Beirat Zukunft Finanzplatz **Juni 2017**

Rahmenbedingungen für die Versicherbarkeit und ein effizientes Management von Cyber Security Risiken

Inhaltsverzeichnis

1 Einleitung

Dieses Papier analysiert notwendige Rahmenbedingungen, um die Versicherbarkeit von Cyber Risiken in der Schweiz zu fördern und gleichzeitig den Umgang mit Cyber Risiken in Schweiz zu verbessern. Hierzu benötigt es ein holistisches Zusammenspiel der Aufgaben und Verantwortlichkeiten der verschiedenen Akteure: Unternehmen, Versicherungswirtschaft und Staat (national wie international). Aufgabe der Unternehmen ist es hier, ausreichend in Cyber Security zu investieren und effiziente Risikomanagement Massnahmen zu implementieren. Die Rolle der Versicherer ist, umfangreichen Risikotransfer zur Verfügung zu stellen, über eine risikoadäquate Prämie, Anreize für Cyber Security Investitionen zu setzen und Unternehmen in Bezug auf ein effizientes Cyber Risikomangement und Krisenmanagement beratend zu unterstützen. Der Staat setzt Rahmenbedingungen, die einen effizienten Markt für Cyber Risikotransfer ermöglicht und die Resilienz des Gesamtsystems sicherstellt. Alle staatlichen Massnahmen sollten im Kontext internationaler Standards und Legislation gesehen werden und keinen zusätzlichen Hürden für den Zugang zum Schweizer Markt setzen.

2 Ausgangslage

2.1 Cyber: Risiko für die Schweizer Volkswirtschaft?

Die Medien illustrieren täglich die zunehmende wirtschaftliche und gesellschaftliche Bedeutung von Cyber Risiken. Die Schätzungen der mit Cyber Risiken verbundenen Schäden liegen global im Bereich mehrerer hundert Milliarden USD (McAfee 2014), wobei diese Schätzungen einer grossen Unsicherheit und Dynamik ausgesetzt sind. Sowohl die Schäden, die aus Cyber Risiken resultieren, als auch der Wert von Cyber Risikomanagement-Massnahmen sind für Unternehmen schwer zu bewerten. Dies liegt an der Komplexität des Risikos selbst, jedoch auch an der Unsicherheit bzgl. der Effektivität von Risikomanagement-Massnahmen. Cyber Security Investitionen mit konkreten Kosten stehen folglich unklaren Resultaten gegenüber. Dies führt zu Anreizen für Unternehmen, nicht ausreichend in Cyber Security zu investieren. Zudem weisen Investitionen in Cyber Security so genannte positive Externalitäten auf, also unkompensierte positive Auswirkungen auf Dritte, die sich nicht im Preis für das Gut selbst spiegeln. Das Bestehen positiver externer Effekte führt zur Unterinvestitionen in diese Güter und folglich zu einem nicht optimalen Ressourceneinsatz. Tatsächlich zeigt die Forschung auf der Grundlage von Experimenten ein tendenziell zu geringes Investitionsniveau, welches über die Zeit weiter sinkt (Laury und Holt 2008). Dies ist insofern kritisch, da bereits ein Grossteil sämtlicher Cyber Vorfälle vermieden werden könnte, wenn einfache IT Hygiene Massnahmen beachtet würden. Im Bereich Cyber Security deuten einige Studien an, dass in der Tat das Management von Cyber Risiken unterentwickelt ist (KPMG 2017a), wobei die genauen Gründe hierfür zahlreich sind.

Der Gruppe der Cyber Risiken wird auch die Eigenschaft des Kumulrisikos zugeschrieben. Der zufällige Eintritt eines Vorfalls kann gleichzeitig bei vielen weiteren Marktteilnehmern Vorfälle auslösen.[1] Die erhöhte Verletzlichkeit einzelner Marktteilnehmer ist daher für das ganze System relevant, bzw. hat einen negativen externen Effekt. Eine systematische Unterinvestition in das Management von Cyber Risiken kann so zu einem ökonomisch relevanten Risiko für die Schweizer Volkswirtschaft werden.

In einer ersten Bestandsaufnahme deutet vieles darauf hin, dass das Fehlen geeigneter staatlicher Rahmenbedingen nicht zu einem optimalen Einsatz der Ressourcen—hier zu einer Unterinvestition in Cyber Security führt.

[1] Z.B. aufgrund zahlreicher „Single-Points-of-Failure“ (z.B. Stromversorgung, Zugang zum Internet, SWIFT/RTGS, Cloud Anbieter, etc.).

2.2 Probleme der Versicherbarkeit von Cyber Risiken

Geht es nun darum, die Anreize zur Investition in Cyber Security zu verbessern, um einen effizienteren Ressourceneinsatz zu erreichen, erscheint der Marktmechanismus des Risikotransfers (z.B. über Versicherung) grundsätzlich geeignet. Versicherer unterstützen Unternehmen im Risikomanagement und nehmen dabei eine Reihe volkswirtschaftlich wichtiger Aufgaben wahr. Im Rahmen der Prämienermittlung wird jedem Risiko ein entsprechender Preis zugeordnet. Positive Externalitäten (zumindest im Kollektiv der Versicherten) werden dadurch berücksichtigt, dass Versicherer neben dem Einzelrisiko den Beitrag des Einzelrisikos zum Gesamtrisiko im Portfolio berücksichtigen. So setzen Versicherer Anreize für risikoadäquates Verhalten. Sie unterstützen Unternehmen vor Abschluss und während der Laufzeit einer Police, insbesondere durch die Bewertung der Risiken. Hier stellen Versicherer ihre Expertise zur Verfügung und unterstützen die Unternehmen auch darin, das Verständnis für die entsprechenden Risiken zu schärfen und Massnahmen der Prävention zu entwickeln. Im Falle eines Schadens leisten sie die Finanzierung des Schadens und unterstützen Unternehmen im Krisenmanagement zur Wiederherstellung der Betriebsfähigkeit. Mit einem globalen Prämienvolumen, welches in 2016 zwischen 3 und 4 Mrd. USD liegt, ist im Bereich Cyber nur ein geringer Teil der Risiken versichert (KPMG 2017b). Dies ist dadurch bedingt, dass der Versicherungsmarkt für Cyber Risiken einige Friktionen aufweist, welche die Versicherbarkeit einschränken.

Eine systematische Kategorisierung von Risiken, die effizient über den Mechanismus der Versicherung abgesichert werden können und solchen, bei denen dies nicht möglich, erfolgt üblicherweise anhand von neun Kriterien der Versicherbarkeit (siehe Tabelle 1 nach Berliner 1982). Neben objektiven Kriterien, welche dem Risiko inhärent sind, hängt die Versicherbarkeit sehr stark von den individuellen Kapazitäten und Präferenzen der Marktteilnehmer ab. Folglich existieren keine allgemeinen Grenzen der Versicherbarkeit; die Diskussion hilft aber grundlegende Probleme und Tendenzen aufzuzeigen, die auf Marktebene relevant sind.

Tabelle 1: Kriterien der Versicherbarkeit nach Berliner (1982)

Versicherbarkeitskriterien	Anforderungen
Teil A: Versicherungsmathematisch	
Zufälligkeit des Schadenereignisses	Unabhängigkeit und Schätzbarkeit des Verlustrisikos
Maximal möglicher Schaden	Muss für Versicherungsunternehmen handhabbar sein
Mittlere Schadenhöhe	Moderat (relativ geringes Schadenausmass)
Mittlere Schadenhäufigkeit	Relativ gross
Informationsasymmetrien	Geringe Rolle von Adverse Selection und Moral Hazard
Teil B: Marktbezogen	
Versicherungsprämie	Kostendeckend und bezahlbar
Deckungsabgrenzung	Akzeptierbar
Teil C: Gesellschaftsbezogen	
Gesellschaftliche Werte	Im Einklang mit gesellschaftlichen Werten
Gesetzliche Schranken	Erlauben die Deckung

An dieser Stelle sollen einige der kritischen Aspekte aufgezeigt werden; eine detaillierte Analyse aller Kriterien der Versicherbarkeit findet sich in Biener, Eling und Wirfs (2015a,b). Die wesentlichen Probleme lassen sich auf die Bereiche Zufälligkeit des Schadenereignisses und Informationsasymmetrien zurückführen.

Eine zentrale Anforderung für die Bereitstellung von Versicherung für ein spezielles Risiko ist die Unabhängigkeit der Risiken. Unabhängigkeit bedeutet, dass ein Schadenereignis nicht Folge eines anderen Schadenereignisses ist oder die gleiche Ursache hat. Nur wenn sich ein Versicherungsportfolio aus unabhängigen Risiken zusammenstellen lässt, konvergiert der durchschnittliche Gesamtschaden gegen den erwarteten Schaden bei zunehmender Portfoliogrösse (Böhme 2005; Biener 2013). Diese zentrale Unabhängigkeitsbedingung minimiert das sogenannte Kumulrisiko, welches die Solvenz von Versicherungsunternehmen gefährdet. Für Cyber Risiken stellen einige Studien fest, dass diese grundsätzliche Voraussetzung verletzt wird. So sind IT-Systeme vielfach in einer ähnlichen Weise aufgebaut und greifen auf die gleichen Komponenten (z.B. Hard- und Soft-Ware) zurück und sind so ähnlich anfällig (Baer

und Parkinson 2007). Dies deutet darauf hin, dass Vorfälle zwischen Firmen nicht unabhängig sind. In der Tat zeichnen einige Studien derartige Korrelationen von Cyber Risiken empirisch nach (Hofmann und Ramaj 2011; Ögüt, Raghunathan und Menon 2011; Bolot und Lelarge 2009).[2] Ein weiteres grundsätzliches Problem bei der Bewertung von Cyber Risiken resultiert aus dem Mangel an Daten (ENISA, 2012; Herath und Herath, 2011; Baer und Parkinson, 2007; Gordon et al., 2003). Ungeachtet dessen wie gut die Modellierungen für Cyber Risiken sind, sind die Modelle von geringem Nutzen, wenn Daten zum Testen und Kalibrieren der Modelle nicht vorhanden sind. Ein weiteres Problem in diesem Kontext ist das Änderungsrisiko, also die systematische Änderung von wesentlichen Charakteristika des Risikos (Haas und Hofmann, 2013; ENISA, 2012). In diesem Fall ist eine Analyse historischer Daten nicht Aussagekräftig für die Beschreibung des aktuellen und zukünftigen Risikos. Der Mangel an Daten, insbesondere zu Grossschäden, verstärkt zudem die Schwierigkeiten bei der Abschätzung der oben beschriebenen Kumulrisiken.

Bei vollkommener Symmetrie der Informationen führt der Versicherungsmechanismus dazu, dass Versicherungsnehmer ihre Ressourcen effizient zwischen Cyber Security und Risikotransfer aufteilen und Prämien nach Risikotypen differenziert werden können. Eine besondere Problematik von Cyber Risiken ist jedoch, dass hier ein hohes Mass an Informationsasymmetrie gegeben ist. Die schlechter informierten Marktteilnehmer—hier die Versicherer—können die „schlechten" Risiken nicht von den „guten" unterscheiden und werden einen Preis setzen, zu dem nur noch die schlechten Risiken bereit sind, ihr Risiko zu transferieren. Es kommt zu einer negativen Auslese (Adverse Selektion) und in extremen Fällen zu einem vollständigen Marktzusammenbruch. Um diesem Problem zu begegnen, nehmen Versicherer zuvor eine intensive Überprüfung der Cyber Security Architektur vor; solche Abklärungen sind aber aufgrund der Komplexität der heutigen Infrastruktur nur bedingt in der Lage, das tatsächliche Risiko zu identifizieren. Ein weiteres Problem von Informationsasymmetrien entsteht aus dem Mangel an Anreizen für die Versicherungsnehmer, Präventionsmassnahmen zu ergreifen, die die Schadenwahrscheinlichkeit verringern (Moral Hazard). Diese Problematik lässt sich klassischerweise mit Selbstbehalten adressieren, welche jedoch den Versicherungsnutzen mindern, wenn Versicherungsnehmer eine Präferenz für Vollversicherungen haben. Einige Studien zeigen, dass Unternehmen, die bereits Schäden durch Cyber Risiken erlitten haben, mit einer höheren Wahrscheinlichkeit eine Versicherung abschliessen (Shackelford 2012), was als Indiz sowohl für das Vorhandensein von Negativauslese als auch von Moral Hazard ausgelegt werden kann.

Die oben beschriebenen Probleme führen im Markt zudem dazu, dass Prämien in der Tendenz als zu hoch wahrgenommen werden und dass Versicherungsausschlüsse und Deckungsgrenzen für einige Kundengruppen nicht optimal ausgestaltet werden können. Es ist jedoch zu erwarten, dass Verbesserungen bei der Modellierung von Cyber Risiken und der Abbau von Informationsasymmetrien dazu führen werden, dass sich das Angebot von Deckungsgrenzen ausweitet.

Bezüglich der Versicherbarkeit von Cyber Risiken lässt sich zusammenfassend feststellen, dass Kumulrisiken, Mangel an Daten und Informationsasymmetrien grundlegende Probleme darstellen, die gelöst werden müssen, um die hohen Wachstumserwartungen zu rechtfertigen.[3]

---

[2] Wichtig ist allerdings anzumerken, dass die Korrelation nicht unbedingt bei allen Kategorien von Cyber Risiken auftreten und somit Zufälligkeit auch immer in Bezug zum aktuellen Vorfall gesehen werden muss (z.B. physische Datendiebstähle).

[3] Eine aktuelle Studie von KPMG (2017b) erwartet, dass Cyber in 20 Jahren die grösste Nichtleben-Sparte sein wird.

Key Message: Cyber Risiken stellen ein ökonomisch relevantes Thema für die Schweizer Volkswirtschaft dar. Es gibt Anzeichen dafür, dass das Fehlen geeigneter staatlicher Rahmenbedingungen und damit die alleinige Koordination über den Markt zu einer Unterinvestition in Cyber Security und Cyber Resilienz führt. Dies stellt ein potentiell sehr grosses Risiko für die Schweizer Volkswirtschaft dar. Es ist daher essenziell, ein sinnvolles Rahmenwerk mit klaren Rollen und Verantwortlichkeiten zu definieren, um Wirtschaftswachstum, technischen Fortschritt, politische und finanzielle Stabilität und gesellschaftlichen Fortschritt zu fördern. Versicherung leistet dabei einen wichtigen Beitrag hinsichtlich Risikotransfer, Anreizen zur Prävention und Kompetenzen im Risikomanagement. Heute sind global, aber insbesondere in Europa und der Schweiz, nur ein geringer Teil der Cyber Risiken versichert. Dies ist dadurch bedingt, dass der Versicherungsmarkt für Cyber Risiken noch einige Herausforderungen aufweist, welche die Versicherbarkeit einschränken. Kumulrisiken, Mangel an Daten und Informationsasymmetrien sind hier die zentralen Probleme, die adressiert werden müssen, um die Herausbildung eines effizienten und nachhaltigen Marktes zu ermöglichen.

3 Welche Rahmenbedingungen braucht ein nachhaltiger Markt für Cyber Versicherung?

Grundsätzlich kann die Versicherung einen Mechanismus darstellen, um einen effizienteren Ressourceneinsatz zu erreichen und hierbei ein effizientes Mass an Cyber Security mit gleichzeitig geringerem Risiko für die Unternehmen sicherzustellen. Um die bestehenden Probleme bei der Versicherbarkeit zu adressieren, gibt es verschiedene Massnahmen, die zum einen auf Marktebene und zum anderen auf Staatsebene ansetzen.

3.1 Markt

Um dem Mangel an Daten zur Bewertung und Modellierung von Cyber Risiken zu begegnen, kann ein konzertiertes Sammeln und Zurverfügungstellen von Daten (Datenpooling) in einem Konsortium aus Versicherern und potentiell weiteren Akteuren eine Möglichkeit darstellen.[4] Verbesserungen an dieser Stelle können zu einem breiteren Angebot und geringeren Prämien führen, sofern nicht der Wettbewerb durch eine einheitliche Datenbasis verringert wird. Vorstellbar wäre, das Datenpooling auf Extrem-Risiken einzuschränken, welche die grössten Probleme bei der Modellierung im Bereich Cyber verursachen.[5] Somit würde bei kleinen bis mittleren Schäden zwischen den Marktteilnehmern ausreichend Variation in den Schadenstatistiken bestehen bleiben, was zu einer grösseren Bandbreite an Prämien und höherem Wettbewerb beitragen würde. Sofern die gesetzlichen Rahmenbedingungen einen Austausch von Daten zwischen den Versicherern zulassen, liesse sich ein Datenpool im Markt realisieren; er bedarf nicht zwangsläufig einer staatlichen Organisation.

Versicherungspools, Rückversicherung und Alternativer Risikotransfer am Kapitalmarkt (z.B. Cyber Cat Bonds) können die für einen Transfer von Cyber Risiken verfügbaren Kapitalressourcen erhöhen und insbesondere der Unsicherheit in Bezug auf Wahrscheinlichkeit und Ausmass von Extremereignissen entgegenwirken. Mit einem globalen Cyber Prämienvolumen für explizite Deckungen von 3 bis 4 Mrd. USD (KPMG 2017b) bewegt sich der Markt jedoch noch in einem Bereich, der für Erstversicherer zu bewältigen ist. Sollten die hohen Wachstumserwartungen, die einige Studien äussern (KPMG 2017b; PWC 2015), jedoch gerechtfertigt sein, wird das Thema Risikotragfähigkeit weiter an Bedeutung gewinnen. An dieser Stelle stellt sich dann auch die Frage nach den Grenzen der Versicherbarkeit in Bezug

[4] Vorschläge zu einer Strukturierung von Cyber Risiken, die als Grundlage für ein Datenpooling genutzt werden können, wurden kürzlich z.B. vom CRO Forum erarbeitet (CRO Forum 2016).

[5] Dieser Ansatz wird bereits im Kontext einer Initiative des CRO Forums umgesetzt. Zu analysieren wäre hier, inwieweit ein solcher Datapool nur von den „grossen Player“ gefüllt wird, während alle anderen „kleineren Player“ davon profitieren; ein solcher Ansatz wäre auf Dauer weniger erfolgreich, so dass eine gewisse Balance gefunden werden muss. Ein Datenpooling ist für Versicherer nicht nur aus Underwriting-Sicht interessant, sondern auch aus Operational Risk Sicht für interne Risk Management Überlegungen (z.B. Hinterlegung von Risk Capital, interne Kontrollen etc.). Siehe entsprechende Überlegungen von Seiten des CRO-Forum.

auf die maximale Risikotragfähigkeit der Assekuranz: Ab wann der Staat intervenieren sollte und mit welchen Massnahmen.

3.2 Staat

Mindeststandards für Cyber Security können das Investitionsniveau in Cyber Security erhöhen, da sie externe Effekte internalisieren, dadurch das generelle Level an Cyber Security in der Schweizer Volkswirtschaft erhöhen und im Kontext von Versicherungen eine extreme Negativselektion verhindern. Ein wichtiger Ausgangspunkt für Überlegungen zu Mindeststandards ist, dass ein grossteil der Schweizer Unternehmen und insbesondere KMUs Schwierigkeiten haben, sich dem Thema Cyber Security aufgrund seiner Komplexität anzunehmen. Zudem fehlt ein Verständnis dafür, dass Cyber Vorfälle Schäden bei Dritten verursachen können.[6]

Mindeststandards können allerdings bürokratisch und schwer umsetzbar sein. Bei gesetzlichen oder regulatorischen Mindeststandards besteht ausserdem die Gefahr, dass alle Marktteilnehmer unabhängig ihrer Grösse, Industrie, Geographie, und der Art von Daten, die vorgehalten werden, und somit auch unabhängig ihres Beitrags zum Gesamtrisiko (ihrer Systemrelevanz) gleichbehandelt werden. Wenn hingegen nicht alle Marktteilnehmer die Standards erfüllen müssen, entstehen Anreize, die Regeln durch gezielte Umgehungsmanöver auszuhöhlen. Es ist zudem zu erwarten, dass eine Art technischer Mindeststandard im Bereich Cyber Security wenig effektiv ist, da die technologische Entwicklung zu dynamisch ist, als dass gesetzliche oder regulatorische Vorgaben, die man üblicherweise aus Gründen der Rechtsstabilität längerfristig ausrichtet, hier nützlich sein können. Aufgrund der internationalen Dimension von Cyber Risiken wären regionale technische Mindeststandards insbesondere für internationale Firmen eine grosse Herausforderung und mit erheblichen Kosten verbunden, ohne dass es einen eindeutigen positiven Effekt auf Cyber Security hätte.[7]

Sinnvolle Mindeststandards im Bereich Cyber Risiko können nur Prinzipien-basiert ausgestaltet sein. Beispiele solcher Prinzipien-basierten Standards können sein, dass die Verantwortung für Cyber Security auf Vorstands-Ebene aufgehängt sein muss, ein Cyber Security Beauftragter mit bestimmten Verantwortlichkeiten zur Aufklärung und Prävention bestimmt werden muss (vgl. Sicherheitsbeauftragter (SIBE) im Bereich Arbeitssicherheit)[8] sowie ausreichend Ressourcen vorgehalten werden müssen, um mit den aktuellen Herausforderungen adäquat umzugehen.[9] In jedem Fall sollten Mindeststandards verhältnismässig sein und differenzieren nach Branche und Grösse der Unternehmen. Zudem sollten Mindeststandards international abgestimmt werden – dies ist besonders für interational tätige Unternehmen kritisch. Zusätzlich können Mindeststandards mit regelmässigen Stresstests für systemkritische Firmen ergänzt werden, um der Kritikalität solcher Firmen gerecht zu werden. Allerdings sollten der

---

6 Eine mögliche „Awareness Kampagne“ könnte neben Mindeststandards sinnvoll sein, um dem Thema die nötige Wichtigkeit beizumessen. Sowohl die Versicherungs- als auch die IT Security Branche stehen gerne zur Verfügung, um diese Themen breiter zu adressieren und als Anlaufstelle für mögliche Lösungen und Aufklärung (Mindestanforderungen, Best Practices, Risk Management Wissen etc.) beigezogen zu werden.

7 Die kürzlich in der EU eingeführte Network and Information Security (NIS) Directive geht in diese Richtung und schreibt für bestimmte kritische Infrastrukturen erstmals Mindeststandards für Cyber Security vor.

8 Die Vorgaben von MELANI (2016) zum Umgang mit dem Thema Cyber Security können hier beispielhaft herangezogen werden.

9 Risikomanagement wird im Corporate Governance als eine der wichtigsten Führungsaufgaben der obersten Leitung einer Organisation oder eines Unternehmens gesehen (Romeike und Brühwiler 2010). So wird auch im “Swiss Code of Best Practice for Corporate Governance“ ein für das Unternehmen angepasstes Risikomanagement gefordert. In einigen Unternehmen wird Risikomanagement noch primär als ein Instrument des internen Kontrollsystems verstanden, welches sich vordringlich mit den Fragen der finanziellen Berichterstattung und Gesetzeskonformität (Reporting und Compliance) befasst. Viele Unternehmen verknüpfen das Risikomanagement aber auch immer stärker mit dem strategischen Management und definieren Risikomanagement als Aufgabe auf Vorstandsebene. Die Implementierung eines Chief Information Security Officer kann die Durchschnittskosten bei Cyber Vorfällen um über 30% (Shackelford, 2012) senken.

Aufwand für die Prüfung der Einhaltung von Mindeststandards (sowohl regel- als auch prinzipien-basiert) und die Implementierung von solchen Stresstests bei systemkritischen Firmen nicht unterschätzt werden.

Neben einem ersten Level an prinzipien-basierten Mindeststandards, wäre ein sinnvolles zweites Level ein Marktstandard von Mindestanforderungen, die zu erfüllen sind, um Versicherungsschutz zu erhalten. Einen solchen Standard können Versicherer in Kooperation mit IT-Security Unternehmen eigenständig umsetzen, um die Effektivität von prinzipien-basierten Mindeststandards zu erhöhen und gewisse Mindestanforderungen am Markt zu forcieren – ähnlich der Verwendung von Winterreifen in der KfZ-Versicherung. Versicherer arbeiten schon heute eng mit IT-Security Unternehmen und ihren Kunden zusammen, um eine holistische Perspektive auf Cyber Risiken zu bekommen und state-of-the-art Cyber Security bei ihren Kunden zu unterstützen. Notwendigerweise wirken diese Anforderungen allerdings nur auf solche Firmen, die ihre Cyber Risiken versichern. Prinzipien-basierte Mindeststandards addressieren so das Problem eines generell zu niedrigen Niveaus an Cyber Security und marktbasierte technische Mindestanforderungen lösen das Selektionsproblem und erhöhen die Versicherbarkeit.
Grundsätzlich ist ein sowohl als auch dieser beiden Ansätze aus Sicht der Versicherungswirtschaft zu begrüssen, wobei die Bewertung des relativen Nutzens noch en détail weiter diskutiert werden muss.

Meldepflichten haben im Sinne der Marktdisziplin insbesondere eine Wirkung für Unternehmen, für die der Business Impact eines Cyber Vorfalls bedeutsam ist. Meldepflichten könnten sich an entsprechenden Vorschriften aus den USA und der EU im Bereich Data Breach orientieren—Verstösse gegen die Datensicherheit und den Datenschutz, bei denen personenbezogene Daten unberechtigten Dritten bekannt werden. Die Wirksamkeit dieser Meldevorschriften in den USA wurde bereits in mehreren wissenschaftlichen Untersuchungen belegt und es ist wahrscheinlich, dass diese zur Marktentwicklung beigetragen haben.[10] Auch in der Schweiz wird die Umsetzung eines derartigen Meldesystems im Rahmen der Revision des Bundesgesetzes über den Datenschutz (DSG) angestrebt und könnte entsprechend positive Effekte für den Schweizer Marktplatz bewirken. Data Breach als Teilmenge aller Cyber Risiken ist derzeit das am besten dokumentierte Risiko, was zu einem grossen Teil den Meldevorschriften zuzuschreiben ist. Es bildet jedoch nur einen kleinen Teil der Gefahrenlandschaft ab. Zudem liesse sich die Nutzung der vorhandene Daten optimieren, in dem der Nutzerkreis ausgeweitet würde.

Es stellt sich daher die Frage, ob es neben Meldepflichten zu Data Breach einer umfassenderen Pflicht zur Meldung von Cyber Vorfällen bedarf. An dieser Stelle stehen sich verschiedene Interessen potenziell diametral entgegen. Geht es um Sicherheit, also dem Schutz kritischer Infrastrukturen und der Volkswirtschaft als Ganzes, haben sich teilweise freiwillige Meldesysteme durchgesetzt (siehe Department of Homeland Security (DHS) in den USA sowie Melde- und Analysestelle Informationssicherung (MELANI) in der Schweiz), die darauf abzielen, die Gefahrenlandschaft, deren Ursachen und Hintergründe zu verstehen, um die Widerstandsfähigkeit des Gesamtsystems zu stärken. Die Freiwilligkeit dieser Systeme basiert auf der Erfahrung, dass eine Meldepflicht zu einer schlechten Datenqualität und zu keiner über die Meldung hinausgehenden Kooperation der Marktteilnehmer führt; es fehlt der Anreiz für eine Kooperation, die über das Mindestmass hinausgeht. Damit Marktteilnehmer in einem freiwilligen Meldesystem Anreize zur Kooperation und Meldung haben, wird auf verschiedene Art ein Nutzen erbracht. In erster Linie ist dies im Zugang zu Informationen über die Gefahrenlandschaft zu sehen, die nur eine übergeordnete staatliche Instanz liefern kann, aber auch in der Unterstützung bei der Gefahrenbewältigung. Zudem ist eine rechtliche Absicherung der Haftpflichtrisiken bei einer Datenweitergabe an solche offiziellen Stellen wichtig.

Besteht der Zweck in der Förderung des gesamtwirtschaftlichen Nutzens und einer nachhaltigen Entwicklung, haben Meldepflichten im Kontext der Entwicklung von Märkten für Risikotransfer (z.B. Versicherung) einen potenziellen Wert. Auch in Bezug auf den Schutz kritischer Infrastrukturen gibt es Argumente für Meldepflichten, die z.B. in Deutschland zu verpflichtenden Meldesystemen geführt haben. Generell stärken Meldepflichten die Marktdisziplin und vermitteln Anreize zur Investition in Cyber

[10] Vgl. etwa Campbell et al. (2003), Hovav und D'Arcy (2003, 2004), Cavusoglu et al. (2004), Ishiguro et al. (2006), Hovav et al. (2007); Goel und Shawky (2009), Gatzlaff et al. (2010), Yayla & Hu (2011), Das et al. (2012).

Security, wenn Cyber Vorfälle publik werden und dadurch die Reputation potenziell leidet. Dies erhöht die Versicherbarkeit durch den Abbau von Informationsasymmetrien. Zum anderen führt eine Meldepflicht dazu, dass erstmalig eine Datenbasis geschaffen würde, welche repräsentativ die Cyber Gefahrenlandschaft in der Schweiz abbilden und sowohl dem Bund, der Forschung, als auch den Versicherern dienlich ist. Derartige Daten können dem Bund als Grundlage für Sicherheitsstrategien und Präventionsmassnahmen dienen und die Assekuranz dabei unterstützten, Cyber Risiken und deren Abhängigkeiten (Kumulrisiken) besser zu verstehen und das Angebot auszuweiten. Die Bewertung der Risiken ist eine zentrale Voraussetzung, um Risikotransfer im Bereich Cyber überhaupt nachhaltig anzubieten. Es ist demzufolge zu überlegen, ob es sinnvoll sein kann, neben dem bestehenden System für kritische Infrastrukturen ein identisches System für alle Industrien aufzubauen. Ob dies auf Basis freiwilliger oder verpflichtender Meldungen erfolgen soll, bleibt zu definieren und die Vor- und Nachteile abzuwägen (siehe Tabelle 2). Zu bemerken ist hier noch, dass die Europäische Zentralbank derzeit an der Umsetzung einer Meldepflicht für Cyber Vorfälle innerhalb ihres Regulierungsbereiches arbeitet.[11] Dies ist eine Silolösung für den Bankenbereich, die wichtig für den Bankenregulierer ist, jedoch nicht für ein System taugt, das die Gesamtwirtschaft einschliesslich kleiner und mittlerer Betriebe in nichtregulierten Sektoren umfassen soll.

Tabelle 2: Vor- und Nachteile freiwilliger und verpflichtender Meldesysteme

Teil A: Verpflichtendes Meldesystem	
Vorteile	*Nachteile*
Gesamtschau der Cyber Bedrohungslage	Potentiell geringere Datenqualität
Awareness-Effekt	Eingeschränkte Kooperation
Teil B: Freiwilliges Meldesystem	
Vorteile	*Nachteile*
Gute Datenqualität	Bei geringer Beteiligung keine Gesamtschau
Hohes Mass an Kooperation	Awareness-Effekt nur für Beteiligte

Ein freiwilliges System, welches eine hohe Meldepenetration erreicht, stellt den Optimalfall dar. Gelingt dies nicht, sollte ein Pflichtsystem weitergehend diskutiert werden. Die Einsetzung eines freiwilligen Systems kann in jedem Fall ein erster Schritt sein, wobei die Meldepenetration dann ein wichtiges Entscheidungskriterium für weitergehende Veränderungen zu einer Meldepflicht ist. Um eine hohe Penetration zu erreichen, ist es zentral, Anreize zur Erstattung von Meldungen zu schaffen und darauf hin zu arbeiten, schnellst möglich eine kritische Masse an Unternehmen zu gewinnen. Wichtig erscheint in diesem Kontext, eine zentrale Stelle zur Meldung zu definieren, die eine starke Aussenwirkung hat, z.B. durch den Ausbau von MELANI oder durch die Schaffung einer neuen Stelle. Die Analyse und Verarbeitung der Daten könnte, wenn nötig, an verschiedene Stakeholder ausgelagert werden (z.B. an MELANI für systemkritische Infrastrukturen sowie an weitere Stellen für andere Industrien).

Grundsätzlich weisen beide Systeme aus Sicht der Versicherungswirtschaft klare Vorteile und Nachteile auf, die sich aber noch nicht auf eine klare Position für das eine oder andere aggregieren lässt. Für eine holistische Perspektive auf Cyber Risiken ist eine umfangreichere Datenbasis zentral und somit ein Meldesystem wichtig. Eine Zwischenlösung, welche Teilaspekte des Datenproblems addressieren kann ist das Datenpooling (siehe Abschnitt *Markt*). Hierfür bedarf es jedoch kurfristig Rechtssicherheit darüber, dass ein solcher Datenaustausch zwischen Unternehmen (z.B., Versicherern, IT-Security Firmen) möglich ist.

[11] Bei der Umsetzung ergeben sich jedoch zahlreiche Probleme. Unternehmen wissen möglicherweise für lange Zeit nicht, dass es einen Vorfall gab (es dauert zum Teil Monate bis Vorfälle entdeckt werden) und selbst wenn Unternehmen darüber wissen, dauert es i.d.R. sehr lange, bis Ursache und Folgen identifiziert sind. Zudem muss klar definiert werden, wann ein Vorfall zu melden ist.

Versicherungsobligatorien finden wir heute insbesondere dort, wo Drittparteien zu Schaden kommen können (z.B. Motorhaftpflicht; Haftpflicht für bestimmte Berufsgruppen wie Ärzte, etc.).[12] In Europa ist die Cyber Versicherung heute weitgehend auf „Eigenschaden"-Komponenten fokussiert im Gegensatz zu Drittschadenkomponenten aus der Haftpflicht, wogegen in den USA der Fokus auf dem Haftpflichtgeschäft liegt. Dies ist allerdings zu einem grossen Teil durch das Rechtssystem mit grossen Haftpflichtklagen im Milliardenumfang bedingt, die häufig bereits die komplette Versicherungssumme ausschöpfen. Diese Situation ist mit der in Europa (noch) nicht zu vergleichen ist, so das gerade ein Obligatorium im Bereich Haftpflichtversicherung im Kontext Schweiz ins Leere greifen würde.[13] Aus theoretischer wie aus praktischer Perspektive birgt eine Versicherungspflicht in einem Umfeld grosser Informationsasymmetrien zudem grundsätzlich Gefahren. Bei einer Nichtbeobachtbarkeit von Cyber Security Investitionen besteht ein grosses Risiko von Moral Hazard. In diesem Fall reduzieren Unternehmen, die Pflichtversichert sind, ihre Investitionen in Cyber Security, da sie keine ökonomischen Anreize haben weiter zu investieren. Dies steht dem Ziel einer erhöhten Cyber Sicherheit entgegen. Hier müsste mit unrealistisch hohen Selbstbehalten gearbeitete werden, um überhaupt Anreize zu schaffen, weiterhin in Cyber Security zu investieren und somit den gesamtschweizerischen Standard auf einem vernünftigen Niveau zu halten. Diese unreastisch hohen Selbstbehalte wiederum hebeln den Nutzen eines Versicherungobligatoriums aus. Moral Hazard und die geringe Relevanz von Drittschadenkomponenten sind daher zentrale Argumente gegen ein Versicherungsobligatorium. Eine Versicherungspflicht ist ebenfalls nicht attraktiv aus einer Risikoselektions-Perspektive. Versicherer sollten aus ökonomischen Überlegungen heraus entscheiden können, welche Risiken sie ins Portfolio nehmen und zu welchen Konditionen, sofern es keine gesellschaftlichen Obliegenheiten gibt, die einem freien Markt entgegenstehen wie z.B. bei der Sozialversicherungspflicht. Dies ist eine Voraussetzung, um effiziente Versicherungslösungen anbieten zu können. Ein Obligatorium würde zudem bedingen, dass fächendeckende Kapazitäten bestünden. Die Verfügbareit dieser Kapizitäten ist zum aktuellen Zeitpunkt fraglich.

Schliesslich stellt sich die Frage, ob es ein *staatliches Backup* für Cyber Risiken analog zum Elementarschadenpool braucht. Derartige extreme staatliche Eingriffe finden wir heute insbesondere bei Risiken, die zu potenziell schwerwiegenden Schäden bei Dritten führen können oder für die der Markt keine Absicherung aufgrund verschiedenster Probleme der Versicherbarkeit anbietet. Beispiele hierfür sind Terror- (Terror Risk Insurance Act, Pool Re), Naturkatastrophen- (japanisches Erdbeben Rückversicherungs-Programm) oder Atom-Risiken. Der Staat kann hier die entsprechenden Risiken entweder direkt (als Erstversicherer) selbst tragen, als Rückversicherer der Assekuranz für Gross-Schäden auftreten, als „Lender of Last Resort" agieren und kurzfristig die Liquidität der Assekuranz sicherstellen oder die Herausbildung eines Versicherungsmarktes unterstützen, indem er ein Umfeld schafft, in dem der private Versicherungssektor sich entwickeln kann. In vielen dieser Konstruktionen können im Optimum das Wissen privatwirtschaftlicher Versicherer und Rückversicherer bezüglich der Risiken mit den finanziellen Ressourcen der öffentlichen Hand kombiniert werden.

Hier lassen sich zwei Bereiche unterscheiden. Es gibt ein breites Spektrum an Cyber Risiken und Industrien, für die die Assekuranz derzeit bereits Deckungen anbietet bzw. durch Verbesserungen der Versicherbarkeit anbieten kann. Hier bedarf es für explizite Cyber Deckungen (sog. affirmative Deckung) aus heutiger Sicht grundsätzlich kein staatliches Backup. Die Entwicklung des Ausmasses und insbesondere der Frequenz von Extremszenarien bleibt aber kritisch zu beobachten und bedeutet, dass das Thema staatliches Backup regelmässig diskutiert werden muss. Darüber hinaus gibt es den Bereich der heute nicht versicherten Risiken, zu denen auch (aber nicht nur) die kritischen Infrastrukturen gehören, und sogenannten „stillen" Deckungen. Stille Deckungen resultieren aus Deckungen in klassi-

---

[12] Ferner gibt es Versicherungspflicht im Bereich der Sozialversicherung; so sollten aus sozialen Gesichtspunkten und aufgrund der Adversen Selektion alle Arbeitnehmer in der Arbeitslosenversicherung sein; die sozialen Argumente sind für commercial insurance allerdings nicht so naheliegend.

[13] Zu beachten ist aber die zunehmede Konvergenz des US und europäischen Rechtsystem, z.B. im Bereich der Sammelklagen. Dennoch ist aus heutiger Sicht eine Versicherungspflicht für Cyber Risiken nicht naheliegend, wobei sich diese Einschätzung nach der Einführung von Meldepflichten (die in der aktuellen Revision des Schweizer Datenschutzgesetzes vorgesehen ist) und einer weiteren Konvergenz des US und europäischen Rechtssystems ändern kann.

schen Policen, welche heute zusätzlich durch Cyber Risiken ausgelöst werden können. Die Cyber-Komponente ist hier nicht explizit eingeschlosse und somit eingepreist noch explizit ausgeschlossen und das Ausmass von Schäden aus Extremszenarien derzeit unklar. Für kritische Infrastrukturen und einige der derzeit nicht versicherten Risiken besteht typischerweise ein geringerer Risikoappetit der Assekuranz vollumfängliche Deckungen anzubieten (bzw. nur zu bestimmten Konditionen), insbesondere da Schäden aus einigen Extremszenarien die Kapazitäten der Versicherungswirtschaft übertreffen. Sollte die Versicherungswirtschaft in diesem Bereich eine aktivere Rolle spielen oder weitere Deckungslücken, für die die Assekuranz keine Deckungen anbieten kann, offensichtlich werden, so wäre eine Partnerschaft mit dem Staat als zusätzlicher expliziter Risikoträger sinnvoll.[14] Hier wäre zu definieren, wo die Grenzen liegen und anhand welcher Kriterien Grenzen gezogen werden. Die Bestimmung klarer Deckungsgrenzen, bei der der Staat einspringt, kann zudem generell der Marktentwicklung dienlich sein, da diese für Anbieter von Cyber Versicherungen – v.a. im Rückversicherungsbereich – Unsicherheiten in Bezug auf Maximalverluste reduzieren würde.

Key Message: Um die Versicherbarkeit von Cyber Risiken zu verbessern und somit die Effizienz dieses Mechanismus und dessen Nutzen zu erhöhen, können sowohl der Markt als auch der Staat intervenieren. Eine Rolle des Staates bei Extremereignissen, z.B. bei kritischen Infrastrukturen, ist implizit im Staatszweck verankert, ausserhalb dieses Rahmens ergeben sich zahlreiche potenzielle Eingriffsmöglichkeiten, von denen hier einige diskutiert werden. (1) Prinzipien-basierte, gesetzliche oder implizite Markt-basierte Cyber Security Mindeststandards sind technischen, Regel-basierten gesetzlichen Vorgaben vorzuziehen und können der Marktentwicklung wie auch gesamtschweizerischen Cyber Resilienz Niveau dienen; (2) freiwillige oder verpflichtende Meldesysteme können Wege sein, sowohl Sicherheit als auch den gesamtwirtschaftlichen Nutzen zu fördern. Unternehmen können sich in Datenpools zusammenschliessen, um die Bewertbarkeit und Modellierung insbesondere von Extremereignissen zu verbessern. Hierfür müssen die rechtlichen Rahmenbedingungen geschaffen werden. (3) Von einem Versicherungsobligatorium ist sowohl aus gesamtwirtschaftlicher wie auch versicherungstechnischer Sicht abzusehen. (4) Ein staatliches Back-up ist eine Option, die möglicherweise zu einem späteren Zeitpunkt nochmals in Erwägung gezogen werden muss, falls nicht genüngend Marktkapazität oder wesentliche Marktlücken entstehen aufgrund adverser Entwicklungen hinsichtlich Ausmass und Frequenz von Cyber Vorfällen.

[14] Letztendlich geht ein staatliches Backup für gravierende Ereignisse im Bereich der kritischen Infrastrukturen implizit aus dem Staatszweck hervor (Nach Art. 2 der Bundesverfassung ist Aufgabe der Staatsorgane die Sicherheit des Landes zu gewährleisten).

4 Quellenverzeichnis

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

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

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

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

Biener, C., Eling, M., and J. H. Wirfs, 2015b, Cyber Risk: Risikomanagement und Versicherbarkeit, I.VW Schriftenreihe, Band 54.

Böhme, R., 2005, Cyber-insurance revisited, 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.

Cambridge Centre for Risk Studies, 2016, Managing Cyber Insurance Accumulation.

Campbell K, Gordon L.A, Loeb M.P. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. Journal of Computer Security, 11, 431-448.

Cavusoglu H, Mishra B, Raghunathan S. (2004). The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers. International Journal of Electronic Commerce, 9(1), 69-104.

CRO Forum, 2016, CRO Forum Concept Paper on a proposed categorisation methodology for cyber risk.

Das S, Mukhopadhyay A, Anand M. (2012). Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. Journal of Information Privacy & Security, 8(4), 27-54.

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.

Gatzlaff, A. Mccullough. (2010).The Effect of Data Breaches on Shareholder Wealth. Risk Management and Insurance Review, 13(1), 61- 83.

Goel S, Shawky H. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. Information & Management, 46(7), 404-410.

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.

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.

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.

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.

Hovav A, Andoh-Baidoo F, Dhillion G. (2007). Classification of Security Breaches and Their Impact on the Market Value of Firms. In Proceedings of the 6th Annual Security Conference.

Hovav A, D'Arcy J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. Risk Management and Insurance Review, 6(2), 97-121.

Hovav A, D'Arcy J. (2004). The Impact of Virus Attack Announcements on the Market Value of Firms, Information Systems Security, 13(3), 32-40.

Ishiguro M., Tanaka H, Matsuura K, Murase I. (2006). The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market. In: The Workshop on the Economics of Securing the Information Infrastructure, WESII.

KPMG, 2017a, Transforming companies must put cyber security front and center, Global Cyber Security

KPMG, 2017b, Insurance Thinking Ahead: Versicherungen im Zeitalter von Digitalisierung und Cyber Studienteil B: Cyber

Laury, S. K., and C. A. Holt, 2008, Chapter 84 Voluntary Provision of Public Goods: Experimental Results with Interior Nash Equilibria, in: Handbook of Experimental Economics Results, Volume 1: pp. 792–801.

McAfee, 2014, Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, Center for Strategic and International Studies.

MELANI, 2016, Merkblatt IT-Sicherheit für KMUs.

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.
PWC, 2015, Insurance 2020 & beyond: Reaping the dividends of cyber resilience.
Romeike, F., B. Brühwiler, 2010, Praxisleitfaden Risikomanagement.
Shackelford, S. J. (2012): Should your firm invest in cyber risk insurance? In: Business Horizon 55, 349-356.
Yayla A.A, Hu Q. (2011). The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors. Journal of Information Technology 26(1), 60-77.