Allianz Global Corporate & Specialty SE

MANAGEMENT VON CYBER-RISIKEN

MEHR ALS VERSICHERUNGS-EINKAUF

Michael Daum
Senior Underwriter Cyber

München, 9.5.2019

Allianz

CYBER IST HEUTE EIN TOP UNTERNEHMENSRISIKO

1 37%

Betriebsunterbrechung
(inkl. Lieferkettenunterbrechung)

= 2018: 42% (1)

1 37%

Cybervorfälle
(z.B. Cyberkriminalität, IT-Ausfall, Datenschutzverletzungen, Geldbußen und Strafen)

= 2018: 40% (2)

3 28%

Naturkatastrophen
(z.B. Sturm, Überschwemmung, Erdbeben)

= 2018: 30% (3)

4 27%

Rechtliche Veränderungen
(z.B. Handelskriege und Zölle, Wirtschaftssanktionen, Protektionismus, Brexit, Zerfall der Euro-Zone)

⬆ 2018: 21% (5)

5 23%

Marktentwicklungen
(z.B. Volatilität, verstärkter Wettbewerb/neue Wettbewerber, M&A, stagnierende Märkte, Marktschwankungen)

⬇ 2018: 22% (4)

6 19%

Feuer, Explosion

= 2018: 20% (6)

7 19%

Neue Technologien [2]
(z.B. Auswirkung der Vernetzung von Maschinen, Nanotechnologie, künstliche Intelligenz, 3D-Druck, autonome Fahrzeuge, Blockchain)

= 2018: 15% (7)

8 13%

Klimawandel/steigende Volatilität des Wetters

⬆ 2018: 10%(10)

9 13%

Reputationsverlust oder Beeinträchtigung des Markenwerts [3]

⬇ 2018: 13% (8)

10 9%

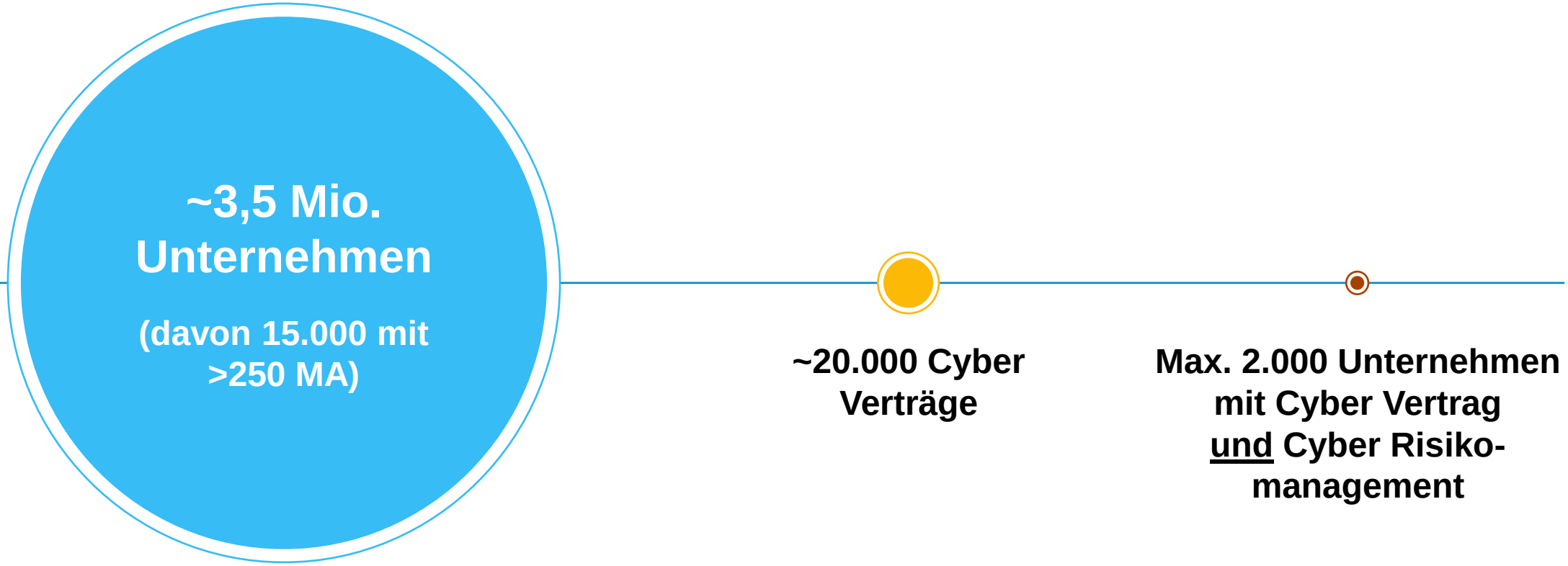
Fachkräftemangel

⬆ 2018: 6% (15)

Quelle: Allianz Global Corporate & Specialty. Fotos: Adobe, iStock. Die Zahlen geben die Anzahl der ausgewählten Risiken als Prozentsatz aller Umfrageantworten (hier: 2.882) an. Die 2.451 Befragten konnten Antworten für bis zu zwei Branchen und bis zu drei Risiken pro Branche auswählen. Die Prozentwerte addieren sich daher nicht auf 100%

CYBER RISIKOMANAGEMENT UND CYBER VERSICHERUNG IN DER BREITE KAUM ETABLIERT

Werte für Deutschland



CYBER RISIKOMANAGEMENT KOMMT VOR CYBER RISIKOTRANSFER

Cyber Risiken erfassen

- Erfassung der Cyber Angriffsvektoren (extern wie intern)
- Betrachtung der Auswirkungen auf qualitativer Ebene

Cyber Risiken modellieren

- Bewertung nach Frequenz und Schadenhöhe (Quantifizierung)
- Priorisierung und Fokussierung auf die Top Cyber Szenarien

Cyber Risiken managen

- Entscheidung zum Umgang:
  - Vermeiden
  - Reduzieren
  - Akzeptieren
  - Transferieren (u.a Cyber Versicherung)

Risiko einer Pflichtverletzung für Führungskräfte steigt!

BEISPIEL RISIKOMODELLIERUNG/-QUANTIFIZIERUNG: EXPONIERUNG AUS PERSONENBEZOGENEN DATEN

Exponierung =

Anzahl Personenbez. Daten

- Abschätzung über **Zählung** der Kunden, Interessenten, etc.
- Herausforderung: Mehrfachzählung vermeiden

X

Schaden pro Datensatz

- Studien verfügbar, z.B. „Ponemon Studie“[1]; Kosten für jeden verlorenen Datensatz bei **durch-schnittlich 167€** (in Deutschland)
- **Klassifizierung** der Daten, v.a. Anteil sog. besonderer Kategorien personenbezogener Daten

X

Eintrittswahrscheinlichkeit

- Mehr Transparenz aufgrund **Meldepflichten nach DSGVO**
- „Ponemon Studie“[1]: für Deutschland **14% Wahrscheinlichkeit** innerhalb der nächsten 2 Jahre
- Individuelle **Kalibrierung nach eigenen Risikofaktoren** (z.B. Schutzmaßnahmen, Attraktivität der Kundendaten, etc.)

1. IBM/Ponemon: 2018 Cost of a Data Breach Study

CYBER DECKUNG HAT SICH DEUTLICH ENTWICKELT

Deckungsumfang 2011

Drittschaden

- Datenschutz- bzw. Vertraulichkeitsverletzungen
- Weitere Haftpflichtansprüche

Eigenschaden

- Betriebsunterbrechung (eingeschränkt)
- Wiederherstellung
- Cyber Diebstahl
- Erste Assistance-Dienstleistungen

+

Deckungsumfang 2016

Allgemein

- Deckung auch für nicht-zielgerichtete Angriffe
- Weniger Ausschlüsse

Eigenschaden

- Betriebsunterbrechung (weite Deckung)
- Einschluss benannter ext. IT-Dienstleiter
- Systemverbesserungen

+

Deckungsumfang 2019

Drittschaden

- Vertragsstrafen/Pönale

Eigenschaden

- Cyber Erpressungs-versicherung
- Sachschäden an der IT-Hardware
- Breite Assistance-Dienstleistungen
- Pauschaler Einschluss Externer IT-Dienstleiter / Cloud-Provider für BU

CYBER SCHADENERFAHRUNG – ÜBERBLICK & AUSBLICK

Gesamtüberblick

Durchschnittliche Schadenhöhe

Schadenhäufigkeit

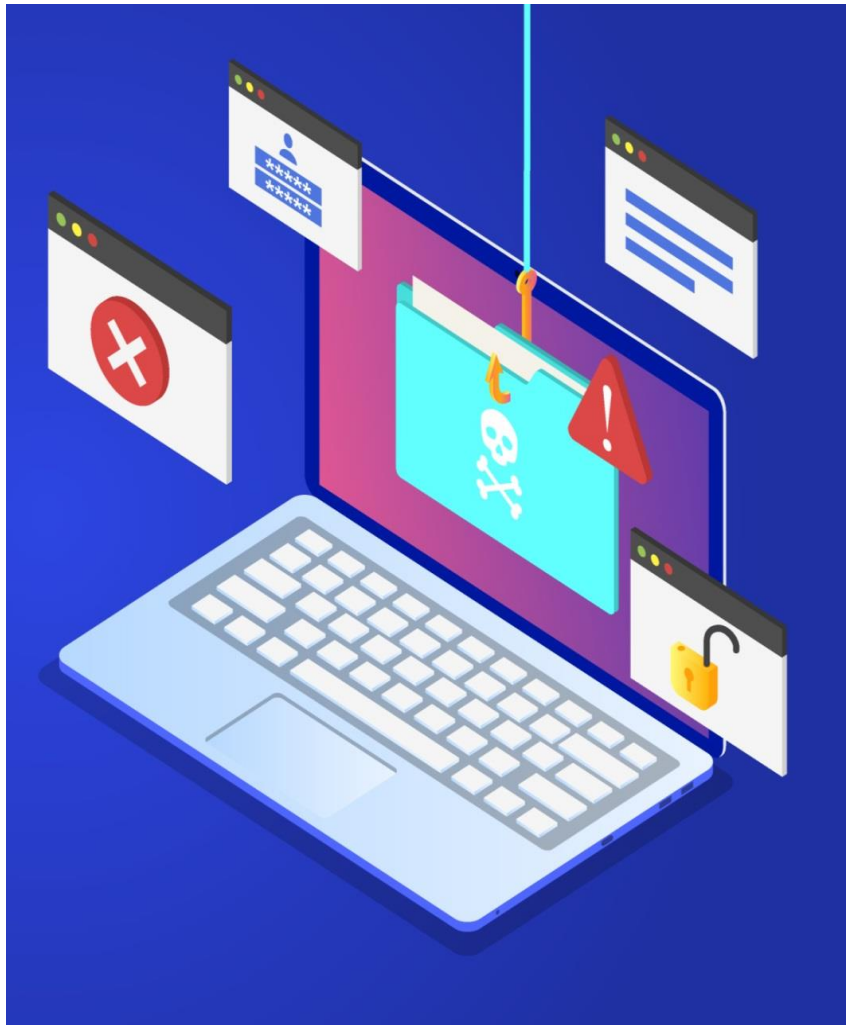
	Selten	Mittel	Häufig
Hoch	Allg. Haftpflicht-ansprüche	Betriebsunter-brechung	
Mittel	Vertraulichkeits-verletzungen	Cyber Diebstahl	Datenschutz-verletzungen Assistance Dienstleistungen
Niedrig	Rechtswidrige Kommunikation E-Payment/PCI		Cyber Erpressung

Trends 2018/2019

- Erpressung nach ziel-gerichteten Angriffen häufiger
- Betriebsunterbrechung tritt verstärkt auf
- Cyber-Diebstahl nimmt zu
- Kosten für Assistance Dienstleistungen steigen
- Bußgelder nach EU-DSGVO noch nicht erhöht
- E-Payment / PCI Schäden seltener

REALES SCHADENBEISPIEL: PHISHING MAIL FÜHRT ZU DATENSCHUTZVERLETZUNG UND BETRUG

Ein Betrüger gibt sich als Vorstand aus und schickt **gefakte Mail** (von außen, kein Cyber Angriff) an HR-Mitarbeiter einer US Tochter unseres deutschen VN. Dieser lässt ihm die **Personalstammdaten** (inkl. Social Security Nummern, Steuernummern, etc.) **von ca. 2500 Mitarbeitern** zukommen. Der Angreifer nutzt diese für diverse Betrügereien wie Steuerrückerstattungen. Die betroffenen Mitarbeiter klagen im Rahmen einer Consumer Class Action.



Ist der Fall gedeckt?

- Deckung bei Datenschutzverletzungen auch ohne Cyber Angriff? ***Ja!***
- Ist (grobe) Fahrlässigkeit bzw. Vorsatz des Mitarbeiters schädlich? ***Nein!***

Welche Leistungen werden fällig?

- Rund **USD 1 Mio.** für das Settlement + ca. **USD 1 Mio.** für Rechtskosten
- Schaden somit bei knapp **USD 1.000 pro Datensatz**!

Was sind Implikationen für das Risikomanagement?

- Umfassende **Modellierung** Cyber Szenarien notwendig
- **Informationssicherheit** ist mehr als technische IT-Security

CYBER TAKE-AWAYS FÜR MANAGER/ENTSCHEIDER

Erfassen und Quantifizieren Sie Cyber Risiken im Ihrem (Enterprise) Risk Management – Sie brauchen die IT dazu, es ist aber keine Aufgabe der IT

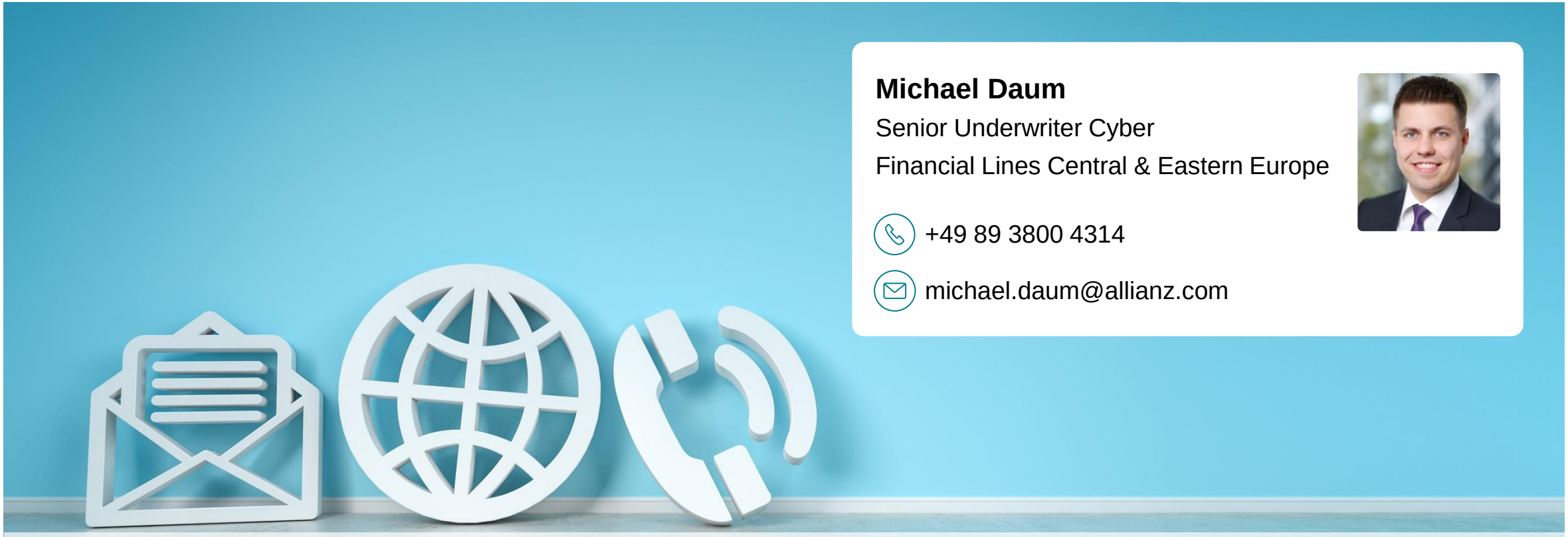
Treffen Sie eine qualifizierte Entscheidung zum Umgang mit Cyber Risiken – dies kann auf Versicherungseinkauf hinauslaufen, muss aber nicht!

Integrieren Sie Cyber Incidents in Ihrem Business Continuity Management und in den allg. Krisenreaktionsplänen

Kümmern Sie sich um professionelle externe Unterstützung für den Tag X – er wird kommen!

ALLIANZ GLOBAL CORPORATE & SPECIALTY

IHR KONTAKT



Michael Daum

Senior Underwriter Cyber

Financial Lines Central & Eastern Europe

+49 89 3800 4314

michael.daum@allianz.com

Follow AGCS

Sign up for ‘eUpdate’, our regular newsletter on www.agcs.allianz.com

DISCLAIMER

Vorbehalt bei Zukunftsaussagen

Soweit wir in diesem Dokument Prognosen oder Erwartungen äußern oder die Zukunft betreffende Aussagen machen, können diese Aussagen mit bekannten und unbekannten Risiken und Ungewissheiten verbunden sein. Die tatsächlichen Ergebnisse und Entwicklungen können daher wesentlich von den geäußerten Erwartungen und Annahmen abweichen.

Neben weiteren hier nicht aufgeführten Gründen können sich Abweichungen aufgrund von (i) Veränderungen der allgemeinen wirtschaftlichen Lage und der Wettbewerbssituation, vor allem in Allianz Kerngeschäftsfeldern und -märkten, (ii) Entwicklungen der Finanzmärkte (insbesondere Marktvolatilität, Liquidität und Kreditereignisse), (iii) dem Ausmaß oder der Häufigkeit von Versicherungsfällen (zum Beispiel durch Naturkatastrophen) und der Entwicklung der Schadenskosten, (iv) Sterblichkeits- und Krankheitsraten beziehungsweise -tendenzen, (v) Stornoraten, (vi) insbesondere im Bankbereich, der Ausfallrate von Kreditnehmern, vii) Änderungen des Zinsniveaus, (viii) Wechselkursen, einschließlich des Euro/US Dollar-Wechselkurses, (ix) Gesetzes- und sonstigen Rechtsänderungen, insbesondere hinsichtlich steuerlicher Regelungen, (x) Akquisitionen, einschließlich anschließender Integrationsmaßnahmen, und Restrukturierungsmaßnahmen, sowie (xi) allgemeinen Wettbewerbsfaktoren ergeben. Terroranschläge und deren Folgen können die Wahrscheinlichkeit und das Ausmaß von Abweichungen erhöhen.

Keine Pflicht zur Aktualisierung

Die Gesellschaft übernimmt keine Verpflichtung, die in dieser Meldung enthaltenen Informationen und Zukunftsaussagen zu aktualisieren, soweit keine gesetzliche Veröffentlichungspflicht besteht.

DANKE