CYBER-RESILIENZ

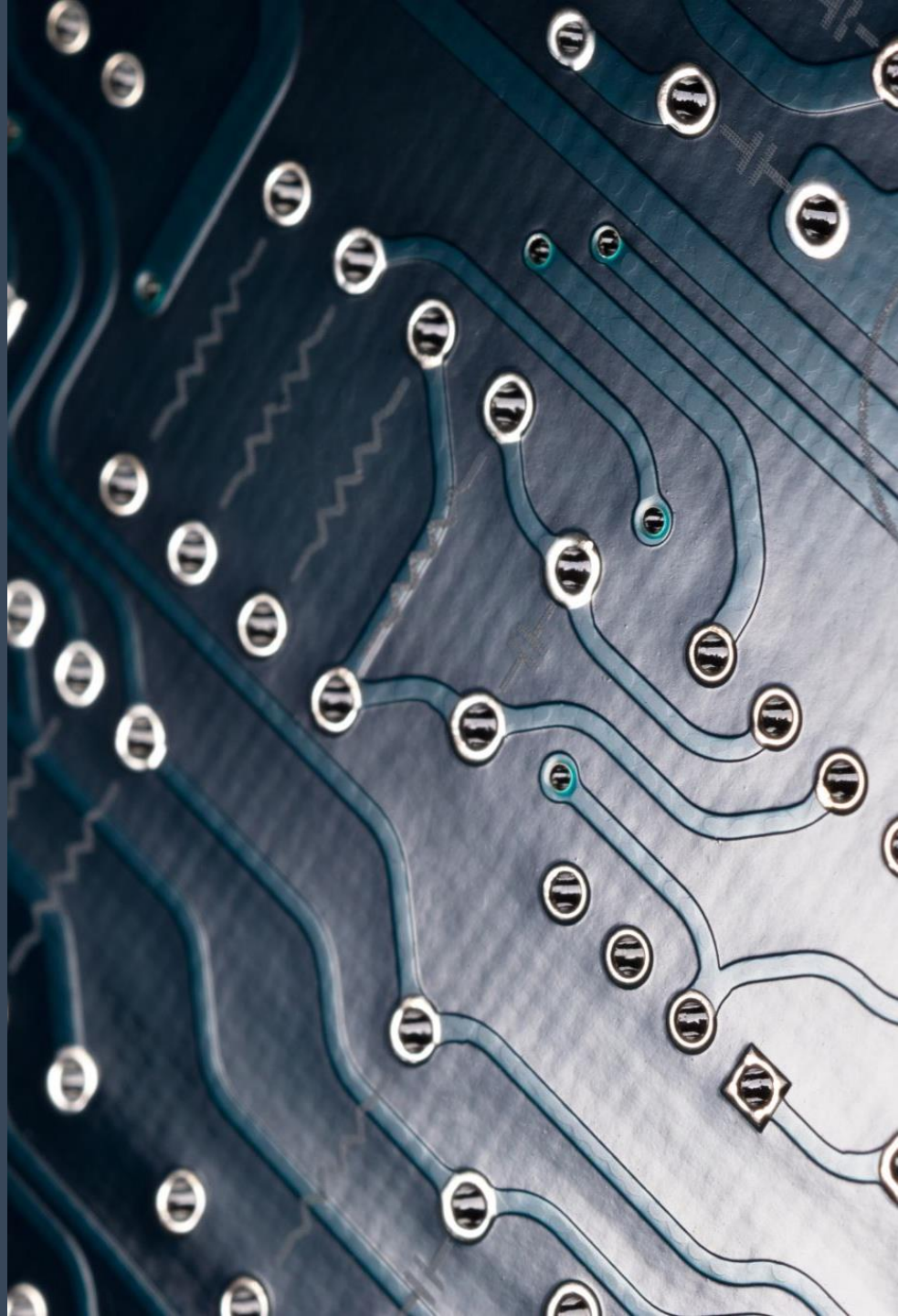
Eine Annäherung

STRUKTUR

1) Was ist (Cyber-)Resilienz?

2) Warum ist das Konzept nützlich (und notwendig)?

3) Wie können wir es umsetzen?



WAS IST RESILIENZ?

"(…) resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

National Infrastructure Advisory Council (US DHS)

= Die Fähigkeit eines Systems, Teilausfälle kompensieren zu können und/oder mit Störungen gut umzugehen

= Widerstandsfähigkeit

CYBER-RESILIENZ

System = Computer-Netzwerk (und abhängige Dienstleistungen)... und Menschen!

→ Es geht IMMER um sozio-technische Systeme!

Ziel von Cyber-Resilienz: Schaden eines Cyber-vorfalls so gering wie möglich halten

Cyber-Resilienz als Teilbereich der IT-Sicherheit (Incident Management)

Resilienz ist notwendig, wenn Prävention «versagt» (Plan B)

RISIKOMANAGEMENT

IT-Sicherheit basiert auf Risikomanagement

(Risiko = Eintretenswahrscheinlichkeit x Schaden)

ABER:

- Statistiken limitiert (globale Daten schlecht, Exposure teilweise spezifisch)
- Ungewissheit und Unvorhersehbarkeit sind hoch → menschliche Akteure!
- Komplexe Systeme (oftmals verborgene Zusammenhänge)
- Risikowahrnehmung ≠ Handeln

→ Prävention / Schutz ist wichtig, reicht aber nicht

RISIKOMANAGEMENT VS. RESILIENZ

1) Resilienz als Ziel des Risikomanagements

- Ersetzt Schutz als Hauptziel
- Ziel: Auswirkungen von Risiken mindern, sie aber nicht ausmerzen

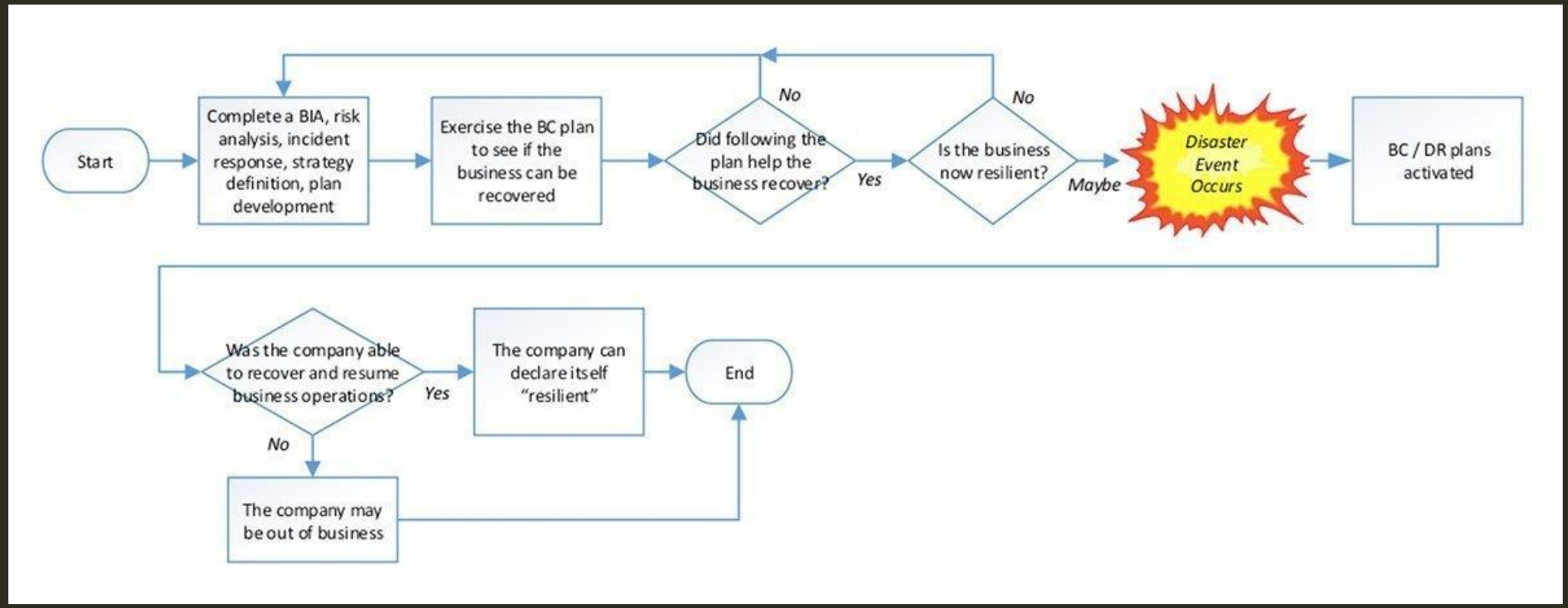
2) Resilienz als ergänzender Teil des Risikomanagements

- Systematischer Weg, um «Restrisiken» zu begegnen
- Hilft, mit potenziellen, aber unerwarteten Risiken umzugehen

3) Resilienz als Alternative zum Risikomanagement

- Ersetzt Risikoanalyse, die nicht mit komplexen, nichtlinearen Risiken umgehen kann
- Konzentriert sich auf Verständnis des «Systems», sucht Schutzmassnahmen, die unabhängig von Art und Ausmass eines Risikos sind

IST RESILIENZ = BCM?



Quelle: https://www.computerweekly.com/de/tipp/Der-Unterschied-zwischen-Business-Continuity-und-Resilience

KOMPONENTEN VON RESILIENZ (DIE 6 RS)

Robustheit

Aufrechterhaltung des Betriebs; Schaden während eines Vorfalls widerstehen oder verhindern

Resourcefulness (Einfallsreichtum)

Effektives Management in einer schwierigen Situation

Rapid Recovery

Fähigkeit, sich schnell durch Krisen zu bewegen und Systeme/Funktionen wiederherzustellen

Redundanz

Fähigkeit, alternative Prozesse für kritische Systeme/Prozesse bereitzustellen

Remembrance (Erinnerung)

Informationen aufnehmen und aus einer Krise lernen

Re-Visioning the Future

Vision & Zielstrebigkeit; wer wir sind und wohin wir gehen

UMSETZUNG

Umsetzung einer erfolgreichen Cyber-Resilienz erfordert ganzheitliche Betrachtung («Big Picture»)

- Risikoappetit und Ownership bestimmen

Voraussetzung sind abteilungsübergreifende Analysen, Zusammenarbeit und Verteilung von Verantwortlichkeiten

- Orchestrierung über Menschen, Prozesse und Technologien hinweg

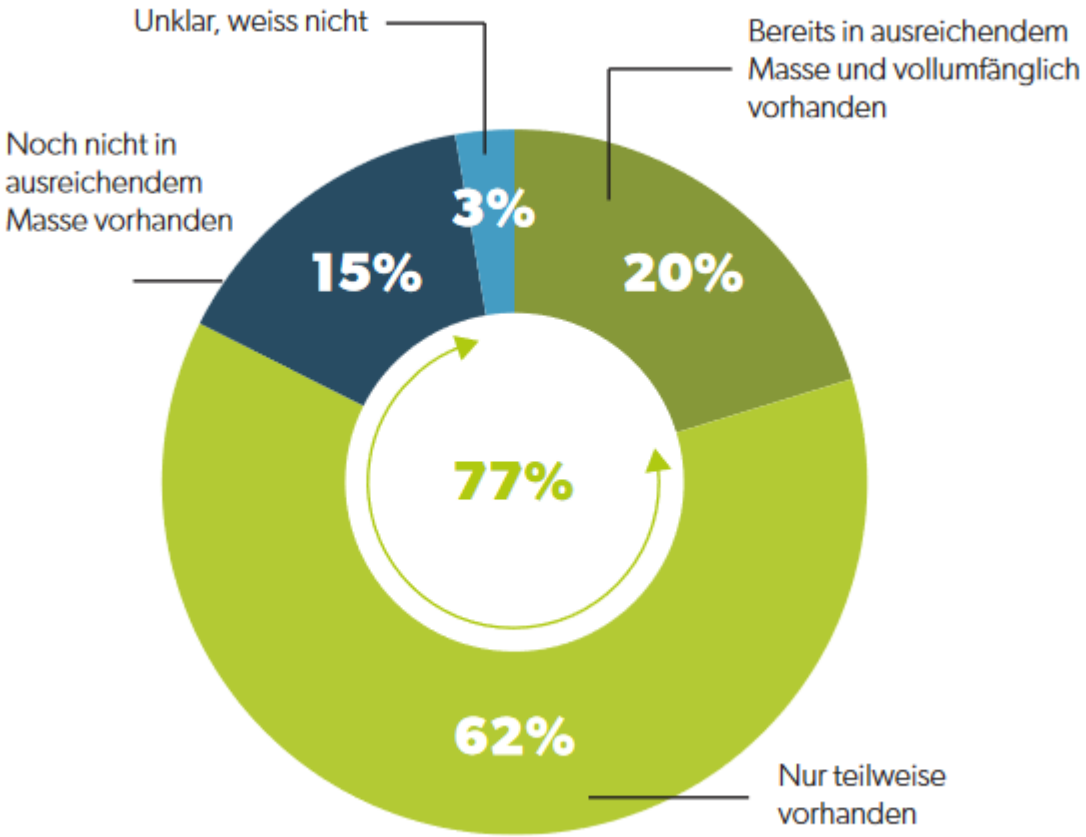
Cyber-Resilienz in der Unternehmenskultur verankern (Wegkommen von der Floskel: «Humans are the weakest link»)

- Verwaltungsrat & Führungsebene einbeziehen!
- Inside Job unattraktiv machen
- Schulungen & Angriffssimulationen

Erwarten Sie den Vorfall – kommunizieren Sie clever, wenn er da ist (nicht nur Meldepflicht, sondern auch themenbezogener Austausch mit Investoren, Partnern, Lieferanten, Kunden, etc.)

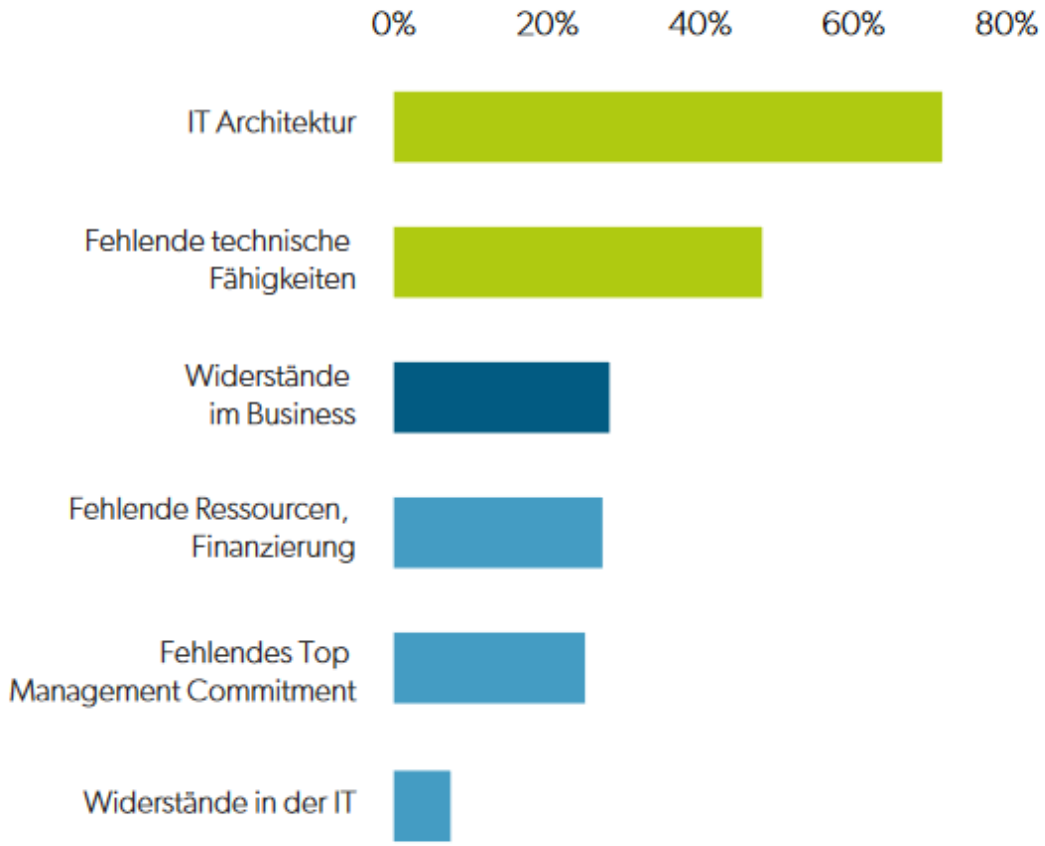
Lernen Sie aus Vorfällen und machen Sie es besser

EINSCHÄTZUNG & GRÖSSTE HÜRDEN



Verfügbarkeit der notwendigen Cyber-Resilienz Fähigkeiten

Grösste Hürden für den Aufbau der erforderlichen Cyber-Resilienz



Quelle: AWK Cyber Resilience Studie 2020

FAZIT

Cyber-Resilienz können Sie nicht als Produkt kaufen

Cyber-Resilienz ist ein kontinuierlicher Prozess (Nach der Krise ist vor der Krise)

Cyber-Resilienz geht weit über technische Faktoren hinaus (und hängt doch stark mit technischen Lösungen zusammen)

Cyber-Resilienz ist «emergent»: Sie hängt von allen Teilen eines Systems und dessen Interaktionen ab

Cyber-Resilienz gehört zum «Muss» für alle Unternehmen

VIELEN DANK!

Myriam Dunn Cavelty

dunn@sipo.gess.ethz.ch