Cybersecurity Frameworks & Aufbau einer robusten Governance

Netzwerk Risikomanagement

17. September 2024

Building a better working world

Agenda

1 Aktuelle Situation in der Schweiz

2 Frameworks als Grundlage für eine robuste Governance

3 Assessment und Risikomanagement

4 Key Takeaways

1

Aktuelle Situation in der Schweiz

Business as usual, auch in der Schweiz: diverse Cyber Vorfälle

Ransomware payments doubled to more than $1 billion in 2023

$75 Million Record-Breaking Ransom Paid To Cybercriminals, Say Researchers

Steigende Rate an Ransomware
02.2024

Staatliche Hacker aus China stehlen Daten von Versicherungen, Behörden oder Hotels.

Russland intensiviert Cyberangriffe auf die Schweiz

Russische Cyberangriffe auf die Schweiz intensivierten sich in den letzten Monaten. Bund und Privatwirtschaft bereiten sich alarmiert auf mehr Angriffe vor.

Krisenstab für Cybercrime

«Für russische Hacker ist die Schweiz ein Topziel»

Bande erbeutete 700 Gigabyte

Russische Hackerattacke auf Schweizer Stromkonzern wirft Fragen auf

Vermehrt sind auch staatliche Player involviert
06.2024

WELTWEITE OPERATION

FBI informierte sie: Schweizer Parlamentarier wurden von chinesischen Staatshackern angegriffen

Schutzmassnahmen für Botschafter und Bundesräte im Darknet

Hacker-Angriff wird zum Super-GAU

Nach dem Datenklau bei der Bundespolizei sind Interpol-Anfragen sowie die Sicherheitsdispositive für Staatsgäste und Magistraten im Netz frei zugänglich. Aus dem Parlament werden personelle Konsequenzen gefordert.

Neuer Hackerangriff

Verträge der Schweizer Luftwaffe im Darknet aufgetaucht

Bedrohung in der Schweiz steigt kontinuierlich

gemeldet, davon 16'395 als Cyberbetrug. Im Schnitt wurde alle elf Sekunden ein Schweizer Unternehmen mit einem Ransomware-Angriff konfrontiert.

Steigende Rate auch in der Schweiz
02.2024

Cyberangriff auf Zuger Krypto-Börse Lykke: 22 Millionen Dollar gestohlen

Cyberattacken in der Schweiz

Hacker greifen überall und immer öfter an

Auch Comparis wurde 2021 Opfer einer Attacke. Kriminelle verschlüsselten wichtige Dateien des Internet-Vergleichsdienstes – das Unternehmen hatte keinen Zugriff mehr. Im Darknet handelte man das Lösegeld aus. Medien nannten die Summe von 400'000 Dollar.

CYBERKRIMINALITÄT

Nach Hackerangriff: Comparis knickt ein und zahlt Lösegeld

Firmen zahlen Lösegeld
04.2023

Per Phishing-Mails

Kriminelle haben Cyberangriff auf SBB verübt

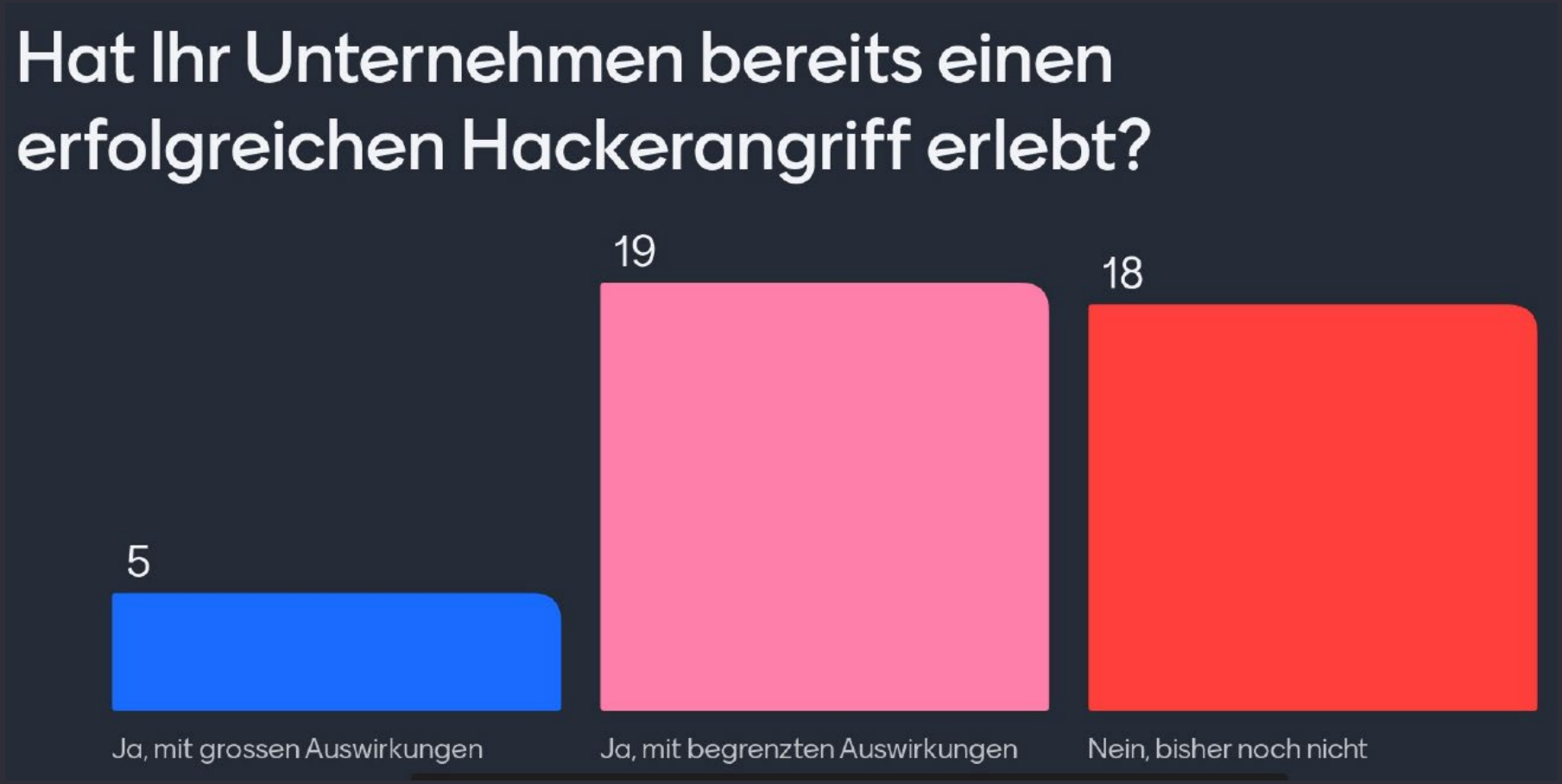
Cyberangriff grösser als angenommen

SBB und Kanton Aargau von Datenleck betroffen

Quellen: sind als Hyperlink hinterlegt

Ihre Erfahrungen im Bereich Cyberangriffe

Mentimeter



Ihre Erfahrungen im Bereich Cyberangriffe

Mentimeter

In welchem Bereich Ihres Unternehmens sehen Sie die grössten Cyber Gefahren?

45 responses

Business as usual, auch in der Schweiz: steigende Zahlen

Statistiken aus der Schweiz

Cybervorfälle in der Schweiz sind nicht nur auf einem Höchststand, sondern wachsen auch mit einer konstanten Rate jedes Jahr weiter an. Deshalb wird eine klare Cybersecurity Governance und ein umfangreicher Schutz dagegen immer wichtiger.

Cyberangriffe in der Schweiz

Meldungen ans BACS, pro Woche

(Die Zahlen beinhalten Berichte über Betrug, Malware, Phishing, Spam und DDoS-Angriffe)

CYBERVORFÄLLE

79%

Wachstum von Cybervorfall-Meldungen in 2024 – starker Anstieg zum Vorjahr

PHISHING

150%

Wachstum von Phishing Meldungen in 2024 – mehr als eine Verdoppelung zum Vorjahr

CYBERVORFÄLLE MIT SCHADENFOLGE

30%

Durchschnittes jährliches Wachstum an Cybervorfällen mit Schadensfolge

MELDUNGEN

50k

Anzahl Meldungen zu Cybervorfällen im Jahr 2023

Quellen: NCSC Current figures (admin.ch) & BACS Halbjahresbericht 2023/2

2

Frameworks als Basis für eine robuste Governance

Aufbau einer robusten Governance

Wie etabliert man eine robuste Cybersecurity Governance?

1

Führungsebene einbinden
Sicherstellen, dass die Unternehmensleitung Cybersecurity als strategische Priorität versteht und unterstützt.

2

Richtlinien und Standards definieren
Entwicklung klarer Sicherheitsrichtlinien und -standards, die auf etablierten Frameworks und Best Practices basieren.

3

Rollen und Verantwort-lichkeiten festlegen
Klare Zuweisung von Cybersecurity-Verantwortlichkeiten innerhalb der Organisation.

4

Risikomanagement-prozess implementieren
Einen kontinuierlichen Prozess zur Identifikation, Bewertung und Minderung von Cyber-Risiken etablieren.

5

Schulung und Bewusst-sein fördern
Regelmässige Schulungen und Sensibilisierungskampagnen für alle Mitarbeiter durchführen.

6

Incident Response Plan erstellen
Einen detaillierten Plan für den Umgang mit Sicherheitsvorfällen vorbereiten und regelmässig testen.

7

Überwachung und Compliance
Kontinuierliche Überwachung der Cybersecurity-Massnahmen und Einhaltung rechtlicher sowie regulatorischer Anforderungen gewährleisten.

8

Kontinuierliche Verbesserung
Regelmässige Überprüfungen der Cybersecurity Strategie und -Massnahmen durchführen, um Verbesserungspotenziale zu identifizieren und umzusetzen.

Zusammenspiel von Cybersecurity Frameworks und rechtlichen Vorgaben bei der Integration in eine robuste Governance

Eine robuste Governance ist wichtig, weil sie klare Richtlinien und Verantwortlichkeiten festlegt, um Risiken zu minimieren und auf Sicherheitsvorfälle effektiv reagieren zu können.

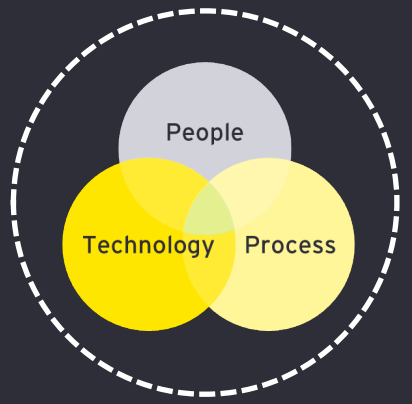
Cybersecurity Frameworks

Robuste Governance

Rechtliche Vorgaben

Cybersecurity Frameworks

NIST 2.0



ISO 27001/2

4 übergreifende Domains:

Non exhaustive

Organizational

- Segregation of duties
- Classification of information
- Access control

People

- Remote working
- Information security awareness, education and training

Physical

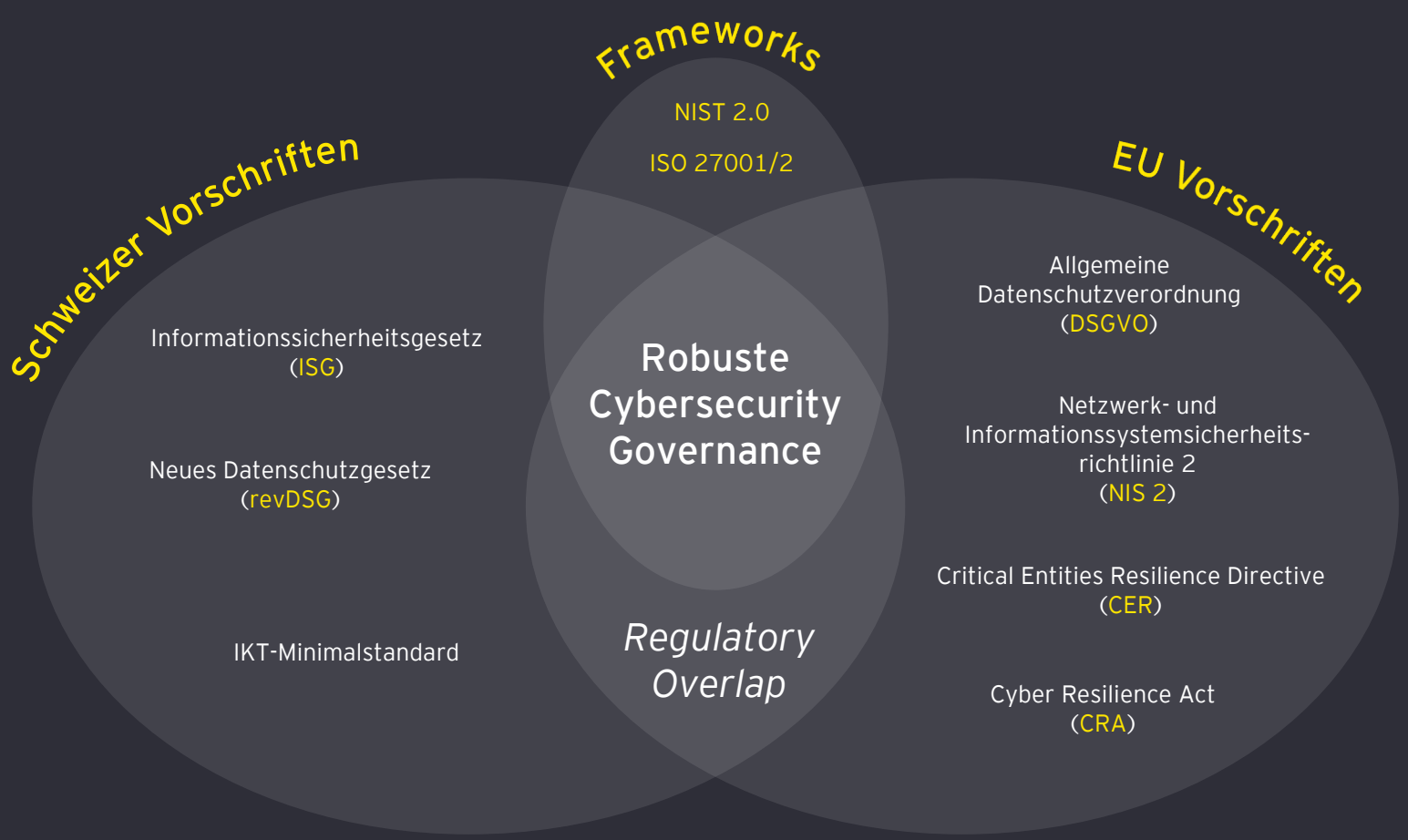
- Storage media
- Physical entry
- Working in secure areas

Technological

- Information backup
- Use of cryptography
- Data leakage prevention

Quellen: The NIST Cybersecurity Framework (CSF) 2.0 & ISO/IEC 27001:2022 - Information security management systems

Überblick von rechtlichen Vorgaben

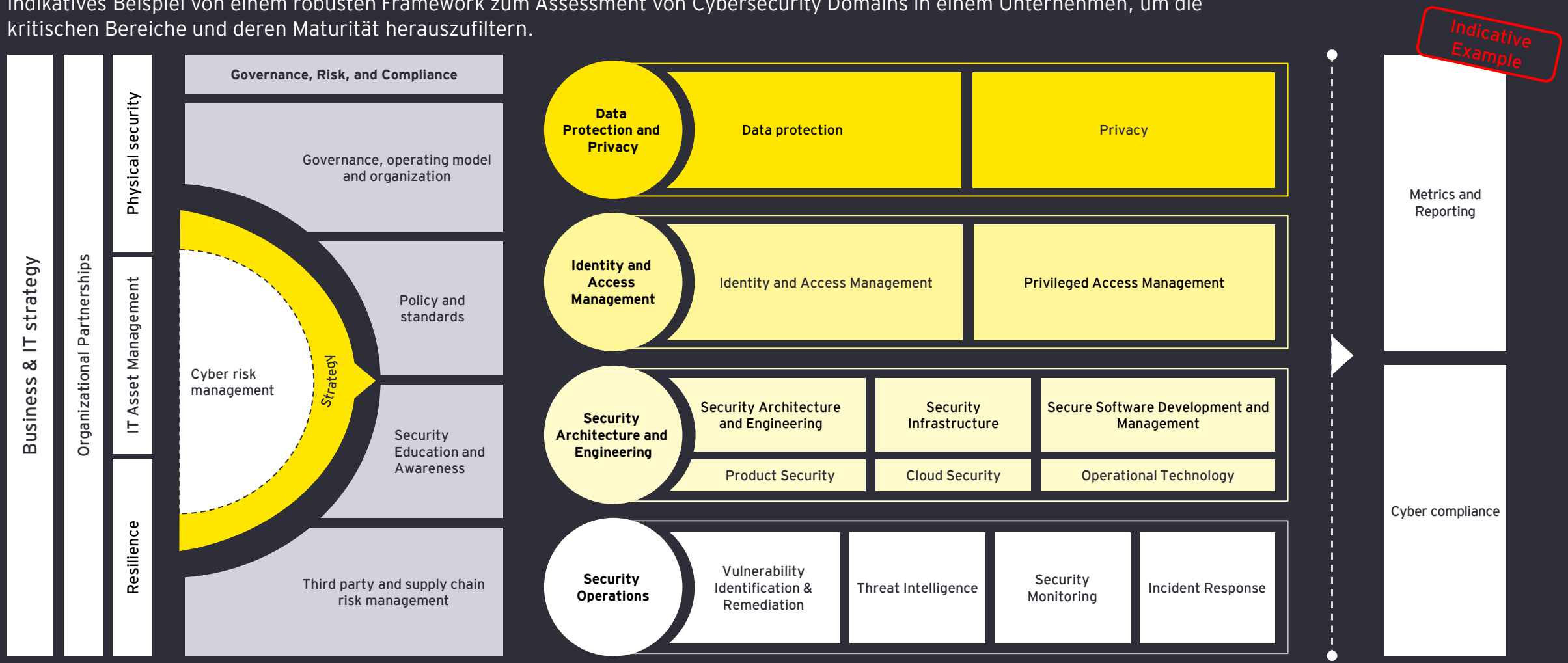


3

Assessment und Risikomanagement

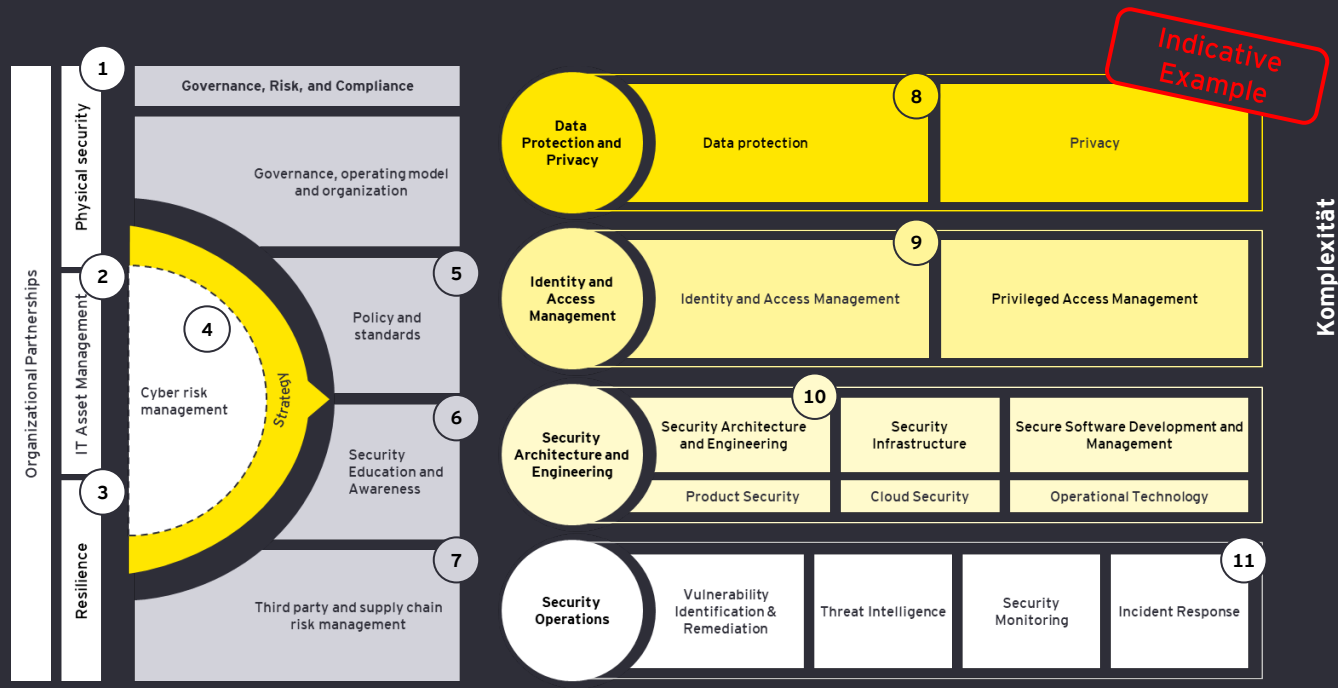
Robustes Framework zum Assessment von Cybersecurity Domains

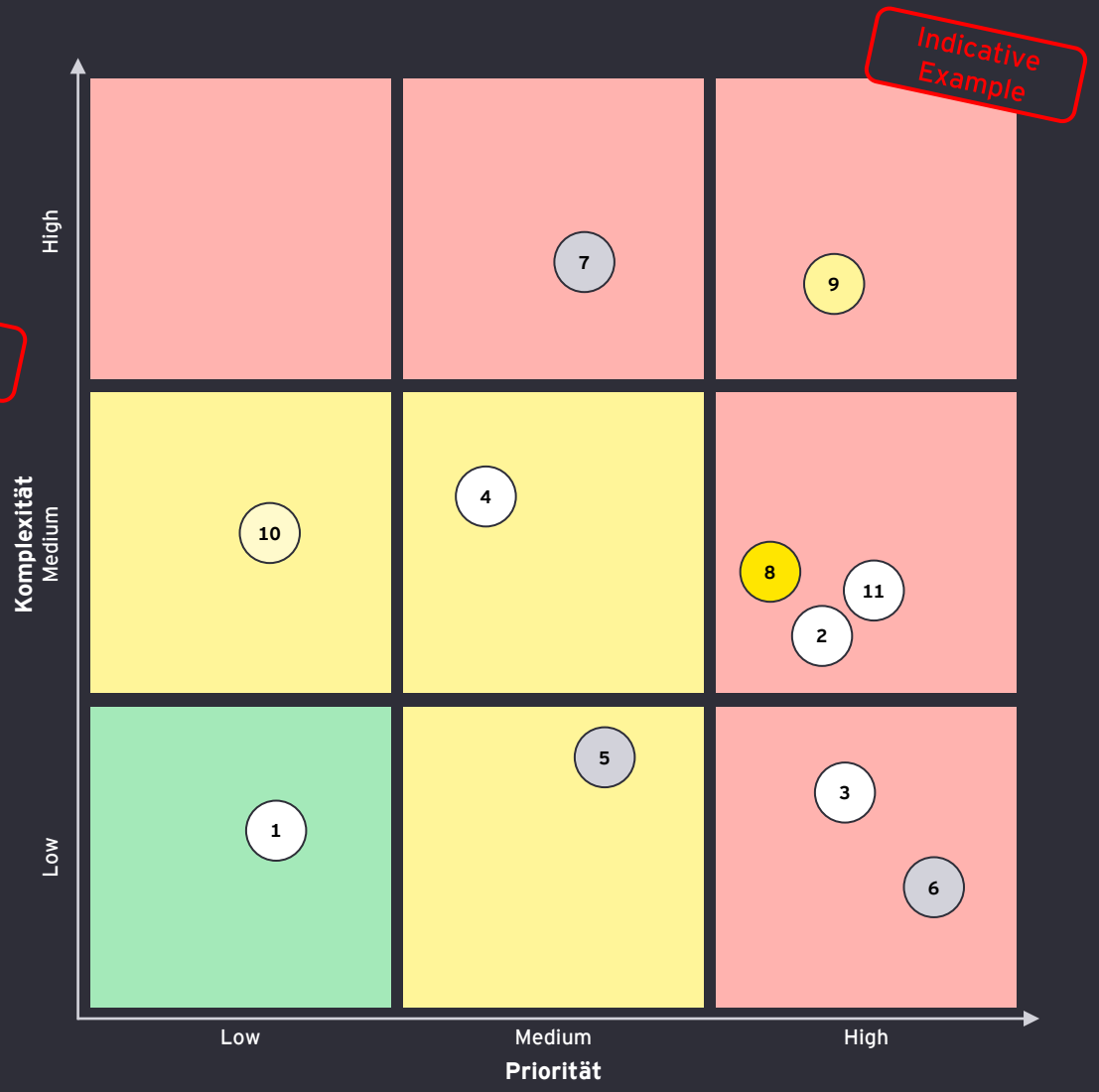
Indikatives Beispiel von einem robusten Framework zum Assessment von Cybersecurity Domains in einem Unternehmen, um die kritischen Bereiche und deren Maturität herauszufiltern.



Cybersecurity Risiko Heatmap

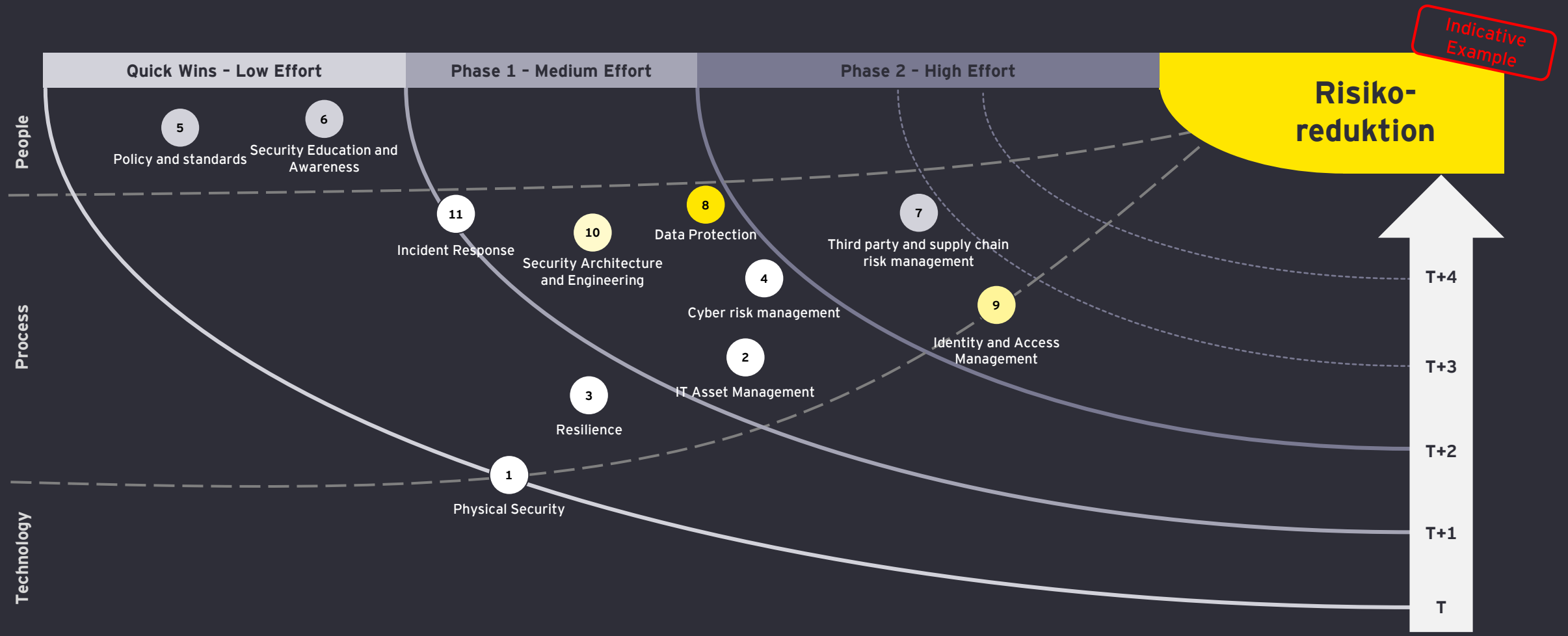
Indikatives Beispiel wie diese Cybersecurity Domains in einer Risiko Heatmap, sortiert nach der Priorität und Komplexität, eingegliedert werden können. Diese Einordnung ermöglicht es, einen klaren Aktionsplan zu entwickeln und Ressourcen effektiv zuzuweisen, um die jeweiligen Cybersecurity Ziele zu erreichen.





Cybersecurity Roadmap & Risikomitigation

Indikatives Beispiel wie diese identifizierten Risiken mitigiert und in einer dazugehörigen Roadmap integriert werden.



4

Key Takeaways

Key Takeaways

Cybersecurity ist aufgrund zunehmender Angriffe von immer entscheidenderer Bedeutung.

Eine robuste Cybersecurity Governance, gestützt auf Frameworks und Vorschriften, ist unerlässlich.

Cybersecurity bezieht sich auf People, Process und Technology.

Die Maturität der Cybersecurity Domains variiert je nach Unternehmen, was zu unterschiedlichen Prioritäten auf Ihrer Roadmap führt.

Eine Roadmap mit klar definierten Prioritäten führt zur nachhaltigen Risikomitigation.

Jeff Dicken

Senior Manager, EY
Cybersecurity Strategy Lead Switzerland

jeff.dicken@ch.ey.com
+41 79 579 75 66
LinkedIn

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

ey.com/ch