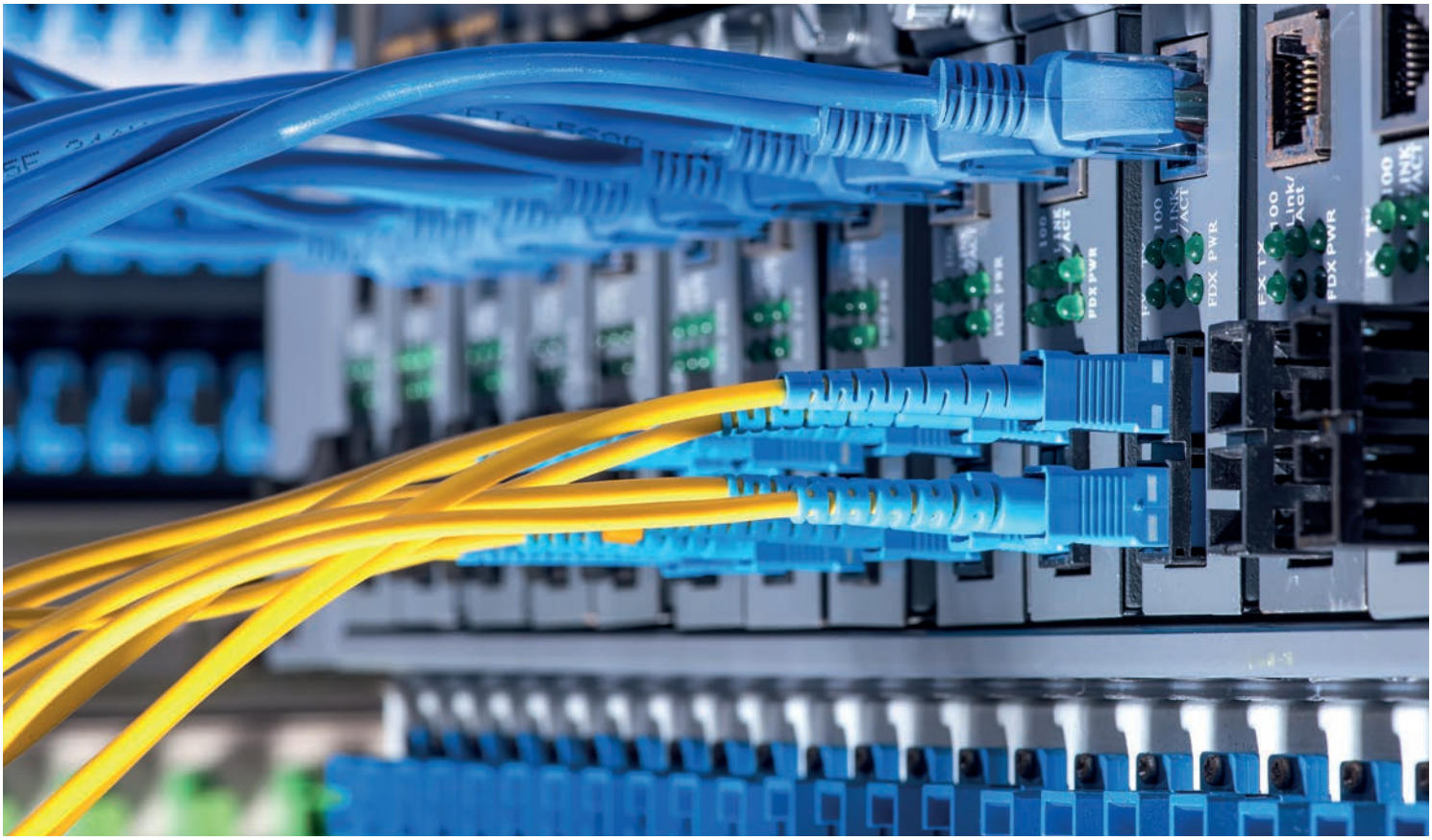
KESSLER

# CYBER RISK SURVEY REPORT 2018
# CYBER RISK AUS SCHWEIZER SICHT



MIT SICHERHEIT VORAUS.

# CYBER RISK SURVEY REPORT 2018
# CYBER RISK AUS SCHWEIZER SICHT

# 1 VORWORT

### CHANCE DER DIGITALISIERUNG

Die Digitalisierung hat auf die Unternehmen und deren Geschäfts- und Kundenbeziehungen fundamentale Auswirkungen. Mit dem Internet of Things werden neben Annehmlichkeiten und neuen digitalen Schnittstellen viele neue Angriffsstellen geschaffen.

Die Digitalisierung soll als Chance verstanden werden, darf aber Unternehmen keinen unverhältnismässigen Gefahren aussetzen. Es gilt, die wertvollen Daten und Business relevanten Prozesse zu kennen und zu schützen. Die EU-Datenschutzgrundverordnung (EU-DSGVO) stützt diesen Denkansatz: Das Cyber Risk Management erhält durch die EU-DSGVO eine berechtigte Grundlage.

### RISIKOFAKTOR SUPPLY CHAIN MANAGEMENT

Die zunehmende Nutzung von Outsourcing-Dienstleistungen senkt zwar Betriebskosten, geht in der Regel aber zulasten der Daten-Transparenz, insbesondere wo sich die Daten befinden und wer letztlich Zugriff darauf hat. Der Ausfall eines zentral geführten IT-Systems birgt schwer kalkulierbare Kumulrisiken. So können diverse Betriebsbereiche/Standorte gleichzeitig und in unterschiedlicher Art und Weise von einer Cyber-Attacke getroffen werden oder Angreifer erhalten über den Angriff auf einen IT-Provider Einsicht in sämtliche IT-Systeme und Softwares verschiedener Firmen. Wie die vorliegende Umfrage zeigt, wird die Abhängigkeit der Zulieferer leider noch zu wenig in den firmeneigenen Cyber-Risk-Management-Prozess miteinbezogen.

### UMFRAGE VON MARSH

Unser Netzwerkpartner Marsh hat im Mai 2017 eine globale branchenübergreifende Umfrage durchgeführt, welche den Umgang von Unternehmen mit Cyber-Risiken und deren Gefahrenpotenzial im Geschäftsalltag sowie damit zusammenhängende Datenschutzrechtsrisiken untersucht. Wir haben uns daran beteiligt und alle unsere international tätigen Kunden zur Teilnahme am «Global Cyber Risk Perception Survey» eingeladen. Die Ergebnisse wurden Ende Februar 2018 von Marsh veröffentlicht.

### DIE HEILE SCHWEIZ?

Die Bedrohungslage aus dem Cyber Space wird in den nächsten Jahren nicht nachlassen. Die digitale Welt kennt keine Schweizer Grenzen. Die Schweizer Unternehmen haben dies realisiert. Der Report bestätigt: Erkannt ist bereits einiges, doch fehlt es an der gezielten Umsetzung.

Auf den folgenden Seiten haben wir für Sie die Ergebnisse der Umfrage von Marsh für die Schweiz ausgewertet und die wichtigsten Erkenntnisse für Sie kommentiert.

Wir wünschen Ihnen eine spannende 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 Marsh «Global Cyber Risk Perception Survey» von Februar 2018. Auf den folgenden Seiten finden Sie die wichtigsten Erkenntnisse aus Schweizer Sicht zusammengefasst und kommentiert.**

An der Cyber-Risiko-Umfrage haben weltweit über 1860 Unternehmen teilgenommen; 386 aus Europa, davon 178 (15 %) unserer Schweizer Kunden.

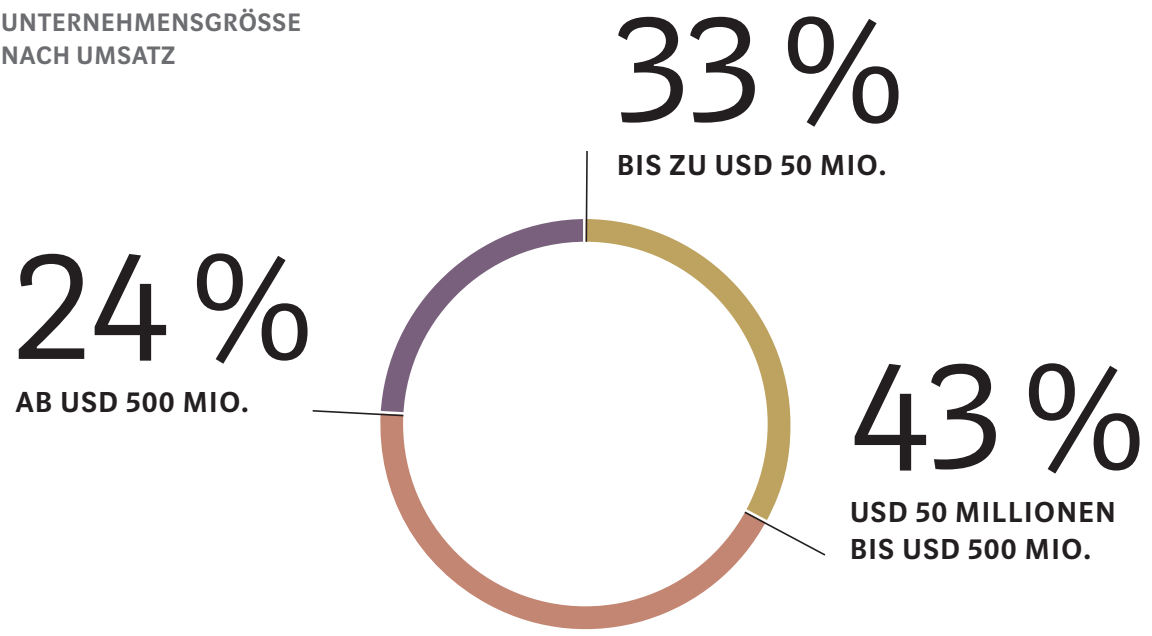
33 % der Unternehmen, die an der Umfrage teilnahmen, generieren einen jährlichen Umsatz von bis zu USD 50 Mio., während 43 % einen Umsatz in der Höhe von 50 Mio. und 500 Mio. erwirtschaften. Von den Unternehmen mit einem Jahresumsatz über 500 Mio. sind 24 % in dieser Umfrage vertreten.

Die Branchenzugehörigkeit der Schweizer Umfrageteilnehmer ist vielfältig. Mit einem Viertel ist die Energie-, Strom-, Versorgungs- und Infrastrukturbranche am stärksten vertreten. Das Interesse dieser Branche an der Umfrageteilnahme erstaunt uns unter dem Aspekt, dass kritische Infrastrukturen angesichts der aktuellen Bedrohungslage zu den Top Cyber-Angriffszielen gehören, nicht.

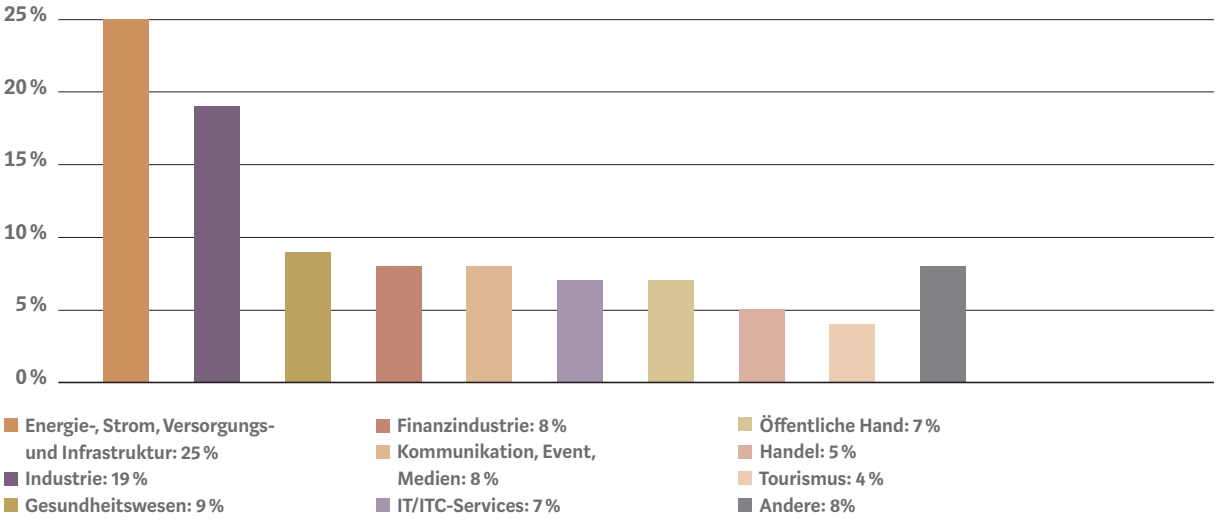
Zu den wichtigsten Absatzmärkten der Umfrageteilnehmer gehören nebst der Schweiz und Kontinentaleuropa, auch die USA/Kanada, UK/Irland sowie Asien.

Aussagekraft hat unseres Erachtens die vielfältige sowie ausserordentlich starke Abhängigkeit der Umfrageteilnehmer von digitalen Hilfsmitteln und Dienstleistungen (Textbox rechts). In diesem Kontext ist unbestritten: Cyber-Risiko ist kein Hype, sondern eine kausale Konsequenz der heutigen digitalen Wirtschaft.

**UNTERNEHMENSGRÖSSE NACH UMSATZ**



## BRANCHENZUGEHÖRIGKEIT




## ABHÄNGIGKEITEN DER UMFRAGETEILNEHMER VON DIGITALEN HILFSMITTELN UND DIENSTLEISTUNGEN

- Ein oder mehrere Computer sind mit dem Internet vernetzt: 98 %
- Elektronische Verarbeitung und Speicherung von Mitarbeiterakten: 88 %
- Mitarbeitende und Dritte können ihre mobilen Geräte am Unternehmensnetzwerk anschliessen: 87 %
- Elektronische Speicherung und/oder Verwaltung von Kundendaten: 86 %
- Elektronische Verarbeitung von Bankinformationen: 75 %
- Elektronische Speicherung von Lieferanteninformationen: 74 %
- Cloud-Services: 54 %
- Elektronische Bearbeitung von privaten Gesundheitsinformationen von Mitarbeitenden oder Kunden: 31 %
- Elektronische Abwicklung von Kreditkartentransaktionen: 28 %
- Erfassung personenbezogener Daten (inkl. Cookies und ähnliche Instrumente) auf einer Website: 25 %
- Elektronische Weitergabe von Personendaten an Lieferanten oder andere Drittparteien: 24 %

# 3 ERKENNTNISSE UND KOMMENTARE

## 3.1 BEWUSSTSEIN FÜR CYBER-RISIKEN NIMMT ZU

**Cyber-Risiken sind infolge der medialen Dauerpräsenz kaum zu ignorieren. Das Problem bzw. die Möglichkeit selbst betroffen zu werden, scheint grösstenteils erkannt. Dennoch wird in Anbetracht des Schadenpotenzials von Cyber-Vorfällen zu wenig unternommen.**

Die diesjährigen Umfrageergebnisse bestätigen, dass Cyber-Risiken im Risikoregister der Unternehmen mittlerweile zu den Top Risiken gehören (Grafik 1). Bereits 56 % der Schweizer Unternehmen zählen Cyber-Risiken zu den Top 5 Unternehmensrisiken (2016: 26 %). Der Aufstieg des Cyber-Risikos unter die Top 5 Unternehmensrisiken lässt sich nebst der erhöhten Medienpräsenz von Cyber-Schadenfällen wohl auch mit der am 25. Mai 2018 in Wirkung tretenden EU-DSGVO sowie mit der zunehmenden Erkenntnis, dass es keine 100 %ige IT-Sicherheit geben kann, erklären. Der grosse Schadenfall wird kommen, es ist lediglich eine Frage der Zeit. Als Vorbereitung auf den Schadenfall reicht eine erhöhte Sensibilisierung gegenüber Cyber-Risiken bei weitem nicht. Die Kluft zwischen Wahrnehmung und Bekämpfung der Cyber-Risiken ist unseres Erachtens nach wie vor zu gross. Hier besteht eindeutig Handlungsbedarf.

GRAFIK 1

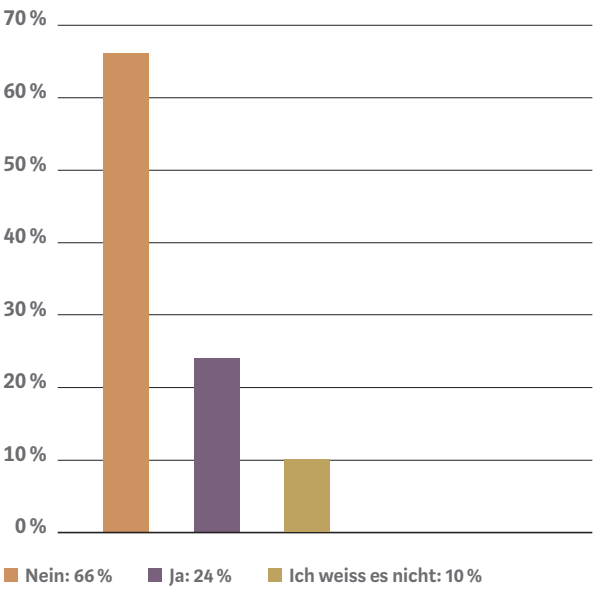
**Welchen Stellenwert haben Cyber-Risiken in Ihrem Unternehmen?**


- Cyber-Risiken sind gemäss Risikoregister unsere grössten Risiken: 3 %
- Cyber-Risiken gehören zu den Top 5 im Risikoregister: 56 % (2016: 26 %)
- Cyber-Risiken gehören gemäss Risikoregister nicht zu den Top 5: 32 % (2016: 58 %)
- Cyber-Risiken haben keinen Stellenwert: 6 % (2016: 15 %)
- Ich kenne den Stellenwert der Cyber-Risiken in meinem Unternehmen nicht: 3 %

Auf die Frage, ob das eigene Unternehmen in den letzten 12 Monaten Opfer einer Cyber-Attacke wurde, haben 66 % mit Nein, 24 % mit Ja und 10 % mit «ich weiss es nicht» geantwortet (Grafik 2). Insofern ist zu vermuten, dass ein Teil dieser 66 % der Unternehmen, die mit Nein geantwortet haben, noch nicht bemerkt haben, dass sie gehackt wurden. Nicht selten wird Schadsoftware erst nach vielen Wochen oder Monaten entdeckt – wenn überhaupt.

**GRAFIK 2**

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



## 3.2 BEDEUTUNG DER CORPORATE GOVERNANCE

**Die Tendenz, dass die Unternehmensleitung zunehmend die Verantwortung für das Cyber-Risk-Management übernimmt, erachten wir als sehr positiv (2017: 34 %; 2016: 13 %). Dennoch sind in der Schweiz in erster Linie immer noch die operativen Bereiche für das Cyber Risk Management verantwortlich. Die Nachteile dieser Aufteilung der Verantwortlichkeit werden in der Regel erst im Cyber-Schadenfall spürbar.**

Im Zeitalter von Big Data und der Industrie 4.0 wird vermehrt von Interesse sein, ob Führungskräfte mögliche Cyber-Schadensszenarien in die Finanzplanung miteinbeziehen oder bewusst vernachlässigen. In Anbetracht dessen, dass 56 % der Schweizer Unternehmen Cyber-Risiken zu den Top 5 Unternehmensrisiken zählen (Grafik 1), ist zu hoffen, dass die Verantwortlichkeit für Cyber-Risiken künftig häufiger von der strategischen Führungsebene wahrgenommen wird.

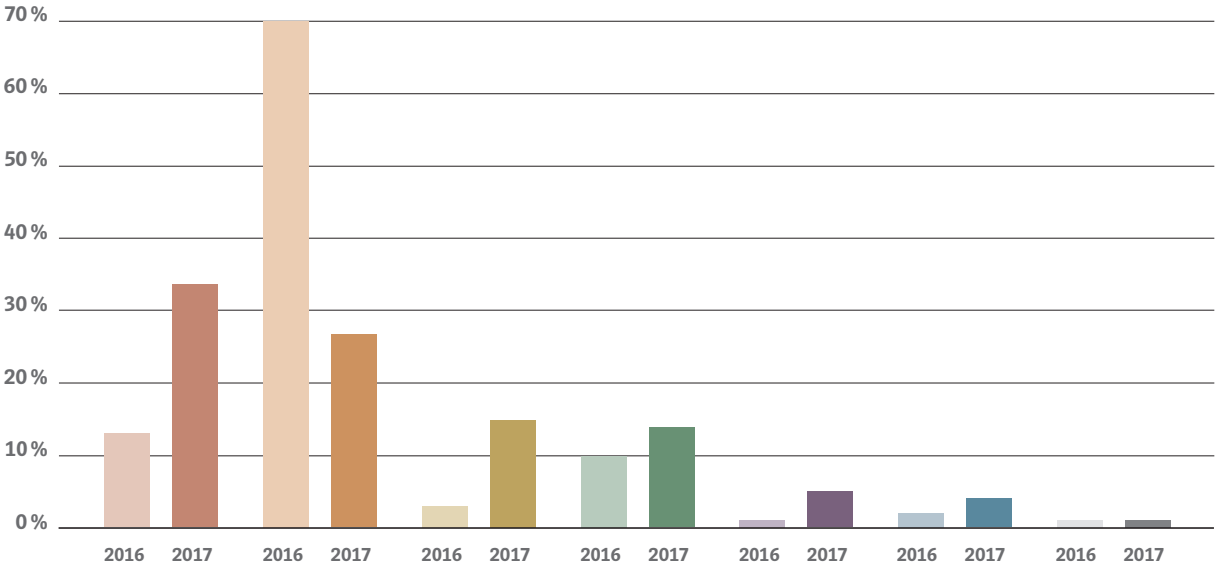
Unabhängig davon, ob die Risikobeurteilung im Rahmen eines Lageberichts eine rechtliche Pflicht darstellt oder nicht, ist die Führung gut beraten, ihre Firmenrisiken zu kennen und diese zu budgetieren. Gemäss Murphy's Law, wonach alles schiefgeht, was schiefgehen kann, ist stets mit Cyber-Schäden zu rechnen und somit deren Bewältigung von Spezialisten sorgfältig zu planen.

Im Falle eines Konkurses oder eines bilanzschädigenden Cyber-Schadenvorfalls wird von Gesetzes wegen vor allem gegen die Unternehmensführung vorgegangen. Die Quantifizierung von noch nicht erfolgten Cyber-Schadensszenarien ist und bleibt – zumindest in naher Zukunft – die grosse Herausforderung der Unternehmen bzw. der gesamten Weltwirtschaft. Gerade aufgrund dieser unberechenbaren Kostenfaktoren wird die Grob-Budgetierung von Cyber-Risiken zentraler denn je. Cyber Security Due Diligence sowie Cyber Insurance Due Diligence werden ebenfalls im M&A-Prozess Alltag werden. Die Katze im Sack zu kaufen wird sich kaum ein Käufer mehr leisten wollen.

Obwohl die Unternehmensführung im Vergleich zum Vorjahr vermehrt die Verantwortung über die Cyber-Risiken trägt, liegt in der Schweiz in erster Linie die Verantwortung immer noch bei den operativen Einheiten. Dennoch, ein erster Schritt ist getan: Heute tragen zumindest nicht mehr die IT-, sondern insbesondere die Finanz- und die Risikoabteilungen die Verantwortung für Cyber-Risiken im Betrieb (Grafik 3). Dank dieser Umverteilung innerhalb der operativen Ebene ist auf eine intensivere Auseinandersetzung mit der finanzielle Tragbarkeit der Cyber-Restrisiken zu hoffen.

**GRAFIK 3**

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



## 3.3 CYBER RISK MANAGEMENT: WAS BRINGT ES DEN UNTERNEHMEN?

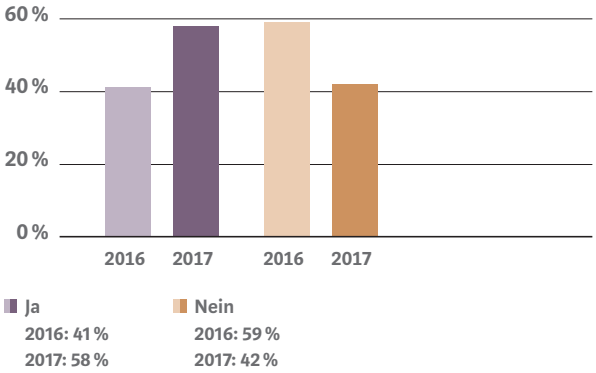
**Cyber-Risiken zu erkennen und sie in der Folge bewusst zu bewältigen scheint in der Theorie eine logische Konsequenz zu sein. In der Praxis fehlt es allerdings gerade an diesem Übergang vom Bewusstsein zur Handlung an Zeit, Wissen und an Motivation der Unternehmensführung, die grosse Unbekannte «Cyber-Risiken», nebst den anderen Top Firmenrisiken, proaktiv anzugehen. Cyber-Risiken werden sich in den nächsten Jahren nicht auflösen; vielmehr sollten sich die Unternehmen ihrer Cyber-Exposition bewusst sein und die Cyber-Widerstandsfähigkeit ihrer Institution verbessern.**

Bereits 58 % der Umfrageteilnehmer haben die finanziellen Auswirkungen eines betrieblichen Cyber-Ereignisses quantifiziert (2016 waren es lediglich 41%). Diese Resultate sind erfreulich und zeigen unseres Erachtens einmal mehr auf, dass die Cyber-Risiken zunehmend als ernst zu nehmende Unternehmensrisiken wahrgenommen werden (Grafik 4).

Quantifizieren Unternehmen Cyber-Vorfälle, werden die finanziellen Auswirkungen von über der Hälfte auf zwischen USD 1 und 10 Mio. geschätzt (Grafik 5). Im KMU-Sektor können Schäden bereits ab CHF 1 Mio. existenzbedrohend sein. Umso mehr erstaunt es, dass die Massnahmen in der Cyber-Prävention im Verhältnis zum erwähnten Schadenspotenzial auffallend hinterherhinken und die Auseinandersetzung mit Cyber-Versicherungslösungen trotz mittlerweile attraktiver Deckungs- und Prämienangebote tendenziell langsam erfolgt (Grafik 6).

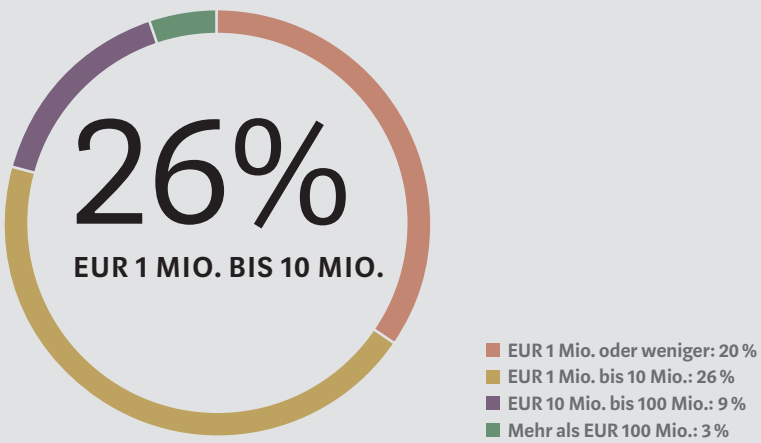
GRAFIK 4

**Haben Sie die finanziellen Auswirkungen eines Cyber-Ereignisses in Ihrem Unternehmen abgeschätzt?**




GRAFIK 5

**Sofern Ihr Unternehmen die finanziellen Auswirkungen eines Cyber-Ereignisses abgeschätzt hat, wie hoch ist der höchste potenzielle Verlustwert?**



GRAFIK 6

**Welche der nachfolgenden Schritte im Cyber-Risk-Management-Prozess hat Ihr Unternehmen in den letzten 12 bis 24 Monaten unternommen?**

### BEURTEILEN UND ANALYSIEREN

- Abschätzung finanzieller Auswirkungen von Cyber-Vorfällen: 58 %
- Durchgeführte Cyber-Security-Gap-Analyse: 46 %
- Modellierung potenzieller Cyber-Loss-Szenarien: 25 %

### SICHERN UND VERSICHERN

- Verschlüsselung von Desktops und Laptops des Unternehmens: 54 %
- Multi-Faktor-Authentifizierung für den Fernzugriff auf das Unternehmensnetzwerk: 45 %
- Penetrationstest durchgeführt: 41 %
- Cyber-Versicherung abgeschlossen: 40 %
- Implementierung Präventionsmassnahmen bei Datenverlust: 39 %
- Schwachstellen- und Patch Management verbessert: 31 %
- Vernetzung von externen Systemen reduziert: 26 %
- Neustrukturierung der bereits vorhandenen Cyber-Versicherung oder Deckungserhöhung: 14 %

### REAGIEREN UND WIEDERHERSTELLEN

- Einführung und Verbesserung von Social Engineering Awareness für Mitarbeitende: 69 %
- Entwicklung eines Cyber Incident Response Plan: 29 %
- Konkrete Verbesserungen bei der Erkennung von Cyber-Risiko-Ereignissen: 25 %
- Organisation externer Supportdienste (Recht, PR, IT-Security): 12 %

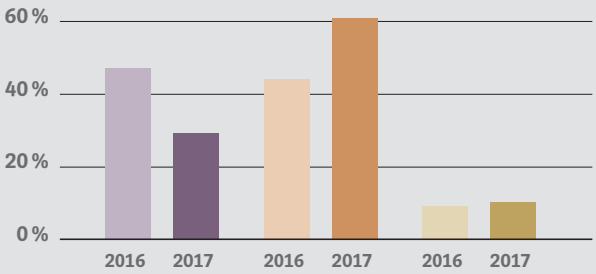
Wie auch immer das subjektive Empfinden der Befragten letztlich ist, es hat auf jeden Fall Auswirkungen auf das Cyber-Risikomanagement, vor allem auf das Einleiten oder Weglassen von Präventivmassnahmen:

Auffallend ist, dass rund 40 % der Umfrageteilnehmer angeben, eine Cyber-Versicherung abgeschlossen zu haben (Grafik 6 und 12). In Anbetracht des noch jungen Cyber-Versicherungsmarktes und der aktuellen Prämienvolumen in der Schweiz schätzen wir die Prozentzahl platzierter Cyber-Versicherungspolicen als deutlich niedriger ein. Vielmehr gehen wir davon aus, dass diese 40 % der Befragten entweder keine Cyber-Versicherung abgeschlossen haben, aber irrtümlicherweise davon ausgehen, dass die Risiken in den bestehenden Policen gedeckt sind oder dass einzelne Deckungskomponenten mit Cyber-Bezug als eine ausreichende Cyber-Deckung wahrgenommen haben. Viele Unternehmen wiegen sich deshalb in falscher Sicherheit und vernachlässigen als Folge tendenziell die Reaktions- und Wiederherstellungsmassnahmen (Grafik 6).

Im Weiteren führen die Ergebnisse im Bereich Reaktionsmassnahmen führen zur Annahme, dass 69 % der Unternehmen-Social-Engineering-Präventivmassnahmen getroffen haben. Aufgrund der Tatsache, dass die meisten Cyber-Risiken im Zusammenhang mit dem Faktor Mensch ausgelöst werden, wäre dieses Resultat sehr erfreulich. Bezugnehmend auf unsere täglichen Kundengespräche ist diese Angabe dennoch mit Vorsicht zu geniessen. So gelten zum Beispiel einmalige IT-Einführungsveranstaltungen oder gelegentliches Informieren der Mitarbeitenden über aktuelle Phishing-Versuche oft bereits als Social-Engineering-Awareness-Schulungen. Allen Zahlen zum Trotz erkennen wir dennoch eine deutlich grössere Bemühung der Unternehmen, den Faktor Mensch als schwächstes Glied in der Cyber-Sicherheitskette proaktiv anzugehen. Die menschlichen Eigenschaften, Hilfsbereitschaft, Gutgläubigkeit und Neugierde sind bei den Mitarbeitenden die grössten Schwachstellen und somit auch die grössten Gefahren. Deshalb bedarf es hier unbedingt einer jährlich wiederkehrenden Schulung – einmalige Schulungen verfehlen in der Regel einen langfristigen Nutzen.

## GRAFIK 7

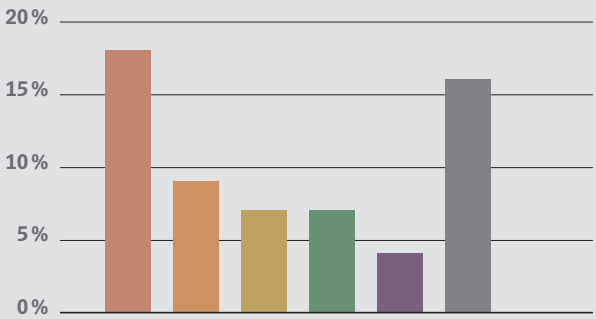
**Hat Ihr Unternehmen in den letzten 12 bis 24 Monaten einen Notfall-Reaktionsplan für Cyber-Ereignisse entwickelt?**




- Ja
  2016: 47 %
  2017: 29 %
- Nein
  2016: 44 %
  2017: 61 %
- Ich weiss es nicht
  2016: 9 %
  2017: 10 %

## GRAFIK 8

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




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

Die Investition in einen Notfall-Reaktionsplan zählt heute zu den absolut wichtigsten und langfristig günstigeren Präventivmassnahmen: Dennoch geben mindestens 61 % der Befragten an, in den letzten 12–24 Monaten keinen Notfall-Reaktionsplan entwickelt zu haben (Grafik 7). Dies obwohl die durchschnittliche Schadenhöhe infolge eines Cyber-Vorfalls von den meisten, die den Cyber Worst Case geschätzt haben, auf über USD 1 Mio. beziffert wird (Grafik 5). Begründet wird das Fehlen des Krisenplans zum grossen Teil mit dem Vorhandensein eigener Cyber-Sicherheit/Firewall sowie mit fehlendem Know-how (Grafik 8).

IT-technische Massnahmen werden hinsichtlich Cyber-Sicherheit vielfach noch überbewertet: Im Zeitalter der zunehmenden digitalen Vernetzung und Abhängigkeiten von Dritten rechtfertigen weder eine State of the Art aufgebaute Cyber/IT-Sicherheit/Firewall noch mangelndes Know-how das Fehlen eines Notfall-Reaktionsplans.

Wenigen ist bewusst, dass Cyber-Risiken und Naturkatastrophen ähnlich grossen wirtschaftlichen Schaden anrichten. So kann die Aussergefechtsetzung eines Cloud-Providers einen wirtschaftlichen Gesamtschaden von USD 50 bis 120 Mrd. betragen, was dem Schadenausmass von Hurrikan Sandy oder Katrina entspricht (WEF Report 2018). Die Abhängigkeit von integren Daten und verfügbaren Systemen ist hoch, ebenso die Schäden, und doch wird in Präventivmassnahmen wenig investiert: Der NotPetya-Angriff auf die Reederei Maersk vom Juni 2017 war ein teurer Weckruf: Der 10-tägige Betriebsunterbruch führte zu einer Umsatzeinbusse von 20 %, was einer Schadensumme von mindestens USD 250 Mio. entspricht. Mit einem vorab entwickelten Notfallmassnahmenplan (Desaster Recovery Plan) wären die Kosten um einiges geringer ausgefallen.

DIE BESTEN KARTEN HAT DERJENIGE, DER MIT EINEM ANGRIFF RECHNET UND AUF DIESEN VORBEREITET IST.

Massnahmen gegen Cyber-Risiken sollen nicht den Geschäftsbetrieb behindern, sondern die sensiblen Stellen im Betrieb besonders schützen. Wer den Umgang mit Sturmwellen trainiert, hat bei tatsächlichem Sturm die besseren Voraussetzungen, die Wellen geschickt und mit der notwendigen Ruhe zu meistern.

Wie im Vorjahr fürchten sich die meisten Schweizer Unternehmen vor einem Betriebsunterbruch. Der Reputationsschaden stellt die zweitgrösste Bedrohung dar, gefolgt vom Daten-/Softwareschaden sowie vom Verlust von Kundendaten. Dahinter folgen Erpressung/Ransomware, Unterbrechung von Industrieanlagen oder anderer Betriebstechnik, Haftung gegenüber Dritten aufgrund Systemverletzung, Verlust/Diebstahl von geistigem Eigentum, Betriebsunterbruch bei relevanten Lieferanten sowie Sach- und Personenschäden (Grafik 9).

Der cyberbedingte Betriebsunterbruch wird unseres Erachtens zu Recht in ganz Europa (Grafik 9) am meisten gefürchtet; die Schadenshöhe und die vielfältigen Schadensszenarien gleichen letztlich einer Wundertüte und werden mitunter davon beeinflusst, ob die IT-Systeme zentral oder dezentral angelegt sind, welche und wie viele IT-Dienstleister involviert sind, welches Backup-Konzept verfolgt wird etc. Der Gerichtsstand und das anwendbare Recht können ebenfalls grossen Einfluss auf die Kosten im Eigen- oder Drittschadenbereich haben.

Bezüglich Reputation wird die Meldepflicht im Rahmen der EU-DSGVO eine interessante Rolle spielen: Dank der bisher «erschwinglichen» Datenschutzbussen in der Schweiz und in Europa nahmen Unternehmen eher eine Busse in Kauf, um einen Hacker-Angriff auf die Kundendaten der Reputation zuliebe geheim zu halten. Wie sich die angedrohten hohen Bussen der EU-DSGVO in der Rechtspraxis

**GRAFIK 9**

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

| | Italien | Frankreich | |
|---|---|---|---|
| **Betriebsunterbruch** | 69 % | 83 % | |
| **Daten-/Softwareschaden** | 71 % | 83 % | |
| **Reputationsschaden** | 46 % | 42 % | |
| **Verlust von Kundendaten** | 40 % | 42 % | |
| **Haftung gegenüber Dritten aufgrund Systemverletzung** | 34 % | 42 % | |
| **Unterbrechung von Industrieanlagen oder anderer Betriebstechnik** | 34 % | 33 % | |
| **Erpressung/Ransomware** | 31 % | 33 % | |
| **Verlust/Diebstahl von geistigem Eigentum** | 26 % | 17 % | |
| **Betriebsunterbruch bei relevanten Lieferanten** | 20 % | 33 % | |
| **Sachschäden/Personenschäden** | 6 % | 25 % | |
| **Andere** | 34 % | 33 % | |
| **Ich weiss nicht** | 3 % | 0 % | |

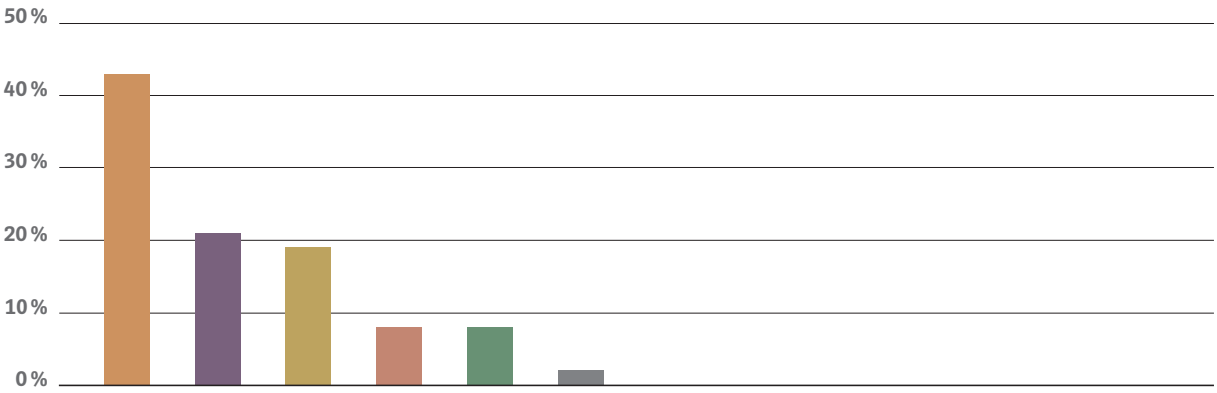
tatsächlich gestalten, bleibt abzuwarten. Klar ist: Der Kosten-Nutzen-Entscheid «Können/wollen wir uns eine Busse oder einen Reputationsschaden leisten?» wird den Unternehmen neue Strategien in Transparenzangelegenheiten und Kostenüberlegungen abverlangen.

Der Verlust von Kundendaten dürfte im Hinblick auf die EU-DSGVO und weitere europäische Datenschutzgesetze oder auch mit dem Datenschutz gekoppelte Gesetze – was das Schadenausmass anbelangt – eine zweite grosse Unbekannte werden. Dies nicht nur aufgrund des Kundendatenverlustes und allenfalls damit verbundener Meldepflichten an Betroffene oder Behörden, sondern vielmehr aufgrund anderweitig drohender hoher Bussen (bis zu 4 % des konsolidierten weltweiten Jahresumsatzes oder EUR 20 Mio.; DSGVO Art. 83) nach Zuwiderhandlung der EU-DSGVO. Zudem kann ein von einer EU-Behörde initiiertes Datenschutzuntersuchungsverfahren weitere Kosten im Eigenschadenbereich generieren, die sich zum heutigen Zeitpunkt nur schwer quantifizieren lassen.

| Spanien | Portugal | Deutschland | Schweiz | Rumänien | Belgien | Benelux |
|---|---|---|---|---|---|---|
| 84 % | 81 % | 75 % | 86 % | 82 % | 60 % | 63 % |
| 53 % | 54 % | 17 % | 53 % | 59 % | 47 % | 52 % |
| 53 % | 51 % | 25 % | 57 % | 41 % | 60 % | 63 % |
| 32 % | 49 % | 33 % | 52 % | 47 % | 47 % | 52 % |
| 37 % | 27 % | 17 % | 30 % | 29 % | 13 % | 24 % |
| 32 % | 41 % | 33 % | 33 % | 29 % | 27 % | 33 % |
| 42 % | 51 % | 25 % | 37 % | 29 % | 43 % | 41 % |
| 21 % | 24 % | 50 % | 22 % | 47 % | 37 % | 33 % |
| 32 % | 35 % | 25 % | 17 % | 29 % | 30 % | 30 % |
| 16 % | 5 % | 8 % | 11 % | 12 % | 13 % | 9 % |
| 32 % | 41 % | 33 % | 34 % | 29 % | 27 % | 33 % |
| 5 % | 0 % | 0 % | 2 % | 0 % | 0 % | 0 % |

**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: 43 %
- Menschliches Versagen von Mitarbeitenden oder Vertragspartnern: 21 %
- Ein böswilliger Mitarbeiter: 19 %
- Böswilliger/nicht böswillig handelnder Dritter mit autorisiertem Zugriff auf die IT-Ressourcen unseres Unternehmens: 8 %
- Technisches Versagen/Betriebsfehler: 8 %
- Politisch motivierte Bedrohung: 2 %

Malware ist bösartige Software, die entwickelt wird, um einem Computer-Nutzer zu schaden. Die mittlerweile kostengünstigen Hacker Tools sowie der zunehmende «Let's Share Knowledge»-Trend begünstigen die Verbreitung von Malware auch durch IT-Laien. Die Cyber-Angriffswellen vom Juni 2017, angeführt durch die Krypto-Trojaner WannaCry, Petya und NotPetya, zeigen nicht nur auf, welche Gefahren von Cyber-Kriminellen ausgehen, sondern verdeutlichen einmal mehr die in Europa vorherrschende Cyber-Kriminalität begünstigende IT-Monokultur. Die Neigung der Unternehmen, ähnliche Software, Sicherheitsprogramme sowie IT-Infrastruktur einzusetzen, öffnet bei erfolgreichen Cyber-Angriffen die Tür in andere Organisationen (Sigma Report 1/2017, SwissRe).

Die Diskussion über die Frage der meistgefürchteten Bedrohungsakteure im Zusammenhang mit einer Malwareinfizierung (Grafik 10) führt in unseren Kundengesprächen vielfach zu emotional geladenen Diskussionen. Weshalb ist das so? Der unrechtmässige Zugang zu Unternehmenssystemen erfolgt nicht selten über die Mitarbeitenden. Sie bilden das schwächste Glied der Cyber-Security-Kette. Der Mensch ist aufgrund seines emotionalen Wesens schwer berechenbar (vgl. auch Kommentar zu Grafik 6). Auch langjährige loyale, ältere oder jüngere, gut oder schlecht etablierte Mitarbeitende können ohne Vorzeichen nach gewissen Ereignissen kriminelle Energie gegen den Arbeitgeber entwickeln; oder gut ausgebildete Mitarbeitende können auf ein auf sie zugeschnittenes Phishing-E-Mail hereinfallen. Diese Problematik ist vielen bekannt. Dennoch fällt es unseren Kunden in Bezug auf ihre Mitarbeitenden vielfach schwer, diese als häufigste aktive oder passive Verursacher eines Cyber-Risikos in die Cyber-Restrisikoauseinandersetzung miteinzubeziehen. Unseres Erachtens wäre ein wichtiger Schritt getan, wenn das Restrisiko im Zusammenhang mit potenziell kriminellen oder leicht zu manipulierenden Mitarbeitenden ohne emotionalen Beigeschmack objektiv in die Cyber-Risikoanalyse miteinbezogen würde. Das vom Menschen ausgehende Cyber-Restrisiko schätzen wir auf mindestens 50 %.

## 3.4 RISIKOBEWERTUNG VON IT-ZULIEFERERN

**Um sich auf ihre Kernkompetenzen zu fokussieren, lagern immer mehr Unternehmen ihre Informationstechnologie und Informationssysteme aus. Nebst offensichtlichen Vorteilen ist Outsourcing immer mit Risiken verbunden. Wertvolle Daten und Business relevante Prozesse müssen in guten Händen sein, weshalb der IT-Provider mit Sorgfalt zu wählen ist. Outsourcing ist Vertrauenssache.**

IT-Outsourcing bedeutet, dass innerbetriebliche Aufgaben, basierend auf einem Vertragsverhältnis, abgegeben werden wie zum Beispiel Applikationen, Infrastruktur, Prozesse, Personal oder einzelne IT-Wartungsaufgaben. Effizienz- und Effektivitätssteigerung sowie niedrige Kosten sind klare Vorteile des Outsourcing. Die Nachteile wie Kontrollverlust über die Daten, fehlende Isolierung der verschiedenen Datenverarbeitungen zu anderen Cloud-Nutzern, Compliance-Risiken, Lock-in-Effekte sowie der Zugriff ausländischer Behörden auf Daten wiegen in der Regel schwerer, werden aber erstaunlicherweise oftmals ohne grosse Widerrede in Kauf genommen (Ausnahme sind Finanzinstitute, welche infolge strengerer Vorschriften des BaFin oder der FINMA weniger Wahlmöglichkeiten haben).

OUTSOURCING IST VERTRAUENSSACHE.

Der gezielte Angriff auf eine IT-Lieferkette ist lukrativ. Über den angegriffenen IT-Provider wird bspw. versucht, die Kontrolle über diverse Organisationen gleichzeitig zu erlangen, was zu enormen Cyber-Schäden führen kann. Die Haftungsrisiken werden im Rahmen des gesetzlich Möglichen in der Regel auf den Kunden abgewälzt. Insofern ist diesem bewusst zu machen, dass selbst führende Telekommunikationsunternehmen unter optimalen Service-Level-Bedingungen nur bedingt IT/Cyber-Sicherheit bieten und ein Unternehmen letztlich nicht vor Liquiditätsverlust oder gar Konkurs schützen können. Je grösser die Abhängigkeit von externen Dienstleistern, desto eher sollte deren Ausfall in das betriebliche Cyber Risk Management miteinbezogen werden. Hierzu liefert Grafik 11 interessante Zahlen.

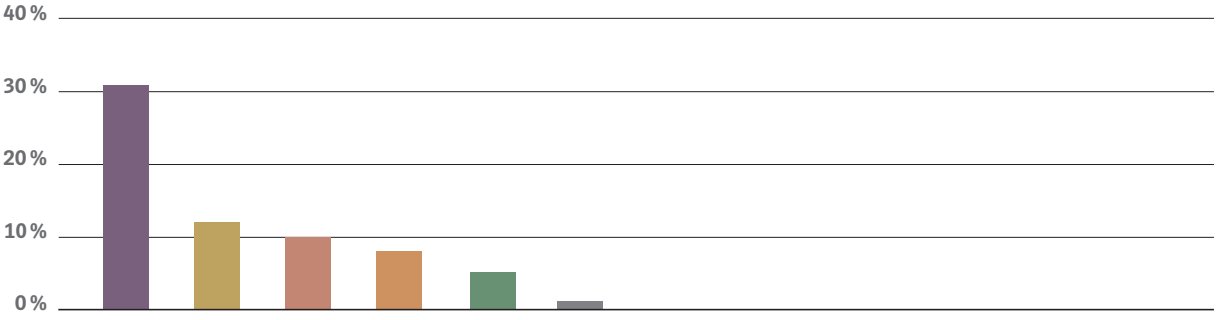
33 % BEWERTEN IHRE ZULIEFERER HINSICHTLICH CYBER-RISIKO-GEFÄHRDUNG. 46 % VERZICHTEN DARAUF. 21 % WISSEN ES NICHT.

Mittlerweile bewerten 33 % der Unternehmen ihre Zulieferer hinsichtlich Cyber-Risiko-Gefährdung; 2016 waren es erst 20 %. Dieses Resultat zeigt einen grossen Fortschritt zum letzten Jahr.

Dennoch zeigt Grafik 11 auf, dass die qualitative Auseinandersetzung der Unternehmen mit ihren IT-Lieferanten Verbesserungspotenzial aufweist. So gehören die Bewertung der Zulieferer hinsichtlich ihrer Cyber-Sicherheit, das Verlangen von Garantien für anhaltende Cyber-Sicherheit und -Monitoring, vertragliche Vereinbarungen im Hinblick auf Haftungsgrenzen für cyberbedingte Verluste, Analyse der Finanzkraft der Lieferanten sowie Verpflichtung von Lieferanten, selbst eine Cyber-Versicherung abzuschliessen, noch zu den seltenen Vorkehrungen.

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: 31 %
- Bewertung der Zulieferer hinsichtlich Cyber-Sicherheit sowie Verlangen von Garantien betreffend Cyber-Sicherheitshaltung: 12 %
- Vertragliche Regelungen im Hinblick auf Haftungsgrenzen für Cyber-Verluste: 10 %
- Regelmässiges Monitoring der Lieferanten im Hinblick auf deren Cyber-Sicherheitshaltung: 8 %
- Analyse der Finanzkraft der Lieferanten: 5 %
- Verpflichtung der Lieferanten, eine Cyber-Versicherung abzuschliessen: 1 %

## 3.5 ABSCHLÜSSE VON CYBER-VERSICHERUNGEN NEHMEN WEITERHIN ZU

**Der Cyber-Versicherungsmarkt entwickelt sich infolge neuer Cyber-Risiken stetig weiter, während die Unternehmen sich ebenfalls verändern. Je besser Unternehmen ihre Schwachstellen und Bedürfnisse im Cyber-Bereich erfassen, desto leichter fällt ihnen der Entscheid über die Finanzierungsstrategie: Eine Cyber-Versicherung kann Präventivmassnahmen niemals ersetzen, sondern soll im Schadenfall die Gefährdung von Bilanz und Erfolgsrechnung wie auch den Verlust liquider Mittel verhindern.**

Seit der Welle an Cyber-Attacken Mitte 2017 interessieren sich nebst Grossunternehmen zunehmend auch KMU für Cyber-Versicherungspolicen. Bei unseren Schweizer Kunden liegt der Fokus der Cyber-Versicherung nach wie vor auf der Deckung des cyberbedingten Betriebsunterbruchs. Aktuell bzw. noch vor direkter Wirkung der EU-DSGVO ab dem 25. Mai 2018 ist aufgrund noch fehlender europäischer Rechtsprechung und noch nicht vollständig geklärter bussenvollstreckungsrechtlicher Fragen schwer abzuschätzen, ob die EU-DSGVO infolge erhöhter versicherbarer Kostenrisiken in den Bereichen Datenschutzbussen, Benachrichtigungs- sowie regulatorischer Verfahrenskosten einen spürbaren Einfluss auf die Zunahme der Anzahl Cyber-Versicherungsabschlüsse in der Schweiz haben wird.

Gemäss der vorliegenden Umfrage haben 40 % unserer Kunden eine Cyber-Versicherung abgeschlossen, während 29 % planen, in den nächsten 12 Monaten eine entsprechende Versicherung zu platzieren oder die bestehende Deckungssumme zu erhöhen (Grafik 12).

DER UMGANG MIT DEM BUSSENRISIKO GEHÖRT EBENSO AUF DIE AGENDA DER UNTERNEHMENSFÜHRUNG WIE DER BEWUSSTE ENTSCHEID ÜBER DIE RISIKO-FINANZIERUNGSSTRATEGIE.

Die hohe Abschlussquote von 40 % erstaunt uns aufgrund der uns als Broker anvertrauten Cyber-Platzierungsaufträge sowie im Hinblick auf die aktuelle Marktlage für eigenständige Cyber-Versicherungen sehr. Wir vermuten, dass der Begriff Cyber-Versicherung unterschiedlich interpretiert wird, bspw. dass von einigen Befragten von einer stillschweigenden Cyber-Deckung im Rahmen eines Standardproduktes ausgegangen wird oder einzelne Cyber-Deckungskomponenten in konventionellen Versicherungsprodukten als Cyber-Deckung interpretiert werden.

GRAFIK 12

**Wie ist Ihr Unternehmen derzeit beim Cyber-Versicherungsschutz aufgestellt?**


- Meine Organisation hat eine Cyber-Versicherung abgeschlossen: 40 %
- Meine Organisation plant in den nächsten 12 Monaten eine Cyber-Versicherung abzuschliessen oder deren Deckungssumme zu erhöhen: 29 %
- Meine Organisation hat keine Cyber-Versicherung und hat nicht die Absicht, eine Cyber-Versicherung abzuschliessen: 16 %
- Ich weiss es nicht: 15 %

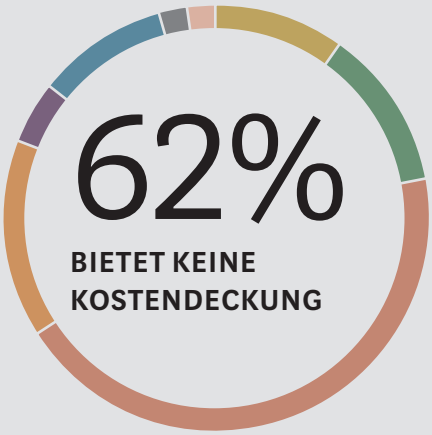
GRAFIK 13

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


- Cyber-Risk-Management-Pläne: 44 %
- Angeregt durch einen Cyber-Angriff auf andere Unternehmen: 30 %
- Selber einen Cyber-Angriff erfahren: 10 %
- Versicherungsnachweispflicht: 3 %
- Regulatorische Anforderungen wie bspw. von der EU-DSGVO: 16 %
- Auftrag des Verwaltungsrates: 26 %
- Ich weiss es nicht: 13 %

GRAFIK 14

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




- Fehlende interne Abstimmung über den Bedarf: 14 %
- Unsere Cyber-Sicherheit ist stark genug, sodass wir keine Cyber-Versicherung brauchen: 17 %
- Die Cyber-Versicherung bietet keine ausreichende Deckung der Kosten: 62 %
- Die verfügbare Deckung wird nicht verstanden: 21 %
- Unzureichendes Budget oder Ressourcen: 7 %
- Die Cyber-Deckung ist in einer anderen Police enthalten: 14 %
- Unsere Cyber-Risiken werden von unserem Captive getragen: 3 %
- Ich weiss es nicht: 3 %

Dass von über 40 % der Befragten, die bereits eine Cyber-Versicherung abgeschlossen haben oder gedenken, ihre Deckungssumme zu erhöhen, knapp die Hälfte als Treiber den aktuellen Cyber-Risk-Management-Plan angeben, ist nachvollziehbar (Grafik 13). Denn wer sich intensiver mit Cyber-Risiken und möglichen Folgeschäden auseinandersetzt, erkennt relativ rasch, dass ein mehrstündiger Betriebsausfall zu erheblichen finanziellen Verlusten führen kann.

Solange potenzielle Cyber-Worst-Case-Szenarien nicht quantifiziert werden, bleiben Cyber-Schäden für die Unternehmensführung reine «Überraschungspakete». Das Prinzip der Hoffnung ist unbestritten ein schlechter Ratgeber, wenn es um die Verhinderung der Haftung der Geschäftsführungsorgane geht – bspw. infolge nicht ausreichender IT-Sicherheitsmassnahmen oder entsprechendem Monitoring. Insofern erscheint wenigstens nachvollziehbar, dass Verwaltungsräte bei der Cyber-Risikofinanzierungsstrategie im eigenen Interesse vermehrt eine Top-down-Strategie vorgeben (vgl. auch Grafik 13).

31 % der Schweizer Unternehmen haben keine Cyber-Versicherung, haben nicht die Absicht, eine Cyber-Versicherung abzuschliessen oder verfügen über keinen entsprechenden Plan (Grafik 12). Als Hauptgrund wird die nicht ausreichende Kostendeckung (62 %) angegeben (Grafik 14).

In Bezugnahme auf die Resultate in Grafik 14 sehen wir einen Beratungsbedarf. Denn für Laien ist es kaum möglich, die unterschiedlichen Deckungskomponenten der Versicherer sowie die verlangten Kriterien der divergierenden Risikobeurteilungen auseinanderzuhalten. Die Sprache eines jeden Versicherers ist eine eigene, weshalb von einer Standard-Police, ohne Hinzuziehung eines Cyber-Fachspezialisten sowie ohne sorgfältige Marktprüfung, abzuraten ist. Die Bedürfnisse jedes Kunden sind zu ermitteln. Entsprechend ist jede Cyber-Police einzigartig. Der Cyber Worst Case sollte von der Deckung nicht ausgeschlossen sein.

# 4 EU-DSGVO ALS CHANCE ZUR STÄRKUNG DES CYBER-RISIKO-MANAGEMENT

## 4.1 URSACHE UND WIRKUNG DER EU-DSGVO COMPLIANCE

**Von vielen Schweizer Unternehmen als zeit- und kostenintensiv und daher oft als geschäftsbehindernd empfunden, hat die EU-DSGVO mindestens einen positiven Effekt: Unternehmen werden quasi gezwungen sich mit Cyber-Risiken auseinanderzusetzen und deren Bewältigung zu optimieren.**

Anfallende Kosten sind im Zusammenhang mit Datenschutzgesetzverletzungen kalkulierbar und grösstenteils (noch) versicherbar. Der bewusste Entscheid über einen sinnvollen Umsetzungsgrad der EU-DSGVO gehört unseres Erachtens ebenso auf die Agenda der Unternehmensführung, wie der bewusste Entscheid über die Risikofinanzierungsstrategie von Top Risiken.

Von den befragten Unternehmen, die der EU-DSGVO unterliegen, gaben Mitte 2017 nur 6 % an, vollständig EU-DSGVO-konform zu sein, während 51 % an der Entwicklung eines Plans sind, die EU-DSGVO entsprechend ihrer EU-Exponierung einzuhalten. Tatsache ist, dass 43 % der Schweizer Unternehmen entweder noch keinen Plan haben, die EU-DSGVO im Unternehmen zu integrieren, oder nicht wissen, wo das Unternehmen hinsichtlich Umsetzung der EU-DSGVO steht (Grafik 15).

In Anbetracht der Anstrengungen, die nötig sind, um die Vorschriften der EU-DSGVO einigermassen einzuhalten, ist davon auszugehen, dass in den letzten Wochen vor Inkrafttreten der EU-DSGVO (bis zum 25. Mai 2018) oder spätestens zum Zeitpunkt der ersten rechtskräftigen Bussenurteile eine weitere grössere Umsetzungswelle zur EU-DSGVO-Compliance die Unternehmen beschäftigen wird. Klar ist, dass durch die Sanktionsandrohungen der EU-DSGVO in Artikel 83 erhebliche Haftungsrisiken auf Schweizer Unternehmen zukommen können.

Dennoch ist der positive Effekt der EU-DSGVO nicht wegzureden: Unternehmen werden quasi gezwungen, ihre Fähigkeit zur Risikobewältigung und zur Reaktion auf eingetretene Risiken in der sich täglich ändernden Cyber-Risikolandschaft zu verbessern, um letztlich auch den Schutz personenbezogener Daten besser zu gewährleisten. Zum Beispiel enthält die EU-DSGVO die Verpflichtung, personenbezogene Daten so zu verarbeiten, dass eine angemessene Sicherheit gewährleistet ist, einschliesslich der Verhinderung des unbefugten Zugriffs oder Nutzung personenbezogener Daten und der für die Verarbeitung verwendeten Geräte. Daher sollte das für die Verarbeitung verantwortliche Unternehmen oder der Auftragsverarbeiter (z. B. der IT-Provider) die mit den personenbezogenen Daten verbundenen Risiken bewerten und Massnahmen zur Minderung dieser Risiken ergreifen (EU-DSGVO 32). Bei Zuwiderhandlung diverser Vorschriften gibt die EU-DSGVO überdies klare Regeln über die Bedingungen für die Verhängung von Verwaltungsstrafen vor: Künftig können gegen Unternehmen hohe Geldbussen verhängt werden, wenn jene ihre Kunden bspw. nicht über die erfolgte Kompromittierung personenbezogener Daten informiert haben, oder allenfalls auch, wenn die Benachrichtigung erst auf Druck von aussen erfolgte.

Jeder weiss, dass ein entsprechender Notfallreaktionsplan für ein definiertes Risiko zu den wirksamsten kostensenkenden Massnahmen gehört (man vergleiche die weit verbreiteten «Feuerwehrübungen» mit der gesamten Belegschaft). Daher erstaunt es, dass lediglich 23 % der Befragten einen Reaktionsplan im Hinblick auf Datenschutzverletzungen entwickelt haben (Grafik 16).

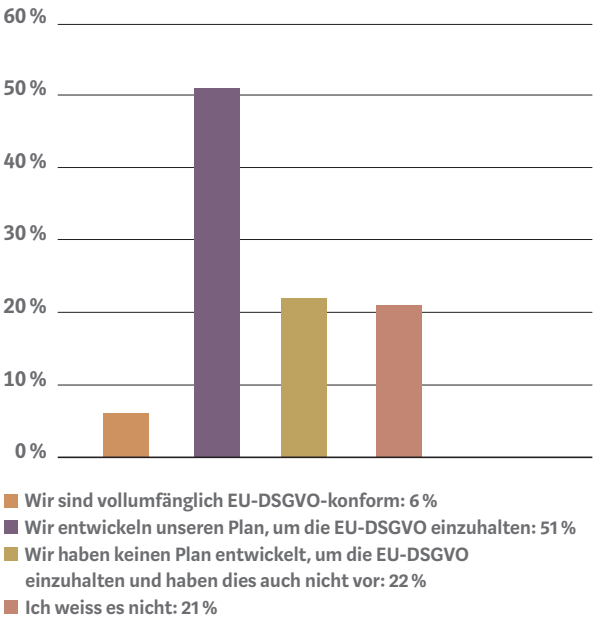
Zwar schreibt die EU-DSGVO keinen Notfallreaktionsplan für Cyber-Vorfälle vor, verlangt aber die Benachrichtigung der Aufsichtsbehörden innerhalb von 72 Stunden nach Bemerken eines Datensicher-

heitsvorfalles. Es liegt auf der Hand, dass diese fristgerechte Benachrichtigung mit einem Notfallmassnahmenplan eher gelingt als ohne. Wenn die Kosten infolge Cyber-Vorfällen von Anfang an klein gehalten werden sollten, ist der Kosten-Nutzen-Entscheid (Kostenaufwand/interner Aufwand versus Verminderung des Schadensausmasses im Notfall) vor dem ersten Cyber-Vorfall zu treffen.

Aller Vernunft zum Trotz: Der Unternehmensführung steht es frei, einen risikofreudigen Kurs einzuschlagen und damit auch allfällige IT-Sicherheitsvorkehrungen bewusst zu unterlassen. Wichtig erscheint, dass der Umgang mit dem Bussenrisiko aufgrund der EU-DSGVO ebenso auf der Agenda der Unternehmensführung steht wie der bewusste Entscheid über die Risikofinanzierungsstrategie von Top Risiken. Aufgrund der bisher erschwinglichen Datenschutzbussen ist davon auszugehen, dass Schweizer Unternehmen eine Busse bislang eher in Kauf nahmen, um einen Hacker-Angriff auf die Kundendatenbanken der Reputation zuliebe geheim zu halten, als die Betroffenen oder die Behörde zu informieren. Diese Praxis wird sich mit der Einführung der EU-DSGVO und allenfalls auch im Zuge der 2. Revision des Schweizer Datenschutzgesetzes ändern.

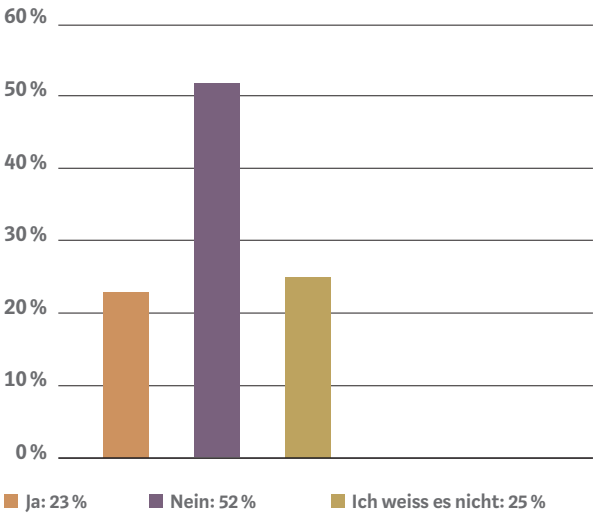
**GRAFIK 15**

**Welche Fortschritte hat Ihre Organisation in Richtung EU-DSGVO-Compliance-Bereitschaft gemacht?**




**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

Die Fortschritte der digitalen Geschäftsmodelle führen zu einem schwer überblickbaren Datenverkehr, zu einer unvorstellbar grossen digitalen Datenmenge und dadurch zu einem Anstieg von Cyber-Risiken. Vielen Unternehmen fehlt es am praktischen Know-how, sich diesen Herausforderungen zu stellen und sie sinnvoll zu bewältigen.

Cyber-Risiken sind komplex und bergen die Gefahr erheblicher Kumulschäden, womit die eigenen Cyber-Risiken, aber auch diejenigen der zur Lieferkette gehörenden IT-, Rohstoff- oder Teilkomponentenlieferanten im Blickwinkel des betrieblichen Risk Management sein sollten. Der Initialaufwand für einen sinnvollen Umgang mit Cyber-Risiken ist zeitaufwendig, generiert Kosten und ist zusätzlich zu den übrigen ebenfalls ernstzunehmenden Unternehmensrisiken unbestritten mühsam.

Klar ist: Cyber-Risiken können wir angesichts der fortschreitenden Digitalisierung nicht aus der Welt schaffen. Umso wichtiger wird ein gezieltes Cyber Risk Management, das den Geschäftsbetrieb nicht behindert, sondern die Cyber-Widerstandsfähigkeit der Unternehmen bzw. letztlich die Schweizer Wirtschaft stärkt.

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 anspruchsvoll. Einen Beratungsbedarf sehen wir weiterhin bei der Zuteilung der Verantwortlichkeit für Cyber-Risiken im Unternehmen, bei der Lokalisierung und Analyse der Cyber-Risiken im Unternehmen sowie verstärkt in der Umsetzung angemessener diversifizierter Präventivmassnahmen. Cyber Risk Management beinhaltet nebst den diversifizierenden Präventivmassnahmen weitere auf die Finanzkraft und Risikoversicherungspolitik angepasste Risikofinanzierungsstrategien.

**Sie haben Fragen? Vereinbaren Sie ein persönliches Beratungsgespräch:**

**Dr. Helmut Studer**
Mitglied der Geschäftsleitung
helmut.studer@kessler.ch
T +41 44 387 87 17

**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