HSLU Hochschule Luzern

Cyber Risk Management in grösseren Schweizer Unternehmen

Mit Fokus auf Cloud-Computing

Autoren: Prof. Dr. Stefan Hunziker, Prof. Armand Portmann, Prof. Viviane Trachsel, Fernand Dubler

Mehr Infos unter
hslu.ch/ifz
hslu.ch/informatik

Partner:

die Mobiliar

economiesuisse

FH Zentralschweiz

Impressum

Autorenschaft:

Prof. Dr. Stefan Hunziker
Prof. Armand Portmann
Prof. Viviane Trachsel
Fernand Dubler

Partner:

Schweizerische Mobiliar Versicherungsgesellschaft AG (nachfolgend «Mobiliar»)

Ein Unternehmen der Schweizerischen Mobiliar Genossenschaft
Kontakt:
Medienstelle der Mobiliar
Bundesgasse 35
3001 Bern
T 031 389 88 44
media@mobiliar.ch

economiesuisse
Verband der Schweizer Unternehmen
Hegibachstrasse 47
Postfach
8032 Zürich

Hochschule Luzern – Wirtschaft
Institut für Finanzdienstleistungen Zug IFZ
Campus Zug-Rotkreuz
Suurstoffi 1
CH-6343 Rotkreuz
ifz@hslu.ch
www.hslu.ch/ifz

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz
Suurstoffi 1
CH-6343 Rotkreuz
informatik@hslu.ch
www.hslu.ch/informatik

ISBN 978-3-906877-97-6

Vorwort Hochschule Luzern

Es scheint fast überflüssig zu erwähnen, dass Cyber Risiken mittlerweile eine global relevante Risikokategorie bilden, die zunehmend an Relevanz gewinnt. Es ist deshalb kaum überraschend, dass z. B. der WEF Risk Report 2022, der Cambridge Global Risk Index 2021 sowie die Funk Global Risk Consensus-Studien Cyber Risiken unter den globalen Top-Risiken führen. Gründe für die stark zunehmende Bedrohung durch Cyber Risiken sind vielfältig. Nicht zuletzt hat die durch die Pandemie ausgelöste Verlagerung der Arbeit ins Homeoffice für neue Herausforderungen gesorgt. Ganz allgemein nehmen wir Entwicklungen in Richtung Cloud-Computing, zunehmender Virtualisierung des Arbeits- und Privatlebens, stärkere Vernetzung mit dem Internet, auch im industriellen Umfeld (Industrial Internet of Things) u. v. m. wahr, die nebst allen Vorteilen auch zusätzliche Cyber Risiken bergen. Eine Neuerscheinung sind Cyber Risiken aber keinesfalls. Sie existieren, seit es Computer-Netzwerke gibt. Cyber Risiken haben sich aber u. a. mit den Entwicklungen in Technologie, digitalen Geschäftsmodellen und den immer stärker vernetzten Informations-, Kommunikations- und Lieferketteninfrastrukturen nach und nach zu einem unternehmerischen, aber auch systemischen «Top-Risiko» entwickelt.

Besondere Erwähnung sollten an dieser Stelle Cloud-Services und die damit verbundenen Risiken bekommen. Cloud-Services haben in den vergangenen Jahren einen regelrechten Boom erlebt. Dies liegt insbesondere daran, dass sie in vielerlei Hinsicht äusserst attraktiv sind. Die eigene IT muss nicht für jede neue Anwendung eine/n Spezialisten/-in ausbilden, die Anbieter sorgen für die kontinuierliche Weiterentwicklung der Services, Wachstum kann einfach durch eine Erhöhung des eingekauften Leistungsvolumens abgedeckt werden, die Systeme werden von den oft zertifizierten Anbietern seriös gewartet, um nur einige der Vorteile zu erwähnen. Dem stehen aber nicht zu unterschätzende Risiken gegenüber: Datenschutz und weitere rechtliche Unsicherheiten, Vertraulichkeit der Daten, Abhängigkeit von einem einzelnen Anbieter (Vendor Lock-in), Know-how Verlust, Kontrollverlust, Zunahme der Komplexität, da Cloud-Anbieter in diverse Massnahmen und Prozesse eingebunden werden müssen (z. B. Business Continuity Management (BCM)).

Aufsichtsorgane sind zunehmend gefordert, ihre rechtlichen Kontroll- und Aufsichtspflichten auch im Bereich Cyber Risk Management wahrzunehmen. Der angemessene Umgang mit Cyber Risiken gehört zu den unübertragbaren und unentziehbaren Aufgaben jedes Aufsichtsorgans. Nebst dieser rechtlichen Verpflichtung, die u. a. mit den Entwicklungen bez. der Datenschutz-Grundverordnung der EU (DSGVO) sowie der Revision des Schweizerischen Datenschutzgesetzes (DSG) zunehmend anspruchsvoller wird, gibt es auch aus betriebswirtschaftlicher Sicht gute Gründe, in das Cyber Risk Management zu investieren. Cyberangriffe können einen erheblichen Schaden in Organisationen verursachen, die im schlimmsten Fall hohe Bussen, starke Reputationseinbussen, einen Entzug der Betriebsbewilligung oder den Konkurs bedeuten können.

Organisationen und ihre Leitungsgremien tun gut daran, Cyber Risiken nicht ausschliesslich als «technisches IT-Problem» zu verstehen. Vielmehr sollten sie diese als integralen Bestandteil ihres Risikoportfolios betrachten und ihre Auswirkungen auf Organisationsziele (Finanzen, Reputation, Strategie) analysieren.

Prof. Dr. Stefan Hunziker	**Prof. Armand Portmann**	**Prof. Viviane Trachsel**	**Fernand Dubler**
Leiter Kompetenzzentrum Risk & Compliance Management	Themenfeldverantwortlicher Information & Cyber Security | Privacy	Dozentin und Projektleiterin mit Schwerpunkt Controlling	Wissenschaftlicher Mitarbeiter Information & Cyber Security | Privacy

April 2022

Vorwort Mobiliar

Die Digitalisierung erleichtert unser Privat- und Berufsleben. Aber sie birgt Risiken. Geschäftsmodelle werden vernetzter. Services verlagern sich vermehrt in die Cloud. Informations- und Kommunikationsprozesse und Abhängigkeiten zu Lieferanten bergen weitere Cyber Risiken. Die Gefahrenkategorie «Cyber» ist ein systemisches Top-Risiko für Unternehmen geworden.

Wir als Versicherer sind deshalb gefordert. Mit unserer Cyber Versicherung ermöglichen wir Unternehmen einen bedürfnisgerechten Risikotransfer. Und wir stehen unseren Kund/-innen kompetent zur Seite. Seit fünf Jahren haben wir ein Kompetenzzentrum Cyber Risk, das passende Cyber Risiko Lösungen sowie Services und Dienstleistungen im Bereich der Sensibilisierung, Prävention und Assistance im Ereignisfall anbietet. Und es kennt sich bei Fragen zur IT- und Informationssicherheit aus.

Wir wissen also, wovon wir reden. Als Versicherungsunternehmen ist die Mobiliar eine Teilnehmerin am Finanzmarkt, auf dem verschiedene Regeln und Vorschriften gelten. Dabei gilt nicht nur die IT-Sicht: den Einfluss von Cyber Risiken in die Geschäfts- und Unterstützungsprozesse stimmen wir mit unserem Risk Management ab. Dabei ist der personelle und finanzielle Aufwand für die Cybersicherheit und damit für den Datenschutz unserer Kund/-innen gross.

Die Ziele für einen vereinfachten digitalen Kundenalltag und einem angemessenen Schutz vor Cyber Risiken gehen oft auseinander. Wer hat Recht? Der Manager, der seinen Kund/-innen einfache digitale Zugänge zum Geschäft bieten will? Der CISO, der seine Vorgaben und Vorschriften durchsetzen muss? Der Risikodialog zwischen diesen Funktionen ist ein Erfolgsfaktor für eine ganzheitliche Risikobetrachtung, -steuerung und -kontrolle. Die Studie sagt aus, dass Organisationen Cyber Risiken nicht nur aus einer technischen Perspektive beurteilen. Sie sollten auch deren Auswirkungen auf die Organisationsziele wie Risikobewusstsein, Finanzen, Reputation oder Strategie berücksichtigen.

Die aufgezeigten Schwachpunkte in der Studie in Bezug auf deren Anwendbarkeit muss jedes Unternehmen für sich beurteilen. Ungeachtet der technischen Massnahmen kann ein Unternehmen mit dem gezielten Aufbau einer Risikokultur gegenüber Cybergefahren bereits viel erreichen. Für diese Stärkung der Widerstandsfähigkeit ist ein Mix von personenbezogenen, technischen, organisatorischen und physischen Massnahmen wichtig.

Als Leiter vom Kompetenzzentrums Cyber Risk handle ich für unsere Kund/-innen im Breitengeschäft für Privatpersonen und KMU sowie im Individualgeschäft für grössere Unternehmen. Letztere wurden in der Studie deshalb auch nach der Rolle der Versicherungsgesellschaften bei der Cyber-Risikoidentifikation befragt. Mich erstaunt es, dass die steigende Gefahr von Cyber Risiken kaum Thema in den Gesprächen mit den Versicherungsgesellschaften ist. Auch Handlungsempfehlungen und Bedarfsabklärungen bei einem etwaigen Restrisiko werden wenig angesprochen. Dieser Cyber-Risikodialog würde nicht nur im Risikoverständnis und Bewusstsein helfen, sondern unter anderem auch in der Risikoeinschätzung, Festlegung der Risikoakzeptanz sowie Überwachung. Deshalb sollte nicht nur die Minderheit der Befragten, sondern die Mehrheit der Firmen auf den Cyber-Risikodialog mit der Versicherungsgesellschaft setzen. Diesen Dialog wollen wir als Mobiliar mit unseren Unternehmenskunden auf jeden Fall fördern.

Ich danke der Hochschule Luzern und economiesuisse, welche die vorliegende Marktstudie für grössere Unternehmen gemeinsam mit uns ermöglicht haben. Die Erkenntnisse helfen uns, die Herausforderungen, Bedürfnisse und Anforderungen unserer Kund/-innen zu verstehen und mehrwertbringende Services im Bereich Cyber Risk weiterzuentwickeln.

Andreas Hölzli

Leiter Kompetenzzentrum Cyber Risk
Mobiliar

April 2022

Vorwort economiesuisse

Das Thema Cybersicherheit betrifft uns alle, die Wirtschaft wie auch die Gesellschaft. Sie ist längst nicht mehr ein abstraktes, isoliertes Thema für Computerspezialisten/-innen, sondern ausgesprochen konkret und überall präsent. Immer wieder liest man Artikel über Cyberangriffe auf Schweizer Unternehmen und Verwaltungen oder man wurde sogar selbst Opfer von Kriminalität im Internet. Dabei widerspiegelt die Zahl der medial besprochenen Attacken mit hoher Wahrscheinlichkeit nur einen Bruchteil der tatsächlichen Angriffe. Zum einen ist das auf die schiere Menge der Angriffe zurückzuführen zum anderen aber auch darauf, dass nicht alle Cyberangriffe bekannt oder überhaupt erst entdeckt werden. Unter Cyberexperten/-innen gibt es dazu ein passendes Bonmot: Es existieren heute nur noch zwei Arten von Unternehmen – solche, die bereits gehackt wurden und solche, die dies noch nicht wissen.

Die fortschreitende Digitalisierung hat mehrheitlich positive Folgen. Leider ergeben sich damit einhergehend auch immer mehr und neue Angriffsflächen für Kriminalität im digitalen Raum. Vieles ist heutzutage vernetzt und mit dem Internet verbunden, sei dies der Firmenwagen, die Videoüberwachung oder die Fräsmaschine. Jedes neue Gerät, welches wir an unsere Netzinfrastruktur anschliessen, erhöht das Risiko, dass Cyberverbrecher/-innen eine Lücke finden und diese für sich nutzen. Entscheidend ist vor diesem Hintergrund, dass wir lernen, mit welchen Mitteln wir uns zielgerichtet und effizient schützen können. Dazu braucht es ein Minimum an Disziplin. Die nötigen Updates müssen durchgeführt, Passwörter regelmässig geändert und die Funktionsfähigkeit der Systeme überprüft werden. Nachlässigkeiten führen direkt zu einer erhöhten Angriffsfläche für Internetkriminelle. Während viele Unternehmen hier bereits wichtige Vorkehrungen getroffen haben, ist dies im Privaten häufig nicht der Fall. So wurde mit der vermehrten Arbeit im Homeoffice, eine beachtliche Zunahme an Angriffen festgestellt. Statt Angriffe über das Unternehmensnetzwerk vorzunehmen, wurden Sicherheitslücken der privaten Netzwerke der Arbeitnehmenden ausgenutzt.

Gegen Angriffe im Cyber-Raum ist niemand gefeit. Wöchentlich werden dem Nationalen Zentrum für Cybersicherheit weit über 200 Meldungen gemacht – von einer hohen Dunkelziffer darf hierbei ausgegangen werden. Auch im Jahr 2022 gab es bereits gewichtige Opfer aus der Wirtschaft und der Verwaltung. Eine beliebte Form der Kriminalität ist die Ransomware: Eine stetige Anzahl Schweizer Unternehmen sieht sich plötzlich vor die Frage gestellt, ob sie für die durch Schadsoftware vorgenommene Ver- und Entschlüsselung ihrer Daten Geld bezahlen soll.

Zu viele leichte Opfer versprechen schnelle Beute und motivieren neue Angriffe. Doch was bedeutet diese Gefahr für die Schweizer Wirtschaft und was gilt es zu tun? Die von Cyberangriffen ausgehende Gefahr ist zwar im Bewusstsein vieler von uns angekommen. Damit ist es jedoch nicht getan. Es braucht darüber hinaus eine abgeklärte Analyse der Risiken und die Bereitschaft, sich mit den Gefahren auseinanderzusetzen und angemessene Lösungen zu finden.

Das Thema kann dabei nicht einfach an einen Informatik-Verantwortlichen delegiert werden. Sowohl die Unternehmensführung als auch die einzelnen Mitarbeitenden sollten sich den Gefahren noch stärker bewusst sein, denn letztlich ist trotz aller Digitalisierung weiterhin der Mensch das grösste Sicherheitsrisiko. Dafür braucht es ein Firmenkultur, die das Thema ernst nimmt.

Darüber hinaus braucht es aber auch das nötige Know-How, um Angriffen bestmöglich vorzubeugen sowie konkrete Lösungsansätze, wie bei einer Cyberattacke vorgegangen werden soll. Für alle Unternehmen, nicht nur die in der Studie abgedeckten, sondern auch für KMU, sind solche Massnahmen oftmals eine Herausforderung. Doch auch für sie ist Cybersecurity von grundlegender Bedeutung für den Erfolg und sogar das Überleben ihres Betriebs.

Als Verband möchten wir dazu beitragen, dass wir uns alle - Wirtschaft wie auch Gesellschaft - der Risiken im digitalen Raum stärker bewusst werden. Wir müssen unser Verhalten anpassen und uns mit den geeigneten Mitteln schützen. Es ist mir ein persönliches Anliegen, hierzu einen Beitrag zu leisten und die Schweizer Wirtschaft betreffend Cybersecurity zu informieren. Die vorliegende Studie soll dazu beitragen das Thema sichtbar zu machen und den Handlungsbedarf in den Unternehmen aufzuzeigen und uns allen helfen, unsere Abwehrkraft gegenüber den Risiken der digitalen Wirtschaft zu stärken.

Monika Rühl

Vorsitzende der Geschäftsleitung
economiesuisse

April 2022

Inhaltsverzeichnis

Die Studie im Überblick

Hintergrund und Methodik

Im Rahmen der Studie wurden 33 Interviews mit Risk Management-Verantwortlichen und CISOs in 18 grösseren Schweizer Unternehmen aus unterschiedlichen Branchen geführt. Ziel der Studie ist es, ein tiefgreifendes Verständnis über die Herausforderungen im Umgang mit Cyber Risiken und Cloud-Computing zu erhalten.

Risk Governance

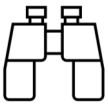
Zentrale Herausforderungen in den Organisationen sind die Definition von Cyber Risikoappetit (Risikobereitschaft), die Integration von Cyber Risiken in das Enterprise Risk Management (ERM) sowie die Zusammenarbeit zwischen CISO und Risk Management-Verantwortlichen. Zu oft liegt die Verantwortung von Cyber Risiken noch bei der «IT».

Risikokultur

Die Awareness bez. Cyber Risiken ist in den Leitungsgremien in allen Organisationen hoch bis sehr hoch, allerdings bestehen häufig Know-how-Defizite bez. der relevanten Cyber Risiken, deren Einfluss auf die Organisationsziele sowie den schützenwerten Assets in den Aufsichtsorganen.

Risk Management im Cyber Raum

Cyber Risiken durchlaufen grundsätzlich denselben Risk Management-Prozess wie alle anderen Risikokategorien. Einige Organisationen verlassen sich in Bezug auf die Identifikation und Beurteilung dieser Risiken auf externe Dienstleister, die meisten nutzen kein systematisches Vorgehen anhand einer Norm oder eines Standards.



Ausblick

In Zukunft gilt es die Lücke zwischen der bereits hohen Aufmerksamkeit der Leitungsgremien bez. Cyber Risiken und dem tatsächlichen Reifegrad des Cyber Risk Managements zu schliessen, insbesondere im Bereich der Risk Governance.

Teil I: Einleitung

Die vom Institut für Finanzdienstleistungen Zug IFZ und dem Departement Informatik durchgeführte Praxiserhebung in grösseren Schweizer Unternehmen nimmt sich verschiedenen Fragen rund um die Themen Cyber Risk Management, dessen Integration in das unternehmensweite Risk Management (ERM) und Cloud-Computing an. Die Studie wurde in Kooperation mit der Mobiliar und economiesuisse durchgeführt.

1. Hintergrund und Relevanz

Aufgrund der unbestrittenen Relevanz von Cyber Risiken müsste man heutzutage annehmen dürfen, dass in den meisten Organisationen ein entsprechender Reifegrad im Umgang mit dieser Risikokategorie erreicht worden ist. Allerdings sind zahlreiche praktische Herausforderungen im Umgang mit Cyber Risiken bekannt, die teilweise auch auf andere Risikokategorien zutreffen. Cyber Risiken sind grundsätzlich operative Risiken, jedoch weisen sie innerhalb dieser Risikokategorie einige spezifische Eigenschaften auf, die den Umgang mit ihnen erschweren. Z. B sind Cyber Risiken «emergent», sie zählen also zu den neuartigen, zukunftsbezogenen Risiken, die sich dynamisch entwickeln («Emerging Risks»). Das heisst, Cyber Risiken entstehen durch Innovationen im IT-Bereich laufend neu, so dass wir viele heute noch gar nicht kennen, die aber morgen hochgradig relevant sein können. Zudem sind Emerging Risks oft so genannte «low-probability, high-impact»-Risiken, die speziell im IT-Umfeld sehr dynamisch sein können: Neue Risiken treten schnell und unverhofft auf und verändern sich laufend über die Zeit, eine Art «Katz-Maus-Spiel» zwischen neuen Risiken und entsprechender Gegenwehr wäre hier eine angemessene Metapher. Cyber Risiken bringen oft eine hohe Unsicherheit bei der Bewertung von Eintrittswahrscheinlichkeit und finanziellem Schaden mit sich, und hier eröffnet sich gleichzeitig ein grosses Problem im ERM: Dieses steuert in erster Linie bereits bekannte Risiken (Rückspiegel) und ist per se weniger geeignet, angemessen mit Emerging Risks umzugehen.

Weiter fokussiert die Risikobeurteilung von Cyber Risiken traditionell eher die technischen Aspekte, da sie oft in den «technischen Silos» auf Systemebene beurteilt werden und sich den technischen Standards bedienen. Dies ist grundsätzlich korrekt und auch sehr wichtig. Allerdings fehlen oft die betriebswirtschaftlichen Verbindungen zu den nächsten Organisationseben (z. B. Geschäftsbereich) und in die oberste Unternehmensführung (z. B. Konzernebene). Eine Szenarioanalyse, die Folgerisiken u. a. für Mensch, Reputation, Finanzen, Strategie und Unternehmensziele sicht- und bewertbar macht und Risikoabhängigkeiten mit anderen Unternehmensbereichen analysiert, bleibt meist noch aussen vor. Oder sie geschieht eher ad hoc und unsystematisch. Der Risikoeintritt eines Cyber Risikos kann z. B. zu einem Reputations- und Vertrauensverlust in der Öffentlichkeit oder bei der Kundschaft führen. Ebenso zeigt die Literatur, dass der Fokus bei der Mitigation von Cyber Risiken stark auf der Anwendung von präventiven Grundschutzmassnahmen liegt. Welche tatsächlichen Schäden bei Risikoeintritt resultieren und wie man damit umgehen soll (z. B. ist das Restrisiko akzeptabel? Müsste eine Cyber-Versicherung abgeschlossen werden?), ist oft wenig analysiert.

Lohnen sich Investitionen in das Cyber Risk Management? Eine Möglichkeit wäre, den so genannten ROSI (Return on Security Investment) zu messen. Allerdings zeigen Praxiserfahrungen, dass viele Unternehmen diesen nicht berechnen. Auch weist die Kennzahl konzeptionelle Probleme auf, da leider nur Kosten versus Kosten verglichen werden. Ein «echter» Return on Investment, der direkt über Mehreinnahmen oder Kosteneinsparungen bestimmt wird, liegt mit ROSI nicht vor. Zudem sind die zu verwendenden Parameter nur so gut, wie der zugrunde liegende Cyber Risk Management-Prozess, der die Inputfaktoren «(glaubwürdige) Verlusterwartungen», «Eintrittshäufigkeiten» und «Wirksamkeit der Massnahmen» hervorbringen muss. Cyber Risk Management kann einen strategischen Return generieren: Kompetitive Vorteile (Erträge, Gewinne, generelle Zielerreichung), organisatorische Effektivität und erhöhte Resilienz sind die Früchte, die mit gutem Cyber Risk Management geerntet werden können. Allerdings beobachtet man trotz der unbestrittenen Relevanz dieser Risikokategorie in der Unternehmenspraxis eher ein latentes «underinvestment» in der Cybersicherheit. Das hat verschiedene Gründe: Nebst der Wahrnehmung, dass Cyberrisiken nicht nur unternehmensspezifische, sondern gesellschaftliche und staatliche Bedrohungen darstellen, sorgen auch die meist nicht direkt ersichtlichen und komplexen Ursache-Wirkungsketten (Cyberrisiko führt unmittelbar zu bewertba-

rem finanziellem Schaden) sowie der Fokus auf Kostenvermeidung (und nicht auf Gewinnerhöhung) eher für eine Unterinvestition in diese Risikokategorie.

«Risk Governance eats Risk Management for breakfast», inspiriert vom berühmten Zitat von Peter Drucker, passt (allerdings nicht nur) im Umgang mit Cyber Risiken meistens recht gut. Darunter verstehen wir alle Herausforderungen bezüglich Rollen, Verantwortlichkeiten, Risikokultur, Vorleben durch die Unternehmensleitung und organisatorischer Kompetenz im Umgang mit Cyber Risiken. Haben Sie auch schon einmal jemanden sagen hören, für Cyber Risiken sei die IT-Abteilung oder der CISO verantwortlich? Oder Cyber Risiken seien ein «IT-Problem»? Vermutlich ja. Aus einer rechtlichen und einer Governance-Perspektive ist dies selbstverständlich höchst problematisch, da damit die Verantwortlichkeiten für Cyber Risiken von der Unternehmensleitung an die IT delegiert werden und Cyber Risiken aus dem Zuständigkeitsbereich des Risk Management-Verantwortlichen faktisch wegfallen. Ein diesbezügliches Extremszenario wäre z. B., wenn der CISO in Anlehnung an das Three Lines of Defense-Modell alle «Verteidigungslinien» bezüglich Cyber Risk Management bei sich selbst vereint. Besser wäre, wenn der CISO zusammen mit dem Risk Manager die second-line Funktion übernimmt und die Aktivitäten und Umsetzung der IT/des CIO (first-line) kritisch hinterfragt. Selbstverständlich übernimmt die IT eine zentrale Funktion im Cyber Risk-Puzzle, allerdings primär auf Systemebene. Ohne eine Zusammenarbeit von IT, HR, Datenschutz, Recht, Compliance und Geschäftsbereichen ist ein ganzheitliches Cyber Risk Management nicht möglich.

Berechtigterweise stellt sich die Frage, ob es Standards, Normen, Rahmenwerke, Guidelines oder Empfehlungen gibt, wie Cyber Risiken in das ERM integriert werden, damit alle Risiken auf oberster Unternehmensebene verglichen und gesteuert werden können. Werden z. B. die beiden populärsten Empfehlungen für ERM (ISO31000:2018, COSO ERM 2017) mit Standards und Normen der Informationssicherheit (ISO, BSI, NIST etc.) verglichen, stellt man schnell fest, dass diese Standards nur schwerlich vereinbar sind. Paradoxerweise plädieren ISO und COSO zwar für ein ERM, bleiben allerdings eine nachvollziehbare Empfehlung zur Integration von Cyber Risiken schuldig. Die Standards verwenden eine andere Sprache, definieren und bewerten Risiken anders, oder verfolgen keinen risikoorientierten Ansatz, sondern einen kontrollorientierten, der sich nicht einfach in das Risk Management übersetzen lässt.

Allerdings sind in den letzten Jahren erste Bemühungen sichtbar, Cyber Risiken die nötige Aufmerksamkeit im ERM zu widmen. So etwa gibt es das von COSO und Deloitte herausgegebene Papier «Managing Cyber Risk in a digital Age» und das vom National Institute of Standards and Technology (NIST) verfasste Dokument mit Titel «Integrating Cybersecurity and Enterprise Risk Management (ERM)». Beide adressieren grundsätzlich die Forderung nach einer Integration («Alignment») von Cyber Risiken in das Risk Management. Allerdings legen sie lediglich einen ersten Grundstein, der noch viele konkrete Fragen der praktischen Umsetzung offenlässt.

Heute stehen wir vor der Herausforderung, die aus der Forschung stammende Empfehlung, Cyber Risk Management und ERM abzustimmen, in der Praxis erfolgreich umzusetzen. Leider existieren bisher kaum belastbare Praxiserkenntnisse, wie diese Integration am besten umgesetzt wird. Einig ist man sich zumindest, dass Risk Management-Verantwortliche eine zentrale Rolle bei der Abstimmung von Cyber Risk Management und ERM spielen. Sind Unternehmen den Anforderungen gewachsen, die Unternehmensleitung zu sensibilisieren, technische Risiko-Silos zu überwinden, Cyber Risiken zu bewerten, strategische Partnerschaften mit CIO, CFO, CISO und weiteren aufzubauen, Cyber-Versicherungen (mit-)zu prüfen und die Risk Governance future-ready zu gestalten?

Die Autor/innen der vorliegenden Studie führen folgende Herausforderungen hinsichtlich Cyber Risk Management an:

- Cyber Risiken sind teilweise zu wenig in den ERM-Prozess integriert. Diese Integration scheint organisatorisch, kulturell und methodisch herausfordernd zu sein.
- Es existiert grundsätzlich keine kompatible Sprache (Terminologie) zwischen Cyber Risk Management und ERM (CISO und Risk Manager «verstehen» sich oft nicht).
- Abhängigkeitsanalysen zwischen Cyber Risiken und anderen Risiken sind zu wenig vorhanden (z. B. die Pandemie hat Cyber Risiken verursacht, welche wiederum ökonomische Folgen haben).
- Es besteht die Gefahr, dass das Cyber Risk Management zu tief in der Hierarchie verortet ist (IT-Abteilung). Dies kann dazu führen, dass Cyber Risiken zu wenig in die Entscheidungsprozesse bei der Strategie-Entwicklung/-umsetzung eingebunden werden.

- Eine ausgeprägte Risikokultur ist zwingend, um das Risikobewusstsein zu erhöhen und einer Selbstüberschätzung im Umgang mit Cyber Risiken vorzubeugen.
- Der traditionelle Risk Management-Prozess ist nur bedingt geeignet für den proaktiven Umgang mit Cyber Risiken. Diese Risiken sind wenig vorhersehbar, oft noch unbekannt und schnell ändernd in Abhängigkeit der Abwehrmechanismen.
- Die Bewertung der Cyber Risiken folgt einer anderen methodischen Vorgehensweise als bei anderen Risikokategorien. Sie sind oft nicht quantifiziert, berücksichtigen nur das negative Risiko, weisen eine schwache Datengrundlage auf, sind hochdynamisch und lassen sich kaum über Erwartungswerte sinnvoll bewerten.
- Es besteht die Gefahr, zu stark auf die Cyber Risk-Prävention zu fokussieren und die Stärkung der Cyber Resilienz (Sicherung des Geschäftsbetriebs im Schadenfall) zu vernachlässigen.

Die vorliegende Studie hat sich zum Ziel gesetzt, dieses wichtige, aber auch hochkomplexe Thema des Cyber Risk Managements aufzugreifen und nebst der oben angesprochenen Abstimmung mit dem ERM einen Fokus auf die zunehmende Relevanz des Cloud-Computings und der damit einhergehenden Risiken und Herausforderungen zu legen. Ebenso dienten oben zusammengefasste Mängel als Motivation, die vorliegende Studie durchzuführen und zu verstehen, ob und wie diese in der Praxis adressiert werden. Anhand umfangreicher Interviews mit zahlreichen Risk Management-Verantwortlichen und CISOs (oder äquivalente Funktionen) in grösseren Schweizer Unternehmen ist es gelungen, neue Erkenntnisse zu gewinnen, die Licht auf einige der zentralen Herausforderungen im Umgang mit Cyber Risk Management werfen.

Mit dieser Studie sprechen wir alle Schweizer Unternehmen an, insbesondere auch jene, die freundlicherweise an den Interviews teilgenommen haben. Darüber hinaus richtet sich die Untersuchung an alle weiteren interessierten Fachleute und Institutionen, die mit Risk Management-Aufgaben, IT-Sicherheit, Informationssicherheit, Corporate Governance oder der (Weiter-)Entwicklung von Normen und Rahmenwerken betraut sind. Sie sollen dank den Ergebnissen und den daraus abgeleiteten Empfehlungen einen Überblick über die wichtigsten Ansprüche an ein modernes Cyber Risk Management erhalten.

2. Methodisches Vorgehen

Dieses Kapitel beschreibt das dieser Studie zugrunde liegende qualitative, explorative Forschungsdesign sowie die Entwicklung der Interviewleitfäden und stellt die Stichprobe der Studie vor. Die Auswertung der Interviews folgt den Standards inhaltsanalytischer Auswertungen.

Entwicklung Interviewleitfäden

Es wurden zwei semi-strukturierte Interviewleitfäden entwickelt, welche die beiden Themenbereiche «Cloud-Computing» und «Cyber Risk Management» abdecken. Die Entwicklung der Fragebögen folgte einem induktiv-deduktiven Verfahren, wobei die Fragen aus Erfahrungen der Studienautoren/-innen, dem aktuellen Forschungsstand, der einschlägigen Literatur sowie aktuellen Herausforderungen und Interessengebieten der Kooperationspartner gewonnen wurden. Innerhalb der Hauptfragen gab es so genannte Interviewer-Hinweise, die eine aktive Gesprächsführung unterstützten und nur eingebracht wurden, falls seitens Interview-Teilnehmenden Unklarheit über die Frage herrschte oder explizit nach Beispielen zur Veranschaulichung der Fragestellung gefragt wurde. Eine letzte, offen gestellt Frage ermöglichte den Teilnehmenden, Themen einzubringen, die nicht explizit im Fragebogen abgedeckt waren, aber ergänzend als relevant erachtet wurden.

Der *Cloud-Interviewleitfaden* enthält 21 offene Hauptfragen, wobei die letzten fünf Fragen nur bei ausreichend vorhandener Zeit (zweite Priorität) gestellt wurden. Der Fragebogen wurde thematisch in verschiedene Teilbereiche unterteilt:

- Cloud-Strategie
- Risk Management
- Datenschutz
- Haftung
- Informationssicherheit
- Business Continuity Management
- Beendigung der Cloud-Nutzung
- Auswahl und vertragliche Bindung des Cloud-Dienstleisters (optional)
- Service-Qualität (optional)
- Offene Anmerkungsfrage (optional)

Der *Cyber Risk Management-Interviewleitfaden* enthält 20 offene Hauptfragen, wobei die letzten vier Fragen nur bei ausreichend vorhandener Zeit (zweite Priorität) gestellt wurden. Der Fragebogen wurde thematisch in verschiedene Teilbereiche unterteilt:

- (Cyber) Risk Governance
- (Cyber) Risk Culture
- Risiko-Assessment
- Risikosteuerung
- Risikoappetit-Limiten für Cyber Risk (optional)
- Benchmarking von Cyber Risk Management (optional)
- Offene Anmerkungsfrage (optional)

Die Interviews wurden mit einer Ausnahme (schriftliche Antwort) über die Kollaborationsplattform MS Teams online durchgeführt und aufgezeichnet. Die Interviewdauer war jeweils auf 60 Minuten begrenzt. Die Auswertung der Interviews erfolgte in anonymisierter Form, sodass keine Rückschlüsse auf einzelne Interviewpartner/-innen oder Firmen möglich sind.

Praxiserhebung mit semi-strukturierten Interviews

Für die Teilnahme an der Erhebung wurden explizit zwei Personen von jeder ausgewählten Organisation separat interviewt. Dazu wurde ein nicht-repräsentatives Sample aus grösseren Schweizer Organisationen zusammengestellt, welches möglichst verschiedene Branchen repräsentiert. Weitere bekannte Einflussfaktoren auf die Risk Management-Implementierung sind u. a. die Unternehmensgrösse und der Grad der Internationalisierung (vgl. Gordon et al., 2009). In jeder Organisation wurden je zwei Personen identifiziert, die das Cloud- und das Cyber Risk Management-Interview führen konnten. Für den Cloud-Interviewleitfaden wurden primär CISOs oder bei Nichtexistenz dieser Funktion auch IT-Leiter/in, CIOs, ISOs und IT-Security-Verantwortliche angefragt. Für den Cyber Risk Management-Fragebogen wurden primär Risk Manager oder bei Nichtexistenz dieser Funktion die für das Risk Management verantwortliche Person (z. B. GL-Mitglied, CFO, CEO) angefragt. Die Stichprobe repräsentiert somit ein heterogenes Spektrum von Unternehmen aus verschiedenen Branchen, mit unterschiedlicher Grösse, unterschiedlichem Internationalisierungsgrad und ebenso unterschiedlichen rechtlichen Anforderungen bezüglich ihres Risk Managements.

Die Studienautoren/-innen haben für das Sample Kontakte des Instituts für Finanzdienstleistungen Zug IFZ, des Departements Informatik, der economiesuisse und der Mobiliar genutzt (primär Convenience-Sample für Longlist, für die Verdichtung zur Shortlist nach theoretischen

Einflussgrössen auf das Risk Management, siehe oben). Insgesamt wurden 33 Interviews in 18 Organisationen durchgeführt. Die Branchenverteilung des Samples ist in der Abbildung 1 dargestellt.

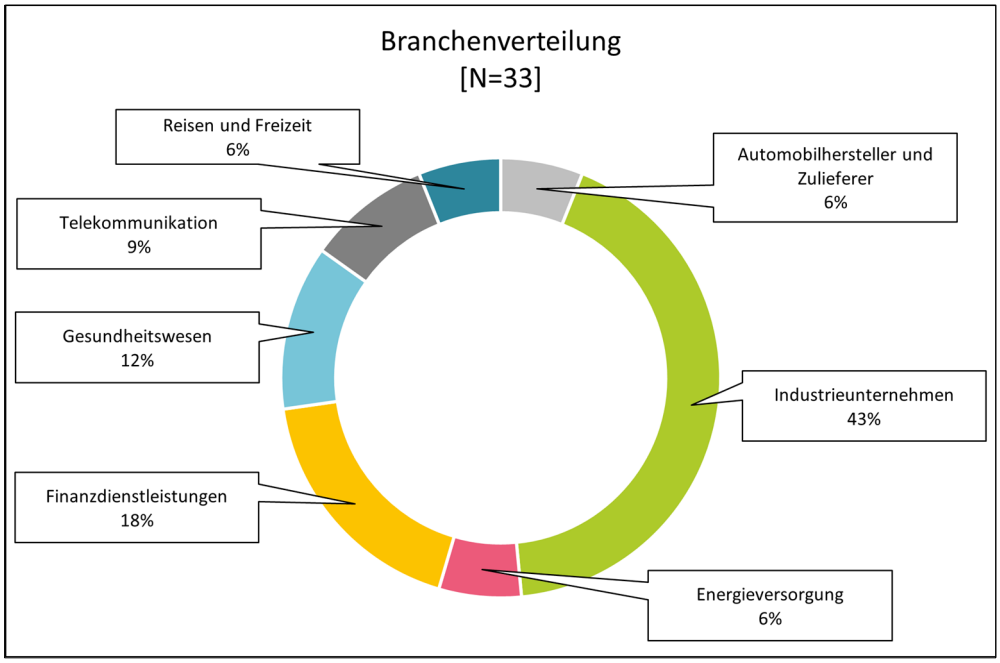


Abbildung 1: Branchenverteilung der Studienteilnehmenden

Inhaltsanalytische Auswertung

Die Interviews basierten auf den oben beschriebenen Interviewleitfäden (zur Konzeption eines Interviewleitfadens vgl. Gläser und Laudel, 2010, S. 142 ff.). Die bewusst offenen gehaltenen Fragen erlaubten ein breites Spektrum an Antworten. Der Vorteil einer qualitativen, explorativen Studie besteht darin, komplexere und bisher wenig erforschte Sachverhalte ganzheitlich und in der Tiefe erfassen zu können. Zudem kann der Interviewer bei Unklarheit Rückfragen stellen. Dies erlaubt es, ein tiefergreifendes Verständnis des noch jungen und wenig erforschten Themas der Integration von Cyber Risiken in das ERM zu erlangen. Dies wäre bei einer grosszahligen, standardisierten Befragung nicht möglich. Nachteilig wirkt sich bei qualitativen Studien hingegen die Nicht-Repräsentativität der Ergebnisse aus.

Basierend auf den Interview-Transkripten wurde eine qualitative und quantitative (deskriptive) Inhaltsanalyse durchgeführt. Die Hauptkategorien für die Inhaltsanalyse wurden deduktiv aus der Struktur der Interviewleitfäden abgeleitet (zur Auswertung der Interviews mittels qualitativer Inhaltsanalyse vgl. Schreier, 2014, S. 6 ff.; Gläser und Laudel, 2010, S. 197 ff.). Die Autorenschaft analysierte die Interviews anhand der Transkripte zunächst selbstständig. Im Anschluss diskutierten die Autoren/-innen die Ergebnisse gemeinsam (vgl. Arena et al., 2010). Bei der Interpretation der jeweiligen Analysen gilt es zu bedenken, dass es sich um qualitative Interviews handelte. Die Ergebnisse können durch die Interviewer und Verfasser/-innen dieser Studie bis zu einem gewissen Grad subjektiv beeinflusst sein. Trotzdem ist die Autorenschaft davon überzeugt, dass die Erkenntnisse die allgemein in der Praxis vorherrschenden Auffassungen und Meinungen zu den Themen Cloud-Computing und Cyber Risk Management angemessen wiedergeben.

Aufbau der Studie

Die Cyber Risk Management Studie ist wie folgt aufgebaut: Teil I führt in die Thematik ein und präsentiert das forschungsmethodische Vorgehen. Danach werden wichtige Begriffe und Konzepte, die für das Verständnis der Studie von zentraler Bedeutung sind, definiert und erläutert. Teil II präsentiert die empirischen Ergebnisse dieser Studie. Die empirische Analyse bedient sich qualitativer, inhaltsanalytischer Forschungsmethoden und hat die Interviewanalyse zum Gegenstand. Im abschliessenden Teil III werden wichtige Empfehlungen für die Praxis formuliert. Ein Fazit und Ausblick runden diese Studie ab.

3. Begriffe und Konzepte

Nachfolgend werden für das Verständnis der Studie wichtige Begriffe und Konzepte eingeführt und definiert.

Enterprise Risk Management (ERM)

Im modernen Verständnis wird unter Risiko die Abweichung von Zielen sowie die Auswirkungen von Unsicherheiten auf Ziele verstanden. Diese Auswirkungen können nicht nur negativ, sondern auch positiv sein. Positive Abweichungen von der Zielgrösse werden als Chancen bezeichnet. Bei Entscheidungen stehen den Risiken also gleichzeitig Chancen gegenüber, die es ebenfalls zu berücksichtigen gilt. Über die beiden Dimensionen Eintrittswahrscheinlichkeit eines Schadensereignisses und die dadurch verursachten Kosten können Risiken gemessen resp. quantifiziert werden.

Im COSO Enterprise Risk Management-Rahmenwerk 2017 «Integrating with Strategy and Performance» wird Risiko als die Möglichkeit des Auftretens von Ereignissen, welche die Umsetzung der Strategie oder die Zielerreichung beeinflussen können, definiert (vgl. COSO, 2017, S. 9). Während sich Unternehmen häufig auf Risiken mit möglichen negativen Konsequenzen fokussieren, müssen auch Ereignisse mit positiven Folgen berücksichtigt werden. Zudem können Ereignisse, die im Hinblick auf einzelne Ziele vorteilhaft sind, gleichzeitig eine Bedrohung für andere Ziele darstellen (Wechselwirkungen zwischen Risiken).

Der dieser Studie zugrundeliegende Risikobegriff wird demnach wie folgt ausgelegt:

> ! *Risiko ist ein mögliches Ereignis, das sich negativ oder positiv auf die geplante Zielerreichung und die Strategieumsetzung von Unternehmen auswirken kann.*

Während das traditionelle Risk Management einzelne Risiken isoliert betrachtet und Wechselwirkungen zwischen den einzelnen Risiken mehrheitlich vernachlässigt (Silodenken), verfolgt das ERM einen ganzheitlichen, integrierten Ansatz. Die Identifikation, Beurteilung, Steuerung und Integration von Risiken und Chancen in Entscheidungsprozessen stehen dabei im Mittelpunkt. Beim ERM-Ansatz werden mögliche Auswirkungen von Unsicherheiten auf die Fähigkeit und Wahrscheinlichkeit, die Unternehmensziele zu erreichen, explizit berücksichtigt. COSO (2017) definiert ERM folgendermassen:

«The culture, capabilities, and practices, integrated with strategy-setting and its execution, that organizations rely on to manage risk in creating, preserving, and realizing value» (S. 10).

Eine detailliertere Betrachtung der Definition von ERM verdeutlicht, dass Risiken und Chancen nur dann effektiv gesteuert werden können, wenn:

1. die Kultur und die unternehmerischen Fähigkeiten berücksichtigt werden,
2. eine Verbindung zur Strategie und deren Umsetzung hergestellt wird,
3. die Risikosteuerung auf die Strategie und die Unternehmensziele ausgerichtet wird,
4. eine Verbindung zur Wertschaffung und -erhaltung hergestellt wird.

Indem Aufsichtsorgane und Führungskräfte über die unternehmensweiten Risiken und Chancen informiert werden, sollen Entscheidungsprozesse verbessert und damit Wert für die verschiedenen Anspruchsgruppen geschaffen werden. Letztendlich stehen beim modernen ERM-Ansatz die konsequente Verknüpfung von Risk Management und wertorientierter Unternehmensführung im Vordergrund.

ERM wird in dieser Studie in Anlehnung an die obigen Ausführungen wie folgt definiert:

> ! *Unter Enterprise Risk Management wird die unternehmensweite Identifikation, Beurteilung, Steuerung, Berichterstattung und Überwachung von Risiken und Chancen verstanden. Eine Integration von Risikoinformationen in Entscheidungsprozesse ist dabei zwingend.*

Cyber Risk Management

Im Kontext von Fragen zur Sicherheit von IT-Systemen und Netzwerken wurde bereits vor der Jahrtausendwende der Begriff «IT-Sicherheit» verwendet. Mit dem wachsenden Bewusstsein, dass primär Informationen geschützt werden müssen, und zwar unabhängig davon, wo oder wie sie bearbeitet werden, gewann der Begriff «In-

formationssicherheit» zunehmend an Bedeutung. Standardisierungsorganisationen wie die ISO (International Organization for Standardization) nahmen den Begriff ebenfalls auf, z. B. in der Reihe 2700x zum Thema Informationssicherheits-Managementsysteme. Mit der zunehmenden Bedeutung der Vernetzung von Computern, aber auch von Alltagsgeräten (IoT) und industriellen Anlagen (IIoT) mit dem Internet bekamen die Gefahren aus dem «Cyber Space» (als Synonym für das Internet) einen immer grösseren Stellenwert. Der Begriff «Cyber Sicherheit» war geboren. Bis heute gibt es dennoch keine einheitliche Definition für diesen Begriff. Ob damit nun nur der Schutz vor Gefährdungen «von aussen» gemeint ist, oder ob auch Gefährdungen, die ihren Ursprung innerhalb der Unternehmung haben, eingeschlossen sind, bleibt offen. Im Rahmen dieser Studie ist jeweils die Gesamtheit aller Gefährdungen gemeint – der Defekt einer Festplatte gilt somit auch als Cyber Risiko.

Klar ist, dass Cyber Risiken eine zentrale Risikokategorie für jedes Unternehmen darstellen. Die Forschung zeigt, dass die begrifflichen Unsicherheiten ein ganzheitliches, interdisziplinäres Cyber Risk Management stark behindern. Werden Cyber Risiken im Rahmen eines Managementsystems (z. B. ERM) systematisch gesteuert, kann von Cyber Risk Management gesprochen werden. Im Unterschied zum Begriff Cyber Risiken verdeutlicht Cyber Risk Management, dass ein Risk Management-Prozess für das Management von Cyber Risiken eingesetzt wird.

Cloud-Computing

Auch für den Begriff Cloud-Computing gibt es keine allgemein gültige Definition. In der Fachliteratur wird jedoch oft die Definition von NIST verwendet, welches Cloud Computing folgendermassen beschreibt (vgl. Mell & Grance, 2011):

> ! *Cloud Computing ist ein Modell zur Ermöglichung eines flächendeckenden, komfortablen und bedarfsgerechten Netzzugangs zu einem gemeinsamen Pool konfigurierbarer Rechenressourcen (z. B. Netze, Server, Speicher, Anwendungen und Dienste), die schnell und mit minimalem Verwaltungsaufwand oder Interaktion mit dem Diensteanbieter bereitgestellt und freigegeben werden können.*

Ergänzend zu dieser Definition werden folgende charakterisierende Eigenschaften des Cloud Modells aufgeführt:

1. Selbstbedienung auf Abruf. Ein Verbraucher kann Services einseitig und automatisch beziehen, ohne zwischenmenschliche Interaktion mit dem Diensteanbieter.
2. Breiter Netzzugang. Die Services sind über das Netz verfügbar und können über herkömmliche Geräte gesteuert werden.
3. Ressourcen-Pooling. Die effektiven Ressourcen (z. B. Datenspeicher, Rechenzeit, Bandbreite) des Anbieters werden logisch zusammengelegt und können den Kunden/-innen dynamisch und standortunabhängig zugewiesen werden. Es ist möglich, dass mehrere Kunden/-innen sich eine physische Ressource teilen.
4. Schnelle Elastizität. Ressourcen können elastisch bezogen und freigegeben werden, in einigen Fällen auch automatisch, um entsprechend der Nachfrage schnell nach aussen und innen zu skalieren. Für die Kundschaft erscheinen die für die Bereitstellung verfügbaren Ressourcen oft unbegrenzt und können in beliebiger Menge und zu jeder Zeit in Anspruch genommen werden.
5. Gemessener Service. Die Ressourcennutzung kann überwacht, kontrolliert und gemeldet werden, wodurch sowohl für den Anbietenden als auch für den Nutzenden des genutzten Dienstes Transparenz geschaffen wird.

Dienstleistungen aus dem Umfeld des Cloud Computing werden in der Regel in einem der nachfolgend aufgeführten Dienstleistungsmodelle (Service Models) angeboten.

– Software-as-a-Service (SaaS). Endkunden/-innen beziehen eine vollständige Anwendung via Thin-Client-Schnittstelle (wie z. B. Webbrowser) oder Programmschnittstelle. Der Service kann von Verbraucherseite ausschliesslich über begrenzte, benutzerspezifische Anwendungseinstellungen verwaltet werden.

– Platform-as-a-Service (PaaS). Endkunden/-innen erhalten eine Umgebung, welche es ihnen erlaubt eigens erstellte oder erworbene Anwendungen auf der Infrastruktur des Cloud-Diensteanbieters zu betreiben. Dabei liegt die volle Kontrolle über die Anwendungen bei der Kundschaft. Die ihr zur Verfügung gestellte Umgebung wird durch den Cloud-Diensteanbieter kontrolliert und kann von Kundenseite höchstens indirekt über explizit dafür vorgesehene Schnittstellen konfiguriert werden.

– Infrastruktur-as-a-Service (IaaS). In diesem Servicemodell werden der Endkundschaft Verarbeitungs, Speicher-, Netzwerk- und andere grundlegende Rechenressourcen zur Verfügung gestellt, auf

denen sie beliebige Software, einschliesslich Betriebssysteme und Anwendungen, einsetzen und ausführen kann. Die Kundschaft verwaltet oder kontrolliert die zugrunde liegende Cloud-Infrastruktur nicht, hat aber die Kontrolle über Betriebssysteme, Speicherplatz und bereitgestellte Anwendungen sowie möglicherweise eine begrenzte Kontrolle über ausgewählte Netzwerkkomponenten (z. B. Host-Firewalls).

Neben den Dienstleistungsmodellen lassen sich Cloud-Dienstleistungen in einer weiteren Dimension, den so genannten Bereitstellungsmodellen, eingliedern. Die bekanntesten Varianten werden nachfolgend erläutert:

– Private Cloud. Die Cloud-Infrastruktur wird für die ausschliessliche Nutzung durch eine einzelne Organisation bereitgestellt, die mehrere Verbraucher (z. B. Geschäftseinheiten) umfasst. Sie kann durch die Organisation selbst, durch Dritte oder einer Kombination aus beiden, verwaltet und betrieben werden. Die Infrastruktur kann sich in oder ausserhalb der Räumlichkeiten der Organisationen befinden.

– Community Cloud. Die Cloud-Infrastruktur wird für die exklusive Nutzung durch eine bestimmte Gemeinschaft von Organisationen bereitgestellt, die gemeinsame Anliegen haben. Sie kann durch eine oder mehrere der Organisationen selbst, durch Dritte oder einer Kombination aus beiden, verwaltet und betrieben werden. Die Infrastruktur kann sich in oder ausserhalb der Räumlichkeiten der Organisationen befinden.

– Public Cloud. Die Cloud-Infrastruktur wird für die offene Nutzung durch die Allgemeinheit bereitgestellt. Die Infrastruktur befindet sich in den Räumlichkeiten des Cloud-Diensteanbieters.

Obschon das Cloud Computing Paradigma keine Neuheit in der Unternehmenswelt darstellt, ist sein Stellenwert im Laufe der letzten Jahre enorm gestiegen. Anfangs wurde es insbesondere aufgrund der Service Modelle IaaS und PaaS als flexible und skalierbare Alternative zu klassischen IT-Infrastrukturen wahrgenommen. Spätestens jedoch seitdem klassische Anwendungen im Bereich der Büroautomation und Telefonie vermehrt als SaaS Lösungen angeboten werden, beobachtet man eine flächendeckende Adaption von Cloud Services.

Integration von Cyber Risiken ins ERM

Latentes Underinvestment in Cyber Risk Management

Führt man sich die Relevanz dieser Risikokategorie vor Augen, mag die Tatsache, dass in der Praxis die latente Gefahr eines Underinvestment in das Cyber Risk Management zu beobachten ist, erstaunen. Allerdings lassen sich dafür einige wissenschaftliche Erklärungsansätze aus der Psychologie und Verhaltensökonomik anführen. Die Verhaltensökonomie untersucht die Auswirkungen psychologischer, kognitiver, emotionaler, kultureller und sozialer Faktoren auf die Entscheidungen von Einzelpersonen und Organisationen. In Bezug auf das Cyber Risk Management können folgende Faktoren eine Rolle für das Underinvestment spielen (vgl. u. a.Ting, 2019):

– Je komplizierter und ungreifbarer etwas scheint (Cyber Risiken), desto mehr neigen Entscheider/-innen aus Selbstschutz dazu, die Dinge zu einfach, zu optimistisch und zu kontrollierbar sehen zu wollen (Optimism Bias).

– Übermässiges Vertrauen in die Technologie und Sicherheitslage eines Unternehmens aufgrund von Firewalls, Antivirenprogrammen oder IDS/IPS und anderen Verteidigungsmassnahmen kann letztendlich zu schweren Sicherheitsverletzungen führen (Overconfidence Bias).

– Vorfällen wie Log4Shell, Heartbleed, Poodle, Wanna Cry, u. v. m. wurde viel Aufmerksamkeit geschenkt, aber vielleicht hätte es zu dieser Zeit auch andere Risiken gegeben, die mehr Aufmerksamkeit erfordert hätten. Im Kontext der Cyber-Risikoidentifikation bedeutet dies, dass sich Entscheidungsträger/-innen auf naheliegende Risiken, die ihnen als Erstes in den Sinn kommen und medial viel Aufmerksamkeit erhalten, ggf. zu stark fokussieren (Availability Bias).

– Cybersicherheitsexperten/-innen mit jahrelanger und umfassender Erfahrung sind für alle Organisationen sehr wertvoll. Dieses grosse Fachwissen birgt jedoch unter gewissen Umständen auch eine Herausforderung. Experten/-innen fällt es teilweise nicht leicht, sich in die Lage von IT-Sicherheitslaien (d. h. der grossen Mehrheit der Mitarbeitenden) zu versetzen. Eventuell verstehen die Cyber-Verantwortlichen die Perspektive der technisch weniger versierten Benutzer nicht so gut. Diese kognitive Voreingenommenheit kann mitunter ein Hinde-

rungsgrund sein, dass technisches Personal eine effektive, benutzerfreundliche IT-Sicherheit entwickeln (Curse of Knowledge-Bias).

– Eine soziale und psychologische Voreingenommenheit, die sich auf fast alle Aspekte des menschlichen Verhaltens auswirkt, ist der grundlegende Attributionsfehler. IT-Sicherheitsexperten/-innen tendieren dazu, sich entsprechend dem Akronym PEBKAC zu verhalten, das für «Problem Exists Between Keyboard and Chair» steht. Mit anderen Worten: Sie machen den Benutzer für den Sicherheitsvorfall verantwortlich (Self-Serving Bias). Umso wichtiger sind diesbezügliche Schulungen und Awareness-Trainings.

– Eingetretene Cyber Risiken werden oft als Fehler der IT-Abteilung verstanden. Paradoxerweise sind diese Risiken möglicherweise indirekt auf Entscheidungen des Managements zurückzuführen, das die Sicherheit zu wenig ernst genommen hat.

– Manager/-innen könnten das bisherige Ausbleiben von Cyber Vorfällen auf gute Entscheidungen bei der Einstellung ihres IT-Security-Personals zurückführen. Eventuell war es aber bis anhin eher Glück, dass nichts passiert ist. Dieser Umstand könnte das Management glauben lassen, genügend in die Cyber Sicherheit investiert zu haben (Korrelation ist jedoch keine Kausalität).

– Das Vorhaben, Cyber Risiken möglichst zu verhindern und deshalb viel in die technische Risikoprävention zu investieren, ist aus Management-Sicht oft attraktiver als sich mit dem Umgang eingetretener Risiken, der Stärkung der Risikokultur und der Erhöhung der Resilienz befassen zu müssen. Es könnte der Eindruck entstehen, dass korrekt durchgeführte Prävention Risikoeintritte beinahe verunmöglicht (Zero Risk Bias, bedeutet die Tendenz, sich für Null-Risiko-Lösungen zu entscheiden, anstelle des Managements von Risiken und der Erhöhung der Resilienz).

– Neue Technologien (z. B. Internet-of-Things [IoT]) führen oft in kurzer Zeit zu grossen Wachstumsmärkten, denen sich Unternehmen wegen den attraktiven Erfolgsaussichten anschliessen, weil es viele andere auch tun. Dies führt zu Entscheidungssituationen, in denen Renditeaussichten die Cybersicherheit dominieren können. Das kann zur Folge haben, dass Cyber Risiken zu wenig prioritär adressiert werden. (Bandwagon-Effekt, zu Deutsch Mitläufereffekt).

Herausforderungen im Cyber Risk Management

Cyber Risk Management-Überlegungen müssen in jedem ERM-Prozessschritt, z. B. nach ISO 31000 oder ERM Playbook explizit gemacht werden. Dabei stellen sich aber in der Praxis einige Herausforderungen, die nachfolgend kurz aufgeführt werden (vgl. NISTIR 8286, 8286A, 8286B, 8286C):

1. Externer und interner Kontext

Teilweise sind die Erwartungen der Stakeholder an das Management und die Kommunikation von Cyber Risiken nicht klar formuliert. Oft fehlt auch die Verbindung der Cyber Risiken zu den Unternehmenszielen. Eine fehlende Definition der Cyber-Risikobereitschaft macht eine zielorientierte Risikosteuerung schwierig. Rollen und Verantwortlichkeiten des Cyber Risk Management sind nicht immer klar geregelt oder aus einer Governance-Perspektive falsch verteilt. So müssen Aufgaben und Verantwortlichkeiten von CRO, CISO, CIO, CFO, Risk Committee, Interne Revision, externe IT-Dienstleister (Cloud-Services, Managed Service Providers, Revisoren, Compliance etc.) klar geregelt werden. Ebenso zeigt sich, dass oft keine systematischen Überlegungen zum Cyber Supply Chain Risk Management (Integration von externen Partnern) gemacht werden. Vor dem Hintergrund der zunehmenden Abhängigkeit von funktionierenden Lieferketten (die aktuelle Pandemie hat diese Fragilität z. T. schmerzlich offengelegt) besteht hier entsprechendes Verbesserungspotenzial.

Generell wird die «IT» als zentrales Nervensystem schwieriger steuer- und überwachbar, und die Risikoauswirkungen von Cyber Risiken auf komplexe Systeme sind oft schwierig abschätzbar («systemische Risiken» ganzer Organisationen / Nationen).

2. Risk Management Prozess

Bei der Risikoanalyse geht es um

– die Identifikation und Beurteilung der kritischen Assets (Daten, Personen, Geräte, Systeme, Geschäftsprozesse, die für die Erreichung der Geschäftsziele kritisch sind, so genannte «Kronjuwelen»),

– die Identifikation von potenziellen Bedrohungen, die die Vertraulichkeit, Integrität und Verfügbarkeit von

diesen Assets (evtl. auch Chancenoptik: Informations- und Technologiepotenziale) gefährden können (Threat Modeling),

– die Berücksichtigung der Vulnerabilitäten (Bedingung, z. B. unpatched Software) dieser Assets, und

– das Abschätzen der Konsequenzen dieser Risikoszenarien, ausgehend von Threats und Vulnerabilitäten (bottom-up) und einer Risikoanalyse der Assets (top-down).

Die Risikoanalyse kann grundsätzlich qualitativ, quantitativ oder in der Kombination beider erfolgen, z. B. mit FAIR, IEC 31010:2019, oder NIST SP 800-30. Dabei ist es zentral, so genannte Folgerisiken zu berücksichtigen. Die Folgerisiken von Cyber-Vorfällen können tangible (z. B. finanzielle Verluste) oder intangible (z. B. Reputationsverluste) Auswirkungen haben. Zudem ist es zentral, in Abstimmung mit dem ERM eine konsistente Haltefrist für die Einschätzung der Wahrscheinlichkeiten zu definieren (z. B. ein Jahr). Ebenso – und dies ist deutlich weniger intuitiv bez. Umgang mit Cyber Risiken – sollen Chancenpotenziale identifiziert und diskutiert werden.

Eine Business Impact Analyse (BIA) kann allgemein helfen, die kritischen Assets zu identifizieren. Hier besteht die Herausforderung, dass zunehmend mehr Assets nicht mehr in der Kontrolle der Organisationen selbst sind (z. B. cloud-basierte Dienstleistungen) und deswegen nicht dieselbe Aufmerksamkeit wie «interne Risiken» erhalten. Die BIA ist – falls mit dem Cyber Risk Management und dem ERM abgestimmt – ein sehr effektives Bindeglied zwischen der technischen Ebene (System) und dem Geschäftsmodell (Business).

Allerdings bestehen im Rahmen der Durchführung der Cyber Risk Assessments erhebliche Herausforderungen in der Praxis, die eine Abstimmung mit dem ERM nur schwer gestalten lassen:

– Oft sind keine Risikoszenarien vorhanden, welche die Ursache(n) der Bedrohung, den Bedrohungs-Event, die Vulnerabilität, die betroffenen Assets und die daraus entstehenden betriebswirtschaftlichen Folgerisiken für die Organisation (z. B. Verfehlen der Geschäftsziele, Reputationsschaden) genügend konkret und vollständig spezifizieren. Hinzu kommt, dass Risikoabhängigkeiten zu anderen Risiken (z. B. Reputation, Rating) oder Unternehmenszielen (z. B. Compliance, Strategie) nur selten systematisch analysiert werden.

– Im Bereich Cyber Risk Management gibt es nur wenige standardisierte Messmethoden/Beurteilungsmethoden; es koexistieren verschiedenste Scoring-Systeme, die je nach Berater/Software-Produkt (bez. Abschätzung von Wahrscheinlichkeiten und Schadenpotenzialen) anders ausfallen. Obwohl es entsprechende Empfehlungen (Guidelines, Rahmenwerke) wie z. B. NIST SP 800-30 gibt, ist in der Praxis nur wenig Standardisierung zu erkennen. Die Quantifizierung von Risiken geschieht oft nur ad hoc und erhält (noch) nicht dieselbe Aufmerksamkeit wie andere Risikokategorien im ERM (z. B. finanzielle Risiken, strategische Risiken, Compliance-Risiken).

– Spezifisch im Bereich des Cyber Risk Management ist es schwierig, die Wirkungen (Effektivität) von Massnahmen und Kontrollen zur Risikosteuerung zu messen. Oft sind diese nicht bekannt.

– Generell lässt sich feststellen, dass die Ergebnisse des Cyber Risk Managements oft nicht in der Art und Weise aufbereitet werden, dass sie direkt als Input für den ERM-Prozess dienen können.

– Cyber Risiken sind hochdynamisch und erfordern einen interdisziplinären Umgang. Sie müssen kontinuierlich überwacht werden. Es sind laufend Anpassungen notwendig, insbesondere in Organisationen, die in einem dynamischen Umfeld agieren. Dies widerspricht teilweise den klassischen Risk Management-Prozessen in der Praxis, die z. B. einen statischen, jährlichen Prozess vorsehen und entsprechend Risikoinventare produzieren, die zum Zeitpunkt der Berichterstattung schon teilweise wieder veraltet sind. Cyber Risk Management erfordert ein proaktives Risk Management, das besonders das Training, die Schulungen, eine angemessene Risikokultur und klar definierte Governance-Strukturen in den Vordergrund stellt. Wenige, aber zentrale Key Risk Indicators helfen, frühzeitig auf etwaige Risiken aufmerksam zu werden.

Teil II: Studienergebnisse

Um in Erfahrung zu bringen, wie Organisationen, ihre Risk Management-Verantwortlichen und CISOs mit den Herausforderungen des Cyber Risk Management im Allgemeinen und mit dem Cloud-Computing im Speziellen umgehen, wurden 33 Interviews in 18 grösseren Organisationen geführt. Nachfolgend werden die Ergebnisse dieser Interviews präsentiert und diskutiert. Die Auswertung erfolgt inhaltlich dreigeteilt. Zuerst wird auf wichtige Aspekte der Risk Governance eingegangen. Sie definiert die Grundsätze guter Organisationsführung hinsichtlich Risk Management. Im zweiten Teil wird die Risikokultur adressiert. Sie beleuchtet Verhaltensweisen und Einstellungen von Organisationmitgliedern im Umgang mit Risiken und Chancen. Schliesslich werden einzelne Aspekte aus einer prozessualen Cyber Risk Management-Perspektive näher beleuchtet.

4. Risk Governance

(Cyber) Risk Governance ist eine Teilausprägung guter Corporate Governance und kann deshalb nicht isoliert davon betrachtet werden. Corporate Governance ist der rechtliche und regulatorische Rahmen für die Überwachung einer Organisation (vgl. von Werder 2015). Neben dem rechtlichen Rahmen mit all seinen Gesetzen, Normen und Standards konzentriert sich die Corporate Governance auf das Ziel einer guten und verantwortungsvollen Unternehmensführung. Sie ermöglicht im Idealfall eine langfristige Wertschöpfung. Die Risk Governance wiederum wendet die Grundsätze der guten Unternehmensführung auf die Identifizierung, Bewertung, Steuerung, Kommunikation und Integration von Risiken in die Entscheidungsprozesse an (adaptiert nach IRGC 2018). Sie umfasst Themenbereiche wie die regulatorischen Anforderungen an das Risk Management, die Risikopolitik, die Risikokultur, die Organisation des Risk Managements sowie die Orientierung an Standards, Normen und Regelwerken.

Eine solide Risk Governance ist eine zentrale Grundlage für die Umsetzung eines wirksamen Risk Managements. Sie befasst sich mit diversen Fragestellungen, welche die Einrichtung eines effektiven Risk Management-Prozesses beeinflussen. Corporate-Governance-Kodizes, Risk Management-Rahmenwerke, Normen und rechtliche Anforderungen wirken sich alle auf das Risk Management von Organisationen aus. Auch die Risikokultur sowie Rollen, Verantwortlichkeiten und Aufgaben mit Bezug zum Risk Management spielen eine wichtige Rolle für die Wirksamkeit des Risk Managements.

Risiko- und Informationssicherheitspolitik

Risikopolitik

Mit einer Risikopolitik legt das Aufsichtsorgan die Ziele und Grundsätze für ein effektives Risk Management fest. Die Risikopolitik bildet die Leitplanken für die operative Umsetzung des Risk Managements mit dem Ziel, unternehmerische Risiken und Chancen ganzheitlich und auf oberster Organisationsebene anzugehen. Sie definiert insbesondere den Risk Management-Prozess, die entsprechenden Funktionen und Verantwortlichkeiten der darin involvierten Parteien sowie die grundsätzlichen Risikostrategien im Umgang mit den wesentlichen Risiken.

Risikopolitik

- 10 Organisationen haben eine Risikopolitik ohne Erwähnung von Cyber Risiken.
- 2 Organisationen haben eine Risikopolitik mit Erwähnung von Cyber Risiken.
- 4 Organisationen haben keine Risikopolitik.

In vier Organisationen bestehen keine risikopolitischen Grundsätze bzw. die Risk Management-Verantwortlichen nannten alternative Dokumente, die jedoch nicht denselben Charakter aufweisen bzw. operativer ausgerichtet sind (z. B. Disaster Recovery Plan, IT-Sicherheitspolitik, Risk Management-Handbuch oder Internes Kontrolldokument). Auffallend ist, dass insbesondere die grösseren Organisationen fast alle eine Risikopolitik besitzen (10),

allerdings ist das Thema «Cyber Risk Management» lediglich in zwei der interviewten Organisationen expliziter Bestandteil der Risikopolitik. Bei allen anderen Organisationen fehlt ein entsprechender Hinweis in der Risikopolitik und es wird auf operativere Dokumente wie z. B. das Risk Management-Handbuch verwiesen.

Dieses Ergebnis ist insofern nicht überraschend, als dass grössere Organisationen mit formalisierten Risk Management-Strukturen grundsätzlich eine Risikopolitik verabschiedet haben. Allerdings haben die Interviews auch gezeigt, dass nicht alle Organisationen nach den darin enthaltenen Prinzipien handeln, weil sie aufgrund mangelhafter Kommunikation auf operativer Ebene gar nicht bekannt sind. Implizit sind entsprechend in der Risikopolitik auch Cyber Risiken abgedeckt. Vor dem Hintergrund der zunehmenden Relevanz dieser Risikokategorie und den speziellen Charakteristika von Cyber Risiken (vgl. Kapitel 3) lässt sich hier ein deutliches Verbesserungspotenzial ausmachen. Eine explizite Erwähnung von Cyber Risiken in den risikopolitischen Grundsätzen würde nicht nur die Aufmerksamkeit der Aufsichtsorgane zusätzlich erhöhen, sondern stärkt auch deren Verantwortungsbewusstsein bez. Cyber Risiken.

Risikoappetit

Weiter wurde in den Interviews diskutiert, ob explizite Risikoappetit-Aussagen spezifisch zu den Cyber Risiken in den Organisationen verfügbar sind. Risikoappetit ist definiert als die Gesamtheit der Risiken, die eine Organisation jederzeit bereit ist einzugehen, um ihre Organisationsziele zu verfolgen. Grundsätzlich drückt der Risikoappetit aus, welche Risiken in welchem Ausmass in welchen Geschäftsbereichen eingegangen werden dürfen, um die Organisationsziele erreichen zu können. Bezogen auf Cyber Risiken bedeutet dies, dass das Aufsichtsorgan explizite Aussagen zum akzeptierbaren Risikoumfang hinsichtlich Cyber Risiken trifft. Risikoappetit-Aussagen können qualitativ und/oder quantitativ definiert werden. Der Risikoappetit muss regelmässig im Aufsichtsorgan diskutiert und allenfalls angepasst werden.

Risikoappetit

- 10 Organisationen haben keinen Risikoappetit für Cyber Risiken definiert.
- 4 Organisationen sind daran, Risikoappetit für Cyber Risiken zu definieren.
- 2 Organisationen haben überhaupt keinen Risikoappetit definiert.
- 2 Organisationen geben an, Risikoappetit könne man nicht «berechnen».

Keine der befragten Organisationen hat einen expliziten Risikoappetit für das Eingehen von Cyber Risiken definiert. Immerhin vier Organisationen diskutieren aktuell die Definition eines solchen. Eine Organisation möchte dies mit Unterstützung der Internen Revision in naher Zukunft machen. Zwei Organisationen definieren generell keinen Risikoappetit, wobei zwei Risk Manager angeben, dass sie diesen nicht berechnen können. Ein Risk Manager erklärt, dass der Risikoappetit faktisch indirekt über den Selbstbehalt ihrer Cyber-Versicherung gegeben sei.

Insgesamt zeigt sich hoher Verbesserungsbedarf bei der Definition von Risikoappetit bez. Cyber Risiken. Grundsätzlich bestätigt sich das bereits bekannte Bild, dass das Entwickeln von Risikoappetit-Statements in der Praxis (sehr) grosse Mühe bereitet. Teilweise fehlen methodische Kenntnisse, teilweise wird der Nutzen grundsätzlich in Frage gestellt und teilweise wird das Konzept des Risikoappetits nicht verstanden («kann nicht berechnet werden»). Für Cyber Risiken fehlen solche spezifischen Risikolimiten komplett, was das Steuern dieser Risiken schwieriger macht, da eine entsprechende Vorgabe fehlt, an der sich die für das Risk Management Verantwortlichen orientieren können. Die Auswertung zeigt jedoch auch, dass einige wenige Risk Manager sich bewusst sind, dass das Definieren solcher Risikoappetit-Statements zwar bisher keine grosse Relevanz hatte, dies sich in Zukunft aber auch ändern könnte.

Orientierungshilfen für das Cyber Risk Management

Im Rahmen der Risk Governance überlegen sich Organisationen in der Regel auch, ob und in welchem Ausmass sich das Management der Cyber Risiken an einem externen Benchmark (z. B. Zertifizierung, Beratungsgesellschaft, externes Assessment) orientieren soll.

Orientierungshilfen für das Cyber Risk Management

- 4 Organisationen prüfen den Reifegrad über ein externes Assessment.
- 2 Organisationen tauschen sich über ihr eigenes Netzwerk von CISOs aus.
- 8 Organisationen orientieren sich an den Standards der Familie ISO 2700x, sind aber nicht zertifiziert.
- 2 Organisation sind ISO 27001 zertifiziert.
- 2 Organisationen geben an, kein externes Benchmarking zu betreiben.
- 1 Organisation orientiert sich am IKT-Minimalstandard.

Lediglich zwölf von 16 interviewten Risk Management-Verantwortlichen konnten zu diesem Aspekt genügend spezifische Auskunft geben. Vier Organisationen nutzen externe Assessments, z. B. von Beratungsunternehmen, die einen Vergleich mit Mitbewerbern bzw. eine Einschätzung des Reifegrads zulässt. Vier Organisationen geben an, dass die Standards der Familie ISO 2700x wichtig sind, jedoch sind nur zwei Organisation nach ISO 27001 zertifiziert. Zwei Organisationen geben an, durch das eigene Netzwerk von Risk Managern und CISOs ein informelles Benchmarking etabliert zu haben. Eine Organisation orientiert sich am BSI-Grundschutz und am IKT-Minimalstandard.

Die Auswertung zeigt kein dominantes Vorgehen der befragten Organisationen hinsichtlich Benchmarkings und Nutzen von Standards für das Cyber Risk Management. Es herrscht ein recht uneinheitliches Bild, so nutzen immerhin vier Organisationen externe Assessments und zwei setzen auf das eigene, gut aufgestellte interne Netzwerk. Ein systematisches Benchmarking ist bei der grossen Mehrheit der befragten Organisationen nicht erkennbar, was sicherlich Verbesserungspotenzial birgt. Lediglich zwei Organisation sind ISO 27001 zertifiziert, drei andere orientieren sich danach. Zwei Risk Management-Verantwortliche gaben an, nicht zu wissen, ob sie explizites Benchmarking betreiben.

Informationssicherheitspolitik und Informationssicherheitsrichtlinien

Die Unternehmensleitung legt mit der Informationssicherheitspolitik die Ziele, Grundsätze, Aufgaben, Kompetenzen und Verantwortlichkeiten im Bereich der Informationssicherheit fest. Die Informationssicherheitspolitik bildet die Grundlage für den Aufbau der Sicherheitsorganisation, die Entwicklung von Informationssicherheitskonzepten und -massnahmen, sowie die Entwicklung von Massnahmen zur Sensibilisierung und Schulung der Mitarbeitenden. Sie definiert die Sicherheitsziele im Hinblick auf den störungsfreien Betrieb sämtlicher Betriebsprozesse und zur Erfüllung von allen gesetzlichen, vertraglichen und regulatorischen Anforderungen in allen Bereichen der Informationsverarbeitung. Schliesslich beschreibt sie auch den Umgang mit Risiken und Restrisiken.

Informationssicherheitsrichtlinien sind anders als die Informationssicherheitspolitik nicht auf strategischer, sondern operativer Ebene angesiedelt. Es handelt sich dabei um detaillierte Weisungen, die sich auf konkrete Produkte oder Systeme beziehen.

Die Fragen nach dem Vorhandensein einer Informationssicherheitspolitik respektive von Sicherheitsrichtlinien für die Cloud-Nutzung zielen darauf ab, das generelle Bewusstsein der Organisation und insbesondere der Geschäftsleitung für das Thema Informationssicherheit abzuschätzen.

Informationssicherheitspolitik

- 14 Organisationen verfügen über eine Informationssicherheitspolitik.
- 4 Organisationen haben bis jetzt keine Informationssicherheitspolitik verfasst.

Die befragten Organisationen verfügen mehrheitlich über eine Informationssicherheitspolitik. Diese wird meist auch gelebt und mit begleitenden Massnahmen durchgesetzt. Vier Organisationen geben an, dass die Informationssicherheitspolitik Grundlage für ein Informationssicherheitsmanagementsystem (ISMS) ist.

Bei vier Organisationen ist keine Informationssicherheitspolitik vorhanden. Davon geben zwei kleinere Organisationen an, dass die Informationssicherheit dennoch gelebt wird und zugehörige Massnahmen vorhanden sind. Eine Organisation plant die Erstellung einer Informationssicherheitspolitik.

Sicherheitsrichtlinien für die Cloud-Nutzung

- 14 Organisationen verfügen über spezifische Sicherheitsrichtlinien für die Cloud-Nutzung oder haben solche Richtlinien geplant.
- 2 Organisationen haben bis jetzt keine spezifischen Sicherheitsrichtlinien für die Cloud-Nutzung verfasst.

Die meisten Organisationen verfügen über Sicherheitsrichtlinien für die Cloud-Nutzung, in der Regel sowohl für die Mitarbeitenden als auch für die Betreiber ihrer IT.

Ergänzend zu organisatorischen Massnahmen (Weisungen, Richtlinien etc.) werden in einigen Organisationen technische Massnahmen eingesetzt. Diese bestehen z. B. darin, nicht konforme Cloud-Dienste zu blockieren. Organisationen, die dies tun, sind in der Regel bestrebt gleichwertige Alternativen zur Verfügung zu stellen.

Sind externe Dienstleister für den Betrieb der IT verantwortlich, so werden bei diesen die Richtlinien für die Cloud-Nutzung vertraglich durchgesetzt. Bei internen Betreibern kommen zur Kontrolle und Steuerung der Cloud-Nutzung Checklisten, Fragebögen oder Cloud-Antragsdokumente zur Anwendung. Diese Massnahmen sind mehrheitlich organisatorischer Natur. Technische Massnahmen werden auch hier ergänzend eingesetzt.

Generell ist in den Geschäftsleitungen grosses Bewusstsein für die Informationssicherheit vorhanden, zumindest wenn man dies am Vorhandensein einer Informationssicherheitspolitik bemisst. Fast alle der befragten Organisationen verfügen über ein solches Dokument. Andere sind im Begriff, eines zu erstellen, oder widmen sich der Thematik zumindest auf operativer Ebene. Auch Sicherheitsaspekte der Cloud-Nutzung finden bei den befragten Organisationen grosse Beachtung. Die Umsetzung ist dabei sehr heterogen, es kommen unterschiedlichste technische und organisatorische Massnahmen zum Mitigieren von Cloud-Risiken zur Anwendung.

Risiko- versus kontrollorientierter Ansatz

In den Interviews wurde diskutiert, ob die Organisationen einen kontroll-basierten Ansatz (Grundschutzansatz, z. B. nach BSI) anwenden oder ob ein risiko-orientierter Ansatz, z. B. nach ISO 27001/27005 dominiert**.**

Die beiden Ansätze unterscheiden sich in der Art und Weise wie die Massnahmen zum Schutz vor Cyber Risiken ermittelt werden. Beim kontroll-basierten Ansatz werden Massnahmen aus einem vorgegebenen Massnahmenkatalog (z. B. IT-Grundschutz-Kompendium des BSI) ausgewählt. Die Auswahl orientiert sich an der zu schützenden Systemlandschaft (Fileserver, Webserver, Virtualisierungsumgebungen, Client-Computer, mobile Geräte etc.). Die implementierten Massnahmen haben somit keinen direkten Bezug zur Risiko-Situation, der eine Organisation gegenübersteht. Dies führt dazu, dass es in bestimmten Bereichen zu einem «Über-Schutz» (zu viele Massnahmen) und in anderen Bereichen zu einem «Unter-Schutz» (zu wenige Massnahmen) kommen kann. Der risiko-orientierte Ansatz setzt genau an diesem Punkt an. Er geht von den Risiken aus, mit denen eine Organisation und damit ihre IT-Landschaft konfrontiert ist und leitet davon die notwendigen Massnahmen ab, um die Risiken auf das akzeptierte Niveau zu senken.

Grundsätzlich sind Zertifizierungen in beiden «Welten» möglich. Entweder als klassische ISO 27001-Zertifizierung beim risiko-orientierten Ansatz oder als «ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz» beim kontroll-basierten Ansatz.

Ansatz für die Definition von Massnahmen

- 8 Organisationen orientieren sich an einem risiko-orientierten Ansatz.
- 5 Organisationen nutzen einen kontroll-orientierten Ansatz.
- 4 Organisationen kombinieren beide Ansätze.
- 8 Organisationen orientieren sich an den Standards der Familie ISO 2700x.
- 2 Organisationen nutzen primär NIST.
- 2 Organisationen geben an, sich an keinem Standard zu orientieren.

Acht Organisationen sagen von sich, dass sie einen risiko-orientierten Ansatz verfolgen. Zwei Organisationen verfolgen einen kontroll-basierten Ansatz. Eine dieser beiden Organisationen ist von einem anfänglich risiko-orientierten Ansatz mit dem Wachstum der Unternehmung zu einem kontroll-basierten Ansatz übergegangen.

Die Mehrheit der befragten Organisationen gibt an, einen risiko-basierten Ansatz zu verfolgen. Die Umsetzung kann sowohl von Seiten CISO wie auch vom Risk Management getrieben werden. Bei den beiden Organisationen, welche einen kontroll-orientierten Ansatz verfolgen, wird das Cyber Risk Management von der IT/CISO-Seite her festgelegt. Vier Organisationen verfolgen beide Ansätze, z. B. für den Grundschutz zur Sicherung der Vollständigkeit einen kontroll-basierten Ansatz und für die Beurteilung einen risiko-orientierten Ansatz.

Organisationen, die einen risiko-orientierten Ansatz verfolgen, sind in der Lage, explizite Bezüge zu den Geschäftsrisiken herzustellen (top down-Ansatz). Dies ist eine Voraussetzung, um Cyber Risiken via Szenarioanalysen ins ERM zu überführen. Organisationen, die diesen Weg begehen, erreichen in der Regel ein effektiveres und mit den Organisationszielen abgestimmtes Cyber Risk Management.

Verantwortung, Rollen und Funktionen

Verantwortlichkeiten

Die oberste Verantwortung für Risiken trägt immer der Verwaltungsrat, unabhängig von der Risikokategorie. Somit ist er zwingend auch für Cyber Risiken ultimativ verantwortlich («accountable»). Dies entspricht einer nicht delegierbaren, unentziehbaren Aufgabe. Die operative Umsetzung des Cyber Risk Managements kann er jedoch an die Geschäftsleitung delegieren, die wiederum weitere Personen mit der Umsetzung («responsible») betraut.

Verantwortlichkeiten

- 7 Organisationen sehen den Verwaltungsrat in der Gesamtverantwortung.
- 7 Organisationen bezeichnen die Geschäftsleitung als hauptverantwortlich.
- 2 Organisationen geben an, dass die IT die Hauptverantwortung für Cyber Risiken trägt.

Die Ergebnisse der Interviews zeigen, dass nicht einmal jedes zweite Unternehmen den Verwaltungsrat in der obersten Verantwortung sieht. Genauso oft wird die Geschäftsleitung als verantwortlich bezeichnet. Nicht zulässig bzw. klar im gesetzlichen Widerspruch sind zwei Organisationen, welche die Verantwortung für Cyber Risiken ausschliesslich in der IT sehen. Einige Interviewpartner/-innen antworteten zögerlich, scheinen sich der Verantwortlichkeiten nicht klar bewusst zu sein.

Aufgrund der Komplexität, der Interdisziplinarität und der Bedeutung des Themas ist zu erwarten, dass viele Akteure und Funktionen im Cyber Risk Management involviert sind. Das wird mit den Interviews mehrheitlich bestätigt. Dabei gilt tendenziell: Je grösser die Organisation,

desto mehr Stellen sind involviert. In sechs Organisationen sind nur jeweils zwei Stellen involviert, während es in drei anderen Organisationen bis zu fünf oder sechs Stellen sind.

Erwartungsgemäss ist bei den meisten die IT bzw. der CIO involviert. Fast gleich oft ist es der CISO. Bei knapp der Hälfte der befragten Organisationen sind (neben anderen Stellen) beide einbezogen. Nur bei vier der befragten Organisation ist der Corporate Risk Officer aktiv ins Cyber Risk Management einbezogen.

Dieses Resultat ist trotz der eingangs geschilderter Schwierigkeiten der Integration des Cyber Risk Managements ins ERM etwas ernüchternd.

«Wir arbeiten vom Audit Committee aus eng mit dem CISO, dem CIO und auch mit externen Beratern zusammen, die uns in diesen Themen regelmässig unterstützen. Ich glaube, wir haben ein gutes Verständnis auf Konzernleitungsstufe was Cyber Risiken angeht.»

(Risk Manager, anonym)

Weitere beteiligte Stellen können die Interne Revision oder auch externe Berater/-innen oder Spezialisten/-innen sein. Der Versicherer spielt bei den meisten Organisationen keine bedeutende Rolle. Lediglich zwei Organisationen haben die Versicherer in der Vergangenheit beratend einbezogen.

Zusammenarbeit der Stakeholder

Eine effektive Steuerung der Cyber Risken entsteht erst durch eine gute Zusammenarbeit der Verantwortlichen mit dem Business, aber auch dem HR, Datenschutzbeauftragten, Legal und Compliance. Immerhin fünf der befragten Organisationen geben an, das Business einzubeziehen.

Zusammenarbeit der Stakeholder im ERM-Kontext

- Keine Organisation sagt von sich, die Zusammenarbeit funktioniere nicht gut.
- 5 Organisationen beziehen das Business ins Cyber Risk Management mit ein.
- Der Austausch findet auf formeller und informeller Basis statt.

In zehn Organisationen arbeitet das Corporate Risk Management eng mit der IT, dem Datenschutzbeauftragten und/oder mit dem Compliance Management zusammen. Die Zusammenarbeit mit dem HR ist nicht sehr etabliert. Auffallend ist, dass die Zusammenarbeit oft als informell bezeichnet wird, wobei diese Form der Zusammenarbeit als gut empfunden wird. Es wurde sogar einmal explizit bemerkt, dass zu viel Struktur und zu viele formelle Regelungen in diesem Kontext hinderlich sein können. Bei mittelgrossen Unternehmen ist es zudem oft so, dass verschiedene Rollen von einer einzigen Person wahrgenommen werden. Ein kleiner Kreis führt zu einem eher informellen Austausch. Interessant ist ein Ansatz, bei dem sog. Risk Cluster Workshops durchgeführt wurden, z. B. für Cyber und Compliance Risiken. Dieses Vorgehen hilft, Silodenken zu vermeiden.

Betrachtet man die Zusammenarbeit zwischen CISO (oder äquivalente Funktion) und Risk Manager genauer, offenbaren sich gewisse Lücken. Der Austausch scheint oft nur informeller Art zu sein. In vier untersuchten Organisationen ist die Zusammenarbeit noch nicht klar definiert, weil es keinen CISO oder keinen CRO gibt. Nur eine Organisation beurteilt die Zusammenarbeit CISO und Risk Management als sehr gut. Sie ist formal über ein spezifisches Assurance-Gremium institutionalisiert. Bei einer Organisation ist der CISO Mitglied der Geschäftsleitung und erhält so die notwendige Awareness für dieses Thema. Lediglich eine Organisation gibt an, die Rollen primär extern vergeben zu haben und erwähnt externe Audits der externen IT-Dienstleister sowie das Zusammenspiel mit der externen Revision.

Die Literatur postuliert, dass Verantwortlichkeiten klar zu regeln sind, am besten in Form einer Verantwortlichkeitsmatrix (RACI-Schema, wobei sich das Akronym aus den folgenden englischen Begriffen Responsible, Accountable, Consulted und Informed zusammensetzt). Keine der befragten Organisationen hat ein RACI-Schema erwähnt. Insgesamt ist viel in Bewegung und die Organisation scheint bei vielen noch nicht optimal zu sein, obwohl die Zusammenarbeit in keiner Organisation als schlecht beurteilt wird. Zwei Organisationen erwähnen den geplanten Aufbau eines Risk bzw. eines Security Boards.

Cyber Risiken als Teil des ERM

Die meisten Organisationen nehmen Cyber Risiken als Teil des Risk Managements wahr. Die organisatorische Umsetzung und Koordination ist aufgrund vieler involvierter Stellen, der erforderlichen Interdisziplinarität und des nötigen Spezialwissens schwierig und führt zu unterschiedlichen organisatorischen Ansätzen.

Integration des Cyber Risk Managements ins ERM

- 9 Organisationen bezeichnen das Cyber Risk Management als Teil des ERM.
- 6 Organisationen betrachten Cyber Risiken getrennt von allen anderen Risken.

Bei neun der 15 befragten Organisationen ist das Cyber Risk Management Teil des Enterprise Risk Managements.

«Ja, Cyber Risiken sind definitiv ein Teil des Corporate Risk Managements, ein wesentlicher Teil, ist eines von den Risiken, die wir am meisten beobachten.»

(Daniel Imhof, Leiter Konzernrisikomanagement, Die Schweizerische Post).

Bei sechs sind die Funktionen weitgehend getrennt. Bei einigen grossen Konzernen beschäftigen sich viele Mitarbeitende mit Cyber Risk Management. Durch den Einsatz von vielen Ressourcen ergibt sich eine Spezialisierung, die dazu führen kann, dass das Thema Cyber Risk bei der IT angesiedelt ist und erst zuoberst im Audit-Committee mit dem ERM zusammengeführt wird. Das bedeutet jedoch nicht, dass in diesen Organisationen ein kontroll-orientierter Ansatz umgesetzt wird. Der Ansatz kann auch risiko-orientiert sein. Und es erklärt auch den scheinbaren Widerspruch, dass nur bei vier der befragten Organisation der Corporate Risk Officer aktiv ins Cyber Risk Management einbezogen ist.

«Der CISO ist auch ein wichtiger Risikofachexperte im ERM, sodass da wirklich auch eine kollaborative Schnittstelle besteht. Und es gibt auch noch eine Verknüpfung insofern, dass der CISO auch Zugriff auf das Enterprise Risk Management Software System hat.»

(Alexander Hilsbos, Leiter Risk Management, Insel Gruppe)

Insgesamt zeigt sich ein doch markanter Gap zwischen der Relevanzeinschätzung der Thematik durch die Studienteilnehmenden und der Art und Weise, wie der Austausch zwischen der für Cyber Risiken verantwortlichen Person mit dem Risk Management organisiert ist. Auffällig ist die Heterogenität der verschiedenen «Rollen-Modelle» sowie auch, dass entgegen der Literaturempfehlung der CRO nicht eng mit dem CISO zusammenarbeitet und daher eine Integration der Cyber Risiken in die Sprache des ERM selten stattfindet. In kleineren Organisationen ist evtl. problematisch, dass diese Verantwortung extern vergeben wird und auf externe Audits und den externen Dienstleister verwiesen wird.

Cloud-Strategie und -Nutzung

Cloud-Strategie

Strategien beschreiben Massnahmen zur Erreichung langfristiger Ziele. Es sind Vorgehenspläne für lange Zeiträume (drei bis fünf Jahre). Cloud-Strategien beschreiben in diesem Sinne Massnahmen zur geplanten Nutzung von Cloud-Services im Hinblick auf das Erreichen von Organisations- und IT-Zielen (Business/IT-Alignment). Konkret beschreiben Cloud-Strategien die Rahmenbedingungen zur Einführung (Migration) und Nutzung von Cloud-Services und schliessen damit auch Fragen bez. der Cloud-Readiness der Organisation ein. Sie setzen die Kenntnis der aktuellen und der anvisierten IT-Landschaft und der Organisationsziele voraus. Anhand der Cloud-Strategie entscheidet die Organisationsleitung, ob und in welchem Umfang eine Cloud-Nutzung umgesetzt wird.

Cloud-Strategie

- 10 Organisationen haben eine Cloud-Strategie erstellt und umgesetzt.
- 4 Organisationen haben eine Cloud-Strategie erstellt, jedoch noch nicht vollständig umgesetzt.
- 2 sind im Begriff, eine Cloud-Strategie zu erarbeiten, oder haben dies geplant.
- 2 Organisationen beabsichtigen nicht, eine Cloud-Strategie zu erstellen.
- 8 Organisationen verfolgen eine Cloud-First-Strategie.

Sämtliche der befragten Organisationen nutzen zumindest in kleinem Rahmen Cloud-Dienste. Auch wenn nicht immer explizit so bezeichnet, so verfügen die meisten Organisationen über eine Cloud-Strategie, oder sind im Begriff, eine zu erstellen. Nur eine Minderheit befindet sich diesbezüglich noch in der Planungsphase oder sieht gänzlich davon ab. Begründet wird letzteres mit dem Fehlen von formalen Voraussetzungen (z. B. weil noch keine IT-Strategie vorhanden ist) oder wegen aktuell geringem Bedarf nach Cloud-Diensten.

Die Auswertung bestätigt die Vermutung, dass das Thema Cloud-Computing bis in die Führungsgremien vermehrte Aufmerksamkeit geniesst. Dies zeigt sich insbesondere in der überraschend hohen Anzahl an Organisationen, welche explizit eine Cloud-First Strategie verfolgt.

Cloud-Servicemodelle

Ein Grossteil der befragten Organisationen gibt an, SaaS-Lösungen zu verwenden. Auch das Servicemodell PaaS ist weit verbreitet; es wird von mehr als der Hälfte der befragten Organisationen verwendet. Neun Organisationen geben an, IaaS und/oder On-Premises Lösungen zu nutzen. Eine Organisation betreibt schliesslich sämtliche Services vor Ort im eigenen Rechenzentrum.

Cloud-Servicemodelle

- 17 Organisationen nutzen SaaS Lösungen.
- 12 Organisationen nutzen PaaS Lösungen.
- 9 Organisationen nutzen IaaS oder noch On-Premises-Lösungen.

Der vermehrte Einsatz von SaaS Lösungen insbesondere im Bereich Büroautomation lässt darauf schliessen, dass die Abhängigkeit von Cloud-Services weiter steigt. PaaS Lösungen werden mittlerweile gegenüber IaaS bzw. On-Premises-Varianten bevorzugt eingesetzt. On-Premises-Lösungen werden insbesondere noch für den Betrieb von geschäftskritischen Anwendungen genutzt. Punktuell werden traditionelle On-Premises-Lösungen auch aus Kostengründen Cloud-Lösungen vorgezogen.

Evaluation und Anbindung von Cloud-Diensteanbietern

Organisationen evaluieren ihre Cloud-Diensteanbieter unterschiedlich. Auch die vertragliche Anbindung des Anbieters wird je nach Organisation unterschiedlich gehandhabt.

Evaluation von Cloud-Diensteanbieter

- 11 Organisationen evaluieren Cloud-Diensteanbieter im Rahmen von Beschaffungsprojekten.
- 4 Organisationen beauftragen externe Beratungsunternehmen mit der Evaluation.

Bei etwas mehr als der Hälfte der befragten Organisationen findet die Evaluation von Cloud-Diensteanbietern im Rahmen der Abwicklung von Beschaffungsprojekten statt. Neben klassischer Marktanalyse und Requirements Engineering stützt sich die Auswahl auf Standards oder interne Anforderungskataloge.

Vier Organisationen geben an, diese Tätigkeiten an externe Beratungsunternehmen auszulagern. Eine Organisation gibt an, ausschliesslich Anbieter zu berücksichtigen, welche vor Ort-Audits zulassen. Eine andere Organisation setzt nur auf am Markt etablierte Produkte. Auch die Datenhaltung in der Schweiz wird explizit als Anforderung genannt.

Die Vollständigkeit der Verträge mit Cloud-Diensteanbietern wird in der Regel durch die Rechtsabteilung sichergestellt. Alternativ werden hierfür auch externe Beratungsunternehmen beigezogen. Zwei Organisationen verwenden zur Sicherstellung der Vollständigkeit Templates bzw. Fragebögen.

Eine Organisation prüft ausgewählte Cloudprovider im Vorfeld und gibt diese dann für die organisationsweite Nutzung frei. Eine interviewte Person gibt an, sich diesbezüglich auch mit Verantwortlichen aus anderen Organisationen auszutauschen. Zwei Organisationen behandeln diese Thematik im Rahmen des Requirements Engineering Prozesses.

Die Hälfte der befragten Organisationen fordern, dass Cloud-Diensteanbieter sich an den Standards der Familie ISO 2700x orientieren, meist wurde dabei ISO 27001 explizit erwähnt. Daneben achten zwei Organisationen auf Konformität mit der DSGVO (Datenschutz-Grundverordnung der EU). Auf cloud-spezifische Zertifizierungen haben zwei Organisationen verwiesen, einmal auf diejenige aus der ISO Reihe (ISO 27017) und einmal auf EuroCloud StarAudit. Daneben wurden die folgenden Frameworks und Standards genannt: COBIT (Control Objectives for Information and Related Technologies), PCI DSS (Payment Card Industry Data Security Standard), BSI Kriterienkatalog C5 sowie SOC1 und SOC2 Reports (System and Organization Controls). Zwei Organisationen verlangen ein «Right to Audit», wobei eines davon als Ersatz auch externe Auditberichte akzeptiert. Vier Organisationen machen hinsichtlich der Berücksichtigung von Standards den Cloudprovidern keine Vorgaben.

Die Auswahl von Cloud-Diensteanbietern läuft in der Regel ähnlich wie die Beschaffung von klassischer Software ab. Allerdings ist die Liste der zu berücksichtigenden Auswahlkriterien komplexer, weshalb öfters auch die Rechtsabteilung einbezogen oder externe Dienstleister beigezogen werden müssen.

Cloud-Risiken

Abhängigkeit von der Cloud

Die Auslagerung von Diensten in die Cloud ist mit Risiken verbunden. Diese betreffen sowohl die Nutzung der Dienste (z. B. Datenschutzverletzungen oder Service-Unterbrüche) als auch deren Beendigung (z. B. Datenlöschung) respektive die Migration in eine neue Umgebung (zu einem neuen Provider).

Meistgenannte Cloud-Diensteanbieter

- 13 Organisationen erwähnen SaaS Lösungen von Microsoft.
- 4 Organisationen nennen SaaS Lösungen von SAP.
- 5 Organisationen erwähnen PaaS Lösungen von Microsoft.
- 2 Organisationen nennen PaaS Lösungen von Amazon.

Obwohl nicht Teil der Befragung, wurden im Rahmen der Interviews oft Aussagen zu konkreten Produkten, insbesondere in den Bereichen SaaS und PaaS, gemacht. Im Bereich SaaS wurde auffällig oft die Firma Microsoft genannt. Etwas weniger häufig wurde SAP erwähnt. Bei den PaaS Lösungen zeigt sich eine ähnliche Verteilung zwischen Microsoft und dem zweitplatzierten Amazon.

Generelle Abhängigkeit von Cloud-Diensten

- 11 Organisationen beurteilen ihre Abhängigkeit von Cloud-Diensten als «hoch».
- 3 Organisationen beurteilen ihre Abhängigkeit von Cloud-Diensten als «hoch», nehmen davon jedoch explizit deren kritische Bereiche aus.
- 4 Organisationen beurteilen ihre Abhängigkeit von Cloud-Diensten als «klein».

Die meisten Organisationen schätzen ihre Abhängigkeit von Cloud-Diensten generell als hoch ein. Drei geben an, dass in kritischen Bereichen jedoch nur eine geringe Abhängigkeit vorhanden ist. Schliesslich beurteilen vier Organisationen ihre Abhängigkeit von Cloud-Diensten generell als gering.

Auf die Frage, ob eine Abhängigkeit von einem spezifischen Anbieter besteht, wird in den meisten Fällen die Firma Microsoft genannt und in je einem Fall die Firmen Amazon und Google. Eine Organisation gibt an, stark von einem Schweizer Rechenzentrum abhängig zu sein. Dies deckt sich mit der Auswertung, welche in Bezug auf die meistgenannten Cloud-Diensteanbieter vorgenommen wurde.

Zusammenfassend lässt sich sagen, dass eine hohe Abhängigkeit von Cloud-Lösungen insbesondere im Bereich der Büroautomation besteht. SaaS Produkte von Microsoft sind in der Stichprobe weit verbreitet. Dementsprechend dürfte die generelle Abhängigkeit der Schweizer Organisationslandschaft von Microsoft als hoch eingestuft werden.

Einige Organisationen reduzieren das generelle Risiko von Abhängigkeiten, indem sie in kritischen Bereichen bewusst versuchen, auf Cloud-Dienste zu verzichten.

«Viele Entscheidungsträger in den Geschäftsleitungen sind sich noch gar nicht gross über die Risiken in Bezug auf Cloud bewusst. Meistens denken sie relativ kurzfristig, und zwar «das kostet ja gar nicht so viel», wenn man dies jedoch in einer fünf oder sechs Jahresrechnung dem bestehenden System gegenüberstellt, dann sieht es vielfach ein bisschen anders aus.»

(CISO, anonym)

Aufgrund der generell hohen Abhängigkeit von SaaS Lösungen muss in den Organisationen das Bewusstsein geschaffen werden, dass für eine sichere, angepasste, wirtschaftliche und langfristig nutzbringende Integration von Cloud-Services in die vorhandene IT-Infrastruktur eine Cloud-Strategie notwendig ist. In dieser müssen insbesondere auch die Risiken, welche aufgrund der Abhängigkeit von einzelnen Cloud-Diensteanbietern entstehen, adressiert werden.

Beendigung der Cloud-Nutzung

Eine Mehrheit der Organisationen (15) stützt sich bei der Frage der Datenlöschung nach Beendigung der Cloud-Dienstleistung auf vertragliche oder rechtliche Bestimmungen. Dabei sind die Organisationen auf die Kooperation des Cloud-Diensteanbieters, den sie verlassen möchten, angewiesen.

Beendigung der Cloud-Nutzung – Datenlöschung

- 15 Organisationen verlassen sich zur Gewährleistung der Datenlöschung bei Beendigung der Cloud-Nutzung auf rechtliche bzw. vertragliche Bestimmungen.
- 2 Organisationen verlassen sich hierfür auf technische Massnahmen (Verschlüsselung).
- 5 Organisationen sehen für die Sicherstellung der Datenlöschung keine Massnahmen vor.

Etwas mehr als ein Viertel der Befragten (5) gibt an, für diesen Fall nichts vorgesehen zu haben oder sich bei diesem Punkt unsicher zu sein. Zwei Organisationen geben an, dieser Anforderung mit der technischen Massnahme der Verschlüsselung zu begegnen.

Für die Sicherstellung einer erfolgreichen Migration zu einem anderen Cloud-Diensteanbieter setzen die befragten Organisationen insbesondere auf technische Massnahmen. Die Verwendung von cloud-agnostischen Architekturen steht dabei im Vordergrund. Bei solchen Architekturen kommen Technologien und Methoden zum Einsatz, die in den Clouds unterschiedlicher Anbieter (oder sogar auf On-Premises-Systemen) lauffähig sind. Konkret wurde der Einsatz von offenen Schnittstellen und freien Dateiformaten, das Verwalten von Quelltext ausserhalb der Cloud-Umgebung und der Einsatz von Containertechnologien genannt. Als weitere Möglichkeit wurde der Verzicht auf Produkte und Technologien erwähnt, die ausschliesslich von einem einzigen Cloud-Diensteanbieter angeboten werden.

Beendigung der Cloud-Nutzung – Migration

- 6 Organisationen verlassen sich zur Gewährleistung einer erfolgreichen Migration in eine neue Umgebung bei Beendigung der Cloud-Nutzung auf rechtliche bzw. vertragliche Bestimmungen.
- 8 Organisationen verlassen sich hierfür auf technische Massnahmen.
- 3 Organisationen verlassen sich auf andere organisatorische Massnahmen (siehe unten).
- 3 Organisationen sehen für die Sicherstellung einer erfolgreichen Migration keine Massnahmen vor.

Die Anzahl Organisationen, welche auch in diesem Kontext auf vertragliche bzw. rechtliche Bestimmungen abstützt, ist im Vergleich zur vorherigen Frage nur halb so gross (6). Auch hier wird bewusst in Kauf genommen, im Falle eines Wechsels auf die Kooperation des Cloud-Diensteanbieters angewiesen zu sein. Drei Organisationen haben organisatorische Massnahmen genannt. So klären zwei Organisationen diese Frage jeweils auf Anwendungs- resp. Projektebene. Dies, indem sie entsprechende Anforderungen pro Anwendungsfall definieren und im Rahmen der Beschaffung bzw. der Softwareentwicklung berücksichtigen. Eine Organisation hat für eine allfällige Überbrückung einen Notfallbetrieb vorgesehen. Drei der befragten Organisationen sehen für die Sicherstellung einer erfolgreichen Migration keine Massnahmen vor oder sind in diesem Punkt unsicher.

Beim Einsatz von proprietären SaaS Lösungen ist man jedoch weiterhin von der Kooperation des Cloud-Diensteanbieters abhängig. Die Beendigung der Cloud-Nutzung ist bei SaaS Lösungen nicht unproblematisch; dort ist man auf spezielle Tools und Vorgehensweisen angewiesen (z. B. wegen fehlender oder nicht standardisierter Schnittstellen). Das Bewusstsein für diese Problematik ist in den Organisationen nicht sehr ausgeprägt vorhanden.

Bedenken, welche in Bezug auf die Verfügbarkeit der Anwendungen sowie auf die Vertraulichkeit der Daten geäussert werden, scheinen den Umstieg zu Cloud-Diensten kaum aufzuhalten. Eine mögliche Erklärung hierfür ist, dass derartige Risiken, welche in der Regel mit einer geringen Eintretenswahrscheinlichkeit und einem hohen Schadenpotential bewertet werden, schwer greifbar sind und deshalb den Faktoren für Underinvestment unterliegen (vgl. Abschnitt «Integration von Cyber Risiken ins ERM»).

Datenschutz und Haftung

Im Rahmen der Nutzung von Cloud-Diensten kommt rechtlichen Fragestellungen eine grosse Bedeutung zu; insbesondere datenschutzrechtliche Fragen sowie Haftungsfragen stehen im Vordergrund.

Datenschutz

Jede Organisation muss sich um die Einhaltung des Datenschutzes kümmern. Sie bleibt auch nach der Auslagerung von Daten und Diensten in die Cloud für den Datenschutz verantwortlich. Der Reifegrad der Massnahmen, die Organisationen zur Einhaltung des Datenschutzes bei sich und bei ihren Outsourcing-Partnern anwenden, ist in den befragten Organisationen sehr unterschiedlich. Anspruchsvolle Fragestellungen entstehen insbesondere dann, wenn Outsourcing-Partner (Cloud-Diensteanbieter) und Outsourcer (interviewte Organisationen) unterschiedlichen Jurisdiktionen unterstehen.

Reifegrad datenschutzrechtlicher Massnahmen

- 5 Organisationen bewerten den Reifegrad ihrer datenschutzrechtlichen Massnahmen mit «optimiert».
- 9 Organisationen bewerten ihren Reifegrad mit «definiert».
- 4 Organisationen bewerten ihren Reifegrad mit «ad hoc».

Die Mehrheit der Organisationen bezeichnet den Reifegrad ihrer datenschutzrechtlichen Massnahmen als «definiert». Das heisst, Prozesse sind definiert und dokumentiert, deren Umsetzungsqualität ist aber noch schwankend. Eine Minderheit der Organisationen nimmt für sich die unterste Reifegradstufe «ad hoc» in Anspruch, d. h. diese Organisationen handeln primär situativ. Dementsprechend gibt es keine definierten Prozesse und die Qualität von Massnahmen lässt sich nicht voraussagen. Etwa gleich viele Organisationen nehmen für sich die Stufe «optimiert» am oberen Ende der Skala in Anspruch. Die Umsetzung ihrer Prozesse ist Routine und es ist ein kontinuierlicher Verbesserungsprozess (KVP) etabliert, um Schwächen systematisch zu identifizieren und auszumerzen.

Die Auslegeordnung zeigt, dass bei den befragten Organisationen ein ziemlich grosses Bewusstsein für datenschutzrechtliche Fragen vorhanden ist. Über zwei Drittel (14) bezeichnen den Reifegrad der von ihnen umgesetzten Massnahmen als «definiert» oder «optimiert».

«Für uns liegt die grösste Herausforderung darin, dass das Datenschutzgesetz kantonale (und nicht nationale) Sache ist und wir in Bezug auf Cloud Lösungen im Spital Umfeld darauf angewiesen sind, uns mit anderen Spitälern zu koordinieren und gemeinsame Resultate zu nutzen. Das setzt voraus, dass wir schweizweit eine einigermassen einheitliche Umsetzungsstrategie und einen einheitlichen Umsetzungsstand des Datenschutzgesetzes haben. Wir werden hier nicht auf Politik warten können.»

(Urs Meier, CISO, Insel Gruppe)

Rechtliche Unsicherheiten aufgrund von unterschiedlichen Jurisdiktionen

- 12 Organisationen haben für den Umgang mit rechtlichen Unsicherheiten aufgrund unterschiedlicher Rechtsprechung ein formalisiertes Vorgehen definiert.
- 4 Organisationen behandeln die Unsicherheiten ad hoc.
- 2 Organisationen sehen bei diesem Problem nicht sich, sondern die Cloud-Diensteanbieter in der Verantwortung.

Allen befragten Organisationen ist die Problematik von unterschiedlichen Jurisdiktionen bei der Nutzung von Cloud-Diensten bewusst. Ein Grossteil hat hierfür ein formalisiertes Vorgehen etabliert. Die Lösungen sind jedoch sehr unterschiedlich. Während einige Organisationen diesen Sachverhalt als Risiko behandeln, setzen andere auf etablierte Standards wie den BSI Kriterienkatalog C5. Die Überwachung der Massnahmen erfolgt in der Regel durch die Rechtsabteilung oder das Compliance-Departement oder sie wird auf Projektebene sichergestellt. Sehr oft werden die Risiken nicht selbst abgeschätzt, stattdessen wird hierfür externe Unterstützung in Anspruch genommen. Einige Organisationen behandeln das Thema ad hoc. Der dadurch entstehende Mangel an Visibilität wird in Kauf genommen. Eine Minderheit verfolgt die Problematik gar nicht und verlässt sich darauf, dass der Cloud-Diensteanbieter die nötigen Massnahmen ergreift.

Haftung

Betreffend Haftung ist vertraglich zu definieren, inwieweit der Cloud-Diensteanbieter in einem Schadenfall haftet. Die Einhaltung der vertraglichen Regelungen ist von

Seiten des Leistungsbezügers mit geeigneten Massnahmen zu überprüfen. Fünf Organisationen berücksichtigen Haftungsfragen gar nicht. Etwas mehr als die Hälfte der befragten Organisationen gibt an, Haftungsfragen zu berücksichtigen. Gemeinsam haben sie alle, dass sie die Thematik im Rahmen von Vertragsverhandlungen mit den Cloud-Diensteanbietern adressieren. Das Vorgehen dabei ist jedoch sehr heterogen. Vier Organisationen übernehmen bei grossen Cloud-Diensteanbietern in der Regel die Standardverträge ohne Änderungen. Zwei Organisation definieren die entsprechenden Anforderungen pro Anwendungsfall, um diese im Rahmen der Vertragsverhandlungen durchzusetzen. Eine Organisation gibt an, neben Vertragsverhandlungen, die Risiken bezüglich Integrität und Vertraulichkeit von Daten mittels Versicherungslösungen zu transferieren. Generell hinterlassen die Aussagen den Eindruck, dass die Thematik grösstenteils von Seiten der Cloud-Diensteanbieter gesteuert wird.

Berücksichtigung von Haftungsfragen

- 10 Organisationen berücksichtigen Haftungsfragen im Rahmen der Vertragsverhandlungen.
- 5 Organisationen setzen sich gar nicht mit Haftungsfragen auseinander.
- 3 Organisationen haben sich zu diesem Thema nicht eindeutig geäussert.

Damit bei einem Schadenfall ein Cloud-Diensteanbieter haftbar gemacht werden kann, muss sein Verschulden nachgewiesen werden. Knapp die Hälfte der Organisationen gibt an, dass die Beweisführung sehr schwierig oder gar unmöglich ist und dass man deshalb auf externe Hilfe (z. B. für forensische Untersuchungen) angewiesen ist. Organisationen, die Vorkehrungen zum Nachweis eines Verschuldens getroffen haben, wenden dafür unterschiedliche Massnahmen an, die zum Teil auch kombiniert werden: Zwei Organisationen nannten rein technische Mittel zur Überwachung des Cloud-Diensteanbieters. Acht Organisationen lassen sich durch Verträge die Einhaltung entsprechender SLAs bzw. KPIs zusichern oder verlassen sich diesbezüglich auf gesetzliche Regelungen. Deren Einhaltung wird in der Regel mit Überwachungswerkzeugen, welche durch den Cloud-Diensteanbieter zur Verfügung gestellt werden, regelmässigen Qualitäts-Meetings oder gezielten Audits geprüft.

Nachweis eines Verschuldens auf Seiten des Cloud-Diensteanbieters

- 8 Organisationen sehen sich gar nicht in der Lage, ein Verschulden des Cloud-Diensteanbieters nachweisen zu können.
- 2 Organisationen stützen beim Nachweis auf technischen Massnahmen ab.
- 8 Organisationen stützen auf vertragliche oder gesetzliche Anforderungen ab.

In einem Fall werden Cloud-Diensteanbieter vertraglich zur Aushändigung von Logs im Falle eines Vorfalls verpflichtet. Eine Organisation beruft sich auf die gesetzlich festgeschriebene Meldepflicht und eine weitere Organisation plant ein Reporting gemäss des BSI Standard einzuführen.

Ein Verschulden seitens Cloud-Diensteanbieters ist schwierig nachzuweisen. Insbesondere bezüglich der Schutzziele Vertraulichkeit und Integrität ist man im Ernstfall auf die Kooperation des Diensteanbieters oder aufwändige forensische Untersuchungen angewiesen. Ob letztere erfolgreich sind, ist fraglich, da die meisten relevanten Informationen aus den Systemen des Cloud-Diensteanbieters herausgelesen werden müssten. Die Verfügbarkeit von Cloud-Diensten (SLAs) kann hingegen relativ einfach von Kundenseite mit technischen Mitteln gemessen werden. Dies zeigt sich in der gängigen Praxis, bei welcher der Kunde im Falle eines Verstosses gegen die SLAs den Cloud-Diensteanbieter abmahnt. Diese Option wird jedoch bei weitem nicht von allen Organisationen wahrgenommen.

Zusammenfassend kann festgehalten werden, dass bei Haftungsfragen die befragten Organisationen gegenüber den Cloud-Diensteanbietern in einer eher schwachen Position sind. Insbesondere in Bezug auf die Schutzziele Vertraulichkeit und Integrität ist man im Ernstfall auf die Kooperation des Cloud-Diensteanbieters oder allfällige forensische Untersuchungen angewiesen. Beim Thema der Verfügbarkeit sind die Kunden/-innen demgegenüber in einer stärkeren Position.

5. Risikokultur

Risikokultur ist wahrscheinlich einer der am häufigsten verwendeten und gleichermassen einer der unschärfsten Begriffe in der Literatur und Praxis. Speziell die Risikokultur wird in jüngster Vergangenheit zunehmend diskutiert und oft in Zusammenhang mit negativen Vorfällen (Betrug, Hinterziehung, Cybervorfälle, Finanzkrise etc.) gebracht. Heute weisen Ausbildungsstätten, Berater, Risk Management-Rahmenwerke und -Normen sowie Wissenschaftler/-innen regelmässig auf die hohe Bedeutung einer «angemessenen» Risikokultur hin. Allerdings herrscht kein Konsens über die Definition der Risikokultur. Darüber hinaus ist es umstritten, wie die Risikokultur mit der Unternehmenskultur zusammenhängt bzw. ob diese überhaupt getrennt voneinander existieren.

Grundsätzlich können zwei verschiedene, jedoch zentrale Aspekte bez. der Risikokultur genannt werden. Erstens bezieht sich die Risikokultur auf die Verhaltensweisen der Organisationsmitglieder im Rahmen ihres Umgangs mit dem implementierten Risk Management-Prozess. Bei dieser Sichtweise geht es darum, Risikokultur primär über die Mentalitäten, Verhaltensweisen und Einstellungen der Mitarbeitenden hinsichtlich Risk Management zu begreifen. Diesbezüglich spielt der so genannte «tone from the top» eine zentrale Rolle, d. h. das Prägen, Vorleben und Kommunizieren eines erwünschten Risikoverhaltens durch die Unternehmensleitung.

Der zweite Ansatz legt den Schwerpunkt darauf, wie viel Risiko das Management und die Mitarbeitenden bereit sind, willentlich und wissentlich einzugehen, um die Organisationsziele zu erreichen (Risikoappetit, Risikoeinstellung). Risikokultur, so verstanden, ist ein Hilfsmittel zur Kommunikation der Risiko- und Ertragskompromisse, die eine Organisation in einem Unternehmen bewusst eingeht, um die Organisationsziele zu erreichen.

Etwas allgemeiner kann festgehalten werden, dass die Risikokultur alle Werte, Normen und Verhaltensweisen umfasst, welche Organisationen und alle ihre Mitarbeitenden beim bewussten Umgang mit Risiken (und Chancen) unterstützen, ermöglichen und beeinflussen. Sie umfasst die impliziten Regeln und die Annahmen, wie das Risk Management zur Erreichung der Organisationsziele beiträgt. Eine positive Risikokultur drückt sich darin aus, dass risikorelevante Informationen, die durch das Risk Management generiert wurden, tatsächlich in die Entscheidungsprozesse der Organisation einfliessen. Risikokultur beinhaltet deshalb auch, inwiefern intuitive Entscheidungsprozesse (z. B. Geschäftsentscheide, die neue Cyber Risiken verursachen) mit rationalen Risikoinformationen abgeglichen werden (vgl. Hunziker 2021).

Tone from the top

Mittlerweile unbestritten ist die Relevanz des «Tons an der Spitze» für die Risikokultur und damit auch für die Wirksamkeit eines (Cyber) Risk Managements. Er repräsentiert das Bekenntnis der Unternehmensleitung zum Risk Management. Dieses Bekenntnis muss in der gesamten Organisation wahrnehmbar sein. Eine zentrale Voraussetzung für einen angemessenen «tone from the top» ist die Aufmerksamkeit («awareness»), welche die Unternehmensleitung dem Umgang mit Cyber Risiken widmet.

Cyber Risiken geniessen durchwegs eine hohe bis sehr hohe Aufmerksamkeit in den Leitungsgremien.

«Auf der Governance Seite ist das Thema auch ganz oben angekommen. Cyber Security ist ein grosses Thema im Audit Committee.»

(Risk Manager, anonym)

Viele Risk Management-Verantwortliche erklären, dass dieses Thema insbesondere in den letzten zwei bis fünf Jahren bedeutend an Relevanz zugenommen hat. Die Gründe dafür sind sehr unterschiedlich, von personeller Affinität zum Thema in den Leitungsgremien, eigenen Erfahrungen mit Cyber Angriffen über Beurteilung als Top-Risiko im Risk Management.

Bedeutung der Cyber Risiken in den Leitungsgremien

- In allen 16 befragten Organisationen geniessen Cyber Risiken eine hohe bis sehr hohe Bedeutung in den Leitungsgremien.
- Die Gründe für die hohe Aufmerksamkeit sind unterschiedlich, u. a.:
  - Organisation wurde selbst Opfer eines Angriffs (2)
  - Wettbewerber wurden Opfer (1)
  - Hohe mediale Präsenz (1)
  - Regulatorisches Erfordernis (1)
  - CISO ist Mitglied der Geschäftsleitung (1)
  - Mitglieder des Aufsichtsorgans mit hoher Affinität zu Cyber Risiken (1)
  - Austausch mit externem Dienstleister (1)
  - Etablierung von Verwaltungsrats- und Geschäftsleitungs-Ausschüssen für Cyber Risiken.
  - Vom Risk Management als Top-Risiko beurteilt (2)
  - Vorhandensein expliziter Budgets für Cyber Risk Management (5)

«Auf der obersten Leitungsebene, also Verwaltungsrat, Ausschüsse, Geschäftsleitung, nimmt man Cyber Risiken sehr ernst. Es gibt sogar zwei Ausschüsse mit Beteiligung der Konzerninformatik, die sich damit beschäftigen, sozusagen ein doppeltes Sicherheitsnetz.»

(Alexander Hilsbos, Leiter Risk Management, Insel Gruppe).

Ebenso spielen teilweise externe Institutionen wie der externe IT-Dienstleister oder der Regulator eine Rolle. Als meistgenannte Schwäche, wieso Cyber Risiken noch nicht ganz die notwendige Aufmerksamkeit erhalten, wurde das fehlende Know-how auf Stufe Aufsichtsorgan und Geschäftsleitung genannt (4). Die Relevanz der Thematik wird auch damit unterstrichen, dass zunehmend mehr Organisationen mit den für das Cyber Risk Management zur Verfügung gestellt Budgets zufrieden sind bzw. diese als «ausreichend» bezeichnen (5).

Die Interview-Erkenntnisse zeigen ein erwartungstreues Resultat: Alle Leitungsgremien beurteilen Cyber Risiken als relevant, mit einer klar zunehmenden Tendenz. Das deckt sich generell mit der Entwicklung und Erkenntnissen aus der Literatur. Mittlerweile ist das Cyber Risiko bereits als global relevantes, systemisches Risiko deklariert worden, neben z. B. Klimarisiken. Eine deutliche Mehrzahl der befragten Risk Management-Verantwortlichen hat erklärt, dass die Geschäftsprozesse in hohem Ausmass von der Informationstechnologie abhängig sind und deshalb auch ein Bewusstsein vorherrscht, dass dies ein grosses Risiko sein kann.

Expertise

Wie oben bereits angetönt, ist die Expertise im Umgang mit Cyber Risiken eine wichtige Voraussetzung für ein effektives Risk Management, die in immerhin einem Drittel der interviewten Organisationen auf Führungsebene angezweifelt wird. Um diesen Aspekt etwas näher beleuchten zu können, wurde für die vorliegende Studie anhand vier Fragen eine Art «Mini-Maturitätstest» im Umgang mit Cyber Risiken entwickelt und in den Interviews mit den Risk Management-Verantwortlichen diskutiert. Die vier Fragen sollten hypothetisch durch die vier Funktionen Geschäftsführer/in (CEO), Finanzverantwortliche/r (CFO), Risk Management-Verantwortliche/r (CRO) und Präsident/in des Aufsichtsorgans (VRP) beantwortet werden.

Schützenswerte Assets (Kronjuwelen)

Von den 16 interviewten Organisationen sind acht Risk Management-Verantwortliche davon überzeugt, dass CFO, CEO und der Vorsitz des Aufsichtsorgans die Kronjuwelen bzw. die schützenswerten Assets kennen und benennen könnten.

Schützenswerte Assets (Kronjuwelen)

a. Kennen CEO, CFO, CRO und VRP die wichtigsten schützenswerten (digitalen) Assets und schützen diese angemessen? (Kronjuwelen)

- 8 Organisationen bejahen diese Frage uneingeschränkt.
- In 5 Organisationen kennen die VRP die Kronjuwelen nicht, alle anderen schon.
- 2 Organisationen geben an, dass diese (wohl) niemand kennt.

«Dadurch, dass wir dieses Thema auch wirklich weit oben im Board und in der Konzernleitung angesetzt haben – der CIO ist Mitglied der Konzernleitung – weiss man, was die wichtigsten Themen sind. Die Kronjuwelen sind bekannt.»

(Risk Manager, anonym)

Fünf Organisationen bejahen diese Frage für die GL-Stufe, denken aber, dass das Aufsichtsorgan diese nicht oder eher nicht kennen. Zwei Organisationen hegen starke Zweifel, dass die GL und das Aufsichtsorgan die schützenswerten Assets kennen. Hier ist erhebliches Optimierungspotenzial auszumachen. Grundsätzlich sollten sich die Geschäftsleitung und das Aufsichtsorgan der schützenswerten Assets bewusst sein. Fast die Hälfte der interviewten Organisationen geben an, dass zumindest das Aufsichtsorgan und teilweise auch Geschäftsleitung diese nicht kennen. Vor dem Hintergrund der Verantwortlichkeiten des Aufsichtsorgans kann dies als problematisch beurteilt werden.

Die wichtigsten Cyber-Schwachstellen

Von den 16 interviewten Organisationen sind nur vier Risk Management-Verantwortliche davon überzeugt, dass CFO, CEO und der Vorsitz des Aufsichtsorgans die wichtigsten Cyber-Schwachstellen kennen und benennen könnten. Fünf Organisationen bejahen diese Frage für die GL-Stufe bzw. den Risk Management-Verantwortlichen, denken aber, dass das Aufsichtsorgan diese nicht oder eher nicht kennen. Drei Organisationen bemerken, dass der CISO diese kennt, nicht aber die Unternehmensleitung. Sechs Organisationen bezweifeln, dass die GL und das Aufsichtsorgan die Cyber-Schwachstellen ihrer Organisation kennen.

Kenntnis über wichtigste Cyber-Schwachstellen

b. Kennen CEO, CFO, CRO und VRP die wichtigsten Cyber-Schwachstellen ihrer Organisation?

- 4 Organisationen bejahen diese Frage uneingeschränkt.
- In 5 Organisationen kennen die VRP die Cyber-Schwachstellen nicht, alle anderen schon.
- 6 Organisationen hegen grosse Zweifel, dass diese überhaupt jemand kennt.
- 3 Organisationen geben an, dass diese höchstens der CISO kennt.

Nur vier von 16 Organisationen schätzen sich selbst so ein, dass die Unternehmensleitung sich den wichtigsten Cyber-Schwachstellen bewusst ist. Dieses Bild zeigt, dass das Cyber-Risk-Assessment ggf. zu wenig ausgeprägt ist, um a) die relevanten Risiken zu identifizieren und b) diese entsprechend der Unternehmensleitung bewusst zu machen. Diese Erkenntnisse bestätigen das bekannte Bild aus der Literatur, dass Cyber Risiken immer noch (zu) stark als «IT-Verantwortlichkeit» verstanden werden.

Strategien zur Steuerung von Cyber Risiken

Von den 16 interviewten Organisationen sind nur vier Risk Management-Verantwortliche im Gespräch mit den Studienautoren/-innen davon überzeugt, dass CFO, CEO und der Vorsitz des Aufsichtsorgans die wichtigsten Strategien zur Steuerung der Cyber Risiken kennen. Acht Organisationen bejahen diese Frage für die GL-Stufe bzw. den CRO, denken aber, dass das Aufsichtsorgan diese nicht oder eher nicht kennen. Drei Organisationen bemerken, dass der CISO bzw. eher die operative Stufe (im

Rahmen eines ISMS) diese kennen, nicht aber die Unternehmensleitung.

Kenntnis über wichtigste Strategien zur Steuerung von Cyber Risiken

c. Kennen CEO, CFO, CRO und VRP Ihre wichtigsten Strategien zur Steuerung von Cyber Risiken?

- 4 Organisationen bejahen diese Frage uneingeschränkt.
- In 8 Organisationen kennt der VRP die Strategien nicht, jedoch alle anderen.
- 1 Organisation bemerkt, dass dies die schwierigste Frage von allen vier sei.
- 3 Organisationen hegen grosse Zweifel.
- 2 Organisationen geben an, dass diese Frage höchstens der CISO oder das «operative Personal» beantworten könnte.

Nur vier von 16 Organisationen geben zu Protokoll, dass die Unternehmensleitung die wichtigsten Strategien zur Steuerung der Cyber Risiken kennt. Dieses Ergebnis zeigt, dass die Massnahmen zur Risikosteuerung von Cyber Risiken in den untersuchten Organisationen noch zu wenig bekannt sind. Dies bestätigt die bereits oben angesprochene Erkenntnis aus der Literatur, dass Cyber Risiken immer noch stark als «IT-Thema» gesehen werden, die dezentral und auf operativer (System-)Ebene gesteuert werden.

Ressourcen für das Cyber Risk Management

Keine (!) Organisation gab zu Protokoll, dass aktuell zu wenig Budget bzw. Ressourcen vorhanden sind für das Cyber Risk Management. Neun Risk Management-Verantwortliche geben an, dass die gesamte Unternehmensleitung sich bewusst ist, dass Budgets für diese Aufgabe bereitstehen müssen. Teilweise hat sich dies aber auch erst in den letzten Jahren zum Positiven verändert, sei es aufgrund eines neuen Vorgesetzten (1) oder eines Cyber-Vorfalls (2). Immerhin sieben Organisationen vermuten, dass das Aufsichtsorgan sich der Budgets und der Ressourcen wahrscheinlich nicht oder zu wenig bewusst sind.

Bereitstellung von Ressourcen für das Cyber Risk Management

d. Werden angemessene Ressourcen (Budget, Personal) zur Begegnung der Cyber Risiken bereitgestellt?

- 9 Organisationen bejahen diese Frage uneingeschränkt.
- In 7 Organisationen könnten die VRP diese Frage (vermutlich) nicht beantworten.

Bezüglich Budgets ist die Mehrheit der befragten Organisationen mittlerweile gut aufgestellt. Allerdings steht dahinter auch meist eine plausible Entwicklung bzw. ein plausibler Trigger (z. B. Erhöhung der Awareness, mediale Präsenz, selbst erlebte Vorfälle). Bei ca. einem Drittel aller interviewten Organisationen ist die Ressourcen-Thematik noch (zu) wenig im Bewusstsein des Aufsichtsorgans, was sich ebenfalls mit obigen Interpretationen (Fragen a - c) deckt.

«I would frame it this way; whenever something unexpected happened, we got the resources to respond adequately.»

(Risk Manager, anonym)

Effektivitätsprüfung

Grundsätzlich gibt es verschiedene Möglichkeiten, die Wirksamkeit (Effektivität) von Risk Management-Aktivitäten zu überprüfen. Allerdings sind nicht alle diesbezüglichen Tests gleich aussagekräftig. Erschwerend kommt hinzu, dass oft Glück und Wirksamkeit miteinander verwechselt werden. Nur weil in einer Organisation «bis jetzt» noch keine Cyber Vorfälle bekannt sind, heisst das nicht, dass das Cyber Risk Management tatsächlich effektiv ist – es könnte eben auch Glück bzw. Zufall sein. Dies illustriert auch das «Assume-Breach-Paradigma», dem die grundsätzliche Annahme zugrunde liegt, dass jede Organisation trotz aufwändiger Sicherheitsmassnahmen davon ausgehen muss, einmal Opfer eines Cyber-Angriffes zu werden.

Risk Management-Systeme können einerseits einer formalen Prüfung unterzogen werden; dieses Vorgehen gleicht einem auditähnlichen Verfahren. Bei diesem «Test» geht es darum zu prüfen, ob die formalen Risk Management-Anforderungen erfüllt werden. Dies erfordert eine Überprüfung aller verfügbaren Dokumente und Richtlinien im Zusammenhang mit dem (Cyber) Risk Management. So können Organisationen Informationen darüber sammeln, wie Cyber Risiken identifiziert, bewertet, aggregiert und berichtet werden. Ausserdem kann die Risk Management Organisation hinsichtlich Rollen, Aufgaben und Verantwortlichkeiten geprüft werden. Risikoberichte können auf Vollständigkeit und Aktualität hin geprüft werden. Diese formale Prüfung lässt allerdings nur einen bedingten Schluss bez. Wirksamkeit des (Cyber) Risk Managements zu. Ergänzend kann die Qualität der Informationen, die der Risk Management-Prozess generiert, beurteilt werden. Dieser Test basiert auf der Frage, ob die Cyber Risk Management-Anforderungen der verschiedenen Interessengruppen erfüllt wurden. Zunächst muss die Unternehmensleitung als zentraler Stakeholder des Cyber Risk Management beurteilen, ob:

- Cyber Risiken als Risikokategorie explizit beurteilt und berichtet werden.
- die Cyber Risiken nachvollziehbar, d. h. in gleicher Terminologie wie andere Risikokategorien, bewertet werden. Dies kann z. B. anhand quantitativer Szenarioanalysen vorgenommen werden.
- die Cyber Risiken grafisch so aufbereitet sind, dass sie zur Entscheidungsfindung herangezogen werden können.
- die einzelnen Cyber Risiken innerhalb oder ausserhalb der definierten Risikobereitschaft liegen.
- die wichtigsten Cyber-Risikoszenarien in verständlicher Form kommuniziert werden, d. h. ihre Auswirkungen hinsichtlich der Erreichung der Geschäftsziele mit relevanten Kennzahlen (Unternehmenswert, EBIT, Cashflow etc.) verknüpft sind.
- regelmässige externe Audits der Cybersicherheit durchgeführt und deren Ergebnisse entsprechend berücksichtig werden.
- die interne Revision (falls verfügbar) den Cyber Risiken auf ihrem Prüfplan entsprechendes Gewicht beimessen.
- Versicherungslösungen verfügbar wären, die unter Kosten-Nutzen-Betrachtungen und der Berücksichtigung des Risikoappetits einen bedeutenden Risikotransfer erlauben.
- die Organisation konkrete Testverfahren anwendet, um die Cyber Resilienz zu prüfen (Vulnerability Scans, manuelle Prüfungen von Webapplikationen, Penetrationstests, Bug Bounty-Programm, Notfall- und Krisenstabsübungen, Awareness-Programme für die Mitarbeitenden (z. B. Phishing-Tests), Abgleich der implementierten Massnahmen mit standardisierten Massnahmenkatalogen, z. B. IT-Grundschutzkompendium u. v. m.).

Ansätze zur Effektivitätsprüfung des Cyber Risk Management

- 5 Organisationen führen regelmässige externe Audits durch.
- 6 Organisationen nutzen regelmässige Penetrationstests.
- 2 Organisationen nutzen Bug Bounty-Programme.
- 1 Organisation verweist auf die ISMS-Zertifizierung.
- 2 Organisationen verweisen auf die Interne Revision.
- 3 Organisationen geben an, keine Wirksamkeitsprüfungen vorzunehmen.
- 1 Organisation verweist auf die BCM-Prozesse.
- Keine Organisation nimmt eine formale Wirksamkeitsprüfung durch.
- Keine Organisation nutzt die Stakeholder-Analyse zur Wirksamkeitsprüfung.

Von den 16 Organisationen, die zu dieser Frage Stellung genommen hatten, verweisen fünf auf regelmässige externe Audits als wichtigste Effektivitätsprüfung und drei auf ihren externen IT-Dienstleistungspartner. Sechs Organisationen führen regelmässige Penetrationstests durch, zwei unterhalten Bug Bounty-Programme. Insgesamt zeigt sich bei der Effektivitätsprüfung ein heterogenes Bild. Zwei Organisationen nennen die Interne Revision als einzige Instanz der Effektivitätsprüfungen, zwei weitere Organisationen geben zu Protokoll, dass sie keine Aussagen machen können, da es bisher zu keinen Cyber-Vorfällen gekommen sei. Eine Organisation gibt zu bedenken, dass sie überhaupt kein Cyber Risk Management betreiben und so auch keine Aussage bez. Effektivität machen kann. Je eine Organisation nennt «einen internen Spezialisten/eine interne Spezialistin», «das Einüben der BCM-Prozesse» oder eine «ISMS-Zertifizierung» als Mittel zur Effektivitätsprüfung. Eine ganzheitliche, formale Prüfung der Risk Management-Prozesse, wie oben vorgestellt, nimmt keine Organisation vor.

Es lässt sich keine dominante Vorgehensweise zur Prüfung der Effektivität des (Cyber) Risk Managements in den untersuchten Organisationen ausmachen. Immerhin die Hälfte (8) nutzt externe Unterstützung in Form von Audits oder externen Dienstleistern und ca. ein Drittel (6) führt Penetrationstests durch. Auffällig ist, dass die Risk Management-Verantwortlichen in dieser Studie primär die technischen, systembezogenen Tests der IT-Infrastruktur in den Vordergrund stellen, obwohl die Risk Governance bzw. die Risikokultur (Faktor «Mensch», «tone from the top», Trainings, Schulungen) bekanntermassen eine wesentliche (oft *die* wesentliche) Rolle bei der Wirksamkeit von Cyber Risk Management einnimmt.

6. Cyber Risk Management

Cyber Risiken durchlaufen grundsätzlich denselben Risk Management-Prozess wie alle anderen Risikokategorien, allerdings oft mit anderen Identifikations- und Beurteilungsmethoden (z. B. basierend auf ISO 27005 oder NIST SP 800-30 Rev. 1). Aus einer ERM-Perspektive machen Cyber Risiken mittlerweile einen Teil des Risikoportfolios jeder Organisation aus, je nach Geschäftsmodell und Branche ist dieser Anteil grösser oder kleiner. Deshalb müssen Cyber Risiken identifiziert, beurteilt und in einer Sprache dokumentiert werden, die kompatibel mit dem ERM ist. Die Ergebnisse aus dem Cyber Risk Assessment dienen als Input zur Erstellung des Risikoprofils auf oberster Organisationsebene. Damit dies gewährleistet ist, müssen Cyber Risiken einigen Anforderungen genügen, u. a. müssen sie konsistent beurteilt, über die Systemebene hinweg auf Organisationebene konsolidiert bzw. aggregiert und anhand von Szenarien hinsichtlich ihres Einflusses auf die Organisationsziele analysiert werden.

Derzeit führen viele Organisationen Cyber Risk Assessments noch nicht in konsistenter, mit dem ERM abgestimmter Weise durch. Die Bewertung der Cyber Risiken in Frankenbeträgen und Eintrittswahrscheinlichkeiten sowie die Aggregation und Berichterstattung von diesen Risken erfolgt teilweise gar nicht, teilweise ad hoc und nur selten mit der gleichen Aufmerksamkeit und methodischen Qualität wie bei anderen Risikokategorien. Eine Verbesserung der im Cyber Risk Management genutzten Methoden sowie eine Integration in das ERM würde insgesamt zu einem wirksameren, entscheidungsrelevanten Risk Management führen.

Identifikation von Cyber Risiken

Zweifelsohne gehört die Identifikation von Cyber Risiken zu den kritischsten Prozessschritten überhaupt und bestimmt die Wirksamkeit aller darauffolgenden Schritte des Cyber Risk Managements. In diesem Schritt geht es darum, die Ursachen und Auswirkungen von Cyber Risiken so präzise und vollständig wie möglich zu beschreiben und z. B. in einem Risikoinventar festzuhalten. Die Ausgangslage der Risikoidentifikation von Cyber Risiken ist die Bestimmung und Beurteilung der relevanten, schützenswerten Assets («Kronjuwelen») der Organisation (z. B. anhand einer Business Impact Analyse [BIA] oder anhand des ERM-Prozesses). Darauf basierend werden potenzielle Bedrohungen identifiziert, welche diese Assets bez. Vertraulichkeit, Integrität und Verfügbarkeit gefährden können. Inwiefern diese Bedrohungen alle relevant sind, hängt von der Beurteilung der eigenen Schwächen («Vulnerabilitäten») ab. In einem letzten Schritt werden die potenziellen Konsequenzen dieser Risiken eingeschätzt (vgl. dazu NISTIR 8286 im Zusammenhang mit NIST SP 800-30).

Ansätze zur Identifikation von Cyber Risiken

- 11 Organisationen nutzen weder einen Standard noch ein Rahmenwerk (ISO, NIST, BSI) zur Risikoidentifikation.
- 2 Organisationen richten sich nach ISO 27001 oder IKT-Minimalstandard aus.
- 3 Organisationen verlassen sich primär auf externe Audits.
- 2 Organisationen kombinieren Top-down- (Business) und Bottom-up-Identifikation.
- 4 Organisationen verlassen sich auf ein Benchmarking mit Experten und Branchenvertretern.
- 3 Organisationen identifizieren diese Risiken nicht explizit oder nur ad hoc.
- Nur in 3 Organisationen ist der Risk Manager (teilweise) involviert.

Es zeigt sich ein sehr heterogenes Bild, was die Methoden, Hilfsmittel und Prozesse zur Identifikation von Cyber Risiken betrifft.

Rund ein Drittel der Organisationen haben dazu einen formalen Risk Management-Prozess installiert, der entweder top-down (4) via Risk Assessment durch das Risk

Management oder top-down/bottom-up (2) via Systeme/Geschäftsprozesse im Zusammenspiel mit Risikoanalysen auf Business-Ebene funktioniert. Alle anderen Organisationen verlassen sich entweder komplett auf externe Partner (Audits, Berater), nutzen Benchmarking oder geben ihr SOC als primäre Quelle für die Risikoidentifikation an. Zwei Organisationen geben an, diese Risken überhaupt nicht (oder nur ad hoc) zu identifizieren. Je eine Organisation richtet sich nach ISO 27001 aus oder orientiert sich am NCSC bzw. IKT-Minimalstandard zur Risikoidentifikation. Zwei Organisationen erwähnen Penetrationstests als Hilfsmittel, eine Organisation bedient sich einer internen Risikocheckliste. Auffällig ist, dass elf Organisationen explizit von der Erfüllung eines Standards absehen oder diese höchstens ergänzend in Erwägung ziehen. Standards werden mehrfach als wenig nutzenstiftend bzw. generell als kritisch angesehen. Die Risikomanager/-innen bzw. die für das Risk Management verantwortlichen Personen sind nur wenig an diesem Prozessschritt beteiligt (als Informationsempfänger oder zum kritischen Hinterfragen der Bottom-up-Informationen).

«Um die Vollständigkeit des Risikoinventars sicherzustellen, machen wir alle 2 Jahre sogenannte Risk Cluster Workshops für verschiedene Bereiche. Damit lässt sich Silo Thinking vermeiden.»

(Peter Jussel, Corporate Risk and Insurance Management, Hilti Corporation)

Die Ergebnisse der 16 Organisationen zeigen auf, dass sich kein dominantes Vorgehen zur Risikoidentifikation herauskristallisiert hat, weder methodisch noch prozessual. Eine Integration in die formalen Prozesse des unternehmensweiten Risk Managements findet nur sehr spärlich statt. In den Interviews wurde auch klar, dass die Risk Management-Verantwortlichen die spezifischen Prozesse und Methoden zur Identifikation von Cyber Risiken nicht lückenlos erklären konnten. Dies liegt teilweise auch an der stark technischen Ausrichtung (Systemebene, IT-Infrastruktur-Ebene) der Risikoanalyse, bei der das ERM nicht oder nur als Informationsempfänger einbezogen wird. Interessanterweise verlässt sich kaum eine Organisation auf Standards wie ISO, BSI oder NIST, vielmehr wird eher auf externe Assessments (Audit, Beratung) zur Risikoidentifikation abgestellt. Lediglich eine Organisation gibt an, Cyber Risiken als Teil der operativen Risiken via ihr Risk Management zu identifizieren. Dies bestätigt die Tendenz, dass sich Risk Management-Verantwortliche nicht explizit an der Risikoidentifikation beteiligen. Diese Erkenntnis wird durch die aktuelle Literatur bestätigt, die zeigt, dass Cyber Risiken noch wenig in bestehende Risk Management-Systeme integriert sind bzw. immer noch stark als eine «technische Sonderkategorie» gelten, die sich nur schwer ins ERM integrieren lässt.

«*An allen Risk Management-Events sind Cyber Risiken ein Thema. Meine Sorge ist der Hype-Charakter der Cyber Risiken. Wie schafft man es als Konzern aus der Fülle an Informationen die richtigen Diskussionen rund um Cyber Risiken zu führen?»*

(Daniel Imhof, Leiter Konzernrisikomanagement, Die Schweizerische Post)

Rolle der Versicherungsgesellschaften

Weiter wurden die Interviewten nach der Rolle der Versicherungsgesellschaften bei der Cyber-Risikoidentifikation befragt. Konkret wurde diskutiert, ob regelmässige Gespräche zur Bedrohungslage mit der Versicherungsgesellschaft stattfinden, welche die Risikoidentifikation unterstützen.

Rolle der Versicherer bei der Risikoidentifikation

- 14 Organisationen führen keine Gespräche mit dem Versicherer über die Bedrohungslage. Gründe dafür sind:
  - 5 Organisationen haben keine Cyber-Versicherung abgeschlossen.
  - 3 Organisationen erkennen den Nutzen darin nicht.
  - 6 Organisationen haben sich dies noch nicht überlegt.
- 6 Organisationen führen zwar Gespräche, jedoch zu anderen Themen:
  - Versicherungsdeckung von Cyber Risiken
  - Prämiensituation nach Berücksichtigung eigener Massnahmen
  - Support der Versicherung bei einem Cyber-Vorfall
  - Evaluation der Vertragserneuerung
- 2 Organisationen konnten dazu keine Angaben machen.

Bei 14 Organisationen finden keine regelmässigen Gespräche über die Bedrohungslage statt, allerdings weisen zwei Risk Management-Verantwortliche darauf hin, dass sie sich nicht sicher sind und selbst nicht einbezogen werden. Gründe für diese tiefe Quote liegen darin, dass fünf Organisationen über keine Cyber-Versicherung verfügen und damit gar nicht mit dem Versicherer in Kontakt sind. Es wäre zu erwarten, dass die Organisationen, welche eine Cyber-Versicherung abgeschlossen haben, solche Gespräche mit dem Versicherer führen. Dies scheint jedoch nur bei wenigen der Fall zu sein. Drei Organisationen sehen den Nutzen darin nicht und andere haben es sich gar nicht überlegt.

Lediglich sechs Organisationen führen regelmässige Gespräche mit ihrem Versicherer, jedoch aus unterschiedlichen Gründen (Abdeckung, Vorgehen im Schadenfall, Vertragserneuerung). Eine Organisation gibt an, selbst kein Gespräch zu suchen, jedoch regelmässig Fragen des Versicherers zu beantworten.

Insgesamt zeigt sich, dass sich beinahe alle Organisationen zumindest mit dem Abschluss einer Cyber-Versicherung auseinandergesetzt haben. Allerdings nutzt keine Organisation das Know-how des Versicherers zur Beurteilung der aktuellen Bedrohungslage. Hier besteht sicherlich Optimierungsbedarf, insbesondere weil der (potenzielle) Versicherer grundsätzlich noch wenig als Sparring-Partner angesehen bzw. genutzt wird. Es herrscht eine eher passive Haltung der Organisationen gegenüber dem Versicherer, d. h. Gespräche werden eher durch formaltechnische Aspekte initiiert und nicht aktiv zum Zwecke des Cyber-Risikodialogs gesucht.

Identifizierte Cyber Risiken

Die wichtigsten Cyber Risiken sind hinlänglich bekannt. Nach den Cyber Risken mit der grössten Bedrohung befragt, gaben die für das Riks Management Verantwortlichen recht unterschiedliche Formen der Cyberkriminalität als grösste Bedrohung an. Das ist einerseits durch die unterschiedlichen Geschäftsmodelle begründet. Anderseits scheinen sich zumindest einige der Interviewpartner/-innen mit den Terminologien des Cyber Risk Managements nicht vollständig vertraut zu sein, weil sie z. B. zu wenig involviert sind oder es an entsprechendem Know-how fehlt.

Bedeutendste Cyber Risiken aus Sicht Risk Management

- 8 Organisationen bezeichnen Ransomware oder andere destruktive Attacken als die grösste Bedrohung.
- 3 Organisationen bezeichnen Datenabfluss bzw. Spionage als die grösste Bedrohung.
- 3 Organisationen nennen beide Bedrohungen, ohne zu priorisieren.

Die meisten CRO bezeichnen Phishing als primären Angriffsvektor. Aus diesem manifestieren sich die meistgenannten Bedrohungen, namentlich destruktive Angriffe wie Ransomware und Datenabfluss. Die Gewichtung dieser beiden Bedrohungen steht in Zusammenhang mit dem Geschäftsmodell. Wo streng vertrauliche Daten zum Geschäftsmodell gehören (z. B. Gesundheit, Altersvorsorge), wird der Datenverlust und die dadurch entstehende Gefährdung der Vertraulichkeit gefürchtet. In der Industrie oder generell, wo operative Prozesse die Kernkompetenz bilden, ist es Ransomware, da dieses vor allem mit Betriebsstörungen in Verbindung gebracht wird. CEO-/CFO-Fraud mit Geldüberweisungen, gezieltes Social Engineering, Zero Day Lücken und destruktive Malware werden vereinzelt zusätzlich genannt.

Drittparteien-Risiken

Zunehmende Komplexität und steigender Wettbewerbsdruck veranlassen Organisationen zunehmend, Prozesse und/oder Infrastruktur an Drittparteien auszulagern – insbesondere durch die Nutzung von Cloud-Computing. Die damit verbundenen Ziele sind vielschichtig, u. a. können Kostensenkungen, Erhöhung der Kundenzufriedenheit oder Rentabilitätsziele im Vordergrund stehen. Für einige Organisationen stellen Auslagerungen an Drittparteien einen kritischen wirtschaftlichen Erfolgsfaktor dar, so können sich diese Organisationen auf ihr Kerngeschäft konzentrieren und dadurch einige Prozesse effizienter gestalten. Allerdings ist auch die Zuverlässigkeit und Integrität von Drittparteien wettbewerbsrelevant; eine Auslagerung an Drittparteien bringt aber auch einige (Cyber-)Risiken mit sich. Diese können mit einem Third Party Risk Management (TPRM) adressiert werden. TPRM wird als eine Aktivität des ERM aufgefasst, die sich auf die Identifizierung und Beurteilung von Risiken im Zusammenhang mit Auslagerungen konzentriert (vgl. Baumann & Hunziker, 2021). In den Interviews wurden die Risk Management-Verantwortlichen gefragt, was ihre Organisation bisher unternommen hat, um sich gegen Third Party Risks abzusichern.

Management von Drittparteien-Risiken

- Keine Organisation hat bisher ein ganzheitliches, formales TPRM eingeführt.
- In 3 Organisationen ist das TPRM in Erarbeitung.
- 1 Organisation hat keine relevanten Auslagerungen.
- 3 Organisationen konnten keine Auskunft geben.
- 12 Organisationen nennen Teilaspekte/-aktivitäten eines TPRM, u. a.:
  - 3 Organisationen führen Vendor Due Diligence durch.
  - 1 Organisation erstellt temporäre Nutzeraccounts.
  - 1 Organisationdokumentiert den externen Zugriff.
  - 2 Organisationen verweisen auf ihre Versicherung.
  - 1 Organisation verlässt sich auf «bekannte» IT-Provider.
  - 1 Organisation verlässt sich auf Zertifizierungen der Partner.
  - 4 Organisationen verlassen sich auf Vertragsprüfungen und SLAs.
  - 2 Organisationen führen Sicherheitsbestände in ihren Lagern.

Die Ergebnisse fallen sehr heterogen aus. Drei Organisationen sind aktuell im Aufbau eines TPRM. Keine Organisation hat ein formales, umfassendes TPRM als Teil ihres Risk Managements installiert, viele Organisationen führen jedoch verschiedene Teil-Aktivitäten durch, die dem TPRM im engeren und weiteren Sinn zuordbar sind. Zwei Risk Management-Verantwortliche verlassen sich explizit auf ihre (zertifizierten, bekannten) Provider. Vier Organisationen führen Vertragsprüfungen durch, weitere drei haben Vendor Due Diligence-Prozesse eingeführt. Festzuhalten ist, dass zwei Risk Management-Verantwortliche nicht wissen, ob ein TPRM existiert und eine Organisation gibt zu Protokoll, dass sie wegen zu geringen Risiken bewusst nichts unternehmen. Zwei Organisationen haben

diese Risiken versichert, ohne näher darauf eingehen zu können. Zwei Organisationen nennen diverse technisch organisatorische Massnahmen (TOMs, z. B. Richtlinien, Weisungen, temporäre Nutzeraccounts) und je eine Organisation nennt weitere Aktivitäten wie redundante Lagerhaltung oder eine Absicherung über ihr BCM.

Insgesamt widmen die interviewten Organisationen dem TPRM noch wenig Aufmerksamkeit, wobei immerhin drei im Aufbau eines solchen Systems sind. Das Bewusstsein um die Relevanz des Themas ist bei fast allen Organisationen in den Gesprächen spürbar, allerdings fehlen die entsprechenden Prozesse teilweise ganz oder es werden nur punktuell Massnahmen ergriffen, insbesondere die Vertragsprüfung oder Vendor Management. Bemerkenswert ist ebenfalls, dass immerhin fast ein Drittel der Organisationen entweder nichts über die Existenz von TPRM in ihrer Organisation wissen oder sich ausschliesslich auf die externen Partner verlassen, was klar als Handlungsbedarf ausgewiesen werden muss.

Bewertung von Cyber Risiken

Die Risikobewertung ist der nächste Schritt im Rahmen des Cyber Risk Management-Prozesse. Alle identifizierten Risiken müssen einer Bewertung unterzogen werden. Erst eine Bewertung macht eine Priorisierung von Cyber Risiken und den Vergleich mit anderen Risikokategorien im Rahmen eines ERM möglich. Zur Bewertung und Priorisierung von Cyber Risiken gibt es unzählige (qualitative und quantitative, deterministische und probabilistische) Möglichkeiten, auf die an dieser Stelle nicht detailliert eingegangen werden kann (z. B. ISO 27001, NISTIR 8286B, NIST SP 800-Familie, OpenFAIR).

Grundsätzlich werden mit der Bewertung von Cyber Risiken die Auswirkungen auf kritische digitale Komponenten («Kronjuwelen») und die damit verbundene Beeinträchtigung von Organisationszielen (z. B. bezüglich Finanzen, Reputation, Strategie) transparent und vergleichbar gemacht. In den Interviews wurde mit den Risk Management-Verantwortlichen diskutiert, wie Cyber Risiken in den jeweiligen Organisationen bewertet werden.

Bewertung von Cyber Risiken

- 7 Organisationen bewerten Cyber Risiken gleich wie alle anderen Risiken (Eintrittswahrscheinlichkeit und Schadenausmass).
- 2 Organisation verweisen externe Unterstützung.
- 2 Organisationen bewerten nur Schadenpotenziale via BIA.
- 5 Organisationen nehmen keine Stellung dazu.

Von den befragten Organisationen geben sieben an, dieselben Bewertungsmethoden wir für alle anderen Risikokategorien zu verwenden, d. h. klassisch anhand von Eintrittswahrscheinlichkeiten und Schadenausmasse. Je eine Organisation verweist auf ein externes Assessment (keine eigene Bewertung) oder auf das Assessment des Versicherungsbrokers. Zwei Organisationen beurteilen nur das Schadenpotenzial mit Hilfe der Business Impact Analyse (BIA).

Sieben Organisationen geben an, Cyber Risiken methodisch gleich wie alle anderen Risikokategorien zu bewerten.

«Cyber Risiken werden mit Unterstützung durch unseren Versicherungsbroker bewertet. Im Endeffekt werden sie wie andere Unternehmensrisiken analysiert und quantifiziert. Mit dieser Systematik können wir Cyber Risiken 1 zu 1 mit anderen Risiken vergleichen und priorisieren.»

(Alexander Hilsbos, Leiter Risk Management, Insel Gruppe).

Grundsätzlich ist dies positiv zu bewerten, obwohl in diesen Organisationen nicht klar ist, inwiefern eine Abstimmung mit den auf Systemebene identifizierten Risiken vorgenommen wird (Bottom-up-Sicht). Allerdings stossen diese klassischen Beurteilungsmethoden im Bereich der Cyber Risiken schnell an ihre Grenzen. Eine Verrechnung von Wahrscheinlichkeiten und Schadenausmasse (= Erwartungswert) kann zu einer Unterschätzung des tatsächlichen Risikos führen. Ebenso stellt sich heute kaum mehr die Frage, «wie wahrscheinlich» ein Cyber Risiko

überhaupt ist, sondern eher «wann» es eintritt. Das rückt das Schadenpotenzial als wichtigeres Beurteilungskriterium in den Vordergrund. Ebenso fehlen vielen der interviewten Organisationen besser geeignete Methoden, die technischen Cyber Risiken in die «Geschäftssprache» zu übersetzen und damit auch den Leitungsgremien verständlich kommunizieren zu können. Hierzu würden sich z. B. Szenarioanalysen eignen, die explizit auch die Auswirkungen auf die Organisationsziele transparent machen. Erwähnenswert ist auch eine in einem Gespräch geäusserte Meinung, dass die eigene Bewertung der Cyber Risiken mit Eintrittswahrscheinlichkeit und Schadenpotenziale nicht mit der Einschätzung des Versicherers übereinstimmt, da dieser sich ausschliesslich auf Schadenpotenziale beziehe. Zwei Organisationen beurteilen diese Risiken nicht selbst, was zu einer mangelnden Awareness auf Führungsebene führen könnte.

Steuerung von Cyber Risiken

In einem guten Risk Management richtet sich die Risikosteuerung nach dem Risikoappetit. Erfolgreiche Unternehmen gehen bewusst gewisse Risiken ein, um die Unternehmensziele zu erreichen. Dabei wird das Gesamtrisiko gesteuert und nicht jedes Risiko einzeln. Risiken können gemäss COSO vermieden, vermindert, geteilt oder akzeptiert werden.

IT-Themen im Risk Management

Ein holistisches Risk Management erfordert, dass auch Cyber Risiken im Unternehmens-Risk Management berücksichtigt werden. In einem Bottom-up-Ansatz werden Cyber Risiken separat auf taktischer Ebene verwaltet und erst in einem zweiten Schritt in aggregierter Form in das Unternehmens-Risk Management aufgenommen. Dies birgt die Gefahr, dass die Risikobewertung tendenziell aus technischer Sicht erfolgt und nicht in einem strategischen Kontext, welcher die Unternehmensziele berücksichtigt. Aus diesem Grund ist ein Top-down-Ansatz zu bevorzugen, in welcher Cyber Risiken aus dem Unternehmens-Risk Management gesteuert und bewertet werden.

Berücksichtigung von IT-Themen im Risk Management

- 15 Organisationen berücksichtigen Cyber Risiken im Unternehmens-Risk Management.
- 7 Organisationen berücksichtigen Cloud Risiken im Unternehmens-Risk Management.

Ein Grossteil der befragten Organisationen berücksichtigen IT-Themen im organisationsweiten Risk Management. Meist werden diese in aggregierter Form im Risk Management berücksichtigt. Bei einer Organisation ist das Cyber Risk Management im Aufbau. Eine weitere Organisation lässt Cyber Risiken durch den CIO und CISO tracken und berücksichtigt diese gar nicht im organisationsweiten Risk Management. Eine Organisation gibt an, dass Cyber Risiken im Unternehmens-Risk Management so stark aggregiert werden (d. h. mit anderen Risiken zusammengefasst), dass sich diese dort nur bedingt berücksichtigen lassen.

Die Cloud Nutzung wird bei rund einem Drittel der befragten Organisationen im Unternehmens-Risk Management berücksichtigt. Eine Hälfte tut dies explizit, die andere Hälfte integriert Cloud-Risiken in anderen Risikokategorien. Der Stellenwert von Cyber Risiken wird von den Organisationen sehr unterschiedlich bewertet.

Der Risikoverminderung durch präventive Massnahmen kommt bei Cyber Risiken eine hohe Bedeutung zu, sei es mithilfe von technischen Massnahmen wie Anti-Virus-Software, Firewalls, Updates, Intrusion Detection Systems oder mithilfe von Schulungen, Trainings und Information der Mitarbeitenden (Awareness), um eine Risikokultur zu etablieren.

«Das schwächste Glied bei Cyber Risiken sind die einzelnen Mitarbeitenden. Hier werden wir – nebst den technischen Aspekten – mit wiederkehrenden Sensibilisierungsaktivitäten vermehrt ansetzen.»

(Maria Nutz, Bereichsleiterin Sachversicherungen / Risk Management, fenaco Genossenschaft)

Cyber-Versicherungen

Cyber Risiken können damit nicht gänzlich verhindert werden. Gerade im Zuge der Pandemie mit dem vermehrten Home-Office oder der steigenden Anzahl Cyber-Attacken in den letzten Monaten rückt die Möglichkeit eines Risikotransfers an einen Versicherer in den Fokus. Aufgrund dieser Entwicklung könnten sich Cyber Risken in den nächsten Jahren zu einer Risikokategorie vergleichbar anderer bekannter Risiken entwickeln, gegen welche sich zunehmend mehr Organisationen versichern. In den Interviews hat deshalb die Frage interessiert, ob bereits Versicherungen abgeschlossen wurden, ob dies geplant ist und welche Herausforderungen sich beim Vertragsabschluss stellen.

Abschlüsse von Cyber-Versicherungen

- 8 Organisationen haben eine Cyber-Versicherung abgeschlossen.
- 2 Organisationen sind aktuell diesbezüglich in Verhandlungen.
- 5 Organisationen haben aus unterschiedlichen Gründen keine Versicherung.
- Deckungsausschlüsse, -limiten und Kosten-Nutzen-Überlegungen werden generell kritisch betrachtet.

Acht der befragten Organisationen haben eine Versicherung gegen Cyber-Kriminalität abgeschlossen, zwei sind in Verhandlungen dazu. Fünf der interviewten Organisationen haben aktuell keine Cyber-Versicherung abgeschlossen bzw. eine Organisation hat diese mittlerweile gekündigt. Gründe sind Kosten-Nutzen-Überlegungen und die mangelhafte Abdeckung bzw. die vielen Deckungsausschlüsse und -limiten. Drei Organisationen sehen das Kosten-Nutzen-Verhältnis kritisch oder investieren lieber in Cyber Security-Massnahmen. Eine Organisation gab an, intern über bessere Expertise zu verfügen. Drei Organisationen melden, dass es zusehends schwieriger wird, eine Deckung zu erhalten. Eine Organisation fand keinen Versicherer, der bereit war, den geforderten Risikotransfer zu übernehmen. Während der Gespräche mit den Risk Management-Verantwortlichen ist insbesondere bei grösseren Organisationen deshalb eine gewisse implizite, unterschwellige, aber auch explizite Skepsis gegenüber Cyber-Versicherungen spürbar geworden.

«Man muss die Balance finden: Ist es klüger, das Geld in die Versicherungslösung zu investieren, oder ist es besser, in Cyber Security zu investieren?»

(Peter Jussel, Corporate Risk and Insurance Management, Hilti Corporation)

Mit einer Ausnahme haben sich alle an der Studie teilnehmenden Organisationen mit dem Abschluss einer Cyber-Versicherung auseinandergesetzt. Viele werden sich auch zukünftig kurz- und mittelfristig mit einem möglichen Abschluss befassen und beobachten die Entwicklungen auf dem Versicherungsmarkt mit Interesse.

Umgang mit Cyber-Versicherungen in der Zukunft

- 5 Organisationen planen in den nächsten drei Jahren einen Versicherungsabschluss.
- 4 Organisationen geben explizit an, den Versicherungsschutz auszubauen zu wollen oder zumindest zu überprüfen.

Insgesamt geben neun Organisationen an, in den nächsten drei Jahren entweder eine Cyber-Versicherung abzuschliessen, eine bestehende Versicherung auszubauen oder zumindest zu überprüfen. Zwei grosse Konzerne ohne Cyber-Versicherung stehen mit Versicherern in konstantem Austausch über alle Themen hinweg, also auch über Cyber Risiken.

Zwei Interviewpartner/-innen sprechen explizit die Schwierigkeit an, zu beurteilen, welche Versicherungsleistungen für sie wirklich nützlich sind bzw. verweisen auf die Schwierigkeit, eine Balance zu finden zwischen Schadenminderung durch eine Versicherung und Investition in Cyber Security mit dem gleichen Ziel. Ein Risk-Management Verantwortlicher meldet, dass es Diskussionen darüber gibt, was überhaupt versicherbar ist und versichert werden sollte. Die meisten Versicherungsleistungen fokussieren auf Schaden aus Betriebsunterbruch. Schäden, die z. B. durch einen Reputationsverlust verursacht sind, können nicht vollumfänglich versichert werden. Bei derjenigen Organisation, welche keine Versicherungsdeckung bekommen hat, liegt der Grund darin, dass aus Sicht des Versicherers die erforderlichen Vorleistungen («Hausaufgaben») im Unternehmen fehlten.

Unterstützungsleistungen durch Versicherer

Es stellt sich demnach die Frage, welchen Bedarf an Unterstützungsleistungen die Organisationen beim Thema Cyber Risk Management sehen und weiter, ob und welche dieser Unterstützungsdienstleistungen durch einen Versicherer erbracht werden könnten.

Nachfrage nach Unterstützungsleistungen vom Versicherer

- 10 Organisationen sehen einen Bedarf an derartigen Unterstützungsdienstleistungen.
- 6 Organisationen können sich vorstellen, Unterstützungsdienstleistungen vom Versicherer zu beziehen.
- 2 Organisationen wünschen sich, dass die Versicherungsgesellschaft ihre Expertise im Themenfeld Cyber Risiko einbringt.
- 1 Organisation erwähnt speziell Unterstützungsleistungen im Schadenfall.

Zehn von 16 Organisationen sehen einen Bedarf an Unterstützungsdienstleistungen. Bezüglich des Potenzials für zusätzliche Dienstleistungen durch den Versicherer zeigt sich ein uneinheitliches Bild. Abgesehen von vier grossen Konzernen, welche inhouse (und teilweise ergänzt mit ausgewählten Spezialisten/-innen) genügend Ressourcen haben, brauchen alle Unterstützung. Sechs können es sich vorstellen, zusätzliche Dienstleistungen über einen Versicherer zu beziehen. Dies sind tendenziell eher kleinere Organisationen. Es geht dabei um das Einbringen von Expertise und/oder um die Unterstützung im Schadenfall. Die anderen setzen eher auf andere externe Partner. Bei einigen schwingt die Befürchtung mit, die Expertise könnte bei den Versicherern zu wenig vorhanden sein.

Risikoberichterstattung

Eine gut funktionierende Risikoberichterstattung gehört zu jedem ERM. Sie stellt den Informationsfluss sicher und fördert die Risikokultur.

Cyber Risiken sind ein Teil unseres ERM. Sie werden speziell im Informationssicherheits-Risikomanagement erfasst, konsolidiert und der Risikocontrolling-Stelle gemeldet. Letztere sammelt und aggregiert alle Risiken. So fliessen auch Cyber Risiken in den Risikobericht ein.»

(Maria Nutz, Bereichsleiterin Sachversicherungen / Risk Management, fenaco Genossenschaft)

Es gilt sicherzustellen, dass die Informationen über potenzielle Risiken fliessen und die verantwortlichen Stellen erreichen und nicht irgendwo versanden oder im Extremfall ignoriert oder verschwiegen werden. Die Informationen sollten dabei von «unten nach oben» wie auch «von oben nach unten», auf formell definierten wie auch auf informellen Wegen erfolgen. Vom regelmässigen Reporting bezüglich Cyber Risiken ist das Incident Reporting in einem Schadenfall zu unterscheiden.

Aus den Interviews geht hervor, dass in den meisten Organisationen der informellen Kommunikation zwischen den vielen involvierten Stellen eine bedeutende Rolle zukommt. Die Analyse der Rollen und Funktionen hat jedoch auch ergeben, dass aufgrund der gewählten Organisation nicht immer alle Stellen einbezogen werden. Aus dem gleichen Grund sind die formellen Berichtswege unterschiedlich ausgestaltet.

Berichterstattung über Cyber Risiken

- Alle Organisationen verfügen über eine Berichterstattung über Cyber Risiken oder führen diese aktuell ein.
- Die Berichtswege unterscheiden sich aufgrund der unterschiedlichen RM-Organisation.
- 3 Organisationen unterscheiden zwischen einer regelmässigen Berichterstattung und einer Berichterstattung bei Vorfall.

Gemeinsam ist allen, dass die Geschäftsleitung und das Aufsichtsorgan (VR, Stiftungsrat) immer Empfängerin der periodischen Risikoberichterstattung ist. Die Berichtswege unterscheiden sich jedoch im Detail je nach Grösse der Organisation und vorhandenen Funktionen. Auffällig ist zunächst, dass die Berichterstattung nur bei fünf Unternehmen unmittelbar via CISO (4) oder via CIO (1) über den Risikomanager läuft. In Organisationen ohne explizite CISO-Funktion rapportiert die IT-Abteilung bzw. der CIO direkt an die Geschäftsleitung (4). In drei Organisationen berichtet der CISO an den CIO (und nicht an den CRO) und dieser wiederum an die GL. In zwei Organisationen hat der CIO und der CRO eine dotted-line Verbindung direkt zum Verwaltungsrat. In einer Organisation berichtet der IT-Leiter an den Leiter Controlling, der für das RM zuständig ist. Bei einer Organisation berichtet der CISO regelmässig vor dem Risk Steering Committee zur aktuellen Risikolage, dieses Gremium setzt sich aus Verwaltungsräten/-innen, GL-Mitgliedern und dem CRO zusammen. Letzteres entspricht einer Best Practice. Diese direkte Linie von CIO, CISO und CRO zum Verwaltungs- oder Stiftungsrat ist nur bei zwei Organisationen vorgesehen, obwohl sie in der Literatur empfohlen wird. Gespiegelt an den Empfehlungen der Literatur werden die Risk Management Verantwortlichen in einigen befragten Organisationen zu wenig in die Berichterstattung einbezogen. Das deutet darauf hin, dass Cyber Risiken schlecht im ERM integriert sind und damit das Gesamtrisiko nicht optimal gesteuert wird.

Nur vier Unternehmen unterscheiden explizit die Berichterstattung im Vorfall. Sechs Unternehmen geben an, dass es keinen offiziellen Berichtsweg im Vorfall gäbe, bei einem Unternehmen ist alles noch im Aufbau. In der Regel sind der CISO, der CEO und Personen aus dem Compliance Management, dem Legal und der IT involviert. Bei einer Organisation besteht eine enge Zusammenarbeit mit dem Versicherer im Schadenfall. Bei zwei Unternehmen wird das Krisenmanagement einbezogen, das je nach Schweregrad den Vorfall übernimmt oder an die IT zurückgibt. Risikomanager/-innen sind kaum in die Entscheidungs- und Berichterstattung bei Vorfällen involviert. Sie werden jedoch über die Schadenfälle informiert. Lediglich vier Unternehmen haben explizit ihre Berichterstattungs- und Entscheidungswege bei Schadenfällen definiert. Insbesondere zeigt sich, dass Unternehmen, bei denen kein Vorfall zum Tragen gekommen ist, auch eher weniger gut aufgestellt sind, was das Incident Reporting angeht. Das deckt sich mit der Literatur. Insgesamt lässt sich hier sicherlich ein erhebliches Verbesserungspotenzial ausmachen. Obwohl Cyber Risiken als sehr relevant eingestuft werden, sind nicht alle Organisationen organisatorisch optimal auf ein Ereignis vorbereitet.

Business Continuity Management

Beim Business Continuity Management (BCM) handelt es sich um einen Geschäftsprozess, dessen Ziel in erster Linie darin besteht, sicherzustellen, dass im Falle einer Betriebsstörung die Produktion und/oder Erbringung von Dienstleistungen auf einem angemessenen Niveau aufrechterhalten und in einem definierten Zeitraum wiederhergestellt werden kann. Das Notfallkonzept (Disaster Recovery) konzentriert sich auf IT-Systeme, welche kritische Geschäftsfunktionen unterstützen und kann als Teil des Business Continuity Management betrachtet werden.

Organisationen müssen zwingend ein Business Continuity Management etablieren und dabei sicherstellen, dass auch ausgelagerte Systeme und Services berücksichtigt werden. Gerade Cloud-Dienste haben in vielen Organisationen hinsichtlich Geschäftsfortführung eine hohe Kritikalität. Die Wirksamkeit der BCM-Massnahmen – Notfallkonzept, Krisenstab, Datensicherungskonzept, Wiederanlaufpläne (Disaster Recovery) aber auch die Fähigkeit auf (Cyber-)Vorfälle zu reagieren (Incidence Response) – müssen im Rahmen von regelmässigen Übungen auf Wirksamkeit hin überprüft werden, um zu garantieren, dass die Massnahmen im Ernstfall funktionieren. Es müssen also Notfall- und Krisenstabsübungen, Wiederherstellungstests etc. durchgeführt werden.

Integration von Cloud-Diensten in Notfallkonzept

Im Rahmen der Interviews wurde abgeklärt, inwieweit ein Notfall- und ein Datensicherungskonzept vorhanden sind und ob diese auch Cloud-Dienste berücksichtigen. Weiter wurde nachgefragt, ob die Wirksamkeit der implementierten Konzepte im Rahmen von Notfall- und Wiederherstellungsübungen überprüft wird. Schliesslich wurde ermittelt, ob Bedarf nach externen Dienstleistungen in diesem Kontext besteht und wie diese gegebenenfalls ausgestaltet sein sollten.

Integration von Cloud-Diensten in Notfallkonzept

- 12 Organisationen verfügen über ein Notfallkonzept.
- 10 Organisationen berücksichtigen in ihrem Notfallkonzept auch Cloud-Dienste.
- 13 Organisationen führen regelmässig Notfall- oder Krisenstabsübungen durch.
- 15 Organisationen verfügen auch über ein Datensicherungskonzept und berücksichtigen darin ihre Cloud-Dienste.

Sämtliche der befragten Organisationen verfügen über ein Notfallkonzept oder sind dabei, eines einzuführen. Mehrheitlich sind Cloud-Dienste im Notfallkonzept berücksichtigt.

Für Datensicherungskonzepte zeigt sich ein vergleichbares Bild: Sie sind vorhanden und in der Cloud gehaltene Daten werden berücksichtigt. Generell können hier zwei Ansätze beobachtet werden: Entweder werden sämtliche in der Cloud gehaltenen Daten gesichert oder die Datensicherung wird pro Anwendung implementiert, unabhängig davon, ob es sich hierbei um eine On-Premises oder um eine Cloud-Anwendung handelt. Eine Organisation gibt an, Cloud-Dienste «umgekehrt» zu nutzen, nämlich als Backup-Lösung für klassische Anwendungen.

15 der interviewten Organisationen geben an, regelmässig Notfallübungen wie z. B. Wiederherstellungstests durchzuführen oder eine regelmässige Durchführung solcher Übungen zu planen. Bei drei Organisationen werden Cloud-Dienste explizit nicht berücksichtigt, da sie als nicht kritisch eingestuft werden. Zwei Organisationen führen nur unregelmässig Notfallübungen bzw. Wiederherstellungstests durch. In einem Fall wird dies damit begründet, dass ein vollständiger Wiederherstellungstest zu riskant sei. Eine andere Organisation gibt an, dass sie sich in diesem Bereich auf die Massnahmen des Cloud-Dienstleisters verlässt.

«Unsere Devise ist, wenn ein Angriff stattgefunden hat, müssen wir einen Notfallbetrieb ohne externe Hilfe bereitstellen und diesen eine gewisse Zeit aufrechterhalten können. Es ist explizit so definiert, dass dies ohne externe Hilfe möglich sein muss.»

(CISO, anonym)

Notfall- wie Datensicherungskonzepte sind bei den befragten Organisationen oft anzutreffen. Sie berücksichtigen auch Cloud-Risiken, sofern diese als businesskritisch angesehen werden. Je nach Organisation werden sämtliche Daten oder nur die businesskritischen berücksichtigt. Nicht alle Organisationen, die angeben über Notfallkonzepte zu verfügen, führen regelmässig Notfallübungen oder Wiederherstellungstests durch. Sie riskieren, dass im Krisenfall die vorgesehenen Massnahmen nicht funktionieren. Dementsprechend relativiert dies Nutzen der Massnahmen.

Beizug externer Unterstützung

Da Notfallmassnahmen zur Geschäftsfortführung mehrheitlich nicht zum Tagesgeschäft gehören, kann der Beizug von externen Dienstleistern für deren Einführung angezeigt sein.

Externe Unterstützung bei Cyber-Vorfällen

- 9 Organisationen greifen im Falle eines Cyberangriffs auf externe Unterstützung zurück.
- 7 Organisationen greifen nur im Falle eines *schwerwiegenden* Cyberangriffs auf externe Unterstützung zurück.
- 2 Organisationen greifen im Falle eines Cyberangriffs grundsätzlich nicht auf externe Unterstützung zurück.

Die Hälfte der befragten Organisationen würde in jedem Fall nach einem Cyberangriff auf externe Unterstützung zurückgreifen. Zwei Organisationen sehen grundsätzlich von externer Untersetzung ab. Dies wird in einem Fall damit begründet, dass möglichen externen Partnern die entsprechenden Kenntnisse über die organisationseigene Infrastruktur fehlen. In einer anderen Organisation wird die Reaktionszeit von externen als zu langsam eingeschätzt; begründet wird dies mit Erfahrungsberichten aus derselben Branche. Die übrigen Organisationen nehmen externe Hilfe punktuell bei schwerwiegenden Angriffen in Anspruch.

Das von den Sicherheitsverantwortlichen meistgenannte Angriffsszenario ist Ransomware. Dies deckt sich mit den Aussagen der Risk Management-Verantwortlichen.

«Bei schwerwiegenden Infektionen würden wir effektiv Spezialisten beiziehen.»

(Claudio Sandmeier, IT-Sicherheitsbeauftragter, ewl energie wasser luzern)

Mögliche Unterstützung von externen Partnern würde in erster Linie für forensische Arbeiten in Anspruch genommen. Weiter wurde Unterstützung aber auch im Kontext der Schadensermittlung erwähnt oder bei der Kompensation von Know-how-Defiziten bei den eingesetzten Technologien. Weiterer Bedarf besteht bei der First Response, bei der Zuordnung von Angriffen und bei der Unternehmenskommunikation.

Die Bereitschaft, externe Unterstützung bei Sicherheitsvorfällen in Anspruch zu nehmen, ist ziemlich hoch. Organisationen, die grundsächlich nicht für alle Vorfällen Hilfe beanspruchen wollen, beschränken sich auf diejenigen Fälle, die grössere Betriebsstörungen zur Folge haben.

Die gewünschten Unterstützungsleistungen sind sehr unterschiedlich. Sie erfordern in der Regel Kenntnisse der organisationseigenen IT-Architektur und -Systeme und auch der Prozesse (First Response, Unternehmenskommunikation, Schadensermittlung). Zudem müssen allfällige Dienstleister über sehr spezifische Fachkenntnisse (Forensik, Zuordnung von Angriffen zu einem Täterkreis etc.) verfügen.

Teil III: Empfehlungen

Eine interviewbasierte Analyse von 18 grösseren Schweizer Organisationen und die Auswertung von 33 Interviews mit Risk Management-Verantwortlichen und CISOs haben wertvolle Erkenntnisse zum Vorschein gebracht. Einige der wichtigsten Ergebnisse werden nachfolgend als Empfehlungen an Aufsichtsorgane, Geschäftsleitungsmitglieder, Risk Management-Verantwortliche und CISOs für künftige Optimierungen ihres Cyber Risk Managements vorgeschlagen. Damit wird ein sehr wichtiger Kreis geschlossen – letztendlich sind es nämlich die Risk Management-Verantwortlichen selbst, die massgeblich an der künftigen Weiterentwicklung von Cyber Risk Management in ihren Organisationen beteiligt sind.

Basierend auf den Interviewergebnissen und in Abstimmung mit der aktuellen Literatur werden nachfolgend konkrete Empfehlungen im Umgang mit Cyber Risiken an die Praxis formuliert.

Integration von Cyber Risiken ins ERM fördern

Ein angemessenes Verständnis über die Zusammenhänge und Abhängigkeiten zwischen Organisationszielen, Organisationsbereichen, kritischen Geschäftsprozessen, kritischen Assets und der Informationstechnologie ist eine zentrale Voraussetzung für ein effektives Cyber Risk Management.

Das bedeutet, dass Organisationen Cyber Risiken nicht nur aus einer technischen Perspektive beurteilen, sondern auch deren Auswirkungen auf die Organisationsziele (z. B. Finanzen, Reputation, Strategie) berücksichtigen sollten. Um dieses Ziel zu erreichen, muss das Cyber Risk Management mit den Prozessen des ERM abgestimmt werden.

Um Cyber Risiken ein entsprechendes Gewicht auf oberster Organisationsebene einzuräumen, müssen Entscheidungen bez. Cyber Risikoappetit getroffen werden (z. B. «geschäftskritische Systeme müssen von allen bekannten Vulnerabilitäten geschützt werden»). Solche Risikoappetit-Aussagen helfen in einem nächsten Schritt,

– Risikotoleranzen zu definieren (z. B. «geschäftskritische Systeme müssen bei Vorliegen von kritischen Softwarevulnerabilitäten [CVSS von 10] innerhalb von zehn Tagen gepatcht werden»),

– Kontrollen zu entwickeln (z. B. periodische Vulnerabilitäten-Assessments), und

– Kennzahlen zu formulieren (z. B. «Anzahl gepatchter Vulnerabilitäten» oder «Anzahl von Systemen mit einer CVSS 10, die nicht innerhalb von zehn Tagen gepatcht wurden»).

Fehlende Risk Governance – fehlendes Fundament

Cyber Risiken müssen in der Corporate Governance jeder Organisation formell verankert werden. Dazu eignet sich die Risikopolitik – eine zentrale Leitlinie, die das Bekenntnis des Aufsichtsorgans hinsichtlich Risk Management klar zum Ausdruck bringt. Die Studie hat gezeigt, dass Cyber Risiken noch zu wenig explizit in der Risikopolitik verankert ist. Dies führt zwangsläufig auch zu fehlenden Aussagen zur Risikobereitschaft (Risikoappetit) im Bereich der Cyber Risiken.

Ebenso zeigt die Studie klar auf, dass eine grosse Heterogenität bez. Rollen, Verantwortlichkeiten und Kollaboration im Umgang mit Cyber Risiken besteht. Die Empfehlung hierzu lautet, dass die Risk Management-Verantwortlichen eng mit den CISOs zusammenarbeiten und damit den Grundstein für eine Integration der Cyber Risiken in die Sprache des ERM gelegt werden kann. In kleineren Organisationen ist es grundsätzlich problematisch, dass die Verantwortung über Cyber Risiken «extern vergeben» wird, d. h. auf externe Audits und den externen Dienstleiser verwiesen wird. Cyber Risiken müssen methodisch so beurteilt und beschrieben werden, dass sie anschlussfähig an das ERM sind. Deshalb ist es von zentraler Bedeutung, dass der Cyber Risk Management-Prozess eng mit dem ERM verzahnt ist. Die Bedeutung des CISOs in der Schnittstelle Cyber Risiken und ERM ist absolut zentral und muss in der Praxis stärker verankert werden.

Weiter zeigt die Studie, dass eine gewisse Lücke zwischen technischer Expertise im Umgang mit Cyber Risiken auf Systemebene (IT-Infrastruktur-Ebene) und der prozessu-

alen bzw. organisatorischen Expertise (Organisationsebene, Führungsebene) feststellbar ist. Anders formuliert werden Cyber Risiken noch zu stark als «IT-Thema» verstanden, entsprechend dezentral und operativ gesteuert und zu wenig in das unternehmensweite Risk Management und die Entscheidungsprozesse der Leitungsgremien integriert. Hier ist eine Diskrepanz der Relevanz des Risikos und der organisatorischen Readiness feststellbar. Das Bewusstsein, dass Cyber Risiken eine wechselseitige Abhängigkeit zwischen der IT und den Organisationszielen («Business») aufweisen, ist oft noch zu wenig ausgeprägt. Die Empfehlung muss demnach lauten, dass Cyber Risiken ganzheitlich und strategisch betrachtet werden bzw. die Konsequenzen auf die Erreichung der Organisationsziele explizit beurteilt und kommuniziert werden. Das Bewusstsein der schützenswerten Assets (Kronjuwelen) in den Leitungsgremien ist eine wichtige Grundvoraussetzung dafür.

Mehrwertbringende Dienstleistungen des Versicherers

Die Ergebnisse haben gezeigt, dass der Versicherer bei der Mehrheit der Organisationen (noch) keine bedeutende Rolle spielt. Im Risikodialog zwischen Kundschaft/Risk Manager und IT-(Security-)Dienstleister oder CISO kann ein Versicherer als Sparring-Partner auftreten und beim Cyber Risk Managements wie folgt unterstützen:

- Aufzeigen und Beurteilen der aktuellen Bedrohungslage, auch aufgrund der gemachten Schadenerfahrungen durch den Versicherer. Der Versicherer kann empfehlen, mit welchen geeigneten personenbezogenen, technischen, organisatorischen und physischen Massnahmen Prävention im Rahmen des Grundschutzes betrieben werden und welcher Teil des Risikos mit welchen Deckungen und Leistungen an ihn transferiert werden kann.
- Bez. Voraussetzungen der Versicherbarkeit der Cyber Risiken kann der Kundschaft aufgezeigt werden, welche minimalen technischen Anforderungen erfüllt sein müssen. So bedeutet dies z. B. das Vorhandensein einer Firewall, eines Antivirusprogramms, regelmässiges Patchmanagement und Erstellen von Log-Dateien für sämtliche kritischen Systeme. Auch kann ein Versicherer bei der Umsetzung von präventiven organisatorischen Massnahmen helfen, wie z. B. bei Mindestanforderungen für Passwort-Regeln, der Sensibilisierung von Mitarbeitenden oder im Bereich des BCM.
- Unterstützung im Aufbau und Unterhalt eines Incident Response Management und ggf. Vermittlung an spezialisierte Partner (z. B. Forensik). Auch können Assistance Dienstleistungen im Bereich BCM, Krisen- und Reputationsmanagement angeboten werden.

Vor allem die kleineren von den befragten Organisationen haben einen Bedarf an weitergehenden Unterstützungsdienstleistungen. Dabei geht es einerseits um Unterstützung vor Vertragsabschluss, um die nötigen Voraussetzungen für den Vertragsabschluss zu schaffen. Andererseits sind auch Leistungen im Schadenfall interessant, die helfen, den Schaden zu begrenzen. Damit könnte auch der Fokus von der reinen Betrachtung des Betriebsausfalls hin zur Steuerung des Reputationsrisikos gelenkt werden. Kritisch bleibt das Vertrauen der Kundenseite in die Expertise des Versicherers sowie ein attraktives Kosten-Nutzen-Verhältnis.

Faktor Mensch – ein lohnendes Investment

Oft werden die einfachsten und gleichermassen wirkungsvollsten Massnahmen im Umgang mit Cyber Risiken (immer noch) vernachlässigt. Die vorliegende Studie bestätigt die Erkenntnisse aus der Literatur, dass der «Faktor Mensch» bzw. menschliche Verhaltensweisen im Bereich der Cybersicherheit tendenziell noch zu wenig adressiert wird. Es ist bekannt, dass viele Cyber Risiken menschenverursacht sind. Gegebenenfalls ist die Definition von «Cyber Risiken» hier deshalb auch etwas irreführend, da viele Risikoursachen nicht im Cyber-Raum zu finden sind, sondern in menschlichen Verhaltensweisen.

Die Terminologie der Cyber Security und des Cyber Risk Managements bedient sich aus Analogiegründen der Biologie: Da ist die Rede von Viren, Würmern und Käfern (Bugs). Es gibt aber auch starke Bezüge zur Medizin. Dort weiss man schon lange, dass richtiges menschliches Verhalten viele Ansteckungen und Übertragungen von Krankheiten verhindert. Regelmässige Desinfektion, diszipliniertes Händewaschen, Abstand einhalten, hygienischer Umgang mit Medizinalprodukten, u. v. m. ist in der

Medizin schon lange habituiertes Verhalten, in der Disziplin «Cybersicherheit» scheint dies erst in den letzten Jahren aufzukommen. Diesen Trend gilt es sowohl medial als auch innerhalb der Organisationen zu unterstützen.

«Man spürt definitiv, dass die Awareness der User stetig steigt ... da wird heute bedeutend mehr nachgedacht, mitgedacht und auch hinterfragt als es vor ein paar Jahren noch der Fall war.»

(Jan Gehrig, Lead Global Information Security, Komax Group)

In das menschliche Verhalten zu investieren, kann sich nur lohnen und wird daher als Empfehlung formuliert. Cybersicherheit ist keine einmalige, technische Intervention. Sie entsteht durch eine permanente und laufend überprüfte Anwendung von technischen und organisatorischen Massnahmen. Der Faktor Mensch macht in diesem kontinuierlichen Verbesserungsprozess (KVP) zwar nur ein Element aus, jedoch ein sehr wichtiges. Menschliches Verhalten im Umgang mit der Cybersicherheit sollte so trainiert werden, dass es gleich selbstverständlich und «normal» wird, wie sich beim Niesen die Hand vor den Mund zu halten.

Cloud-Kosten früh und langfristig planen

Skalierbarkeit ist eines der wichtigsten Argumente für den Einsatz von Cloud-Diensten. Ressourcen können flexibel und rasch entsprechend der Bedarfsentwicklung bezogen werden. Diese Flexibilität ist vor allem für Anwendungen vorteilhaft, deren Ressourcenbedarf sich dynamisch entwickelt und deshalb nur schwer abschätzbar ist. Ist der Ressourcenbedarf über längere Zeit stabil oder die Bedarfsentwicklung vorhersehbar, so kann eine selbst betriebene IT-Infrastruktur (On-Premises) durchaus konkurrenzfähig sein.

Überlegungen dieser Art sollten schon vor einem Outsourcing in die Cloud angestellt werden, damit sich nicht im Nachhinein aus Kostengründen die Frage nach einem "Re-Insourcing" stellt.

Cloud Agnostizismus ermöglicht Flexibilität

Wer Dienstleistungen auslagert, begibt sich in ein Abhängigkeitsverhältnis. Dies ist auch beim Bezug von Cloud-Dienstleistungen der Fall. Durch die Gestaltung einer cloud-agnostischen IT-Infrastruktur, lässt sich der Grad der Abhängigkeit gezielt reduzieren und steuern.

Hierzu setzt man bei der Beschaffung und Entwicklung von Informationssystemen auf Technologien, welche ohne grossen Aufwand bei mehreren Cloud-Diensteanbietern (oder auf On-Premises-Systemen) eingesetzt werden können. Dies ist insbesondere im PaaS und IaaS Umfeld gängige Praxis und wird häufig durch den Einsatz von offenen Schnittstellen und Container-Technologien umgesetzt.

Bei SaaS Lösungen ist ein Cloud-Agnostizismus schwieriger umzusetzen, da bei diesen sehr oft proprietäre Formate und Schnittstellen zur Anwendung kommen. Die Kosten eines Anbieterwechsels hängen damit stark von der Beschaffenheit der aktuellen und der zukünftig zu verwendenden Cloud-Lösung ab.

Das Verfolgen eines cloud-agnostischen Ansatzes bedeutet somit, dass auf Produkte und Funktionen verzichtet wird, die nur von einem einzigen Cloud-Diensteanbieter angeboten werden. Ist dies nicht möglich, lässt sich eine gewisse Unabhängigkeit und Flexibilität wahren, indem darauf geachtet wird, dass unternehmenseigene Daten regelmässig aus der SaaS Lösung exportiert und mit alternativen Lösungen weiterverarbeitet werden können.

Kontrolle behalten – klassifizieren und verschlüsseln

Wer Cloud-Dienste nutzt, vertraut dem Cloud-Diensteanbieter Daten zur Verarbeitung und Speicherung an. Je nach Gesetzeslage und vertraglichen Regelungen übernimmt der Cloud-Diensteanbieter einen Teil der Verantwortung für die Gewährleistung der Vertraulichkeit und Integrität dieser Daten.

Sollten diese Schutzziele verletzt werden, hat jedoch primär der Leistungsbezüger das Nachsehen. Dies zum ei-

nen, weil er entweder als Besitzer der Daten oder als Verantwortlicher gegenüber Dritten (z. B. bei Personendaten) direkt geschädigt ist. Darüber hinaus, weil er, um eine (Mit)Haftung des Cloud-Diensteanbieter zu erwirken, erst dessen Verschulden nachweisen muss. Es dürfte sich für den Leistungsbezüger als schwierig erweisen, einen solchen Nachweis zu erbringen, da sich die entsprechenden Systeme unter der Kontrolle des Cloud-Diensteanbieters befinden.

Um derartigen Risiken zu begegnen, müssen die zu bearbeitenden Daten und die zur Verfügung stehenden Bearbeitungsmöglichkeiten (z. B. in der Cloud) klassifiziert werden. Hierfür muss eine Datenklassifizierung etabliert werden, die jeder Klassifizierungsstufe den Schutzbedarf der zu bearbeitenden Daten und die zulässigen Bearbeitungsmöglichkeiten zuordnet. Es empfiehlt sich, neben den Aspekten der Vertraulichkeit auch datenschutzrechtliche Aspekte zu berücksichtigen. Eine Datenklassifizierung ist somit ein Instrument zur Steuerung des Risikos einer Datenoffenlegung oder eines Integritätsverlusts, indem sie definiert, mit welchen Cloud-Anwendungen oder organisationseigenen Systemen welche Daten bearbeitet werden dürfen.

Möchte man das Risiko eines Vertraulichkeits- oder Integritätsverlust von Seiten des Cloud-Diensteanbieters massgeblich reduzieren, ohne generell auf die Nutzung des Cloud-Services zu verzichten, kann der Einsatz von Verschlüsselungstechnologie in Erwägung gezogen werden. Hierbei werden Daten verschlüsselt in der Cloud-Umgebung aufbewahrt und nur bei deren Nutzung zeitweise entschlüsselt. Dabei ist zu beachten, dass für einen effektiven Schutz die Schlüssel nicht auf den Systemen des Cloud-Diensteanbieters abgelegt sein dürfen. Eine Entschlüsselung und damit Bearbeitung der Daten erfolgt demnach ausschliesslich auf der organisationseigenen Infrastruktur. Auf Seiten des Cloud-Diensteanbieters findet ausschliesslich die Datenhaltung statt.

Soll auch die Datenbearbeitung auf der Infrastruktur des Cloud-Diensteanbieters erfolgen (z. B. bei SaaS), lässt sich eine temporäre Entschlüsselung der Daten und der damit verbundene Verlust der Vertraulichkeit gegenüber dem Cloud-Diensteanbieter nicht verhindern. Auf dem Markt werden unterschiedliche Lösungen beworben, welche das Zeitfenster der Entschlüsselung sowie die Zugriffsmöglichkeiten erheblich reduzieren.

Die konzeptionellen Grundlagen für die so genannte homomorphe Verschlüsselung, welche eine Bearbeitung von verschlüsselten Daten (ohne Kenntnis des Schlüssels) erlaubt, sind vorhanden. Praktikable Lösungen sind zurzeit in Entwicklung.

Vorbereitet für Notfälle durch Planung und Übung

Um einen zuverlässigen Betrieb der organisationseigenen IT zu gewährleisten, muss ein Notfallkonzept etabliert und dessen Effektivität durch regelmässige Notfallübungen überprüft werden. Dabei sind auch die ausgelagerten Systeme wie z. B. Cloud-Dienste zu berücksichtigen.

Die Notfallübungen sollten unterschiedliche Notfallszenarien berücksichtigen (z. B. Ransomware-Befall oder Ausfall eines Cloud-Diensteanbieters). Diese Übungen zeigen, ob und in welchem Ausmass Unterstützung seitens Cloud-Diensteanbieters oder von anderen Drittparteien notwendig ist. Insbesondere wenn sich herausstellt, dass das zu Grunde liegende Szenario die Kompetenzen der Organisation übersteigt und sie somit auf externe Unterstützung angewiesen ist, müssen die zu ergreifenden Massnahmen mit externen Leistungserbringern sorgfältig geplant und koordiniert werden.

Im Zuge einer entsprechenden Vorausplanung kann ein Versicherer als Sparringspartner für die Ausarbeitung realistischer Schaden- respektive Notfallszenarien und als Vermittler zu spezialisierten Dienstleistern auftreten.

Fazit und Ausblick

Anhand von 33 Interviews mit CISOs und Risk Management-Verantwortlichen wurde im Rahmen der vorliegenden Studie der Umgang mit Cyber Risiken in 18 grösseren Schweizer Unternehmen untersucht. Die Ergebnisse zeigen klar auf, dass die Relevanz von Cyber Risiken in allen Organisationen in den letzten Jahren erheblich gestiegen ist. Ebenso ist in den Leitungsgremien eine hohe bis sehr hohe Awareness bez. Cyber Risiken feststellbar. Allerdings wurde eine erhebliche Lücke zwischen der Relevanzeinschätzung und dem Reifegrad der Cyber Risk Governance in vielen Organisationen identifiziert. Das bedeutet, dass die Integration von Cyber Risiken in das ERM methodisch, prozessual und organisatorisch noch zu wenig ausgereift ist. Dieser Umstand verhindert einen konsistenten Vergleich (und damit auch eine sinnvolle Priorisierung) von Cyber Risiken und anderen Risikokategorien

auf oberster Führungsebene. Dies wiederum führt zu einem mangelhaften Verständnis über den tatsächlichen Cyber-Risikoumfang bei den Aufsichtsorganen.

Ebenso fehlen Aussagen zum Risikoappetit, was ein zielorientiertes Management von Cyber Risiken auf operativer Ebene zusätzlich erschwert. Als erster Schritt in die richtige Richtung empfiehlt sich, eine stärkere Zusammenarbeit zwischen CISOs und Risk Management-Verantwortlichen zu fördern, denn hier wird primär die Brücke zwischen der technischen Cybersicherheit auf Systemebene und dem betriebswirtschaftlichen ERM geschlagen. Es ist klar, dass noch viel Forschung notwendig ist, um die Integration von Cyber Risiken in das ERM zu etablieren. Ein wichtiger erster Schritt ist mit dieser Studie getan.

Der Cloud-Teil der Studie zeigt, wo Schweizer Organisationen die Hauptrisiken bei der Nutzung von Cloud-Services sehen, nämlich beim Verlust der Vertraulichkeit, respektive bei der Verletzung des Datenschutzes. Darüber hinaus wird die Abhängigkeit vom Cloud-Diensteanbieter als signifikantes Risiko angesehen.

Im Rahmen der vorliegenden Studie werden Vorschläge zur Verminderung dieser Risiken unterbreitet, u. a. die Verfolgung eines cloud-agnostischen Ansatzes, die Einführung einer Datenklassifizierung und der Einsatz von Verschlüsselungstechnologie. Diese Massnahmen sind in der Regel mit Aufwand verbunden und können gar zu eingeschränkter Funktionalität führen. Dem steht aber der Gewinn an Flexibilität und die verbesserte Kontrolle über die eigenen Daten gegenüber.

Es besteht in diesem Themenkomplex grosses Potential für weitere Forschung, sowohl auf organisatorischer als auch auf technologischer Ebene. Gerade die jüngsten Fortschritte im Bereich der homomorphen Verschlüsselung verändern die Risikolandschaft des Cloud-Computings massgebend.

Literaturverzeichnis

Arena, M., Arnaboldi, M. & Azzone, G. (2010). The organizational dynamics of enterprise risk management, Accounting, Organizations and Society, Vol. 35, p. 659-675.

Baumann, C. & Hunziker, S. (2021). Third Party Risk Management - Erfahrungen bei einer Schweizer Gesundheitsversicherung, Zeitschrift für Risk Management (ZfRM), 01.22, S. 20-26.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2017). *Enterprise Risk Management—Integrating with Strategy and Performance*. Jersey City, NJ: AICPA

Gläser, J. & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*, 4. Aufl., Wiesbaden: Springer Fachmedien.

Gordon, L. A., Loeb, M. P. & Tseng, C-Y. (2009). *Enterprise risk management and firm performance: A contingency perspective*, Journal of Accounting and Public Policy, Vol. 28, pp. 301- 327.

Hunziker, S. (2021). *Enterprise Risk Management – Modern Appproaches to Balancing Risk and Reward*. 2nd Edition. Wiesbaden: Springer Gabler.

IRGC (2018). *Guidelines for the governance of systemic risks.* Lausanne: EPFL International Risk Governance Center.

ISO (2018). *ISO 31000:2018—Risk management Guidelines*. ISO, Genf, Schweiz.

Mell, P. & Grance T. (2011). NIST Special Publication 800-145. *The NIST Definition of Cloud Computing.* Recommendations of the National Institute of Standards and Technology.

National Institute of Standards and Technology (2020). NISTIR 8286, *Integrating Cybersecurity and Enterprise Risk Management (ERM)*, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf, abgerufen am 02.05.2022.

National Institute of Standards and Technology (2021). NISTIR 8286A, *Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management,* https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8286A.pdf, abgerufen am 02.05.2022.

National Institute of Standards and Technology (2022). NISTIR 8286B, *Prioritizing Cybersecurity Risk for Enterprise Risk Management,* https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8286B.pdf, abgerufen am 02.05.2022.

National Institute of Standards and Technology (2022). NISTIR 8286C, *Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight,* https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8286C-draft.pdf, abgerufen am 02.05.2022.

National Institute of Standards and Technology (2012). SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, abgerufen am 31.03.2022.

Schreier, M. (2014). *Varianten qualitativer Inhaltsanalyse: Ein Wegweiser im Dickicht der Begrifflichkeiten*. Forum Qualitative Sozialforschung / Forum: Qualitative Social Research, Vol. 15, No 1.

Ting, D. (2019). *Why Cognitive Biases and Heuristics Lead to an Under-investment in Cybersecurity,* https://www.cs.tufts.edu/comp/116/archive/fall2019/dting.pdf, abgerufen am 12.01.2022.

Von Werder, A. (2015). *Führungsorganisation. Grundlagen der Corporate Governance, Spitzen- und Leistungsorganisation. Grundfragen der Spitzenorganisation.* Springer: Wiesbaden.

Partner

Institut für Finanzdienstleistungen Zug IFZ

Das Institut für Finanzdienstleistungen Zug IFZ der Hochschule Luzern ist das führende Fachhochschulinstitut im Finanzbereich in der Schweiz. Das IFZ bringt seit 1997 für die Finanzbranche und für Finanzfachleute in Unternehmen aller Branchen Mehrwert durch Weiterbildung, anwendungsorientierte Forschung und Beratung. Zur Ausbildungspalette des IFZ gehören bspw. der MSc in International Financial Management oder der MSc in Banking and Finance. Im Bereich der Weiterbildung bietet das IFZ zahlreiche anerkannte Lehrgänge an, so z. B. den CAS Governance, Risk and Compliance oder den MAS/DAS Corporate Finance/Controlling.

Departement Informatik

Die Hochschule Luzern führte als erste Schweizer Fachhochschule ein eigenes Departement Informatik. Seit 2016 bietet die Hochschule Luzern – Informatik auf dem Campus Zug-Rotkreuz Bachelor- und Master-Studiengänge und eine breite Palette an Weiterbildungen in den wichtigsten Informatikdisziplinen an. Namhafte Bereiche sind Artificial Intelligence & Machine Learning, Digital Ideation, Engineering, Information & Cyber Security und Wirtschaftsinformatik. Zahlreiche Partner profitieren von der Projektkompetenz und Expertise der Forschenden und dem ausgezeichneten Netzwerk der Hochschule Luzern.

Mobiliar

Die Gruppe Mobiliar («Mobiliar») ist die führende Schweizer Retail-Versicherung und die Nummer eins für Haushalt-, KMU- und Risikolebensversicherungen. 1826 gegründet, ist sie die älteste private Versicherungsgesellschaft der Schweiz und bis heute genossenschaftlich verankert. Ihre 80 unternehmerisch geführten Generalagenturen mit eigenem Schadendienst garantieren an 160 Standorten persönliche Nähe zu den über 2,2 Millionen Kundinnen und Kunden. So ist jeder dritte Haushalt und jedes dritte Unternehmen in der Schweiz bei der Mobiliar versichert. Als Allbranchenversicherer beschäftigt die Mobiliar rund 6000 Mitarbeitende und bietet 330 Ausbildungsplätze an. Das Cyberschutz Angebot für Unternehmenskunden im Überblick auf www.mobiliar.ch/cyber.

economiesuisse

economiesuisse ist der Dachverband der Schweizer Wirtschaft. Er vertritt die Interessen seiner Mitglieder in allen Bereichen der Wirtschaftspolitik und setzt sich für optimale Rahmenbedingungen für den Wirtschaftsstandort Schweiz ein. Mitglieder sind 100 Branchenverbände, 20 kantonale Handelskammern sowie einige Einzelunternehmen. economiesuisse vertritt insgesamt 100’000 Schweizer Unternehmen aus allen Branchen mit rund zwei Millionen Arbeitsplätzen in der Schweiz: KMU und Grossunternehmen, export- und binnenmarktorientierte Betriebe – im Dachverband economiesuisse sind sie alle vereint.

Autorenschaft

Prof. Dr. oec. HSG Stefan Hunziker
Prof. Dr. Stefan Hunziker ist Professor für Enterprise Risk Management und Interne Kontrollsysteme an der Hochschule Luzern – Wirtschaft, Institut für Finanzdienstleistungen Zug IFZ. Er ist Mitglied der Institutsleitung und leitet das Kompetenzzentrum Risk & Compliance Management am IFZ. Seit mehr als 15 Jahren befasst er sich mit der Weiterentwicklung von Risk Management in der Praxis, stets unter Berücksichtigung aktueller wissenschaftlicher Erkenntnisse.

Prof. Armand Portmann
Prof. Armand Portmann ist Dozent an der Hochschule Luzern – Informatik. Er ist mitverantwortlich für das Themenfeld Information & Cyber Security | Privacy und leitet diverse CAS- und MAS-Programme in diesem Bereich. Er setzt sich seit über 15 Jahren im Rahmen von Dienstleistung, Forschung und Lehre intensiv mit dem Thema Information & Cyber Security auseinander.

Prof. Viviane Trachsel
Viviane Trachsel ist Dozentin und Projektleiterin für Controlling an der Hochschule Luzern – Wirtschaft, Institut für Finanzdienstleistungen Zug IFZ. Sie verfügt über jahrelange Erfahrung in der Aus- und Weiterbildung sowie in Forschungsprojekten u. a. mit Fokus auf Ausgestaltung des Controllings in komplexen Organisationen. Sie betreibt das Controlling-Wiki der Hochschule Luzern – Wirtschaft.

Fernand Dubler
Fernand Dubler ist wissenschaftlicher Mitarbeiter und Forscher an der Hochschule Luzern – Informatik. In erster Linie unterrichtet und betreut er Laborübungen in diversen Weiterbildungsangeboten im Bereich der Informationssicherheit und ist für die Dienstleistung «eBanking – aber sicher!» tätig.

Hochschule Luzern
Wirtschaft
Institut für Finanz-
dienstleistungen Zug IFZ
Campus Zug-Rotkreuz
Suurstoffi 1
6343 Rotkreuz

T +41 41 757 67 67
ifz@hslu.ch
hslu.ch/ifz

AACSB ACCREDITED

Hochschule Luzern
Informatik
Campus Zug-Rotkreuz
Suurstoffi 1
6343 Rotkreuz

T +41 41 757 68 11
informatik@hslu.ch
hslu.ch/informatik

ISBN 978-3-906877-97-6

Mehr Informationen
zum Institut für Finanz-
dienstleistungen Zug IFZ

Mehr Informationen
zur Hochschule Luzern –
Informatik

04-2022