KESSLER

CYBER RISK SURVEY REPORT 2019
CYBER RISK AUS SCHWEIZER SICHT

MIT SICHERHEIT VORAUS.

CYBER RISK SURVEY REPORT 2019
CYBER RISK AUS SCHWEIZER SICHT

1 VORWORT

INDUSTRIE 4.0 WIRD ALLTAG

Insbesondere in der Fertigungsindustrie setzen die Unternehmen zunehmend Komponenten des Internet of Things ein. Dadurch verändern sich die künftigen Sicherheitskonzepte. Die vom Internet of Things ausgehenden Gefahren werden aktuell unterschätzt. Automatisierte Kaffeemaschinen, smarte Lampen oder Kopierer können Einfallstore ins Firmennetzwerk darstellen. Es will wohl niemand behaupten, dass smarte Kaffeemaschinen sicherer sind, als eine von Profis entwickelte Unternehmenssoftware. Cyber Risk Management beinhaltet unter anderem, die betrieblichen Schwachstellen zu kennen, um die Kronjuwelen des Unternehmens zu schützen bzw. die Unternehmensziele erfolgreich zu erreichen.

SUPPLIER CYBER RISK MANAGEMENT

Die Abhängigkeit von IT-Zulieferern wird tendenziell noch stiefmütterlich behandelt. Daten und Prozesse werden aus verschiedenen Gründen ausgelagert. Leider können wir die Verantwortlichkeit für integre, vertrauliche und verfügbare Kundendaten nicht vollständig abgeben. Haftungsfragen sind im internationalen Kontext noch komplexer, als sie bereits im nationalen Geschäftsumfeld sind. Die heute vielfach internationale Wertschöpfungskette verlangt von den Unternehmen deshalb grösste Disziplin hinsichtlich Transparenz ihrer Abhängigkeiten. Transparenz schafft Verständnis für die Cyber-Risikoexponierung im Zusammenhang mit der Supply Chain.

UNSERE UMFRAGE

Im September 2018 haben wir eine schweizweite branchenübergreifende Umfrage durchgeführt, welche den Umgang von Unternehmen mit Cyber-Risiken und deren Gefahrenpotenzial im Geschäftsalltag sowie den damit zusammenhängende Datenschutzrisiken untersucht hat. Wir haben alle unsere international tätigen Kunden sowie weitere international agierende Unternehmen zur Teilnahme am «Cyber Risk Survey Report 2019 – Cyber Risk aus Schweizer Sicht» eingeladen. Die Ergebnisse der 387 Antworten haben wir nun für Sie ausgewertet und die wichtigsten Ergebnisse kommentiert.

DIE SCHWEIZ IST KEINE SCHUTZZONE

Die Resultate des nachfolgenden Reports bestätigen erneut: Auch Schweizer Unternehmen sind Ziele von Cyber-Kriminellen. Gefährlich scheint mir der Gedanke, aus den vergangenen Jahren, in denen die Schweiz von für die Gesellschaft einschneidenden Cyber-Schäden verschont blieb, auf die Zukunft zu schliessen. Zu undurchschaubar gestalten sich die weltweiten Cyber Incidents, zu unberechenbar die damit verfolgten Ziele.

Wir wünschen Ihnen eine kurzweilige Lektüre und freuen uns, Ihre neu gewonnenen Cyber-Einsichten mit Ihnen zu diskutieren.

Melanie Koller
Legal Counsel Cyber Risk

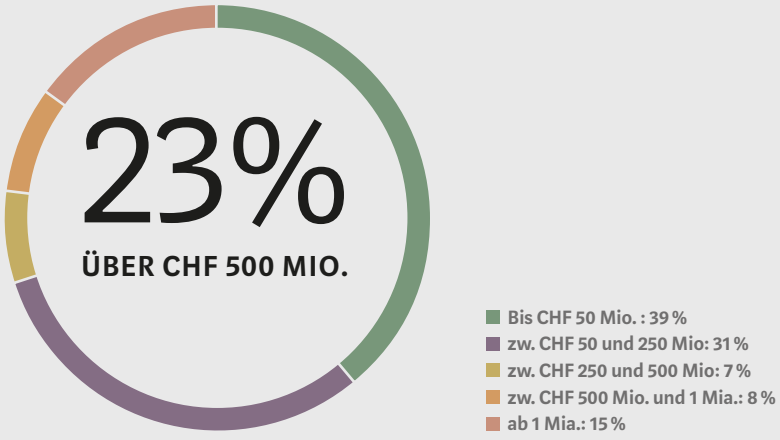
2
ÜBER DEN REPORT

Dieser Report basiert auf den Umfrageergebnissen von Kessler über den Umgang mit Cyber-Risiken unserer Kunden vom September 2018. Auf den folgenden Seiten finden Sie die wichtigsten Erkenntnisse aus Schweizer Sicht zusammengefasst und kommentiert.

An der Cyber-Risiko-Umfrage haben schweizweit 387 international tätige Unternehmen teilgenommen. Dabei wurden die Fragen zu 29 % von Geschäftsleitungsmitgliedern oder von Verwaltungsräten beantwortet; die restlichen 71 % der beantworteten Fragebogen wurden von Personen im Finanz-, Risk Management, IT-, HR- und Legal-Bereich eingereicht.

70 % der befragten Unternehmen generieren einen jährlichen Umsatz von bis zu CHF 250 Mio., während 7 % einen Umsatz in der Höhe von zwischen CHF 250 Mio. und 500 Mio. erwirtschaften. Die restlichen 23 % der Unternehmen erzielen einen Jahresumsatz über CHF 500 Mio.

UNTERNEHMENSGRÖSSE NACH UMSATZ



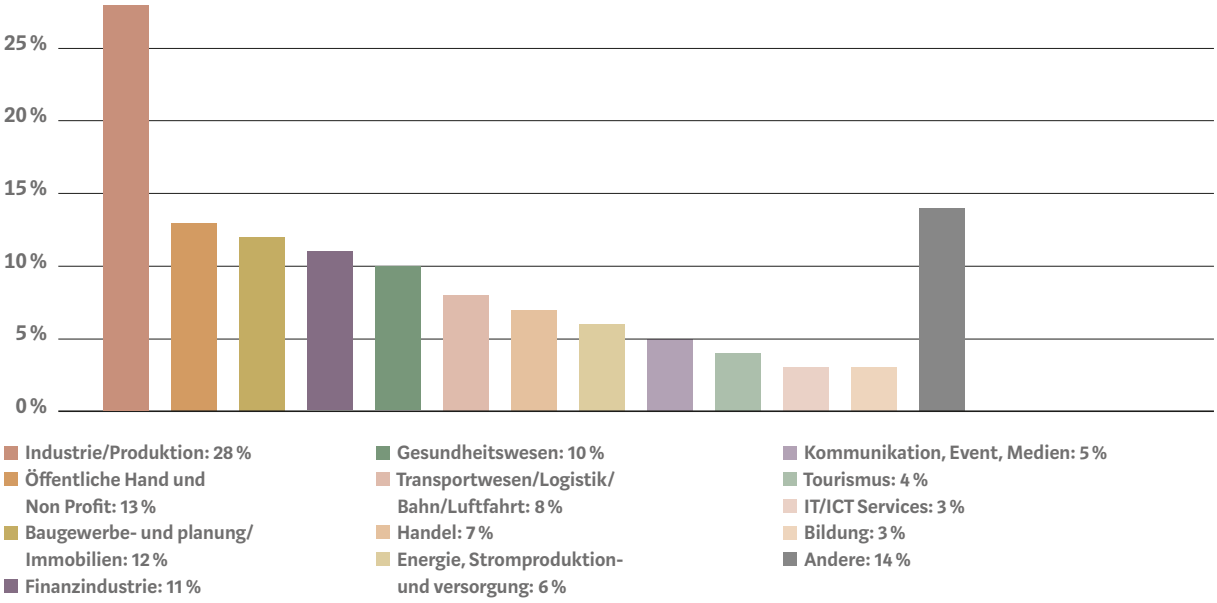
Mit über einem Viertel ist die Industrie- und Produktionsbranche am stärksten vertreten. Das Interesse dieser Branche an der Umfrageteilnahme erstaunt uns nicht. Der in dieser Branche gefürchtete cyberbedingte Betriebsunterbruch weckt das Interesse, den Cyber-Risiken auf den Grund zu gehen.

Zu den wichtigsten Absatzmärkten der Umfrageteilnehmer gehören nebst Kontinentaleuropa vor allem USA/Kanada, Asien sowie der nahe Osten.

Eine grosse Aussagekraft hat, wie bereits letztes Jahr, die ausserordentlich starke Abhängigkeit der Umfrageteilnehmer von digitalen Hilfsmitteln und externen IT-Dienstleistern (Textbox S. 8). Im Vergleich zum letztjährigen Kessler Cyber Risk Report fallen die genannten Abhängigkeiten grundsätzlich ähnlich aus. Eine auffallend gesteigerte Cyber Risk Awareness erkennen wir allerdings darin, dass deutlich weniger Unternehmen ihren Mitarbeitenden und Dritten erlauben, ihre eigenen mobilen Geräte am Unternehmensnetzwerk anzuschliessen. Diese Entwicklung bestätigen auch unsere tagtäglichen Kundengespräche.

2

BRANCHENZUGEHÖRIGKEIT



ABHÄNGIGKEITEN DER UMFRAGETEILNEHMER VON DIGITALEN HILFSMITTELN UND DIENSTLEISTUNGEN

- Ein oder mehrere Computer sind mit dem Internet vernetzt: 97 %(2017: 98 %)
- Elektronische Verarbeitung und Speicherung von Mitarbeiterakten: 71 % (2017: 88 %)
- Mitarbeitende und/oder Vertragspartner können ihren Laptop und/oder ihre mobilen Geräte am Unternehmensnetzwerk anschliessen: 63 % (2017: 87 %)
- Elektronische Speicherung und/oder Verwaltung von Kundendaten: 76 % (2017: 86 %)
- Elektronische Verarbeitung von Bankinformationen: 78 % (2017: 75 %)
- Elektronische Speicherung von Lieferanteninformationen: 67 % (2017: 74 %)
- Cloud-Services: 52 % (2017: 54 %)
- Verwalten von individuell identifizierbaren privaten Gesundheitsinformationen von Mitarbeitenden oder Kunden: 25 % (2017: 31 %)
- Elektronische Abwicklung von Kreditkartentransaktionen: 32 % (2017: 28 %)
- Erfassung personenbezogener Daten (inkl. Cookies und ähnliche Instrumente) auf einer Webseite: 26 % (2017: 25 %)
- Weitergabe von Personendaten an Lieferanten oder andere Drittparteien: 27 % (2017: 24 %)

3
ERKENNTNISSE UND KOMMENTARE

3.1 BEWUSSTSEIN FÜR CYBER-RISIKEN STEIGT MARKANT

Cyber-Risiken haben nicht zuletzt infolge der seit Monaten omnipräsenten EU-DSGVO die Aufmerksamkeit des Verwaltungsräte und der Geschäftsführung erreicht. In Anbetracht des Schadenausmasses wird allerdings nach wie vor zu wenig unternommen. Awareness ist eine Sache – getroffene Massnahmen eine andere.

Die diesjährigen Umfrageergebnisse bestätigen einmal mehr, dass Cyber-Risiken im Risikoregister der befragten Unternehmen zu den grössten Risiken gehören (Grafik 1). 76 % der Schweizer Unternehmen zählen Cyber-Risiken zu den Top 10 Unternehmensrisiken, 39 % der Befragten sogar zu den Top 5. Dennoch: Cyber-Risiken sind nicht die einzigen Risiken, die unsere Kunden 2017 und 2018 beschäftigt haben. Nebst dem Handelskrieg zwischen den USA und China, der für viele Branchen grosse Beeinträchtigungen mit sich bringt, sorgten 2018 auch der Brexit sowie neue Rechtsakte, wie die EU-DSGVO für viel Instabilität und Unsicherheit bei den Unternehmen.

Cyber-Risiko-Awareness alleine reicht nicht aus, wenn es darum geht, diese doch noch intransparenten Gefahrenherde anzupacken bzw. zu minimieren. Aus verantwortlichkeitsrechtlichen Gründen im Sinne von OR 754, sind auch nichtrevisionspflichtige Unternehmen gut beraten, ihre Cyber-Risiko-Exponierung im Lagebericht gemäss OR Art. 961c zu dokumentieren sowie entsprechende Präventivmassnahmen in die Wege zu leiten. Awareness alleine reicht nicht aus.

GRAFIK 1

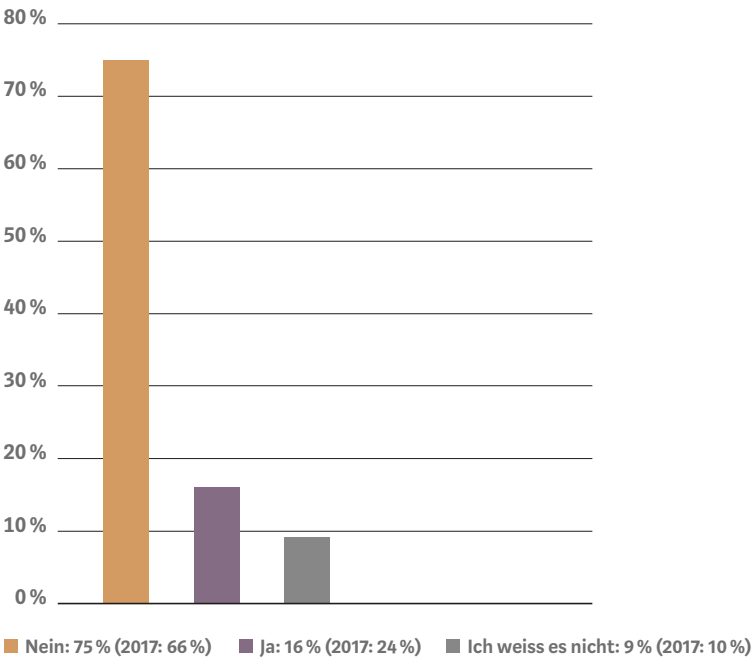
Welchen Stellenwert haben Cyber-Risiken in Ihrem Unternehmen?

- Cyber-Risiken sind gemäss Risikoregister unsere grössten Risiken: 5 % (2017: 3 %)
- Cyber-Risiken gehören zu den Top 2-5 im Risikoregister: 34 % (2017: 56 %)
- Cyber-Risiken gehören zu den Top 6-10 im Risikoregister: 37 % (2017: N/A)
- Cyber-Risiken gehören nicht zu den Top 10 Risiken: 20 % (2017: N/A)
- Cyber-Risiken haben keinen Stellenwert: 0 % (2017: 1 %)
- Ich kenne den Stellenwert der Cyber-Risiken in meinem Unternehmen nicht: 4 % (2017: 3 %)

Auf die Frage, ob das eigene Unternehmen in den letzten 12 Monaten Opfer einer Cyber-Attacke wurde, haben 75 % mit Nein, 16 % mit Ja und 9 % mit «ich weiss es nicht» geantwortet (Grafik 2). Dieses Resultat erstaunt nicht, denn gemäss neuen Erkenntnissen wird Schadsoftware (Malware) weltweit in der Regel erst nach 99 Tagen entdeckt – wenn überhaupt: In Europa wird Malware bspw. durchschnittlich nach 106 Tagen, im mittleren Osten, Asien und Afrika hingegen erst nach 172 Tagen entdeckt. Insofern liegt erneut die Vermutung nahe, dass ein Teil dieser 75 % der Unternehmen, die im September 2018 mit Nein geantwortet haben, noch nicht bemerkt haben, dass sie in den letzten Monaten gehackt wurden. Dieses grosse Problem ist weltweit erkannt. Entsprechend stark wird an Möglichkeiten geforscht, die Entdeckungszeit einer eingeschleusten Malware massiv zu kürzen. Denn, je kürzer die Zeitspanne zwischen Einführung und Entdeckung einer Malware (sog. Breach Detection Gap oder Dwell Time), desto geringer sind die finanziellen Auswirkungen für die Unternehmen.

GRAFIK 2

Wurde Ihr Unternehmen in den letzten 12 Monaten Opfer einer Cyber-Attacke?



3

3.2 BEDEUTUNG DER CORPORATE GOVERNANCE

Letztlich können Organe persönlich für zu verantwortende Cyber-Schäden haften. Gerade deshalb liegt es an der Unternehmensführung und nicht an der IT-Abteilung sicherzustellen, dass ihre Betriebe gegen neue Cyber-Bedrohungen widerstandsfähig sind.

Im diesjährigen Report zeigen die Resultate ähnliche Ausprägungen wie bereits im Vorjahr: Nach wie vor trägt grösstenteils die IT die Verantwortung für das Cyber Risk Management (64 %). Das Management ist nur gerade bei 12 % der Befragten für die Cyber-Risiken zuständig. Diese Resultate bereiten uns Sorgen.

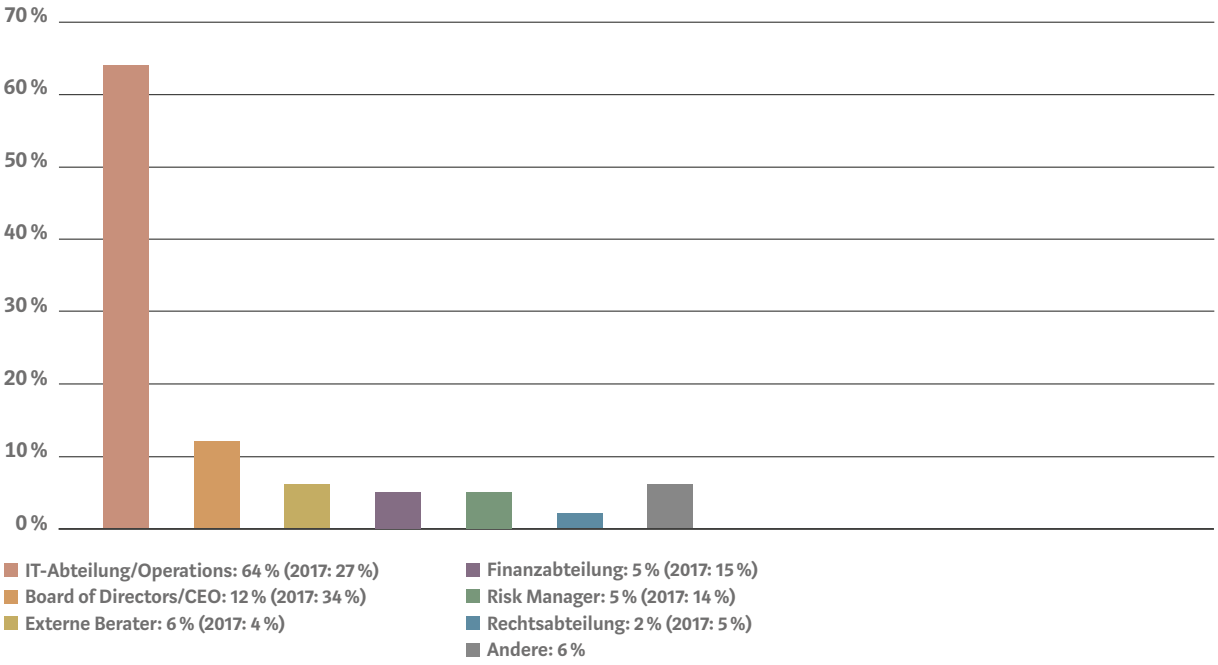
Um mit den neuen Technologien Schritt zu halten, müssen Unternehmen innovativ sein. Risiken und Chancen sind stets abzuwägen, richtige Sicherheitsvorkehrungen haben den erforderlichen Sicherheitsbedarf zur strategischen Erreichung der Unternehmensziele zu decken. Die EU-DSGVO hat zur grösseren Awareness der betrieblichen Cyber-Risiken beigetragen. Die Unternehmensführung, die im Zeitalter von Big Data, Industrie 4.0 und der künstlichen Intelligenz keinen bewussten strategischen und finanziellen Umgang mit Cyber-Risiken festlegt, wird im Cyber-Schadenfall mit unangenehmen Fragen konfrontiert werden.

Aus rechtlicher Sicht kann ein fehlendes oder mangelhaft durchgeführtes Cyber Risk Management unter Umständen als Sorgfalts- oder Treuepflichtverletzung im Sinne von OR 717 qualifiziert werden und möglicherweise zur Haftung von Organen nach OR 754 führen.

Unabhängig davon ist das Management gut beraten, seine top Firmenrisiken zu kennen und diese zu quantifizieren. Gemäss Murphy's Law, wonach alles schiefgeht, was schiefgehen kann, ist stets mit grossen Cyber-Zwischenfällen zu rechnen und damit ebenfalls deren Bewältigung mit Hilfe von Spezialisten sorgfältig zu planen.

GRAFIK 3

Welche der folgenden Funktionsbereiche ist für das Management von Cyber-Risiken in erster Linie verantwortlich?



GRAFIK 4

Sofern das Board of Directors/CEO für Cyber-Risiken zuständig ist, welche der nachfolgenden Berichte erhält es?

- Empfehlung bezüglich Cyber.Risikominimierung: 67 %
- Sensibilisierungsmassnahmen: 48 %
- Bericht über aufgetretene Probleme oder Vorkommnisse: 55 %
- Bericht über die Kontrolltätigkeiten (Patchen, Schulungen, Phishing-Status): 36 %
- Informationen über das Bedrohungsumfeld: 21 %
- Empfehlungen in Bezug auf die Cyber-Risikofinanzierungsstrategie: 12 %
- Ich weiss es nicht: 15 %

3

3.3 CYBER RISK MANAGEMENT: EIN INDIKATOR DER RISIKOAWARENESS

Es gibt kein richtiges oder falsches Cyber-Risk-Management. Jedes Unternehmen hat basierend auf seinem Kerngeschäft und den sich daraus ergebenden strategischen Zielen einen anderen Fokus im Umgang mit Cyber-Risiken. Falsch ist einzig, nichts zu tun. Awareness ist eine Sache, Implementierung erforderlicher Massnahmen eine andere. Im Cyber-Risk-Management gilt es, diese Lücke zu füllen.

Bereits 42 % der Umfrageteilnehmer haben die finanziellen Auswirkungen eines betrieblichen Cyber-Schadenereignisses quantifiziert (2017 waren es 58 %, 2016 waren es 41 %). Diese Resultate sind trotz der unsteten Entwicklung erfreulich und zeigen u.a. auf, dass die Cyber-Risiken zunehmend als ernst zu nehmende Unternehmensrisiken wahrgenommen werden (Grafik 5).

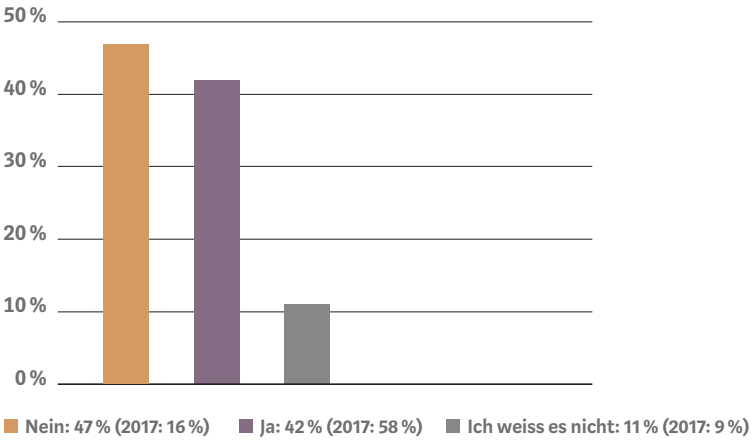
Quantifizieren Unternehmen Cyber-Vorfälle, werden die finanziellen Auswirkungen von 34 % der Befragten auf zwischen CHF 1 und 10 Mio. geschätzt (Grafik 6). Von Schäden über CHF 10 Mio. gehen 25 % der Befragten aus. Uns ist aufgefallen, dass diejenigen Unternehmen, die mit einem Cyber-Schaden von weniger als CHF 1 Mio. rechnen, zu 47 % Betriebe mit einem Umsatz von maximal CHF 100 Mio. sind.

Die Quantifizierung möglicher Cyber-Schadenereignisse, stellt nach wie vor eine der grössten Herausforderungen im Prozess dar. Nach wie vor fehlen verlässliche Erfahrungswerte. Zwar wären erste Schadenzahlen vorhanden, allerdings zeigen die Versicherer grosse Zurückhaltung selbst anonymisierte Schadendaten zu publizieren.

Wie zentral eine grobe Einschätzung des Cyber-Restrisikos sein kann, zeigt das im Herbst 2018 bekannt gewordene Beispiel der Cyber-Angriffe auf die Marriott-Hotelgruppe in den Jahren zwischen 2014 und 2018. Reine Benachrichtigungskosten im Zusammenhang mit gehackten sensiblen Personendaten wären relativ simpel zu berechnen. Umso mehr erstaunt es, dass die angeblich vorhandene Versicherungsdeckung nicht einmal für die grundlegenden Benachrichtigungskosten ausreicht.

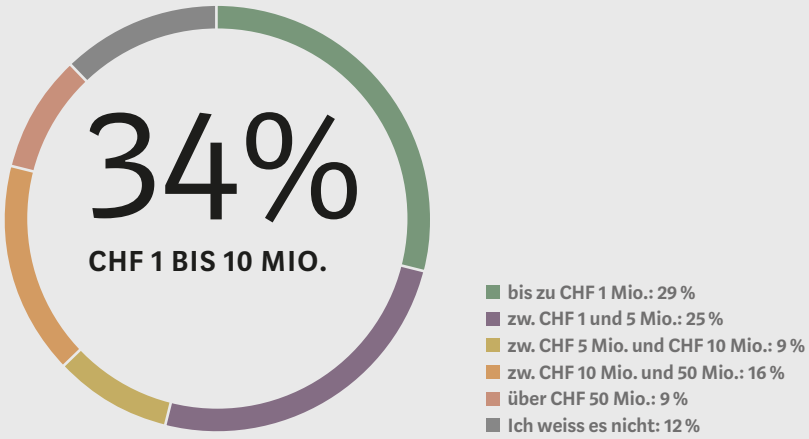
GRAFIK 5

Haben Sie die finanziellen Auswirkungen eines Schadenereignisses in Ihrem Unternehmen abgeschätzt?



GRAFIK 6

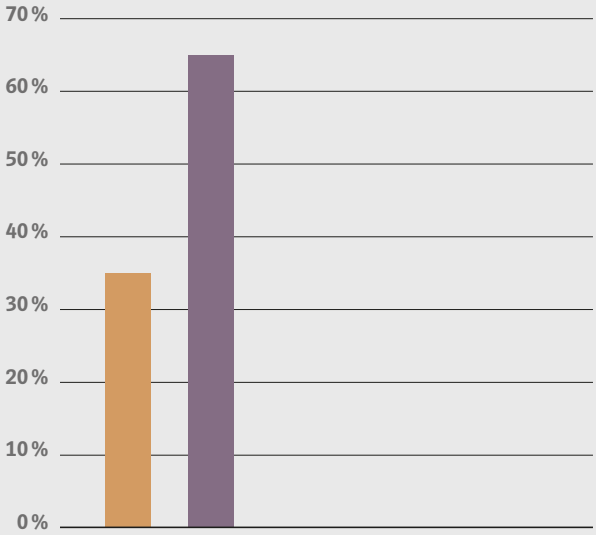
Sofern Ihr Unternehmen die finanziellen Auswirkungen eines Schadenereignisses abgeschätzt hat, wie hoch ist der höchste potenzielle Verlustwert?



3

GRAFIK 7

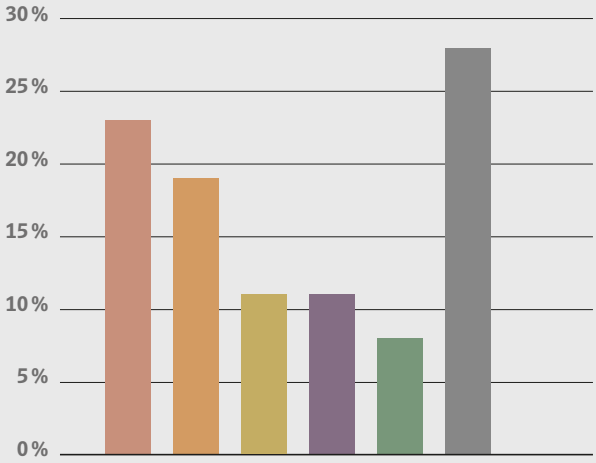
Hat Ihr Unternehmen in den letzten 12 bis 24 Monaten einen Notfall-Reaktionsplan für Cyber-Ereignisse entwickelt?



- Ja: 35 % (2017: 29 %)
- Nein: 65 % (2017: 61 %)
- Ich weiss es nicht: 0 % (2017: 10 %)

GRAFIK 8

Sofern Ihr Unternehmen keinen Notfall-Reaktionsplan für Cyber-Ereignisse entwickelt hat, können Sie erklären weshalb?



- Cyber-Vorfälle werden in anderen Krisenplänen abgedeckt und bedürfen keiner gesonderten Behandlung: 23 % (2017: 7 %)
- Cyber-Sicherheit/Firewalls sind ausreichend, um Cyber Incidents zu verhindern: 19 % (2017: 18 %)
- Der Organisation fehlt das Know-how: 11 % (2017: 9 %)
- Das Cyber-Risiko ist zu gering, um entsprechende Notfallpläne zu rechtfertigen: 11 % (2017: 4 %)
- Wir sehen dafür keine Priorität: 8 % (2017: 7 %)
- Ich weiss es nicht: 28 % (2017: 16 %)

Das Prinzip der Hoffnung ist selten ein guter Berater. Unternehmen, die Cyber-Risiken zu den Top-10 Risiken zählen, sollten die Erstellung eines Notfall-Reaktionsplans zuoberst auf ihrer Prioritätenliste stehen haben. Der Umgang mit den für ein Unternehmen bedrohlichen Cyber-Zwischenfällen ist zu planen und zu trainieren. Wer mit dem Worst Case rechnet und das sollte in der Konsequenz jeder, der Cyber-Risiken zu den Top Unternehmensrisiken zählt, übergibt sein Unternehmen ohne entsprechende Notfallreaktionsplanung in die Hände des Zufalls. Die Notfallplanung der Cyber-Worst-Case-Szenarien gehört letztlich – wie auch die Risikofinanzierungsplanung – in den Zuständigkeitsbereich der strategischen Unternehmensführung. Das Computer Incident Response Team (CIRT) hingegen arbeitet auf der operativ-taktischen Ebene und sorgt für die beste Sicherheit der Kronjuwelen.

OHNE TRAINING KENTERT DAS SCHIFF: WER DAS SEGELN IM STURM TRAINIERT, HAT BEI UNWETTER AUF OFFENEM MEER DIE DEUTLICH BESSEREN ÜBERLEBENSCHANCEN.

Lediglich 35 % der Befragten geben an, in den letzten 12–24 Monaten einen Notfall-Reaktionsplan entwickelt zu haben (Grafik 7). Dies obwohl die durchschnittliche Schadenhöhe infolge eines Cyber-Zwischenfalls von 59 % der Befragten, die den Cyber Worst Case geschätzt haben, auf über CHF 1 Mio. beziffert wird (Grafik 5). Begründet wird das Fehlen des Krisenplans zum einen damit, dass Cyber-Zwischenfälle bereits in anderen Katastrophenplänen integriert seien und zum anderen – wie auch letztes Jahr – mit dem Vorhandensein ausreichender Cyber-Sicherheit oder Firewalls (Grafik 8).

In Bezugnahme auf den Notfallmassnahmenplan leistet die DSGVO indirekt einen nicht zu unterschätzenden Beitrag. Betroffene Unternehmen sind seit dem 25. Mai 2018 in der Pflicht, u. a. ihren Meldepflichtenpflichten nach einem Datensicherheitsvorfall nachzukommen; die Wahrnehmung dieser Pflicht bedingt quasi das Aufsetzen eines Notfallmassnahmenplans (vgl. auch Grafik 16).

3

Wie bereits in den beiden Vorjahren fürchten sich die meisten Schweizer Unternehmen vor einem cyberbedingten Betriebsunterbruch. Der Reputationsschaden stellt die zweitgrösste Bedrohung dar, gefolgt vom Daten-/Softwareschaden. Dahinter folgen die Störung/Unterbrechung von Industrieanlagen oder Betriebstechnik, Kompromittierung von Kundendaten, Erpressung/Ransomware, Verstoss gegen die EU-Datenschutzgrundverordnung oder andere Datenschutzgesetze, Verlust/Diebstahl von geistigem Eigentum sowie Sach- und Personenschäden (Grafik 9).

Der cyberbedingte Betriebsunterbruch wird, wie auch Szenarien im Zusammenhang mit Personendaten, zu Recht am meisten gefürchtet; schliesslich verstecken sich in diesen Schadenfällen in der Regel die grössten Kostentreiber. Hohe Kostentreiber deshalb, weil die für den Schaden verantwortlichen Kriminellen ihre Spuren bisweilen gut zu verwischen wissen. Letztlich bleiben die Unternehmen trotz Strafanzeige gegen Unbekannt auf den gesamten Unkosten und auf einer gehörigen Portion Verunsicherung sitzen.

GRAFIK 9

Welche Szenarien eines Cyber-Angriffs stellt die grösste Gefährdung für Ihr Unternehmen dar?

	Schweiz
Betriebsunterbruch	65 % (2017: 86 %)
Reputationsschaden	49 % (2017: 57 %)
Daten-/Softwareschaden	39 % (2017: 53 %)
Strörung/Unterbrechung von Industrieanlagen oder anderer Betriebstechnik	28 % (2017: 33 %)
Kompromittierung von Kundendaten	25 % (2017: 52 %)
Erpressung/Ransomware	25 % (2017: 37 %)
Verstoss gegen DSGVO oder gegen andere Datenschutzgesetze	22 % (2017: N/A)
Verlust/Diebstahl von geistigem Eigentum	16 % (2017: 22 %)
Haftung gegenüber Dritten aufgrund Systemverletzung	15 % (2017: 30 %)
Sachschäden/Personenschäden	6 % (2017: 11 %)
Andere	2 % (2017: 34 %)
Ich weiss nicht	3 % (2017: 2 %)

Integre und vor fremden Einblicken geschützte Kunden- oder Produktionsdaten sowie die Erfüllung vertraglich vereinbarter Lieferfristen haben einen grossen Einfluss auf eine einwandfreie Reputation.

2018 hat sich u. a. am Verhalten von Uber (Aufdeckung der Vertuschung eines Hacker-Angriffs mit 57 Millionen Opfern aus dem Jahr 2016), Swisscom (mehrere Monate verspätete Bekanntgabe eines Datenverlustes mit 800'000 Opfern aus dem Jahr 2017) und LinkedIn (Aufdeckung, dass LinkedIn Europa die E-Mail-Adressen von 18 Mio. Nichtusern ohne Zustimmung sammelte, die Daten in der USA verarbeitete und für gezielte Werbung an Facebook übertragen wurde) gezeigt, dass Unternehmen versuchen, Datenpannen oder zu spät erkannter Datenmissbrauch möglichst geheim zu halten. Vorbildlich hingegen informierte die Marriott-Hotelgruppe nach dem im Herbst 2018 aufgedeckten Hacker-Angriff ihre Kunden per E-Mail über den Vorfall.

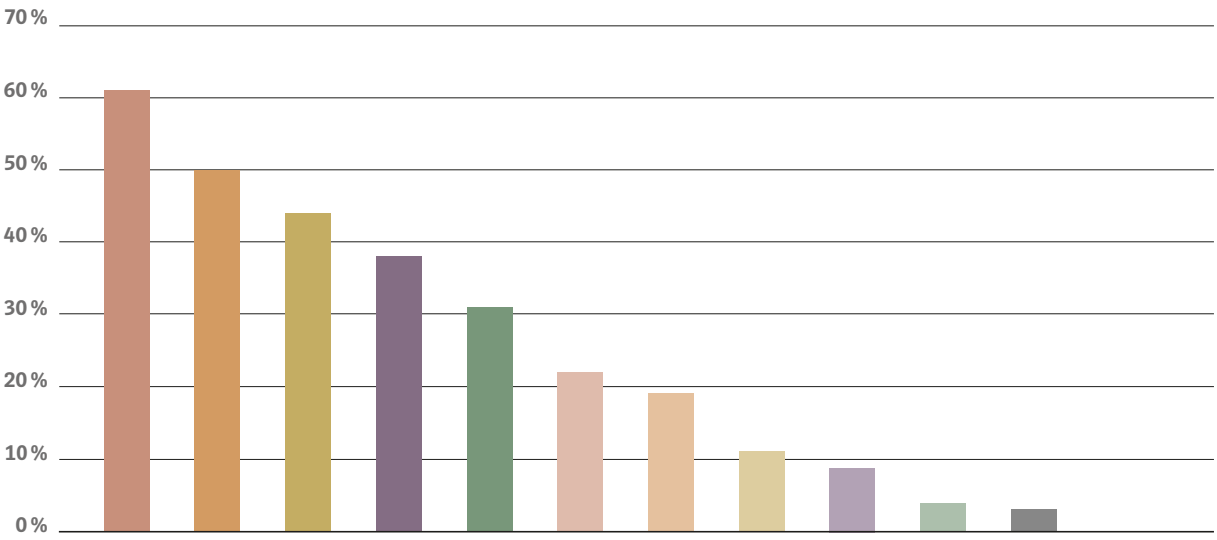
Transparente Kundenorientierung im Krisenfall hat ebenfalls einen Einfluss auf die Reputation, in der Regel einen positiven.

Unverändert zum letzten Jahr: Der Kosten-Nutzen-Entscheid «Können/wollen wir uns eine Busse oder einen Reputationsschaden leisten?» wird den Unternehmen auf jeden Fall neue Strategien in Sachen Transparenz und Kosten abverlangen.

3

GRAFIK 10

Welche Bedrohungsakteure beschäftigen Sie im Hinblick auf einen Cyber-Angriff, der eine Malware liefert, am meisten?



- Finanziell motivierte Bedrohung wie organisierte Kriminalität und/oder Hacktivistengruppen: 61 % (2017: 43 %)
- Menschliches Versagen von Mitarbeitenden oder Vertragspartnern: 50 % (2017: 21 %)
- Ein böswilliger Mitarbeiter oder Vertragspartner mit autorisiertem IT-Zugang zum Unternehmen: 44 % (2017: 27 %)
- Technisches Versagen/Betriebsfehler: 38 % (2017: 8 %)
- Brand/Elementarereignisse: 31 % (2017: N/A)
- Internetausfall: 22 % (2017: N/A)
- Stromausfall: 19 % (2017: N/A)
- Physischer Angriff auf die Hardware: 11 % (2017: N/A)
- Politisch motivierte Bedrohung: 9 % (2017: 2 %)
- Anderes: 4 %
- Ich weiss es nicht: 3 %

Die Cyber-Angriffswellen vom Juni 2017, angeführt durch die Krypto-Trojaner WannaCry, Petya und NotPetya, verdeutlichten auf eine eindrückliche Art und Weise die in Europa vorherrschende IT-Monokultur, die Unberechenbarkeit und den zentralen Faktor Mensch. Dieses spielt insbesondere eine Rolle, wenn es darum geht, mittels eines unabsichtlichen «Klicks» die Installierung der Malware ins Firmennetzwerk zu ermöglichen.

Ein wichtiger Schritt wäre getan, wenn das Restrisiko im Zusammenhang mit potenziell kriminellen oder leicht zu manipulierenden Mitarbeitenden objektiv in die Cyber-Risikoanalyse miteinbezogen werden würde. Das vom Menschen ausgehende Cyber-Restrisiko schätzen wir mittlerweile auf mindestens 95 %; davon gehen wir in 50-80 % der Fälle von einer Täterschaft mit internem Know-how aus – unabhängig davon, ob dieses Know-how aus einer aktuellen oder vergangenen Anstellung angeeignet wurde. Entsprechend sind Präventivmassnahmen gezielt dort anzulegen, wo der Schaden am grössten sein könnte. Dabei sollten IT-Schlüsselpersonen mit umfassenden Administratorenrechten sowie anderweitige Schlüsselpersonen nach dem Need-to-know-Prinzip mit Priorität überprüft werden. Es ist unlogisch und unverhältnismässig, dass eine Banküberweisung ab CHF 1000.- Franken einer Doppelunterschrift bedarf, während IT-Mitarbeitende mit umfassenden Administra-torenrechten und wenigen Klicks das Unternehmen lahm legen können.

3

3.4 SUPPLIER CYBER RISK MANAGEMENT

Zu oft gehen die von IT-Zulieferer ausgehenden Cyber-Risiken vergessen. Tatsache ist, dass Unternehmen vermehrt über ihre IT-Zulieferer angegriffen werden. Je grösser die Abhängigkeit von externen Outsourcingpartnern ist, desto eher sollte deren Ausfall ins betriebliche Cyber Risk Management integriert werden. Der Fokus gilt im Idealfall der gesamten Wertschöpfungskette. Unternehmen können heute nicht mehr isoliert betrachtet werden.

Die Verantwortung für die von IT-Zulieferern verursachten Schäden trägt das Unternehmen zuerst einmal selbst. Mögliche daraus entstehende Haftungsrisiken sind von den Unternehmen in der Regel vorzufinanzieren und bedingen eine entsprechende Liquidität. Weitere Nachteile sind der mögliche Kontrollverlust über die Daten, die fehlende Isolierung der verschiedenen Datenverarbeitungen zu anderen Cloud-Nutzern, Compliance-Risiken, Lock-in-Effekte sowie der sowie der Zugriff ausländischer Behörden auf Unternehmensdaten.

ISO-ZERTIFIZIERUNGEN DER IT-ZULIEFERER SIND KEINE GARANTEN FÜR EINE BESSERE CYBER-SICHERHEIT.

Mittlerweile bewerten 47 % der Unternehmen ihre Zulieferer hinsichtlich Cyber-Risiko-Gefährdung; 2017 waren es erst 33 %. Dieses erfreuliche Resultat widerspiegelt die wachsende Awareness bei diesem wichtigen Thema.

Die Grafik 11 zeigt in aller Deutlichkeit, dass die Inventarisierung der Lieferantenbeziehungen zu den noch seltenen Vorkehrungen gehört. Nebst der Inventarisierung sollten ebenfalls folgende Themen dokumentiert sein: Zugriffsrechte auf Unternehmensdaten und -systeme, Bewertung der Zulieferer hinsichtlich ihrer eigenen Cyber-Sicherheit, das Verlangen von Garantien für Monitoring oder weitere Schutzvorkehrungen, vertragliche Vereinbarungen im Hinblick auf Haftungsgrenzen für cyberbedingte Verluste, Analyse der Finanzkraft der Lieferanten sowie Verpflichtung von Lieferanten, selbst eine Cyber-Versicherung abzuschliessen.

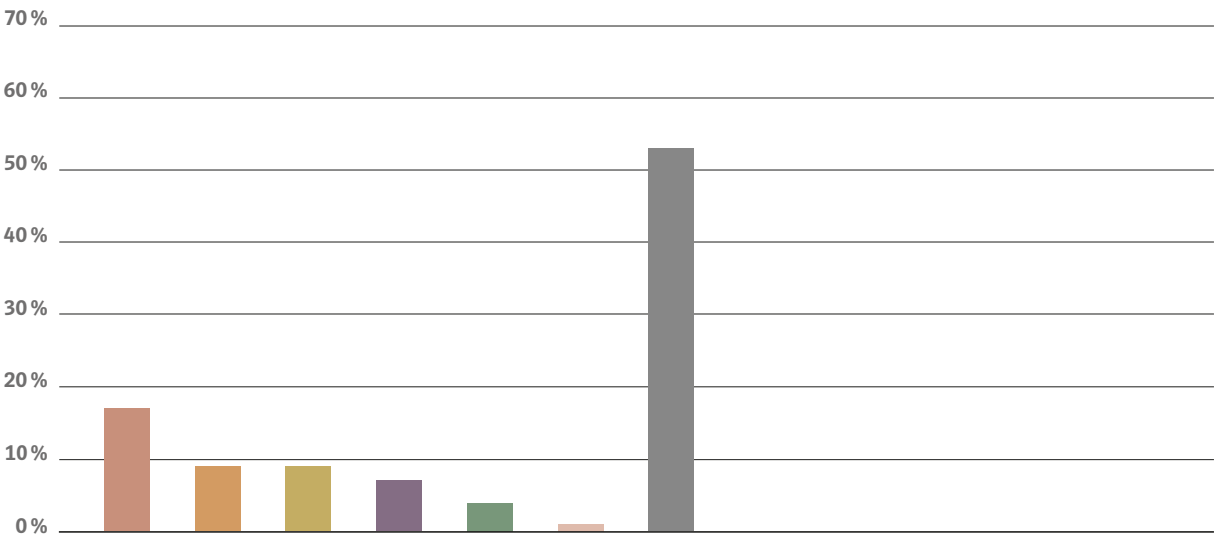
47 % BEWERTEN IHRE ZULIEFERER HINSICHTLICH CYBER-RISIKO-GEFÄHRDUNG.

Grosse Sorgen bereiten uns die fehlende Inventarisierung und damit die grosse Intransparenz bezüglich der vorhandenen quantitativen und qualitativen IT-Lieferantenbeziehungen. Diese Intransparenz ist faktisch gleichzusetzen mit Nichtwissen und Nichtwissen ist gefährlich.

Eine Präventivmassnahme liegt jedenfalls auf der Hand: Eine entsprechende Lieferantenliste kann Transparenz und mehr Verständnis bezüglich Abhängigkeiten im Cyber-Schadenfall schaffen. Dass der Cyber-Versicherer über die gesamte externe IT-Wertschöpfungskette der versicherten Unternehmen Transparenz verlangt, ist demnach nachvollziehbar.

GRAFIK 11

Welche Schritte unternimmt Ihr Unternehmen, um das von Ihrem Lieferanten und anderen Dritten ausgehende Cyber-Risiko zu bewerten und zu managen?



- Inventarisierung von Lieferanten-Beziehungen und Datenzugriffsrechten: 17 % (2017: 31 %)
- Bewertung der Zulieferer hinsichtlich Cyber-Sicherheit sowie Verlangen von Garantien betreffend Cyber-Sicherheitshaltung: 9 % (2017: 12 %)
- Vertragliche Regelungen im Hinblick auf Haftungsgrenzen für Cyber-Verluste: 9 % (2017: 10 %)
- Regelmässiges Monitoring der Lieferanten im Hinblick auf deren Cyber-Sicherheitshaltung: 7 % (2017: 8 %)
- Analyse der Finanzkraft der Lieferanten: 4 % (2017: 5 %)
- Verpflichtung der Lieferanten, eine Cyber-Versicherung abzuschliessen: 1 % (2017: 1 %)
- Wir bewerten unsere Zulieferer nicht oder ich weiss es nicht: 53 %

3

3.5 ABSCHLÜSSE VON CYBER-VERSICHERUNGEN NEHMEN ZU

Die Cyber-Versicherungslandschaft entwickelt sich in Europa und in der Schweiz fortlaufend weiter. Nach wie vor sind die Versicherungsangebote für einen Laien schwer verständlich. Professionelle Beratung und die Prüfung individueller Deckungsbedürfnisse sind deshalb unabdingbar. Infolge zunehmender Kumulrisiken werden Zusicherungen der Unternehmen hinsichtlich deren eigenen IT-Sicherheits- sowie Compliance-Standards in Zukunft an Bedeutung gewinnen. Die Versicherer werden aus guten Gründen immer weniger bereit sein, die Katze im Sack zu versichern.

Eine Cyber-Versicherung soll Vermögensverluste ausgleichen, die durch einen Cyber-Zwischenfall entstanden sind. Der Risikotransfer ist deshalb nicht aus Hype-Gründen, sondern basierend auf Kosten-Nutzen-Überlegungen jährlich zu prüfen.

Dass 16 % der Umfrageteilnehmer bereits über eine Cyber-Versicherung verfügt, beurteilen wir als realistisch: 70 % der Befragten sind aus dem KMU-Bereich mit einem Umsatz von bis zu CHF 250 Mio. Kleine und Mittlere Unternehmen platzieren infolge der günstigen Versicherungskonditionen derzeit die meisten Policen; dies nicht nur über ihren Broker, sondern auch direkt beim Versicherer.

An der diesjährigen Umfrage haben 387 Kunden und Nicht-Kunden von Kessler anonym teilgenommen. 16 % der Befragten geben an, eine Cyber-Versicherung abgeschlossen zu haben, während 23 % planen, in den nächsten 12 Monaten eine entsprechende Versicherung zu platzieren oder die bestehende Deckungssumme zu erhöhen. 12 % geben an, keine Cyber-Versicherung zu haben, gewisse Cyber-Risiken aber über ihre konventionellen Versicherungspolicen abgedeckt zu haben. Und 31 % planen derzeit nicht, eine Cyber-Versicherungspolice abzudecken (Grafik 12).

> CYBER-RISIKEN NEHMEN WEITERHIN ZU. INDIVIDUELLE CYBER-RISIKEN SIND ZU EVALUIEREN UND BESTMÖGLICH ZU VERSICHERN. DABEI IST PROFESSIONELLE BERATUNG UNABDINGBAR.

GRAFIK 12

Wie ist Ihr Unternehmen derzeit beim Cyber-Versicherungsschutz aufgestellt?

- Meine Organisation hat keine Cyber-Versicherung und hat nicht die Absicht, eine Cyber-Versicherung abzuschliessen: 31 % (2017: 16 %)
- Meine Organisation plant in den nächsten 12 Monaten eine Cyber-Versicherung abzuschliessen oder deren Deckungssumme zu erhöhen: 23 % (2017: 29 %)
- Meine Organisation hat eine Cyber-Versicherung abgeschlossen: 16 % (40 %)
- Meine Organisation hat keine Cyber-Versicherung, aber wir verfügen über einen gewissen Cyber-Versicherungsschutz im Rahmen anderer Policen: 12 % (2017: N/A)
- Ich weiss es nicht: 18 % (2017: 15 %)

3

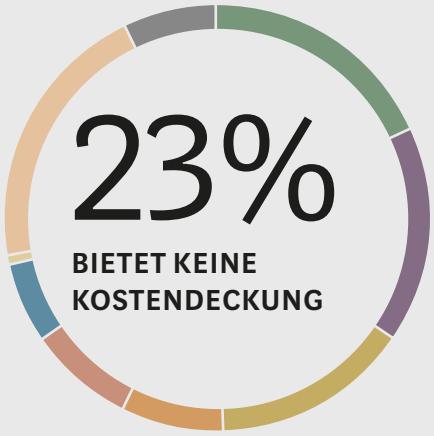
GRAFIK 13

Sofern Ihr Unternehmen eine Cyber-Versicherung hat oder deren Deckung erweitern möchte, was sind die Treiber dafür?

- Cyber-Risk-Management-Pläne: 51 % (2017: 44 %)
- Auftrag des Verwaltungsrates: 14 % (2017: 26 %)
- Selber einen Cyber-Angriff erfahren: 10 % (2017: 10 %)
- Regulatorische Anforderungen, z. B. auf Grundlageder DSGVO: 7 % (2017: 16 %)
- Angeregt durch einen Cyber-Angriff auf andere Unternehmen: 4 % (2017: 30 %)
- Versicherungsnachweispflicht: 4 % (2017: 3 %)
- Andere: 7 % (2017: N/A)
- Ich weiss es nicht: 3 % (2017: 13 %)

GRAFIK 14

Sofern Ihr Unternehmen keine Cyber-Versicherung abgeschlossen hat, was sind Gründe dafür?



- Fehlende interne Abstimmung über den Bedarf: 23 % (2017: 14 %)
- Unsere Cyber-Sicherheit ist stark genug, sodass wir keine Cyber-Versicherung brauchen: 21 % (2017: 17 %)
- Die Cyber-Versicherung bietet keine ausreichende Deckung der Kosten: 19 % (2017: 62 %)
- Die verfügbare Deckung wird nicht verstanden: 10 % (2017: 21 %)
- Die Cyber-Deckung ist in einer anderen Police enthalten: 10 % (2017: 14 %)
- Unzureichendes Budget oder unzureichende Ressourcen: 8 % (2017: 7 %)
- Unsere Cyber-Risiken werden von unserem Captive getragen: 1 % (2017: 3 %)
- Andere Gründe: 26 % (2017: N/A)
- Ich weiss es nicht: 9 % (2017: 3 %)

Über die Hälfte der Befragten, die bereits eine Cyber-Versicherung abgeschlossen haben, gedenken eine Cyber-Versicherung abzuschliessen oder ihre Deckungssumme zu erhöhen, geben als Treiber den aktuellen Cyber-Risk-Management-Plan an (Grafik 13). Dies ist nachvollziehbar, denn wer die Büchse der Pandora öffnet erkennt deren Schadenspotenzial relativ bald.

Cyber-Risk-Management ist gemäss der Umfrage mit 51 % der mit Abstand grösste Treiber für den Abschluss einer Cyber-Versicherung oder einer entsprechenden Deckungserhöhung. Schadenfälle bei anderen Unternehmen scheinen den Befragten keinen grossen Eindruck zu machen. Lediglich 10 % sehen hier einen Treiber für die Platzierung einer Cyber-Versicherung oder für die Erhöhung der Deckung. Ebenfalls ist die Top-Down Cyber-Risikofinanzierungsstrategie als Treiber mit 14 % noch minimal: Den Verwaltungsrat sehen wir als künftigen wichtigen Treiber, die Cyber-Risiko-Diskussion zu starten. Dies alleine schon aufgrund seiner rechtlichen Pflicht, sich bewusst für eine Cyber-Risikofinanzierungsstrategie zu entscheiden, sollte denn das Cyber-Risiko im Betrieb als Toprisiko erkannt werden. (vgl. auch Grafik 1).

43 % der Schweizer Unternehmen haben keine Cyber-Versicherung, haben nicht die Absicht, eine Cyber-Versicherung abzuschliessen, verfügen über keinen entsprechenden Plan oder geben an, keine Cyber-Versicherung zu haben, weil gewisse Cyber-Deckungskomponenten in anderen Versicherungspolicen abgedeckt seien (Grafik 12). Als Hauptgründe der genannten Sachverhalte werden dieses Jahr fehlende interne Abstimmung über den Cyber-Versicherungsbedarf sowie die Stärke der vorhandenen betrieblichen Cyber-Sicherheit angegeben. Nach wie vor ist die nicht ausreichende Kostendeckung ein Grund, ist aber im Vergleich zum letzten Jahr nicht mehr der Hauptgrund (Grafik 14).

4
DIE EU-DSGVO STÄRKT DAS CYBER-RISIKO-MANAGEMENT

4.1 KOSTEN INFOLGE DATENSCHUTZGESETZVERLETZUNGEN

Anfallende Kosten sind im Zusammenhang mit Datenschutzgesetzverletzungen kalkulierbar und grösstenteils versicherbar. Deshalb gehört der bewusste Entscheid über einen sinnvollen Umsetzungsgrad der EU-DSGVO auf die Agenda der Unternehmensführung. Die EU-DSGVO stärkt das Cyber Risk Management.

Es ist davon auszugehen, dass Cyber-Schadenfälle in Europa künftig 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.

Aufgrund der aktuellen datenschutzrechtlichen Entwicklungen wird die Awareness für das Cyber Risk Management und die Cyber Resilience der Unternehmen gestärkt: Denn durch die EU-DSGVO wird die Unternehmensführung quasi gezwungen, sich mit Cyber Risk Management sowie mit datenschutzrechtlichen Themen auseinanderzusetzen. Hohe Kosten drohen. Zudem werden Verbandsklagerechte, welche gemäss der EU-DSGVO zulässig und in Deutschland bereits in Kraft sind, auch in der Schweiz im Rahmen der anstehenden ZPO-Revision ein Traktandum in Verwaltungsratssitzungen werden. Die vorgesehene Möglichkeit der Verbandsklage wird die Awareness hinsichtlich Cyber-Risiken und Datenschutz nochmals markant steigern.

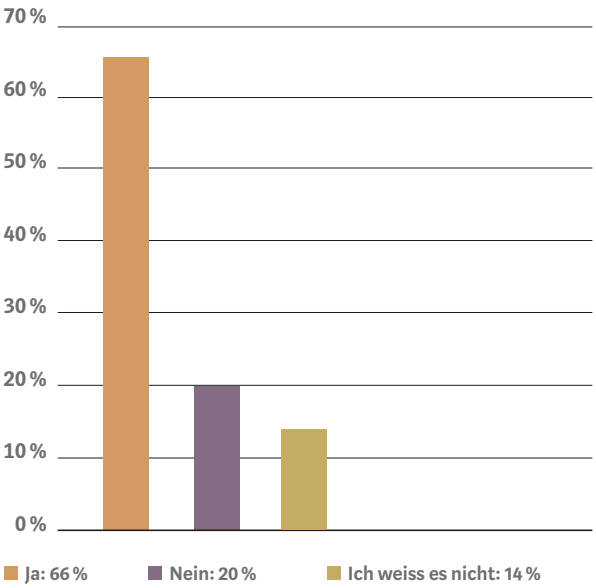
Wer die massgebenden Datenschutzgesetze kennt, kann im Falle eines Datenlecks erforderliche Pflichten wahrnehmen sowie gezielte betriebliche Massnahmen umsetzen, um behördliche Datenschutzverfahren, Geldbussen und anderweitige Folgekosten zu vermeiden. Ein für gewisse Branchen interessanter Aspekt der Cyber-Versicherung ist, dass Kosten im Zusammenhang mit Datenschutzverletzungen grösstenteils gedeckt sind.

Von den befragten Unternehmen fallen 66 % unter den Anwendungsbereich der DSGVO, 20 % fallen nicht darunter und 14 % wissen es nicht (Grafik 15).

Von Denjenigen Unternehmen, die der EU-DSGVO unterliegen, gaben im Herbst 2018 49 % an, über einen Reaktionsplan für den Fall einer Datenschutzverletzung zu verfügen (Grafik 16). Diese Entwicklung ist erfreulich. Im Vorjahr waren es lediglich 23 %. Auffallend ist, dass aktuell immer noch 35 % über keinen entsprechenden Reaktionsplan verfügen, dies obwohl die EU-DSGVO für die EU-Staaten seit dem 25. Mai 2018 und für die EWR-Staaten seit 20. Juli 2018 direkt anwendbar ist: Zwar schreibt die EU-DSGVO keinen Reaktionsplan für Cyber-Vorfälle vor, verlangt u.a. aber eine entsprechende Benachrichtigung der Aufsichtsbehörden innerhalb von 72 Stunden nach Bemerken eines Datensicherheitszwischenfalls. Es liegt auf der Hand, dass die Einhaltung dieser Frist mit einem Reaktionsplan eher gelingt als ohne.

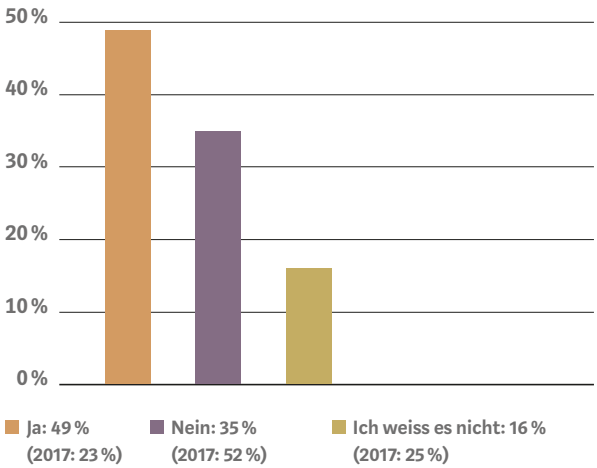
GRAFIK 15

Untersteht Ihre Organisation der EU-DSGVO?



GRAFIK 16

Sofern Ihr Unternehmen der EU-DSGVO untersteht, haben Sie einen Reaktionsplan im Hinblick auf Datenschutzverletzungen entwickelt, der u. a. die Meldung eines Verstosses gegen die EU-DSGVO an die Aufsichtsbehörde in der EU innerhalb von 72 h beinhaltet?



5 SCHLUSSFOLGERUNGEN

ERKENNTNISSE

Cyber-Risiken sind in aller Munde. Awareness ist geschaffen. Awareness alleine reicht zum Erreichen der Unternehmensziele nicht aus. Massnahmen müssen her und ein Umdenken muss stattfinden: Integre und vor fremden Einblicken geschützte und verfügbare Daten sind im digitalen Geschäftsalltag unabdingbar.

Cyber-Risiken sind unberechenbar und bergen diverse nicht vorhersehbare Kosten. Dies nicht zuletzt infolge Intransparenz hinsichtlich der IT Supply Chain sowie infolge des schwächsten Glieds in der gesamten IT-Sicherheitskette: Der Mensch mit seinen typisch menschlichen Eigenschaften wie Hilfsbereitschaft, Gutgläubigkeit, Rachsüchtigkeit, Habgier, Stolz, Egoismus und Angst. Alle diese Faktoren können menschliches Verhalten beeinflussen und aus einem motivierten Mitarbeitenden einen Kriminellen machen. Gezielte Angriffe verbunden mit internem Know-how haben das grösste Schadenspotenzial.

Klar ist ausserdem: Der betriebliche Umgang mit Cyber-Risiken ist individuell und hängt stark von der Risikofreudigkeit der Unternehmensführung ab. Und nicht zuletzt: Wer die EU-DSGVO als Chance sieht, das betriebliche Cyber Risk Management zu überdenken, wird sich konstruktiver mit der Datenschutzthematik auseinandersetzen und diese nicht nur als lästige Pflicht begreifen.

BERATUNGSBEDARF

Der Umgang mit dem Cyber-Restrisiko ist nach wie vor komplex und anspruchsvoll. Einen Beratungsbedarf sehen wir weiterhin bei der Zuteilung der Verantwortlichkeit und bei der Quantifizierung der Cyber-Risiken im Unternehmen sowie verstärkt in der Umsetzung angemessener diversifizierter Präventivmassnahmen. Das grosse pro-Argument, Cyber-Risiken zu transferieren, liegt im unberechenbaren Faktor Mensch, der als Hauptverursacher der heutigen Cyber-Risiken gilt. Cyber-Risiken sind Unternehmensrisiken und sollten jährlich hinsichtlich deren Versicherungswürdigkeit anhand des Kosten-Nutzen-Prinzips geprüft werden.

Sie haben Fragen? Vereinbaren Sie ein persönliches Beratungsgespräch:

Pascal Schweingruber
Mitglied der Geschäftsleitung
pascal.schweingruber@kessler.ch
T +41 44 387 87 65

Melanie Koller
Legal Counsel Cyber Risk
melanie.koller@kessler.ch
T +41 44 387 88 39

ÜBER KESSLER

Kessler ist das führende Schweizer Unternehmen für Risiko-, Versicherungs- und Vorsorgeberatung. Dank Fachwissen und Erfahrung der Mitarbeitenden, Innovationskraft sowie durch unsere Marktstellung schaffen wir nachhaltigen Mehrwert für unsere Kunden aus Dienstleistung, Handel und Industrie sowie der öffentlichen Hand. Der gute Ruf und der wirtschaftliche Erfolg sichern unsere langfristige Zukunft als unabhängiges Familienunternehmen. Gegründet 1915, beschäftigt Kessler heute 275 Mitarbeitende am Sitz in Zürich und an den weiteren Standorten Aarau, Basel, Bern, Genf, Lausanne, Luzern, Neuenburg, St. Gallen und Vaduz. Als Schweizer Partner von Marsh sind wir Teil eines Netzwerkes mit Spezialisten aus allen Gebieten des Risk Management und mit grosser Erfahrung in der Betreuung globaler Versicherungsprogramme. Marsh ist in mehr als 100 Ländern der weltweit führende Versicherungsbroker und Risikoberater und gehört zu Marsh & McLennan Companies, deren Aktie an den Börsen von New York, Chicago und London gehandelt wird (Börsenkürzel: 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

Marsh Network