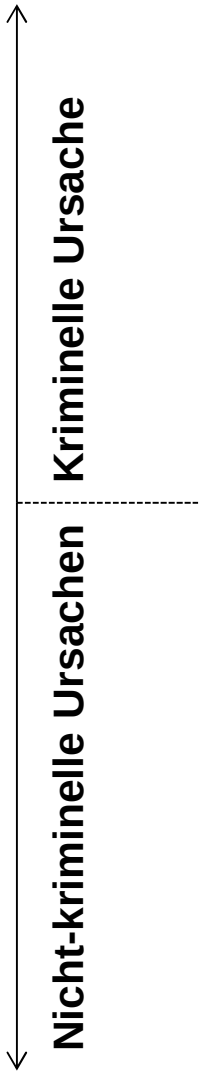
KESSLER

IT-SECURITY INSIDE # 18
SINN UND UNSINN VON CYBER-VERSICHERUNGEN

Melanie Koller, Legal Counsel Cyber Risk, Kessler & Co AG

Zürich, 29. Mai 2018

CYBER RISK UND DER FAKTOR MENSCH



Ursache

Hacker-Attacke

Physischer Angriff

Menschliches Versagen

Technisches Versagen

Naturereignis

95% Faktor Mensch

5% Faktor Technologie

Cyber-Risiken

Datenverlust

IT / ICT-Störung

E-Crime

Allgemeine Konsequenzen
Vertraulichkeit, Integrität, Verfügbarkeit

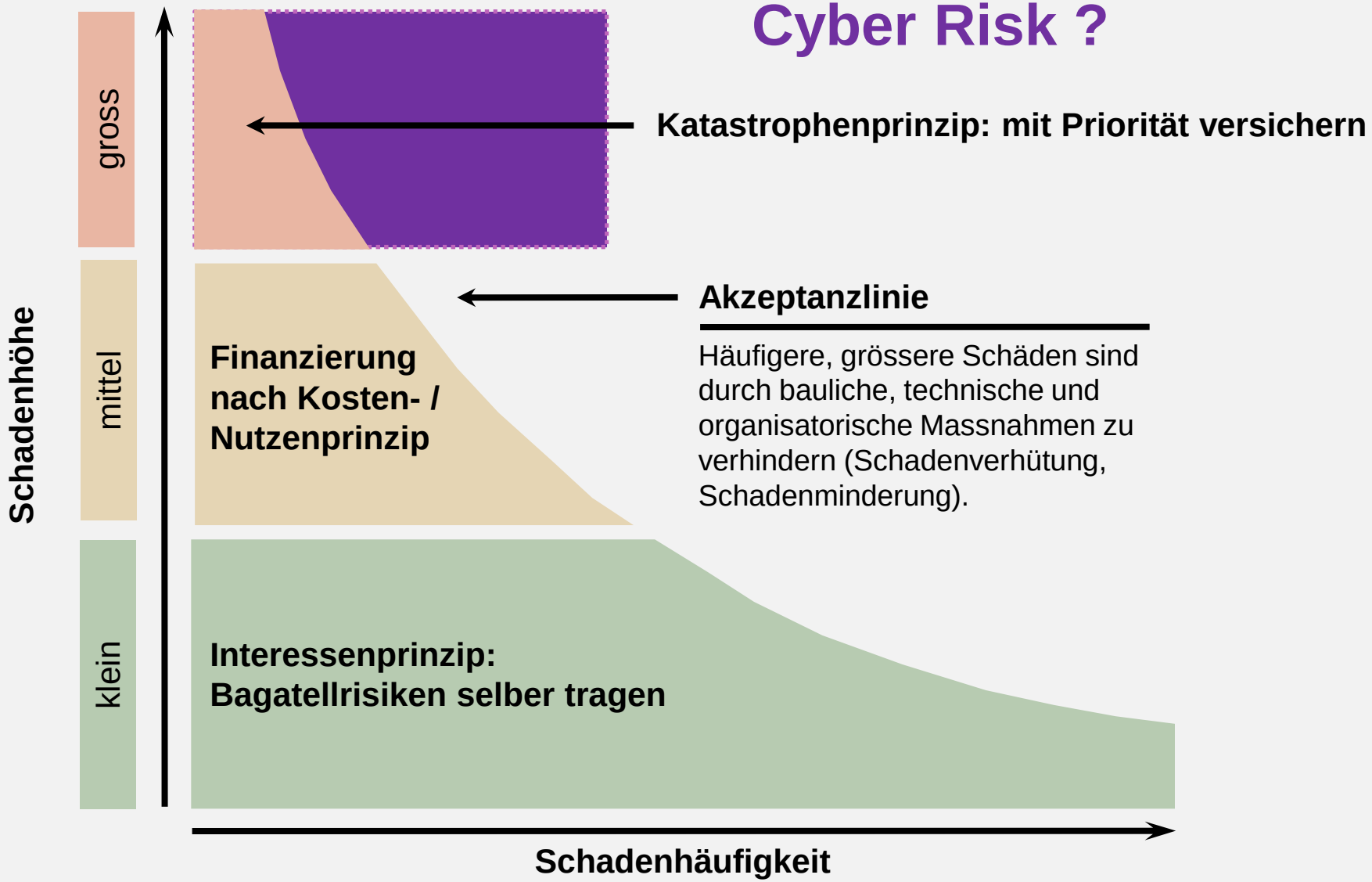
Reputation

Datenschutzgesetzverletzung

Finanzielle Auswirkungen

Bewältigung von Cyber-Risiken
Mit Cyber-Risikomanagement

CYBER-RISIKOMANAGEMENT



LOGISCH? – UNLOGISCH?

Cyber- / IT- Risiken = Unternehmensrisiken.

Unternehmensrisiken dürfen den Strategieplan eines Unternehmens nicht gefährden.

- Sicherheitsstandard für Unternehmenswerte vs. Standard im Umgang mit Daten/Server
- Investitionen in digitalisierte Unternehmensprozesse vs. Investitionen in IT-Prävention
- Schadensausmass > 1 Mio. EUR; dennoch trägt grösstenteils die IT-Abteilung die Verantwortung für Cyber-Risiken; dennoch werden Cyber-Risiken grösstenteils nicht quantifiziert.
- Umgang mit Betriebsunterbruch infolge Feuer vs. Betriebsunterbruch infolge eines Cyber-Incident
- Für das Jahr 2020 massiver Anstieg IoT und Industrie 4.0; ist Cyber Risk ein Hype?

CYBER-RISIKOMANAGEMENT-PROZESS: DIE ROLLE DER IT-ENTSCHEIDUNGSTRÄGER

Die Rolle der IT-Entscheidungsträger

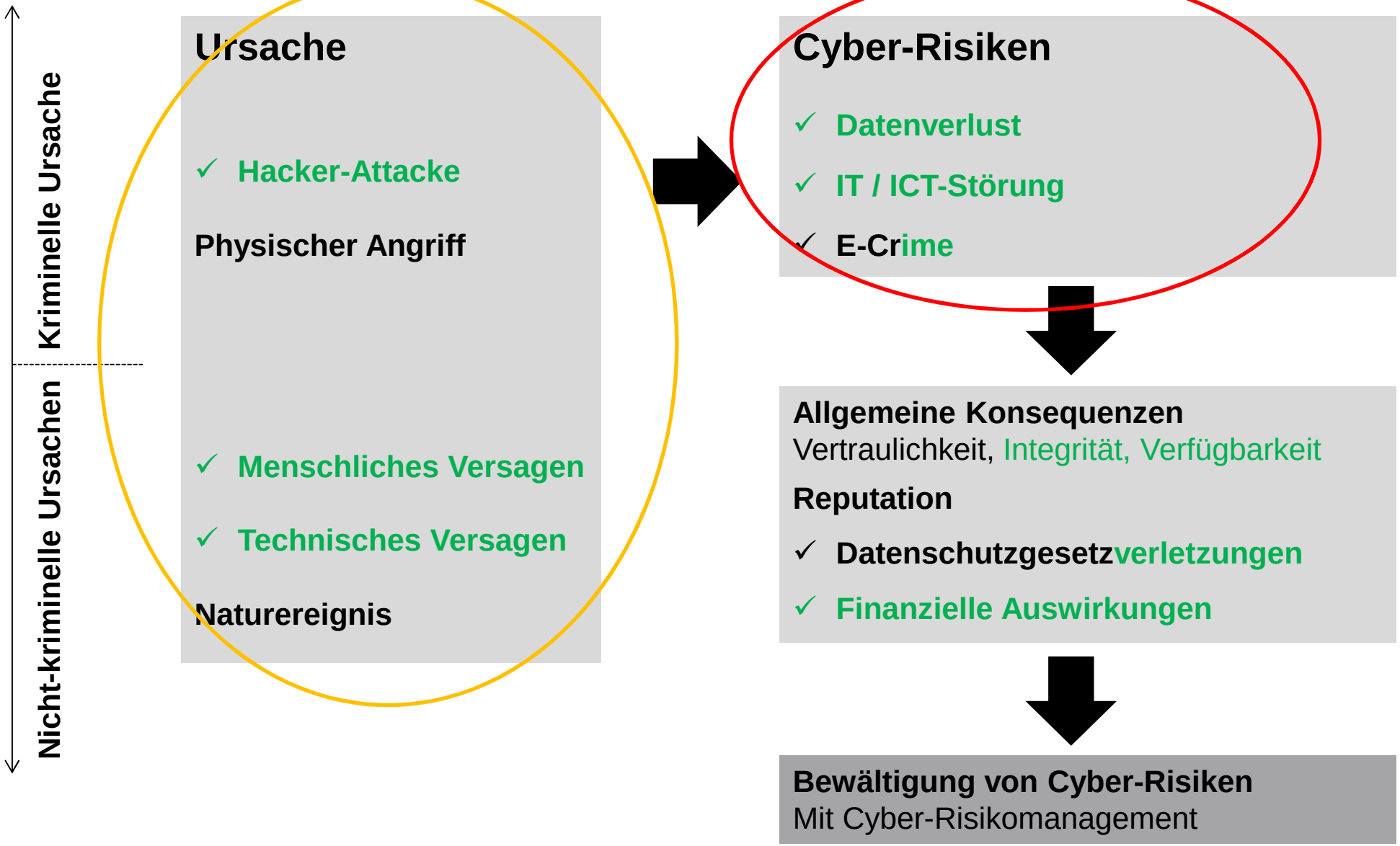
- Cyber-Risiken sind u.a. finanzielle Risiken und deshalb ein zentrales Thema für den CFO; der IT-Entscheidungsträger und der CFO bilden im Cyber-Dialog m.E. optimale Synergien.
- Auch der IT-Entscheidungsträger (u.a. der CFO) sensibilisiert den VR hinsichtlich Cyber-Risiken.
- IT-Entscheidungsträger (u.a. der CFO) ist einer der Schlüsselpersonen im Cyber Risk Management-Prozess.
- Der IT-Entscheidungsträger (u.a. der CFO) sollte das Cyber-Restrisiko quantifizieren können.
- Schutz der grossen Restrisiken: Umsatzrelevante Geschäftsdaten / Business relevante Prozesse, die letztlich für die Erreichung der Jahresziele des Unternehmens in finanzieller Hinsicht relevant sind, sind m.E. mit Priorität zu schützen.

CYBER-VERSICHERUNG

✓ **Cyber-Versicherung**

Voraussetzung 2

Voraussetzung 1



CYBER-VERSICHERUNG: VERSICHERBARE KOSTEN

Grundsätzlich (heute) nicht versichert

- Unterbrechung Internet
- Wiederbeschaffung Hardware
- Geldüberweisung infolge Social Engineering
- Entgangener Gewinn infolge Reputationsschaden
- Abwehr/SE infolge Verletzung geistigem Eigentum Dritter

CYBER-VERSICHERUNG & EU-DSGVO: WELCHE KOSTEN SIND GRUNDSÄTZLICH VERSICHERBAR?

Eigenschaden

- ✓ **Kosten für Krisenmanagement**
- ✓ **Kosten für Benachrichtigung Betroffener / Behörden nach Datenschutzverletzung**
- ✓ **Untersuchungskosten von Datenschutz- oder sonstigen Behörden**
- ✓ **Gewisse Datenschutzbussen, SOFERN … / ABER …**
- ✓ **Abwehrkosten (Passiver Rechtsschutz) nach Datenschutzverletzung**

Drittschaden

- ✓ **Zahlung von Schadenersatzansprüchen Dritter nach Datenschutzverletzung**
- ✓ **Rechts- und Beratungskosten bei regulatorischen Verfahren, Datenschutzbussen und Benachrichtigung Dritter**

CYBER-VERSICHERUNG: SINN ODER UNSINN?

HABEN SIE FRAGEN?

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

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 250 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.

RESERVE

FINANZIELLE AUSWIRKUNGEN: WO ENTSTEHEN HOHE KOSTEN?

Finanzielle Auswirkungen (Schadenausmass) können sein:

Eigenschaden

- Kosten für Krisenmanagement (u.a. externe IT-Forensiker, Juristen, PR-Berater)
- Kosten für Wiederherstellung oder Ersatzbeschaffung von Daten
- Kosten für physischen Schaden an IT-Infrastruktur
- Kosten bei Betriebsunterbruch, welche zur Fortführung der Geschäftsaktivitäten aufgewendet werden inkl. entgangener Gewinn
- Kosten für Benachrichtigung Betroffener/Behörden nach Datenschutzrechtsverletzung, Kosten im Zusammenhang mit regulatorischen Datenschutzverfahren sowie Datenschutzbussen
- Kosten für Durchsetzung eigener verletzter Rechte durch Dritte (Intellectual Property)
- Erpressungszahlungen und zusammenhängende Folgekosten
- Vermögensverlust infolge Social Engineering und zusammenhängende Folgekosten
- Vermögensverlust infolge Diebstahl von digitalen Vermögenswerten oder Geld
- Kosten für Schäden verursacht durch externe IT-Dienstleister (insb. Service-Provider)
- Abwehrkosten (passiver Rechtsschutz); Verfahrenskosten und Bussen
- Kosten infolge Reputationsschaden

Drittschaden

- Zahlung von Schadenersatzansprüchen Dritter nach
  - Datenschutzverletzung samt Rechts- und Beratungskosten bei regulatorischen Verfahren, Datenschutzbussen und Benachrichtigung Dritter
  - nachdem eigene Mitarbeiter oder eigene Systeme an Dritten oder Drittsystemen einen Schaden verursacht haben
  - Persönlichkeitsverletzung oder Ehrverletzung
  - Verletzung oder Verlust von geistigem Eigentum Dritter
- Zahlung von Schadenersatz oder Konventionalstrafen infolge Vertragsverletzung (bspw. SLA)