings, Paper 48.

Wang, Q.-H. und Kim, S. H. (2009b): Cyber Attacks: Cross-Country Interdependence and Enforcement, Working Paper.

Willis (2013a): Willis Fortune 500 Cyber Disclosure Report. http://blog.willis.com/downloads/cyber-disclosure-fortune-500. Letzter Zugriff: 16.12.2013.

Willis (2013b): Willis Fortune 1000 Cyber Disclosure Report. http://blog.willis.com/downloads/cyber-disclosure-fortune-1000-2013. Letzter Zugriff: 16.12.2013.

Wojcik, J. (2012): Cyber Insurance Not Always Enough. In: Business Insurance 46, 4.

World Economic Forum (2010): Global Risks 2010. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2010.pdf. Letzter Zugriff: 04.04.2014.

World Economic Forum (2012): Global Risks 2012. http://www.weforum.org/reports/global-risks-2012-seventh-edition. Letzter Zugriff: 09.01.2014.

World Economic Forum (2014): Global Risks 2014. http://www.weforum.org/reports/global-risks-2014-report. Letzter Zugriff: 03.02.2014.

Yahoo Finance (2013): S&P 500. http://finance.yahoo.com/q?s=^GSPC&ql=1. Letzter Zugriff: 03.02.2014.

Zeit Online (2013): USA klagen Snowden wegen Spionage an. http://www.zeit.de/politik/ausland/2013-06/prism-usa-snowden-anklage. Letzter Zugriff: 03.02.2014.

Zurich (2013): Vertrauensschadenversicherung und Cyber Crime. http://www.zurich.ch/site/de/com/sme/financiallines/vertrauensschaden.html. Letzter Zugriff: 03.02.2014.

Zurich (2014): Cyber Security and Privacy – Factsheet. Zurich Insurance Company Ltd, Zurich.

Autoren



Dr. Christian Biener

Christian Biener legte von 2004 bis 2009 sein Studium der Betriebswirtschaftslehre an der Goethe-Universität Frankfurt und der Karls-Universität Prag ab. Von 2009 bis 2011 war er wissenschaftlicher Mitarbeiter und Doktorand am Institut für Versicherungswissenschaft der Universität Ulm und promivierte mit Auszeichnung zum Dr. rer. pol. im Jahr 2011. Seit 2011 ist er Projektleiter und wissenschaftlicher Mitarbeiter am Institut für Versicherungswirtschaft (I·VW-HSG) der Universität St. Gallen.



Prof. Dr. Martin Eling

Martin Eling studierte Volks- und Betriebswirtschaftslehre an der Universität Münster. Nach Zwischenstationen in Aachen und St. Gallen schloss er 2005 seine Promotion an der Universität Münster unter dem Titel „Hedgefonds-Strategien und ihre Performance im Asset Management von Finanzdienstleistungsunternehmen“ ab. Im Anschluss habilitierte er an der Universität St. Gallen (Titel der Habilitationsschrift „Essays on Risk, Performance, and Solvency in the Financial Services Industry“) und war als Gastprofessor an der University of Wisconsin–Madison in den USA tätig. Von 2009 bis 2011 war er Professor für Versicherungswirtschaft an der Universität Ulm. Seit 2011 ist Martin Eling Direktor am Institut für Versicherungswirtschaft der Universität St. Gallen (I·VW-HSG) und Lehrstuhlinhaber für Versicherungsmanagement. Seine Forschungsschwerpunkte sind neue Versicherungsmärkte, alternative Investments, Regulierung in der Versicherungsbranche, Risikomanagement sowie die Gestaltung zukunftsfähiger Sozialversicherungssysteme.



Andreas Matt

Andreas Matt studierte in seinem Bachelor Management & Economics an der Universität Innsbruck. Im Anschluss absolvierte er die beiden Masterstudiengänge Accounting & Finance und Business Management an der Universität St. Gallen, in denen er seine Masterarbeiten zu den Themen „Cyber Risk – Risikomanagement und Versicherbarkeit“ und „Distributionsmanagement in der Assekuranz – eine empirische Analyse“ schrieb. Während seines Studiums arbeitete er als Assistent am Institut für Versicherungswirtschaft der Universität St. Gallen (I·VW-HSG).



Jan Hendrik Wirfs

Jan Hendrik Wirfs legte im Jahr 2013 sein Diplom in Wirtschaftsmathematik der Universität Ulm ab. Während seines Auslandsaufenthaltes in den USA an der University of Wisconsin–Milwaukee studierte er Mathematik und schloss sein Studium dort im Jahr 2012 mit dem Master of Science in Mathematics ab. Seit Februar 2013 ist Jan Hendrik Wirfs Projektleiter und wissenschaftlicher Mitarbeiter am Institut für Versicherungswirtschaft (I·VW-HSG) der Universität St. Gallen. Im Zuge seiner dortigen Arbeit promoviert er am Lehrstuhl für Versicherungsmanagement zum PhD in Management. Seine Forschungsschwerpunkte liegen in der Risikomodellierung, im Speziellen für Cyber Risk, und in der Performance-Messung in der Versicherungswirtschaft.

Abstract

Cyber Risk stellt eines der grossen neuen Risiken des 21. Jahrhunderts dar. Wir analysieren das Management dieser neuen Risikoart und nehmen eine Einschätzung zur Versicherbarkeit vor. Zu diesem Zweck begutachten wir die bestehende Literatur und nehmen Befragungen unter Kunden und Anbietern von Cyber-Versicherungen vor. Unsere Ergebnisse zeigen, dass ein effizientes Risikomanagement die Wahrscheinlichkeit und das Ausmass eines Cyber-Risk-Schadens erheblich senken kann. Cyber-Versicherungen bieten in diesem Kontext eine gute Möglichkeit, Risiken zu transferieren und können so zu einem effizienten Risikomanagement beitragen. Die Marktbefragung unter Kunden und Anbietern der Cyber-Versicherung unterstreicht die zunehmende Bedeutung von Cyber Risk, aber auch eine gewisse Skepsis vor entsprechenden Versicherungslösungen. Wir zeigen auf, welche Faktoren die Entwicklung dieses Marktes derzeit noch behindern und unter welchen Bedingungen eine Marktentwicklung möglich erscheint. Unserer Prognose nach entsteht mit der Cyber-Versicherung derzeit ein grosser neuer Versicherungsmarkt, der in den kommenden Jahren enorm an Bedeutung gewinnen wird.

Statements aus der Studie

«Das Management von Cyber Risk ist in Unternehmen noch unterentwickelt und bedarf erheblicher Verbesserungen.»

«Das Volumen des Cyber-Versicherungsmarkts wird in der Schweiz auf lediglich fünf Millionen Schweizer Franken geschätzt.»

«Die Befragten gehen davon aus, dass sich der Markt für Cyber-Versicherung in der Schweiz in den kommenden fünf Jahren vervierfachen oder sogar bis zu verzehnfachen wird.»

Einige Highlights der Studie

- Aktuelle Fallbeispiele – International und Schweiz (ab Seite 18)
- Sieben Leitlinien für ein erfolgreiches Cyber-Risikomanagement (Seite 50)
- Schweizer Markt für Cyber-Versicherung im Überblick (Seite 55)
- Versicherbarkeit von Cyber Risk heute nur bedingt möglich (Seite 70)
- Fünf Thesen zu Cyber Risk – Aus Kunden- (Seite 82) und Anbietersicht (Seite 93)
- Pro und Kontra der Cyber-Versicherung (Seite 96)