KESSLER

CYBER RISK & INSURANCE
AKTUALISIERTE 3. AUFLAGE (2021)

MIT SICHERHEIT VORAUS.

VORWORT

Wenn wir fünf Jahre zurückblicken – lediglich fünf Jahre –, drehte sich in der Beratung alles um die Frage «Was kann uns konkret passieren?».

Aus vielen hundert Gesprächen mit Schweizer Unternehmen können wir heute konstatieren, dass das Bewusstsein für Cyber-Risiken in den Entscheidungsorganen sehr gut präsent ist. Die Szenarien sind bekannt und die Unternehmen haben ihre Cyber-Risiken quantifiziert sowie Ausreisser versichert. Mit den Versicherern zusammen haben wir die Produkte stetig weiterentwickelt und Versicherer sowie Broker regulieren heute zahlreiche Schadenfälle. Teilweise war die Lernkurve für uns alle steil. Als Fazit können wir sagen, dass Schweizer Unternehmen robuster geworden sind und vor allem für den Fall vorbereitet sind, dass etwas passiert.

Pascal Schweingruber
Mitglied der Geschäftsleitung

In der Herbstsession 2020 haben die Räte das neue Schweizer Datenschutzgesetz verabschiedet. Dies war für uns Anlass, eine dritte aktualisierte Ausgabe der Publikation Cyber Risk & Insurance herauszugeben, um die neuen rechtlichen Aspekte zu würdigen und unsere Erfahrung im Management der Cyber-Risiken weiterzugeben.

Ich danke den Autorinnen und Autoren Simon Künzler (Risk Consulting), Melanie Koller (Legal), Nadine Janser (Special Risks), Simon Holtz (Sachversicherung) und Patrick Dummermuth (Claims Advocacy) herzlich für ihre Beiträge und Insights.

Ich wünsche Ihnen aufschlussreiche Erkenntnisse.

1
IHR PARTNER AUF AUGENHÖHE

Wir unterstützen Sie beim Aufbau eines Cyber-Dispositivs, das die Widerstandsfähigkeit Ihrer Organisation gegenüber Cyber-Angriffen stärkt. Dieses Ziel erreichen wir dank dem kundenspezifischen und ganzheitlichen Ansatz sowie analyse- und praxisorientierten Fach- und Methodenkompetenzen.

AUSGANGSLAGE UND RISIKOEXPOSITION

Die sich ständig wandelnden Cyber-Angriffe finden ihren Nährboden in vernetzten, komplexen und dynamischen Lieferketten, Informations- und Kommunikationsinfrastrukturen, dem «Internet of Things» respektive «every thing» und insbesondere im nach wie vor unachtsamen Umgang von Mitarbeitenden mit E-Mails und Internet. Digitale Innovationen und Entwicklungen wie zum Beispiel die Industrie 4.0 haben für Organisationen einerseits enorme Rationalisierungs- und Wachstumschancen eröffnet. Andererseits haben sie aber auch zu einer Akzentuierung ihres ohnehin bedeutenden Risikopotenzials geführt. Insgesamt kann ein Versagen im Bereich Cyber Resilience (Widerstandsfähigkeit) die Corporate Governance kompromittieren und letztlich schwerwiegende finanzielle und nicht-finanzielle Auswirkungen auf ein Unternehmen zeitigen. Diese Ausgangslage zeigt, dass Cyber-Risiken umfassend analysiert, bewertet und schliesslich mittels geeigneter präventiver und reaktiver Massnahmen eingegrenzt werden müssen.

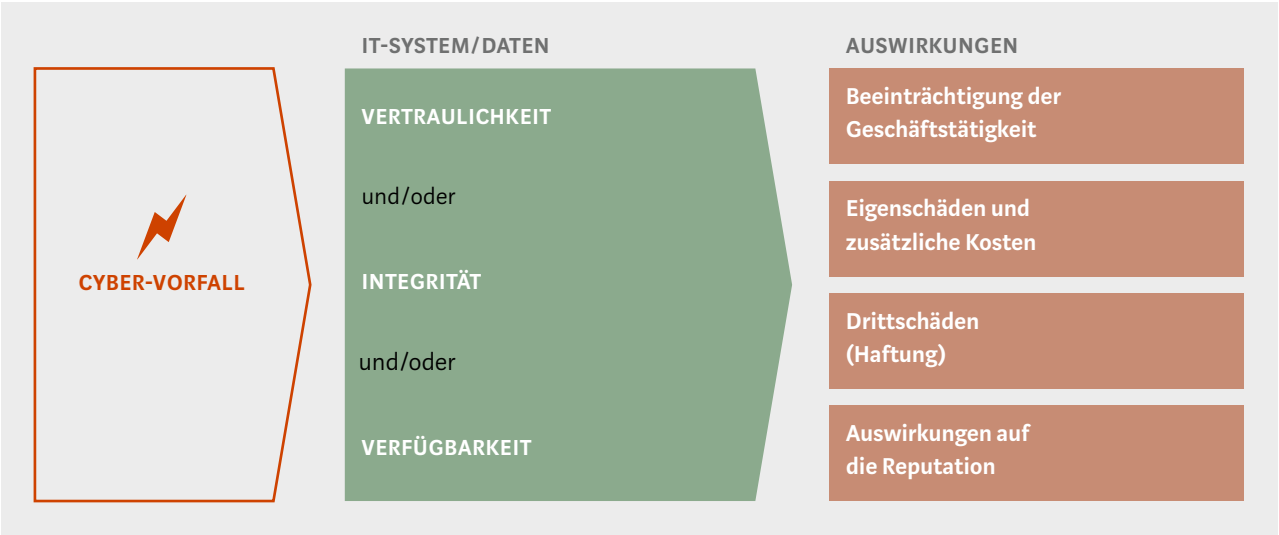
GANZHEITLICHES CYBER-VERSTÄNDNIS

Den meisten Organisationen ist es heute bewusst, dass Cyber nicht alleine der IT-Abteilung zugeordnet, sondern eingebettet in ein ganzheitliches Enterprise Risk Management angegangen werden muss. Dabei spielt der Faktor Mensch beziehungsweise sein Nutzerverhalten eine zentrale Rolle. Damit wird zum Ausdruck gebracht, dass Cyber auch ein Führungs- und Organisationsthema ist. Infolgedessen bedarf es einer Kombination aus technischen, organisatorischen, rechtlichen und finanziellen Massnahmen. Im Wissen darum, dass es keine hundertprozentige Sicherheit geben kann, empfehlen wir, Massnahmen transparent und im Sinne eines kontinuierlichen Verbesserungsprozesses umzusetzen. Jede Organisation sollte sicherstellen, dass im Falle eines Cyber-Zwischenfalles die Funktionsfähigkeit der Organisation gewährleistet ist beziehungsweise dass der Normalbetrieb möglichst rasch wiederhergestellt wird.

DARSTELLUNG DES CYBER-RISIKOS

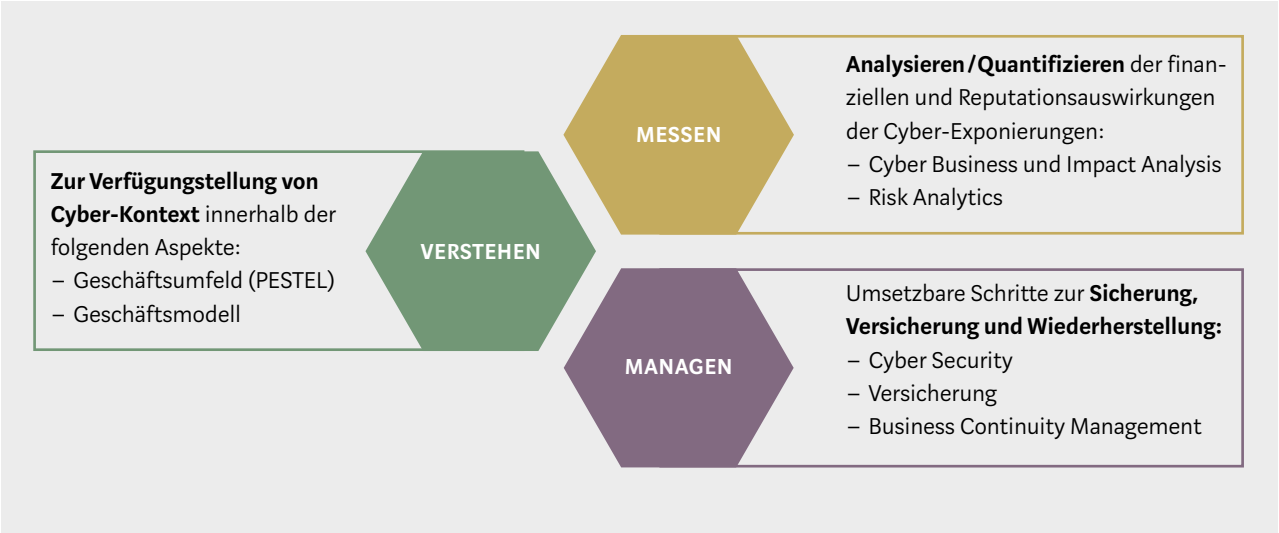
Das Risiko ist ein Angriff auf die IT-Systeme und/oder die Beeinträchtigung der Daten betreffend Vertraulichkeit, Integrität und Verfügbarkeit. Die Auswirkungen können operativer, finanzieller und nicht-finanzieller Natur sein, wie beispielsweise ein gravierender Vertrauensverlust bei wichtigen Stakeholdern.

CYBER-RISIKO



DREISTUFIGER LÖSUNGSANSATZ

Um das vorliegende Cyber-Risiko zu analysieren, wenden wir ein dreistufiges Vorgehen an.



1

PROJEKTVORGEHEN

Dank dem Projektansatz «Cyber Business und Impact Analysis» unterstützen wir Sie dabei, Cyber-Risiken zu verstehen, zu messen und zu managen. Ein zentrales Element stellt der von uns moderierte Workshop mit Teilnehmenden aus diversen Funktionsbereichen dar.

VERSTEHEN Dokumentenanalyse und Interviews	**MESSEN** Interdisziplinärer Workshop	**MANAGEN** Cyber-Projektbericht
– Desktop-Arbeiten – Eruieren potenzieller Exponierungen und Verletzlichkeiten aufgrund der Analyse von Geschäftsumfeld und -modell – Klären von ICT-Abhängigkeiten – Aufnehmen physischer sowie digitaler Werte und Infrastrukturen	– Entwickeln von Cyber-Bedrohungsszenarien – Bewerten und priorisieren der Szenarien nach verschiedenen Kostenparametern (Risiko-Matrix) – Benchmark-Abgleich – Erstellen eines Massnahmenkatalogs zur Verbesserung des Cyber-Dispositivs	– Zusammenfassung der Projekterkenntnisse zur Cyber-Bedrohungssituation – Aufzeigen der Verwendung des aufbereiteten, zur Verfügung gestellten holistischen Massnahmenkataloges – Interne Informationen/ Kommunikation – Sensibilisierung

2
CYBER-RISIKEN

Der Begriff der Cyber-Risiken wird vielfältig und uneinheitlich verwendet und bezieht sich auf eine Vielzahl von Risiken, die im Zusammenhang mit Technologie oder mit Informationen eines Unternehmens stehen. Aus dem Blickwinkel der Versicherungsindustrie werden Cyber-Risiken als operationelle Risiken definiert; darunter ist im Grundsatz ein Datenverlust oder eine IT /ICT-Störung beziehungsweise eine IT/ICT-Fehlfunktion zu verstehen, welche die Vertraulichkeit, die Verfügbarkeit oder die Integrität von Informationen oder Informationssystemen beeinträchtigt.

Das Ursache-Wirkungs-Prinzip ist ein altbewährtes Risk-Management-Instrument und bietet sich zum besseren Verständnis der Cyber-Risiko-Landschaft eines Unternehmens an. Wer sich der möglichen Ursachen von betriebseigenen Worst-Case-Szenarien bewusst ist, kann mithilfe einer sorgfältigen Ursachenanalyse gezielt Präventivmassnahmen treffen und damit insgesamt die IT-technische, aber auch die finanzielle Widerstandsfähigkeit des Unternehmens stärken.

Ein Datenverlust oder eine IT/ICT-Störung kann sowohl kriminelle Ursachen als auch nicht-kriminelle Ursachen haben (s. S. 10). Kriminelle Ursachen sind gemäss dem Schweizer Strafgesetzbuch unabhängig vom daraus resultierenden Cyber-Risiko in der Regel bereits eigene strafbare Handlungen (zum Beispiel unbefugte Datenbeschaffung zum Weiterverkauf auf dem Darknet nach StGB Art. 143 oder das unbefugte Eindringen in ein Datenverarbeitungssystem zu Spionagezwecken gemäss StGB Art. 143bis). Weitere strafbare Handlungen sind zum Beispiel die Infiltrierung eines ERP mit einer Malware und damit die Manipulation der Datenintegrität nach StGB Art. 144bis oder der Identitätsdiebstahl mittels der Fake-President-Masche zur unrechtmässigen Bereicherung nach StGB Art. 147.

Die steigende Komplexität der vernetzten Systeme bietet vor allem auch Cyber-Kriminellen neue Möglichkeiten – seien dies externe Dritte, aktuelle und ehemalige Mitarbeitende, die Konkurrenz oder gar staatliche Organisationen mit unterschiedlichen Motiven. Daten, die für den einen wertlos sind, können für den anderen kostbar sein. Deshalb sind Unternehmen nicht sicherer vor Cyber-Kriminellen, nur weil ihr Management den eigenen Daten keinen grossen Nutzen für Dritte beimisst. Wer in Systeme eindringen will, findet auch einen Weg, und damit ist ein gewisses «Ausgeliefertsein» leider Realität geworden: Einen hundertprozentigen Cyber-Schutz wird es nie geben – und schon gar nicht gegen einen gezielten Angriff (Advanced Persistent Threat, APT).

2

CYBER-RISIKO: URSACHE-WIRKUNGS-MODELL

2.1 FINANZIELLE AUSWIRKUNGEN

Die Cyber-Risikolage erhöht sich von Jahr zu Jahr, weshalb die finanzielle Tragbarkeit des Restrisikos in den Fokus rückt. Die finanziellen Restrisiken zu kennen, bedeutet Sicherheit hinsichtlich deren Finanzierbarkeit. Die durch einen Cyber-Vorfall verursachten Schäden lassen sich aufgrund fehlender Erfahrungswerte weder vollumfänglich noch abschliessend quantifizieren.

EIGENSCHÄDEN

- Kosten für Krisenmanagement (IT-Forensik, Rechtsberatung, PR-Beratung)
- Kosten für Benachrichtigung Betroffener und Behörden nach Datenverlust
- Kosten für Daten-Monitoring nach Datenverlust
- Kosten für Bearbeitung von Auskunftsbegehren
- Datenschutzbussen
- Kosten für Wiederherstellung oder Ersatzbeschaffung von Daten und IT-Systemen
- Kosten für die Aufrechterhaltung der Funktionsfähigkeit der IT-Systeme
- Kosten bei Betriebsunterbruch, welche zur Fortführung der Geschäftsaktivitäten aufgewendet werden müssen inkl. entgangener Gewinn
- Erpressungszahlungen und damit zusammenhängende Folgekosten
- Vermögensverlust infolge Cyber-Betrug und Social Engineering und damit zusammenhängende Folgekosten
- Kosten für durch externe IT-Dienstleister verursachte Schäden
- Kosten für die Durchsetzung eigener durch Dritte verletzte Rechte (Intellectual Property)
- Abwehrkosten im Zusammenhang mit regulatorischen Verfahren
- Abwehrkosten im Zusammenhang mit Haftungsrisiken
- Kosten für die Verhinderung oder Milderung eines möglichen Haftungsrisikos
- Schadenermittlungskosten
- Kosten infolge Reputationsschaden

DRITTSCHÄDEN (HAFTUNGSRISIKEN)

- Zahlung von Schadenersatzansprüchen Dritter nach Datenschutz- oder Sicherheitsverletzung
- Zahlung von Schadenersatzansprüchen nach Persönlichkeitsverletzung oder Ehrverletzung
- Zahlung von Schadenersatzansprüchen nach Verletzung oder Verlust von geistigem Eigentum Dritter
- Zahlung von Schadenersatzansprüchen nach Verletzung des Wettbewerbs-, Urheber- und Markenrechts oder einer Geheimhaltungspflicht
- Zahlung von Schadenersatz oder Konventionalstrafen infolge Vertragsverletzung

2

2.2 IT SUPPLY CHAIN RISK – WER HAT DIE ÜBERSICHT?

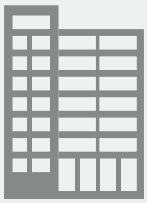
Im heute digital vernetzten Geschäftsumfeld stellt eine funktionierende IT eine der wichtigsten Voraussetzungen für den Unternehmenserfolg dar. Mit ausgelagerten Dienstleistungen, Systemen, Prozessen oder Einrichtungen steigt die eigene Abhängigkeit von Drittunternehmen. Gleichzeitig sinkt in der Regel der Überblick über die vorhandenen Supplier sowie die fehlenden Ressourcen zur fortlaufenden Cyber-Risikoprüfung.

Eine risikobasierte Verwaltung der IT-Geschäftspartner wird heute zunehmend von Investoren, sensibilisierten Kunden oder den Aufsichtsbehörden (wie FINMA oder Aufsichtsbehörden für Pensionskassen) verlangt. Damit die IT Supply Chain für Sie und Ihre wichtigsten Stakeholder keine Black Box wird/bleibt, empfehlen wir Ihnen, die IT-Lieferanten entsprechend den eigenen Bedürfnissen zu prüfen.

- Von welchen IT-Dienstleistern sind wir abhängig? In welchem Geschäftsbereich und welche Art von Daten werden durch wen bearbeitet/verarbeitet (besonders schützenswerte Personendaten, sensitive Produktionsdaten, Vertragskonditionen von Grosskunden, Strategiedokumente etc.)?
- Welche und wie viele Mitarbeitende der IT-Dienstleister haben auf die Systeme unserer Firma Zugriff/Einsicht in diese Daten?
- Welche Mitarbeitenden der Dienstleister haben welche Administratorenrechte?
- Wie ist das Service Level Agreement ausgestaltet? Wer haftet wofür im Falle eines Ausfalls des Netzwerks?
- Sind die Schlüsselpersonen und grössten Cyber-Risiken in der IT Supply Chain bekannt?
- Kennt die Unternehmensführung die finanziellen Auswirkungen infolge der relevanten IT-Lieferanten? Welche Kosten deckt die Versicherung?
- Wer in unserem Unternehmen hat den Überblick über die zu prüfenden Punkte vor Vertragsschluss mit einem IT-Dienstleister?

Grafik rechts: Zu einem durchschnittlichen KMU können gut 20 bis 50 IT-Dienstleister zählen. Je internationaler und je digitaler das Geschäftsmodell ist, desto länger wird die IT Supply Chain. Der Faktor Mensch ist bekanntlich eine der grössten Schwachstellen in der Cyber/IT Security. Wichtig zu wissen sind drei Punkte: Wer gehört zu unserer IT Supply Chain? Welche Mitarbeitenden der eigenen Firma und der IT-Dienstleister sind Schlüsselpersonen für den Erfolg unseres Geschäftsmodells? Und welche Schlüsselperson hat welche Berechtigungen und welche Administratorenrechte? Anhand der Antworten können gezielte Präventivmassnahmen oder ein bewusster Entscheid für die Übernahme eines entsprechenden Cyber-Risikos getroffen werden.

WER GEHÖRT ZUR IT SUPPLY CHAIN UNSERER FIRMA?



Serverhousing
- Rechenzentrum

Infrastrukturbetreiber
- Strom/Wasser
- Internet/Telekom

Freelancer

On-Premises Software oder
On-Premises Software und Serverhousing

FinTechs **InsurTechs** **LegalTechs** **MedTechs**

Support-Dienstleistungen
Kernfunktionen

Support-Dienstleistungen
Unterstützungsfunktionen

Forschung/
Analysen

Rechtsberatung und
Consulting-Dienstleistungen

Externer/interner
Subunternehmer

Gebäude-
überwachung

Software-
Entwickler

Start-up in
anderem Bereich

Regulatoren/
Behörde

Supply Chain End?

Cloud-Dienstleister (IaaS)
Infrastruktur as a Service
- Rechenzentrum
- Physische Server
- Speichersysteme
- Virtualisierung

Cloud-Dienstleister (PaaS)
Platforms as a Service
- Rechenzentrum
- Physische Server
- Speichersysteme
- Virtualisierung
- Betriebssystem
- Middleware
- Datenbanken

Cloud-Dienstleister (SaaS)
Software as a Service
- Rechenzentrum
- Physische Server
- Speichersysteme
- Virtualisierung
- Betriebssystem
- Middleware
- Datenbanken
- Anwendungsdaten
- Standardsoftware
- Fachanwendung

Privat Cloud **Hybrid Cloud**

Multi Cloud **Public Cloud**

Community Cloud **Distributed Cloud**

3
CORPORATE GOVERNANCE

Die Cyber-Sicherheit ist eine Governance-Herausforderung. Grosse Unsicherheit herrscht bei den Fragen: Wie strukturieren die Verwaltungsräte ihre Aufsicht über die Cyber-Sicherheit und wie interagieren sie mit dem Management bei diesem wichtigen Thema? In jedem Schadenfall stellt sich die Frage, ob der Verwaltungsrat die vorhandenen Cyber-Risiken kannte oder hätte kennen müssen. Die Beurteilung der Antworten hängt stark vom Einzelfall und der entsprechenden Branche beziehungsweise den Datensicherheitsvorkehrungen gemäss State of the Art ab. Nach jedem grösseren Cyber-Schadenfall steht deshalb die Frage im Raum, ob der Verwaltungsrat dafür zu haften hat. Umso gewichtiger ist der bewusste Entscheid.

3.1 PFLICHTEN DES VERWALTUNGSRATES

Im Zusammenhang mit dem enormen von Cyber-Risiken ausgehenden Schadenpotenzial rücken unter anderen die komplexer werdenden Pflichten des Verwaltungsrates einer Aktiengesellschaft in den Fokus.

ÜBERTRAGBARE PFLICHTEN

Der Verwaltungsrat ist das geschäftsführende Organ einer Aktiengesellschaft, sofern er die Geschäftsführung nicht übertragen hat. Bei der Delegation von Organaufgaben haftet der Verwaltungsrat für den vom Dritten verursachten Schaden, wenn er nicht nachweist, dass er bei dessen Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat (OR 716 Abs. 2 i. V. m. OR 716b Abs. 1 i. V. m. OR 754 Abs. 2).

UNÜBERTRAGBARE PFLICHTEN

Für die unübertragbaren und unentziehbaren Pflichten des Verwaltungsrates trägt der Gesamtverwaltungsrat die volle Verantwortung. Die Unübertragbarkeit beschränkt sich auf die Entscheidfindung und Entscheidfällung beziehungsweise auf den bewussten Entscheid, womit Vorbereitungsaufgaben sowie die Ausführung von Beschlüssen an operative Organe übertragen werden können.

Gemäss herrschender Lehre gelten unter anderen die folgenden Pflichten als unübertragbare Pflichten des Verwaltungsrates.

- Aufsichts- und Strategieaufgaben mit dem Ziel, die Interessen der Gesellschaft wahrzunehmen.
- Risikobeurteilung: Der Verwaltungsrat hat im Rahmen des Lageberichts unter anderen die Lage der wichtigsten geschäftlichen Risiken zu beurteilen (OR 961c Abs. 2 Ziff. 2). Dies umfasst insbesondere die Beurteilung der aktuellen Marktrisiken, Kredit- und Lieferrisiken sowie der finanziellen und operationellen Risiken wie IT-, Sicherheits-, Produkte- und Rechtsrisiken, Cyber-Risiken sowie der relevanten Zukunftsaussichten. Einen Lagebericht haben alle Unternehmen zu erstellen, die von Gesetzes wegen zu einer ordentlichen Revision verpflichtet sind (OR 961 i. V. m. 727).
- Entscheid über Risikofinanzierungsstrategie und IT/ICT-Sicherheitsstrategie

CORPORATE GOVERNANCE – VORAUSSETZUNGEN FÜR EINEN MANAGEMENT-ENTSCHEID

Unübertragbare Pflichten des Verwaltungsrates
- Aufsichts- und Strategieaufgaben
- Beurteilung der wichtigsten Risiken
- Entscheid über Risikofinanzierungsstrategie beziehungsweise IT/ICT-Sicherheitsstrategie

Management-Entscheid beruht auf
- Angemessener beziehungsweise hinreichender Information = Einholung aller für konkrete Entscheide relevanten rechtlichen Informationen
- Abwägung aller Vor- und Nachteile der Handlungsalternativen und deren Konsequenzen sowie finanzielle Auswirkungen

Sind die Voraussetzungen für einen Management-Entscheid erfüllt?

JA	NEIN
Management-Entscheid = bewusster Entscheid	Management-Entscheid ≠ bewusster Entscheid
Business Judgement Rule erfüllt	Business Judgement Rule nicht erfüllt
Keine Pflichtverletzung beziehungsweise keine Haftung nach OR 754 trotz allfälligem Fehlentscheid	Pflichtverletzung beziehungsweise Haftung nach OR 754 möglich

3

3.2 DIE RELEVANZ DES BEWUSSTEN ENTSCHEIDS

Der Verwaltungsrat schuldet seinem Unternehmen für jeden Entscheid eine sorgfältige Vorbereitung, Evaluation und Umsetzung – nicht aber den Erfolg. Damit wird das Augenmerk auf ein sorgfältig ausgestaltetes Entscheidungsverfahren beziehungsweise auf einen einwandfreien Entscheidungsprozess gelegt. Dies gilt ebenfalls für den Entscheid der Risikofinanzierung von Top-Risiken beziehungsweise ob diese mit Eigenmitteln finanziert oder transferiert werden.

KONSEQUENZEN EINES FALSCHEN GESCHÄFTSFÜHRUNGSENTSCHEIDS

In einem solchen Fall ist eine Pflichtverletzung der Verwaltungsorgane zu verneinen, wenn der Geschäftsführungsentscheid auf einer angemessenen beziehungsweise hinreichenden Informationsbasis und auf einer ernsthaften Entscheidungsfindung beruht. Dies schliesst eine angemessene beziehungsweise hinreichende Informationsbeschaffung für die Einholung aller für konkrete Entscheide relevanten tatsächlichen rechtlichen Informationen mit ein, um eine umfassende Abwägung der Vor- und Nachteile der Handlungsalternativen und deren Auswirkungen zu ermöglichen (vgl. BGer 4A_97/2013, Erw. 5.2; BGE 139 III 26).

ORGANHAFTUNG (D&O-HAFTUNG) OR 754

Experten der Versicherungswirtschaft verweisen auf die USA und prognostizieren, dass Cyber-Schadenfälle in Europa künftig ebenfalls vermehrt im Rahmen der Cyber- und D&O-Versicherung geltend gemacht werden; dies mit Konsequenzen auf die Beachtung von Kumulrisiken, die bereits im Underwriting-Prozess der Versicherer und Rückversicherer zu berücksichtigen sind.

Trifft die Geschäftsführung zum Beispiel nur ungenügende Sicherheitsmassnahmen zur Verhinderung von Hacker-Angriffen respektive schützt sie dadurch das Vermögen indirekt unzureichend, können die einzelnen Organe für diese Unterlassung haften. Aus rechtlicher Sicht kann auch ein fehlendes oder mangelhaft durchgeführtes Cyber Risk Management beziehungsweise ein nicht-bewusster Entscheid über die Risikofinanzierung unter Umständen als Sorgfalts- oder Treuepflichtverletzung im Sinne von OR 717 qualifiziert werden und möglicherweise zur Haftung der einzelnen Organe nach OR 754 führen. Ebenfalls können mit Absicht oder grobfahrlässig unterlassene Pflichten im Rahmen der EU-Datenschutzgrundverordnung, welche die Umsetzung gewisser Sicherheitsstandards verlangen, zu verschärften Haftungslagen der Unternehmensführung führen.

Der D&O-Haftung unterstehen neben den Verwaltungsratsmitgliedern auch alle anderen mit der Geschäftsführung betrauten Personen. Sogenannt faktische Organe nehmen eigenständig Geschäftsaufgaben wahr und haben einen entscheidenden Einfluss auf die Willensbildung der Gesellschaft.

BUSINESS JUDGEMENT RULE

Die Business Judgement Rule wird im Rahmen der Organhaftung nach OR 754 geprüft. Nach der Formel des Schweizerischen Bundesgerichts im Entscheid 4A_74/2012, Erw. 5.1 haben sich Gerichte bei der nachträglichen Beurteilung von Geschäftsentscheiden Zurückhaltung aufzuerlegen, wenn diese Entscheide in einwandfreien Entscheidungsprozessen zustande gekommen sind, die auf einer angemessenen Informationsbasis beruhten und frei von Interessenkonflikten waren. Pflichtwidrig handelt ein Geschäftsführungsorgan bloss, wenn ein Geschäftsentscheid schlicht unvertretbar ist. Deshalb sind Unternehmen gut beraten, ihre Geschäftsentscheide bewusst zu fällen sowie umfassend zu dokumentieren.

EQUIFAX: GRENZEN DER BUSINESS JUDGEMENT RULE

Sammelklagen führen in Zusammenhang mit der gegebenenfalls fehlenden Cyber-Sicherheit nach Datensicherheitsvorfällen zur Haftung von Unternehmen oder der verantwortlichen Organe. Bei der Beurteilung der Frage, ob Entscheidungsträger ihrer Sorgfaltspflicht nachgekommen sind, wird das Gericht nach Beweisen dafür suchen, ob die Verantwortlichen vorsätzlich und sachkundig gehandelt und Alternativen zum bewussten Entscheid bezüglich Umgang mit den relevanten Risiken ermittelt und untersucht haben.

Die Grenze der Business Judgement Rule zeigt sich in der jüngsten Sammelklage gegen Equifax von Anfang 2020: Die Kläger behaupten, dass Equifax den Benutzernamen «admin» und das Passwort «admin» benutze, um ein Portal zur Verwaltung von Kreditstreitigkeiten zu schützen, und damit ein Passwort gewählt habe, das todsicher gehackt werden könne; im Weiteren habe Equifax die Schlüssel zum Entsperren der Verschlüsselung der Server mit sensiblen Daten auf denselben öffentlich zugänglichen Servern hinterlassen, sodass die Verschlüsselung leicht von den Daten entfernt werden konnte. Diese Behauptungen werden es Equifax nicht einfach machen zu beweisen, dass die dem Risiko angemessene Sorgfaltspflicht ausgeübt wurde. In einem solchen Fall nützt auch eine Business Judgement Rule nichts, denn bei der Beurteilung der Frage, ob Verantwortliche ihrer Sorgfaltspflicht nachgekommen sind und gegen die Business Judgement Rule verstossen haben, wird das Gericht nach Beweisen dafür suchen, ob die Entscheidungsträger vorsätzlich und sachkundig gehandelt und Alternativen zur letztlich implementierten Schutzmassnahme ermittelt und untersucht haben. Diejenigen, die ihre Verantwortung für die Cyber-Sicherheit quasi ignorieren oder das Unternehmen leichtsinnig einer Gefahr aussetzen, um die Firma zu schützen, werden mit grosser Wahrscheinlichkeit keinen Schutz durch die Business Judgement Rule finden.

«NATIONALE STRATEGIE ZUM SCHUTZ DER SCHWEIZ VOR CYBER-RISIKEN 2018-2022» UNTERSTREICHT DIE WICHTIGKEIT DER CYBER-RISIKEN

In der Schweiz zeigen diverse Projekte auf Bundesebene wie beispielsweise die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2018–2022» oder der Ausbau der «Cyber-Armee», wie essenziell die Cyber-Risiken sind und mit welcher Priorität sie behandelt werden müssen. Die Omnipräsenz der Cyber- und IT-Risiken in der Privatwirtschaft und der öffentlichen Hand lassen das Ignorieren von diesen Risiken nicht zu. Je grösser und systemkritischer ein Unternehmen ist, desto weniger ist Ignorieren oder Kleinreden der notwendigen Cyber-Präventivmassnahmen eine Option.

DOKUMENTATION VON GESCHÄFTSENTSCHEIDEN

Ein Geschäftsentscheid beziehungsweise der bewusste Entscheid ist zu protokollieren (OR 713 Abs. 3), denn im Rahmen von allfälligen Beweiserhebungsverfahren sind Urkunden wie Verwaltungsratsprotokolle gegebenenfalls herauszugeben (ZPO 160 Abs. 1 lit. b).

Basierend auf den Entscheidungsgrundlagen sind die Vor- und Nachteile der Handlungsalternativen und deren finanzielle Auswirkungen zu dokumentieren. Der bewusste Entscheid ist zu begründen. Geschäftsführungsorgane, die potenziell von Interessenkonflikten betroffen sind, sollten an der Beschlussfassung zum bewussten Entscheid nicht teilnehmen.

4
WAS HABEN DATENSCHUTZ UND DATENSICHERHEIT MIT CYBER RISK ZU TUN?

Praktisch jeder Cyber-Incident führt zur Verletzung der Integrität, Verfügbarkeit oder Vertraulichkeit von Personen- und/oder Unternehmensdaten. Insofern steht bei jeder unbeabsichtigten oder unrechtmässigen Vernichtung, bei Verlust, Veränderung, Offenlegung oder Zugangssperre zu Daten (Betriebsunterbruch) immer die Frage im Raum, welche Datenschutzgesetze und welche anderen sektorspezifischen Gesetze tangiert sind und welche regulatorischen Massnahmen beziehungsweise Pflichten sich daraus ergeben. Datensicherheitsverletzungen können Folgen eines kriminellen Cyber-Angriffs sein, aber genauso gut können nicht-kriminelle Ursachen wie IT-technische Pannen oder ein unbeabsichtigt fehlgeleitetes E-Mail zu einem Datenverlust führen.

Im heutigen Geschäfts- und Rechtsumfeld gewinnt die Rechenschaftspflicht und damit die Dokumentation der datenschutzrechtlichen Massnahmen für die Unternehmensführung an Bedeutung. Dabei spielt auch die Dokumentation des bewussten Entscheids hinsichtlich Umsetzungsart und Priorisierung der datenschutzrechtlichen Pflichten sowie die Begründung der eingeschlagenen Strategie basierend auf den umgesetzten technischen und organisatorischen Massnahmen (TOM) eine wichtige Rolle.

Die TOMs sind gemäss State of the Art beziehungsweise gemäss dem Stand der Technik umzusetzen. State of the Art ist ein unbestimmter, dafür dynamischer, aber gerichtlich voll überprüfbarer Rechtsbegriff, der den branchenspezifischen Sicherheitsstandards entspricht, die sich laufend ändern können. In einem Cyber-Schadenfall müssen die verantwortlichen Unternehmen beweisen, dass die eingesetzten TOMs gemäss State of the Art eingesetzt werden. Auch sind «Stand-der-Technik-Klauseln» in Cyber-Versicherungen weit verbreitet, wobei ein Versicherungsschutz bei Nichtumsetzung der TOMs gemäss State of the Art entfallen oder sich reduzieren kann.

KOSTEN IM ZUSAMMENHANG MIT DATENSCHUTZGESETZVERLETZUNGEN SIND BEI KENNTNIS DES ENTSPRECHENDEN RECHTS KALKULIERBAR UND DERZEIT GRÖSSTENTEILS VERSICHERBAR.

- Benachrichtigung von Behörden oder Betroffenen
- Kosten für regulatorische Verfahren
- Gewisse Datenschutzbussen
- Zahlung von Schadenersatzforderungen Dritter nach Datenschutzverletzung samt Rechts- und Beratungskosten bei regulatorischen Verfahren, Datenschutzbussen, Kosten für Krisenmanagement, Benachrichtigungskosten

4.1 DIE SCHWEIZ UND DER EINFLUSS DER EU: THEMEN BIS 2022

Am 25. September 2020 hat das Schweizer Parlament das revidierte Bundesgesetz über den Datenschutz (DSG) verabschiedet. Aufgrund COVID-19 hat sich das Differenzbereinigungsverfahren länger hingezogen als ursprünglich geplant. Bis zum Inkrafttreten im Jahr 2022 werden entsprechende Verordnungen ausgearbeitet und in die Vernehmlassung geschickt. Die ursprünglich vorgesehene zweijährige Übergangsfrist, wonach die verantwortlichen Unternehmen betreffend ihrer Pflichten die ersten zwei Jahre hätten verschont werden sollen, wurde gestrichen. Umso wichtiger ist es, die Vorbereitungen zur DSG-Compliance frühzeitig mit Fachspezialisten zu planen.

Im Weiteren ist nach wie vor der Angemessenheitsentscheid der EU-Kommission ausstehend, der den ungehinderten Datentransfer von der EU in die Schweiz aufrechterhalten soll. Bis jedoch entschieden wird, gilt nach wie vor der geltende Beschluss der EU vom 26. Juli 2000, denn dieser hat kein Ablaufdatum. Die EU ist nicht gezwungen, diesen Angemessenheitsbeschluss bezüglich der Datenschutzgesetzgebung in der Schweiz zu fällen. Insofern stellt sich die Frage, welche politische Agenda die EU mit diesem Beschluss verfolgt. Wichtig: Die Schweiz gilt für die EU solange als Drittstaat mit einem genügenden Datenschutz, bis dieser Entscheid revidiert wird. Bezüglich der politischen Agenda seitens EU ist auf das Schrems-II-Urteil vom 16. Juli 2020 zu verweisen, wonach der EuGH das EU–US Privacy Shield per sofort für nichtig und damit den Personendatentransfer von der EU in die USA als nicht mehr datenschutzrechtlich sicher erklärt hat. Verlangt wird neu ein zusätzlicher vertraglicher Schutz, der sich bei den Unternehmen vor allem in höheren Kosten und Mehraufwand niederschlägt.

Die Auswirkungen des Schrems-II-Urteils sind auch in der Schweiz spürbar: Zwar ist das Swiss–US Privacy Shield solange gültig, bis es höchstrichterlich für nichtig erklärt wird. Dennoch ist die Stellungnahme des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB), wonach das Swiss–US Privacy Shield ebenfalls keinen genügenden Schutz für den Datentransfer von der Schweiz in die USA bieten soll, gegebenenfalls richtungsweisend für einen künftigen Gerichtsentscheid zum Swiss–US Privacy Shield. Insofern sind Schweizer Unternehmen, die Personendaten in die USA übermitteln, angehalten, die Lage zu beobachten und gegebenenfalls frühzeitig Massnahmen zu ergreifen.

4

4.2 VERGLEICH DER MELDEPFLICHTEN SCHWEIZ–EU

Die Kenntnis der vorhandenen Datenschutzkategorien im Unternehmen hilft bei der Beurteilung, wo Meldepflichten im Falle einer Sicherheitsverletzung verlangt sind. Als Präventivmassnahme und um die Kosten nach einem Data Breach möglichst gering zu halten, empfiehlt es sich, gewisse Vorbereitungen für das Eintreffen eines Data Breach zu treffen.

	AKTUELLE RECHTSLAGE SCHWEIZ **Bundesgesetz über den Datenschutz (DSG)** In Kraft: 1. Juli 1993 (1. Revision 2008)	**ZUKÜNFTIGE RECHTSLAGE SCHWEIZ** **Revidiertes DSG** In Kraft frühestens 2022 (2. Revision)
Datenkategorien und damit verbundene Meldepflichten	– **Personendaten (natürliche und juristische Personen)** – **Besonders schützenswerte Personendaten** Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Daten über die Gesundheit, Intimsphäre oder Zugehörigkeit zu Rasse oder Ethnie; Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen; Daten über Massnahmen der sozialen Hilfe.	– **Personendaten (Revidiertes DSG Art. 5 lit. a)** – **Besonders schützenswerte Personendaten (Revidiertes DSG Art. 5 lit. c)** Daten über religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten; Daten über die Gesundheit, Intimsphäre oder Zugehörigkeit zu Rasse oder Ethnie; genetische Daten; biometrische Daten, die eine natürliche Person eindeutig identifizieren; Daten über verwaltungs- oder strafrechtliche Verfolgungen und Sanktionen; Daten über Massnahmen der sozialen Hilfe. – **Risikobasierter Datenschutz: Daten, bei deren Bearbeitung ein «hohes Risiko» für die Persönlichkeit oder Grundrechte der Betroffenen besteht.** Der E-DSG orientiert sich konsequent an den potenziellen Risiken für die Betroffenen, weil die Privatsphäre der Betroffenen weitgehend von den Aktivitäten der Verantwortlichen und Auftragsverarbeiter abhängt. Es wird unter anderem von einem hohen Risiko ausgegangen, wenn ein Unternehmen zu einer Datenschutz-Folgeabschätzung verpflichtet wird; beispielsweise bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten oder wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.
Meldepflicht	**Keine** ausdrückliche gesetzliche Meldepflicht.	**Meldepflicht bei Verletzung der Datensicherheit,** die voraussichtlich zu einem **«hohen Risiko»** für die Persönlichkeit oder Grundrechte des Betroffenen führt **(Revidiertes DSG Art. 24).** – **Meldepflicht des Verantwortlichen:** Meldung so rasch als möglich an den eidgenössischen Datenschutzbeauftragten (EDÖB). – **Meldepflicht des Auftragsverarbeiters:** Meldung so rasch als möglich an Verantwortlichen. – **Meldepflicht des Verantwortlichen:** Meldung an betroffene natürliche Person, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt (Ermessensspielraum).
Rechtsfolgen bei Verstoss	**Strafrechtliche Sanktionen** Maximal CHF **10'000.-** Busse	**Keine Busse** nach Meldepflichtverletzung. **Haftung, Anspruch auf Schadenersatz der betroffenen Person oder weitere strafrechtliche Sanktionen ausserhalb der DSGVO möglich.**

Wichtig zu wissen:

1. Was ist geschehen? Welche Datenkategorien sind betroffen? 2. Wer ist intern für die Meldung zuständig?
3. An wen müssen wir melden? 4. Wie müssen wir melden? 5. Innerhalb von welcher Frist?

AKTUELLE RECHTSLAGE EU/EWR

EU-Datenschutzgrundverordnung (DSGVO)

In Kraft EU: 25. Mai 2018 / EWR: 20. Juli 2018

- **Personenbezogene Daten**
- **Besondere Kategorien personenbezogener Daten**
  Personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

- **Risikobasierter Datenschutz: Daten, bei deren Verlust ein hohes Risiko für die persönlichen Rechte und Freiheiten besteht.**
  Die DSGVO enthält keine Hinweise, in welchen Fällen kein hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen besteht, weshalb die Risikoabwägung anhand der potenziellen Auswirkungen der Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten vorzunehmen ist. Zum Beispiel bei Verletzung der Vertraulichkeit von Personendaten, die zu Schaden für den Betroffenen führt: Diebstahl von Login-Daten und Kaufhistorien von einem Anbieter, Kompromittierung von Gesundheits- oder Zahlungsdaten, Marketing-E-Mails werden so versandt, dass jeder Empfänger alle anderen Empfänger ebenfalls erkennen kann etc.

Meldepflicht bei Verletzung des Schutzes personenbezogener Daten (DSGVO Art. 33)

- **Meldepflicht des Verantwortlichen:** Meldung unverzüglich und möglichst innerhalb von 72 Stunden an die zuständige Aufsichtsbehörde.
- **Meldepflicht des Auftragsverarbeiters:** Meldung unverzüglich an Verantwortlichen.

Meldepflicht bei «hohem Risiko» für Rechte und Freiheiten der betroffenen Person

- **Meldepflicht des Verantwortlichen:** Meldung **unverzüglich** an betroffene Person.

Busse nach Verletzung der Meldepflicht (DSGVO Art. 83 IV)

Bussgeld von bis zu EUR 10 Mio. oder bis zu 2 Prozent des gesamten, weltweit erzielten konsolidierten Jahresumsatzes.

Haftung, Anspruch auf Schadenersatz der betroffenen Person oder weitere strafrechtliche Sanktionen ausserhalb der DSGVO möglich.

4

4.3 MIT EINEM MASSGESCHNEIDERTEN MASSNAHMENPLAN ZUR DSG-COMPLIANCE: MIT DEN GRUNDLAGEN BEGINNEN

4.4 BUSSENKATALOG IM REVIDIERTEN DSG

Das revidierte DSG beinhaltet einen ausgebauten strafrechtlichen Teil und zudem sind härtere Sanktionen bei Pflichtverletzungen der verantwortlichen Organe als im noch geltenden DSG vorgesehen. Die Bussen werden auf maximal CHF 250'000.- erhöht und richten sich primär an die fehlbare natürliche Person im Unternehmen (insbesondere Entscheidungsträger). Bei Bussen bis zu CHF 50'000.- kann ausnahmsweise das Unternehmen selbst zur Busse verurteilt werden.

Der eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) kann nur Empfehlungen, aber keine Bussen aussprechen. Die Bussenkompetenz liegt weiterhin bei den Kantonen. Es soll nur der Vorsatz, nicht die Fahrlässigkeit bestraft werden. Die Strafverfolgung verjährt nach fünf Jahren (revidiertes DSG 66).

Der nachfolgende Bussenkatalog gibt einen groben Überblick über die strafbaren Pflichtverletzungen.

MIT BUSSE BIS ZU CHF 250'000.- WERDEN PRIVATE PERSONEN BESTRAFT.

Art. 60: Verletzung der Informations-, Auskunfts- und Mitwirkungspflichten, wie ...
- Verletzung/Unterlassung der Informationspflichten gegenüber Betroffenen bei der Beschaffung von Personendaten (Art. 19)
- Verletzung/Unterlassung der Informationspflichten gegenüber Betroffenen bei automatisierten Einzelentscheidungen (Art. 21)
- Verletzung/Unterlassung des Auskunftsrechts gegenüber der betroffenen Person, indem vorsätzlich falsche oder unvollständige Auskunft erteilt wird (Art. 25–27).
- Verstoss gegen die Mitwirkungspflichten, indem dem EDÖB im Rahmen seiner Untersuchung vorsätzlich falsche Auskunft erteilt oder vorsätzlich die Mitwirkung verweigert wurde (Art. 49 III).

Art. 61: Verletzung von Schweigepflicht, wie ...
- Verstoss gegen die Grundsätze bezüglich der Bekanntgabe von Personendaten ins Ausland (Art. 16 I, II)
- Verstoss gegen die Pflichten im Rahmen der Datenverarbeitung durch Auftragsverarbeiter (Art. 9 I, II)
- Nichteinhaltung der Mindestanforderung an die Datensicherheit (Art. 8 III)

Art. 62: Verletzung der beruflichen Schweigepflicht, wie ...
- Wer vorsätzlich geheime Personendaten offenbart, über die im Rahmen der Berufsausübung Kenntnisse erforderlich sind.
- Wer als Hilfsperson oder Auszubildende vorsätzlich geheime Personendaten von einer geheimhaltungspflichtigen Person erfährt und diese offenbart.

Art. 63: Missachten von Verfügungen
- Wer einer durch den EDÖB ergangenen Verfügung oder einem Entscheid der Rechtsmittelinstanzen vorsätzlich nicht Folge leistet.

MIT BUSSE BIS ZU CHF 50'000.- KANN DER GESCHÄFTSBETRIEB BESTRAFT WERDEN (ART. 64).

4

4.5 EXKURS: DATENSCHUTZGESETZE USA

EIN RECHTLICHER FLICKENTEPPICH

In den USA gibt es kein allumfassendes Datenschutzgesetz; dies im Gegensatz zur Schweiz mit dem DSG oder der EU mit der DSGVO. Vielmehr gibt es in den USA diverse Datenschutzgesetze auf nationaler, bundesstaatlicher sowie regionaler Ebene, welche die Daten natürlicher Personen schützen. Zusätzlich oder anstelle kann je nach Themengebiet eines oder mehrere der über 20 sektorspezifischen Datenschutzgesetze beispielsweise im Bereich Finanzen, Gesundheit oder Handel zur Anwendung gelangen. Wie diese Gesetze untereinander in Konkurrenz stehen, ist in jedem Einzelfall zu prüfen.

Im Gegensatz zur Schweiz und der EU stellt der Datenschutz in den USA kein Grundrecht dar, sondern ist Teil des Verbraucherschutzrechtes. Dies ist der Grund, weshalb die datenschutzrechtliche Aufsicht in den USA der Federal Trade Commission zukommt, welche auch für die wettbewerbs- sowie verbraucherschutzrechtliche Aufsicht zuständig ist. Eine unabhängige Datenschutzbehörde wie in der Schweiz oder EU gibt es in den USA nicht.

DATA BREACH NOTIFICATION

Data Breach Notification Laws gibt es in allen 50 US-Staaten. Im Falle eines Datenverlusts oder einer versehentlichen Veröffentlichung von Daten ist das Unternehmen, das von einer solchen Verletzung betroffen ist, verpflichtet, die Regierungen der betroffenen Bundesstaaten davon in Kenntnis zu setzen.

KALIFORNIEN IST IM BEREICH DATA PROTECTION LAW FEDERFÜHREND

Von allen 50 Bundesstaaten setzte Kalifornien 2002 als erster Staat ein Gesetz über die Meldung von Sicherheitsverletzungen (California Civil Code § 1798.82) in Kraft und wurde mit dem California Consumer Privacy Act von 2018 (CCPA, in Kraft seit 1.1.2020) zum Vorbildstaat bezüglich Datenschutzrecht. Der Anwendungsbereich des CCPA beschränkt sich auf den Bundesstaat Kalifornien und räumt Verbrauchern das Recht ein, auf personenbezogene Daten im Besitz von Unternehmen zuzugreifen und diese zu löschen. Darüber hinaus verpflichtet dieses Gesetz die Unternehmen, den Verbrauchern eine angemessene Sicherheit der Daten zu gewährleisten. Aufgrund der extraterritorialen Wirkung können auch Unternehmen ohne physische Präsenz in Kalifornien in den Anwendungsbereich des CPPA fallen.

1. Voraussetzungen Geltungsbereich des CCPA

- Sammeln von persönlichen Informationen von in Kalifornien ansässigen Personen; und
- Unternehmen ist in Kalifornien geschäftstätig; und
- Alternativ: Umsatz $ 25 Mio./Jahr oder Bearbeitung Daten von mehr als 50'000 Personen oder Geräten oder mehr als 50 % des Jahresumsatzes wird durch den Verkauf von Verbraucherdaten generiert.

2. Risiken für Unternehmen

Bussen zwischen $ 2'500 und $ 7'500; Konfrontation mit zivilen Sammelklagen und Schadenersatzzahlungen zwischen $ 100 und $ 750 pro betroffenen Verbraucher pro Vorfall oder tatsächlichen Schaden, je nachdem, welcher Betrag höher ist; Rechtsverfahren auch als ausländisches Unternehmen, sofern vom CCPA erfasst.

3. Wirksamkeit des CCPA

Die Wirksamkeit wird in Frage gestellt, weil es beispielsweise keine obligatorischen Sicherheitsverfahren sowie keine Sanktionen bei Nichteinhaltung gibt und die Geldstrafen insbesondere im Vergleich zur DSGVO gering ausfallen.

5 VERSICHERBARKEIT VON CYBER-RISIKEN

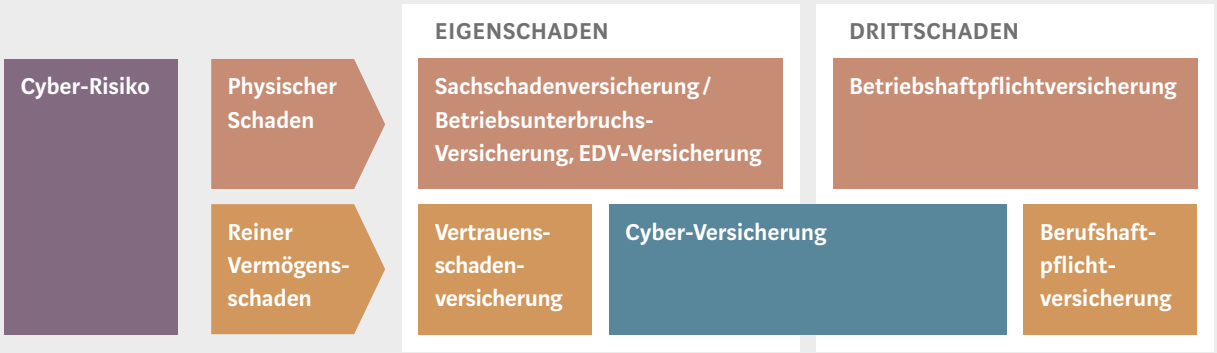
Die Versicherung von Cyber-Risiken stellt die Versicherungswirtschaft vor neue Herausforderungen. Risiken wie Feuer, Sach und Betriebsunterbrechung unterliegen einer natürlichen Risikoverteilung. Es ist unwahrscheinlich, dass am gleichen Tag Hunderte von Grossbränden in der Schweiz auftreten. Ein Cyber-Risiko kann sich jedoch viral verbreiten und gleichzeitig viele Unternehmen schädigen. Das führt bei Versicherern zu einem schwierig zu kalkulierenden Kumulrisiko, bei welchem mehrere beim gleichen Versicherer versicherte Ereignisse durch ein einziges Schadenereignis betroffen sein können.

Die Versicherungswirtschaft hat deshalb spezielle Cyber-Versicherungspolicen entwickelt, die wesentliche Komponenten des Cyber-Risikos eines Unternehmens abdecken können. Indem die Versicherer das Cyber-Risiko in einer separaten Versicherungslösung mit eigenem Underwriting-Prozess konzentrieren, entwickeln sie ein fundiertes Risikoverständnis. Die Kunden wiederum erhalten eine umfangreiche und auf das Cyber-Risiko fokussierte Versicherungslösung.

Um das Kumulrisiko besser kontrollieren zu können, haben die Versicherer in jüngster Vergangenheit zudem begonnen, für konventionelle Versicherungspolicen keinen oder nur einen eingeschränkten Versicherungsschutz für Cyber-Risiken anzubieten. Trotz dieser Entwicklung ist der Deckungsumfang noch nicht in allen Policen transparent dargestellt. Es gibt weiterhin Verträge mit sogenannten stillschweigenden Deckungen (Silent Cyber). Deshalb bleibt die Koordination mit den traditionellen Versicherungspolicen anspruchsvoll und essenziell, um Deckungslücken möglichst zu vermeiden. Unsere Cyber-Fachspezialisten führen für unsere Kunden in jedem Fall eine umfassende Lückenanalyse (Gap-Analyse) durch.

Die nachfolgende Grafik zeigt eine mögliche Einordnung der Cyber-Versicherung in konventionelle Versicherungspolicen. Typischerweise deckt eine Cyber-Versicherung reine Vermögensschäden und kombiniert Eigen- sowie Drittschäden.

CYBER-RISIKO AUS DER SICHT DER VERSICHERUNGSINDUSTRIE



5

5.1 CYBER-VERSICHERUNG: VERSICHERBARE SCHÄDEN

Nicht alle Versicherer bieten unter den gleichen Deckungsbausteinen den gleichen Versicherungsschutz an. Aufgrund der Analyse des Cyber-Risikos Ihres Unternehmens schätzen wir die unterschiedlichen Angebote der Versicherer für Sie ein.

Die Grafik rechts zeigt den Deckungsumfang.

- Krisenmanagement umfasst die Service-Dienstleistungen des Versicherers, die über externe Partnerschaften im Bereich IT-Forensik, Rechtsberatung und PR-Beratung zur Verfügung gestellt werden.
- Der Bereich Versicherung beinhaltet Eigenschäden (beispielsweise Betriebsunterbruch und zusätzliche Kosten) sowie Drittschäden. Eigenschäden sind aufgrund eines Cyber-Vorfalls entstandene Kosten. Drittschäden stehen für die Übernahme von berechtigten Schadenersatzansprüchen sowie für die Abwehr unberechtigter Ansprüche.

In welchem Umfang die Anbieter die in der Grafik umschriebenen Ursachen sowie finanziellen Auswirkungen versichern, ist Bestandteil der von Kessler geführten Verhandlungen. Gleiches gilt für den Deckungsumfang im Bereich des IT-Outsourcings.

VERSICHERTE URSACHEN UND AUSWIRKUNGEN

KRIMINELLE URSACHEN

Hacker-Angriff, Ransomware (Erpressung), Phishing-Attacke

NICHT-KRIMINELLE URSACHEN

Menschliches Versagen, technisches Versagen

Ihr IT-System und Ihre Daten (inhouse oder outsourced)

Auswirkungen auf

Integrität und/oder **Verfügbarkeit** und/oder **Vertraulichkeit**

FINANZIELLE AUSWIRKUNGEN

Krisenmanagement, Eigenschäden, Drittschäden

In einer einfachen, tabellarischen Übersicht zeigen wir Ihnen die versicherten Ursachen und finanziellen Auswirkungen auf und gehen auf die verschiedenen Deckungsvoraussetzungen ein.

5

5.2 VERTRAUENSSCHADENVERSICHERUNG

Für die Assekuranz sind reine Vermögensschäden aus Social Engineering keine eigentlichen Cyber-Risiken, da die Vorgehensweise der Täter keinen Eingriff in das IT-System bedingt. Eine Vertrauensschadenversicherung kann diese Risiken auffangen.

Während die Cyber-Versicherung jegliche Hacker-Angriffe als versicherte Ursache anerkennt, sind nicht alle daraus resultierenden finanziellen Auswirkungen versichert. Ein bekanntes Beispiel sind Delikte im Bereich von Social Engineering: Nach einem Phishing-Angriff erforderliche Datenwiederherstellungskosten aus der Verbreitung von Viren sind unter einer Cyber-Versicherung versichert. Der direkte Vermögensschaden in Form einer fingierten Banküberweisung hingegen ist nicht oder nur beschränkt versichert. Dafür gibt es zwei Gründe.

Erstens erfolgt die Mehrheit dieser Angriffsformen ohne Eingriff in ein IT-System, sondern lediglich mittels E-Mails mit gefälschten Absenderadressen. Darin melden Geschäftspartner Änderungen bei den Bankverbindungen oder in vermeintlichen Benachrichtigungen von Banken wird mit einem Link dazu aufgefordert, die Zugangsdaten zu aktualisieren. In anderen Fällen melden sich Angreifer telefonisch und geben sich als Kunde, IT Support oder CEO aus. Zweitens existiert mit der Vertrauensschadenversicherung aus Sicht des Versicherungsmarkts bereits eine Versicherungslösung, welche die Bilanz der Gesellschaft gegen IT-basierte, strafbare Handlungen schützt und die reinen Vermögensschäden daraus versichert.

Es lohnt sich daher, genau zu prüfen, ob der Versicherungsbedarf auch eine separate Vertrauensschadenversicherung umfasst. Denn Arbeiten im Homeoffice und die damit einhergehenden Änderungen der Arbeitsabläufe und Zugangsberechtigungen zu den IT-Systemen der Unternehmen begünstigen die IT-basierten, strafbaren Handlungen stark. Aber nicht alle Policen versichern solche Schäden. Denn das versicherte Hauptrisiko ist die unrechtmässige persönliche Bereicherung durch einen Mitarbeitenden.

5.3 SACH- UND BETRIEBSUNTERBRECHUNGSVERSICHERUNG UND TECHNISCHE VERSICHERUNG

Die Sachversicherer haben auf die zunehmenden Cyber-Schadenfälle reagiert und ihre Bedingungen angepasst oder präzisiert. Die heutigen Policen enthalten keine Silent-Cyber-Deckungen mehr, also keine Unklarheiten darüber, was versichert ist und was nicht. Der Versicherungsschutz für Cyber-bezogene Sachschäden wird in der Police explizit beschrieben. Die Umsetzung von Versicherer zu Versicherer ist dabei stark heterogen.

Generell gilt, dass ein physischer Sachschaden vorliegen muss, welcher dann kausal für einen Betriebsunterbrechungsschaden sein muss. Daten selber stellen keine Sache dar und können daher auch nicht im Sinne dieser Versicherung «beschädigt» werden. Wird jedoch der Datenträger, auf dem sich die Daten befinden, beschädigt oder zerstört, zum Beispiel durch ein Feuer, dann werden die Kosten für das Wiederherstellen von Daten aus einem Back-up erstattet. Aber die Daten selber werden nicht entschädigt.

Ein gezielter Cyber-Vorfall kann zum Beispiel ein Feuer auslösen, welches eine IT-Anlage, eine Produktionsmaschine oder auch ein Gebäude zerstört. Das wiederum kann im schlimmsten Fall zu einer Betriebsunterbrechung führen. In diesem Fall übernimmt die Sach- und Betriebsunterbrechungsversicherung den Schaden, da ein Sachsubstanzschaden durch das Feuer verursacht worden ist.

Gleich verhält es sich, wenn ein wichtiger Zulieferer ausfällt. Das kann zum Beispiel der Stromlieferant sein oder der IT-Dienstleister. Es muss dort ein Sachschaden entstanden sein, welcher unter der eigenen Police im Rahmen der Rückwirkungsschadendeckung versichert ist. So muss der Grund für den Stromunterbruch oder den Ausfall des IT-Dienstleisters zum Beispiel ein Feuer sein. Die blosse Nichtverfügbarkeit von Strom oder Daten aufgrund eines Cyber-Vorfalls, welcher zum Beispiel wichtige Daten verschlüsselt hat, stellt keinen Sachschaden dar.

Daneben gibt es noch die technischen Versicherungen, unter welche die Elektronik- und Maschinenversicherung fallen. Zwar sind hier typischerweise die versicherten Ereignisse aufgrund des All-Risks-Ansatzes ein wenig weiter gefasst, aber auch hier gilt die generelle Voraussetzung, dass es einen physischen Sachschaden geben muss. Somit fällt das reine Nichtfunktionieren einer IT-Anlage oder einer Maschine aufgrund eines Cyber-Vorfalls nicht unter den Versicherungsschutz.

6
VOM CYBER-VORFALL ZUM CYBER-VERSICHERUNGSFALL

Jede vierte Cyber-Versicherung ist schadenbelastet. Damit steigt auch die Lernkurve bei betroffenen Unternehmen und Experten. Die Versicherer haben das Krisenmanagement und die Schadenabwicklung laufend verbessert und können den Versicherungsnehmern heute die Wirkung von Präventivmassnahmen aufzeigen. Kessler begleitet Sie während des gesamten Prozesses, um eine effiziente Schadenabwicklung zu gewährleisten.

VOR EINTRITT

CYBER-VORFALL

Cyber-Risk-Management-Prozess ausarbeiten
- Identifizieren, schützen, detektieren, reagieren und kontinuierliche Überwachung gewährleisten
- Haftungsklausel in Verträgen mit Kunden, Lieferanten und IT-Dienstleistern prüfen
- Abhängigkeiten von Lieferanten und IT-Dienstleistern prüfen
- Präventivmassnahmen wie Awareness-Trainings für Mitarbeitende umsetzen
- Bewusster Entscheid bezüglich Eigen- oder Fremdfinanzierung von Cyber-Vorfällen treffen

Incident Response Plan, Business Interruption Plan und Disaster Recovery Plan erstellen
- Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung definieren
- Situation, dass IT-Systeme für einige Tage oder Wochen nicht verfügbar oder nicht vertrauenswürdig sind, üben und alternative Kommunikationskanäle aufsetzen
- Pläne regelmässig testen und Ergebnisse auswerten

CYBER-VERSICHERUNGSFALL

Vorbereitende Massnahmen
- Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung definieren, vertraglich binden und Onboarding Meeting durchführen

Versicherungspolice kennen
- Notfallnummer den involvierten Personen mitteilen
- Vertragliche Obliegenheiten einhalten (beispielsweise Meldepflichten bei Gefahrerhöhungen)

	CYBER-VORFALL	CYBER-VERSICHERUNGSFALL
WÄHREND	**Eintritt Cyber-Risiko** – Datenverlust – IT/ICT-Störung – Cyber-Kriminalität/E-Crime **Sofortmassnahmen** – Incident Response Plan konsultieren – Definierte Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung konsultieren – Definierte Massnahmen einleiten und koordinieren (siehe auch Meldungen) – Laufende Dokumentation des Cyber-Vorfalls zu Verlauf und Kosten sicherstellen **Meldungen** – Gesetzliche Meldepflichten oder freiwillige Meldung gegenüber Behörden und Betroffenen prüfen – Polizei zwecks Beweissicherung einbeziehen – Benachrichtigung von Mitarbeitenden, Medien und/oder Ad-hoc-Publizität prüfen	**Sofortmassnahmen** – Notfallnummer wählen: Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung werden konsultiert – Cyber-Vorfall umgehend Kessler und/oder Versicherer melden und enge Zusammenarbeit fortführen **Weitere Massnahmen** – Ausgaben vom Versicherer vorgängig genehmigen lassen – Schadenminderungspflichten einhalten – Sachverständiger für Schadenquantifizierung früh definieren und einbeziehen – Fallabwicklung mit Versicherer: Dokumente zur Sachverhaltsbeurteilung und Deckungsprüfung einreichen; mögliche Akontozahlung erzielen
DANACH	**Lessons Learned** – Leistung der involvierten Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung validieren – Incident Response Plan, Business Interruption Plan und Disaster Recovery Plan überprüfen	**Lessons Learned** – Leistung des/der Versicherer(s) sowie der involvierten Experten aus den Bereichen IT-Forensik, Rechtsberatung und PR-Beratung validieren – Gewählte Versicherungssumme und Selbstbehalte überprüfen

7
DER ZWEI-PHASEN-PROZESS

Für Ihre individuelle Cyber-Versicherungslösung begleitet Sie das Cyber Team, das auf Cyber Risk Management und Cyber Insurance spezialisiert ist. Es verfügt über breites Fachwissen und hat entsprechende Praxiserfahrung. Mit unserem Netzwerkpartner Marsh, der weltweit Cyber-Versicherungslösungen entwickelt, stehen wir im Interesse unserer Kunden in regem Austausch. Für Ihre Cyber-Versicherungsbedürfnisse empfehlen wir einen Zwei-Phasen-Prozess, wobei auch der direkte Einstieg in die Phase 2 möglich ist.

7.1 ERSTE PHASE: CYBER-RISIKO-DIALOG

Im Rahmen des Risk Managements und zur Unterstützung einer optimalen Corporate Governance Ihres Unternehmens besprechen wir mit Ihnen zusammen Ihre unternehmens- und branchenspezifischen Cyber-Risiken, die damit zusammenhängenden internen Organisations- und Informationsprozesse sowie die sich stets verändernden rechtlichen Aspekte insbesondere der Schweiz, der EU und der USA. Dies dient uns als Basis, um die weiteren Schritte zu planen.

7.2 ZWEITE PHASE: EINHOLUNG VON VERBINDLICHEN OFFERTEN

Wir empfehlen, mit drei führenden Anbietern die Verhandlungen aufzunehmen. Nach Erhalt des Cyber-Versicherung-Antragsfragebogens werden wir zusammen den gewünschten Versicherungsumfang festlegen und die Ausschreibung beginnen. Die gewählten Versicherer benötigen vorgängig zur Offertphase auf Ihr Unternehmen zugeschnittene Informationen zum Aufbau des Unternehmens und Geschäftsumfeld, zur IT-Organisation, zur Maturität der IT-Sicherheit sowie zum Risk Management. Diese Informationen werden in der Regel mündlich mittels Präsentation oder Telefonkonferenz übermittelt. Danach erfolgen individuelle Verhandlungen.

Anschliessend erstellen die Versicherer verbindliche Angebote. Die Resultate werden darauf im Kessler-Ausschreibungsbericht zusammengefasst und mit Ihnen persönlich besprochen. Damit liegen die Grundlagen für den Entscheid zum Abschluss einer Cyber-Versicherung vor. Die Abwägung von Kosten und Nutzen einer Cyber-Versicherung ist ein Entscheid über die Art der Risikofinanzierung. Damit sind unseres Erachtens auch die Anforderungen der Corporate Governance (Business Judgement Rule) erfüllt, das Risiko «Cyber» bewusst in den Risk-Management-Prozess der Unternehmung integriert zu haben.

ZWEI-PHASEN-PROZESS – MIT AUSFÜHRLICHEM RISIKO-DIALOG ZUM BEWUSSTEN ENTSCHEID

ÜBER KESSLER

Kessler ist das führende Schweizer Unternehmen für ganzheitliche Risiko-, Versicherungs- und Vorsorgeberatung. Wir betreuen über 1'000 mittlere und grosse Schweizer Unternehmen aus Dienstleistung, Handel und Industrie sowie der öffentlichen Hand. Dank unserer Expertise in den einzelnen Wirtschaftsbranchen, unseren qualifizierten Mitarbeitenden und unserer führenden Marktstellung leisten wir einen wesentlichen Beitrag zum nachhaltigen Erfolg unserer Kunden. Als verlässlicher Partner begeistern wir sie und eröffnen ihnen durch den sicheren Umgang mit Risiken neue Perspektiven. Gegründet 1915, beschäftigt Kessler heute 300 Mitarbeitende am Sitz in Zürich und an den Standorten Basel, Bern, Genf, Lausanne, Luzern, Neuenburg, St. Gallen und Vaduz. Als Schweizer Partner von Marsh sind wir seit 1998 Teil eines Netzwerks mit Spezialisten aus allen Gebieten des Risk Management und mit grosser Erfahrung in der Betreuung globaler Versicherungsprogramme. Marsh ist in über 130 Ländern vertreten und der weltweit führende Versicherungsbroker und Risikoberater und Teil von Marsh & McLennan (NYSE: MMC).

Weitere Informationen finden Sie unter
www.kessler.ch, www.marsh.com, www.mmc.com.

KESSLER & CO AG
Forchstrasse 95
Postfach
CH-8032 Zürich
T +41 44 387 87 11
www.kessler.ch