ZURICH

# Information security vulnerabilities from an insurer’s perspective

## Risk transfer and real-life financial impact on the economy and general public

Lucas Engl

Senior Underwriter for Cyber & Technology

Zürich Versicherungs-Gesellschaft

18.04.2024

# Content

## What am I going to talk about?

### Cyber Insurance

- What does «insurable» mean?
- What is insured under a Cyber policy?
- Risk Exposure
- Most Frequent IT-Security Flaws

### Real-life Impacts from Insurers Perspective

- Risk Interconnections from Cyber Insecurity
- Reported Losses
- Spotlight: Ransomware
- Conclusion

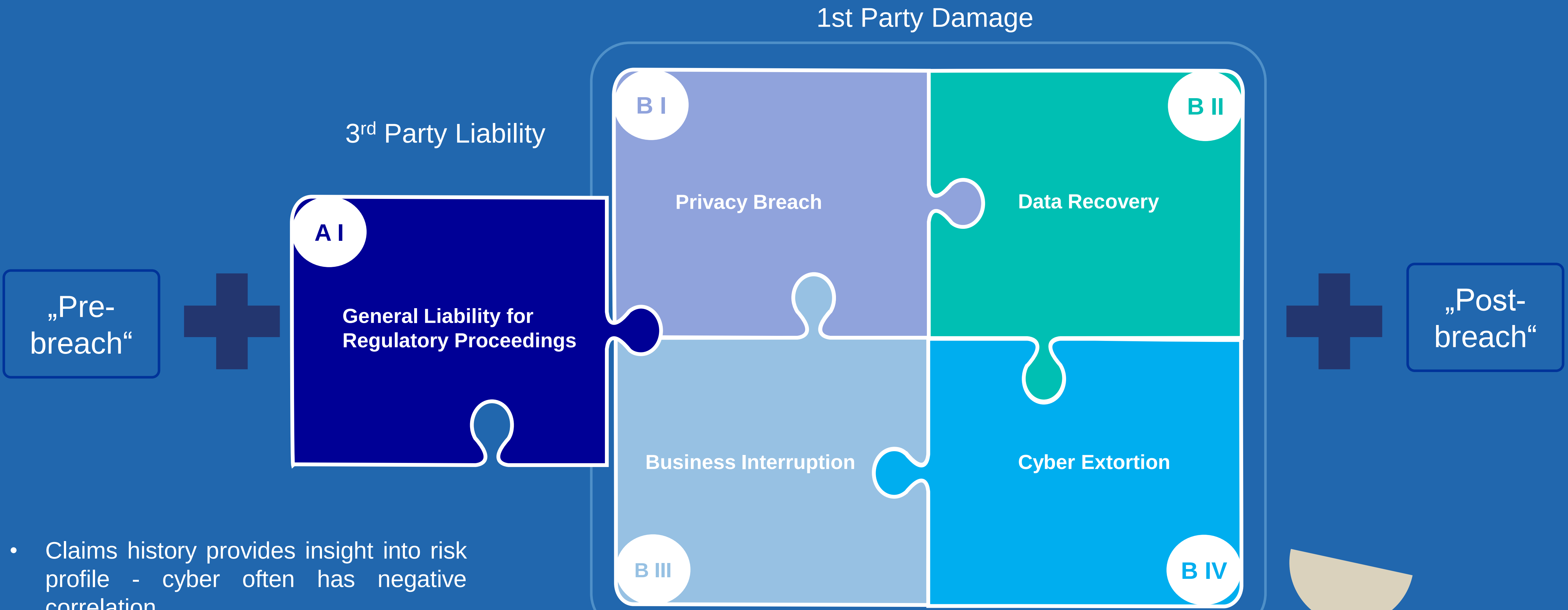
# What does «insurable» mean?

- Policyholders pay **premiums** → **protection** against dangers (e.g. cyber crime) → **occurrence** of the insured circumstance → insurance **indemnity** is paid out
- Circumstance is usually **unpredictable** and **unavoidable**
- Risk or damage must be expressed in numbers or financial values (**quantifiability**)
- Concept of **Impact/Frequency**
- **Restrictions and exclusions** in the insurance conditions
- Insurance model works when **premiums > insurance** benefits

Law of large numbers: average of the results obtained from a large number of samples converges to the true value, if it exists.

→Guarantees stable long-term results for the averages of some random events.

# What is insured under a Cyber policy?



- Claims history provides insight into risk profile - cyber often has negative correlation
- Cyber insurance provides coverage for extreme individual cases and is not project insurance

# Risk Exposure

## Where does the risk come from and how to assess it?

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

Frameworks: NIST, ISO27001, COBIT, etc.

### IT-Security Maturity

- Company Size
  - Revenues / Profit
  - Employees
- Amount of data-set records stored in own network
  - PII, PHI, PCI
  - Biometric Data
- Sector / Industry
- Business Activities

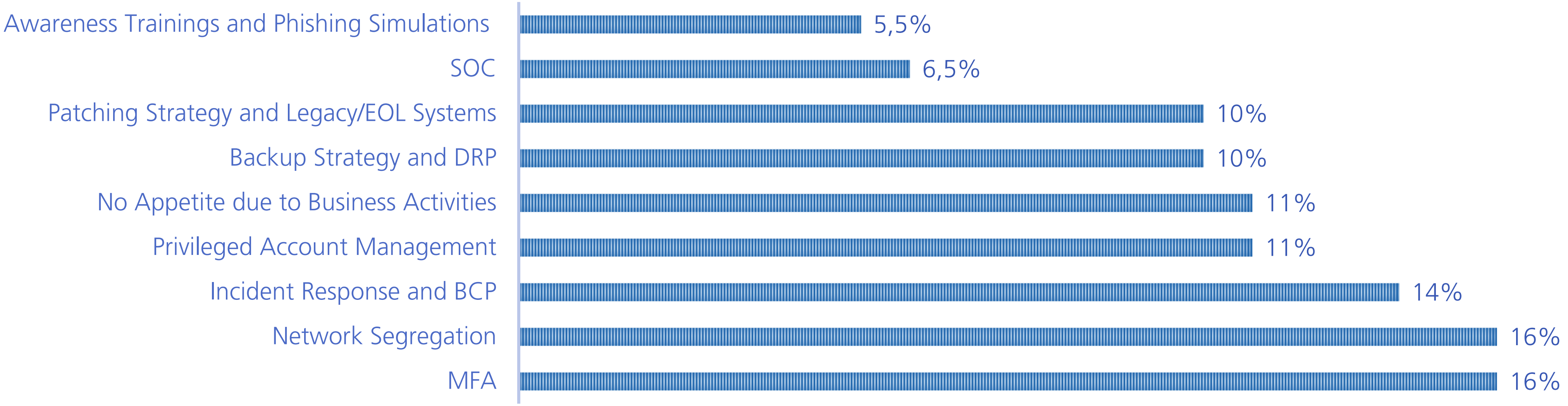
### Business Profile

- GDPR, DSG, US Federal Privacy Bill (Draft);
- HIPAA, PCI-DSS, BIPA;
- SEC
- FINMA, FMA, BAFIN;
- CRA, NIS2,  DORA, EU AI Act;

### Regulators

# MOST FREQUENT IT-SECURITY FLAWS

| Awareness Trainings and Phishing Simulations | MFA | Back-up Strategy and DRP | Patching Strategy and Legacy/EOL Systems | Network Separation and Segregation | Incident Response and BCP | Privileged Account Management | SOC | No Appetite |
|---|---|---|---|---|---|---|---|---|
| Either complete absence or insufficient implementation of awareness trainings and/or phishing simulation. | No MFA for Remote Access, 3rd-party access and/or privileged access | Backups are not stored offsite and/or outside of the business network | Patching cycles are not focusing on critical assets and not done on regular basis.<br>legacy / EOL systems are lacking security measures. | IT and OT environments (or critical systems in general) are not separted and segregated sufficiently | Insufficient definition of incident response process and roles.<br>Absence of BCP | No PAM | No 24/7 SOC or even none at all | Not within the Risk Appetite due to the company's business activities. |

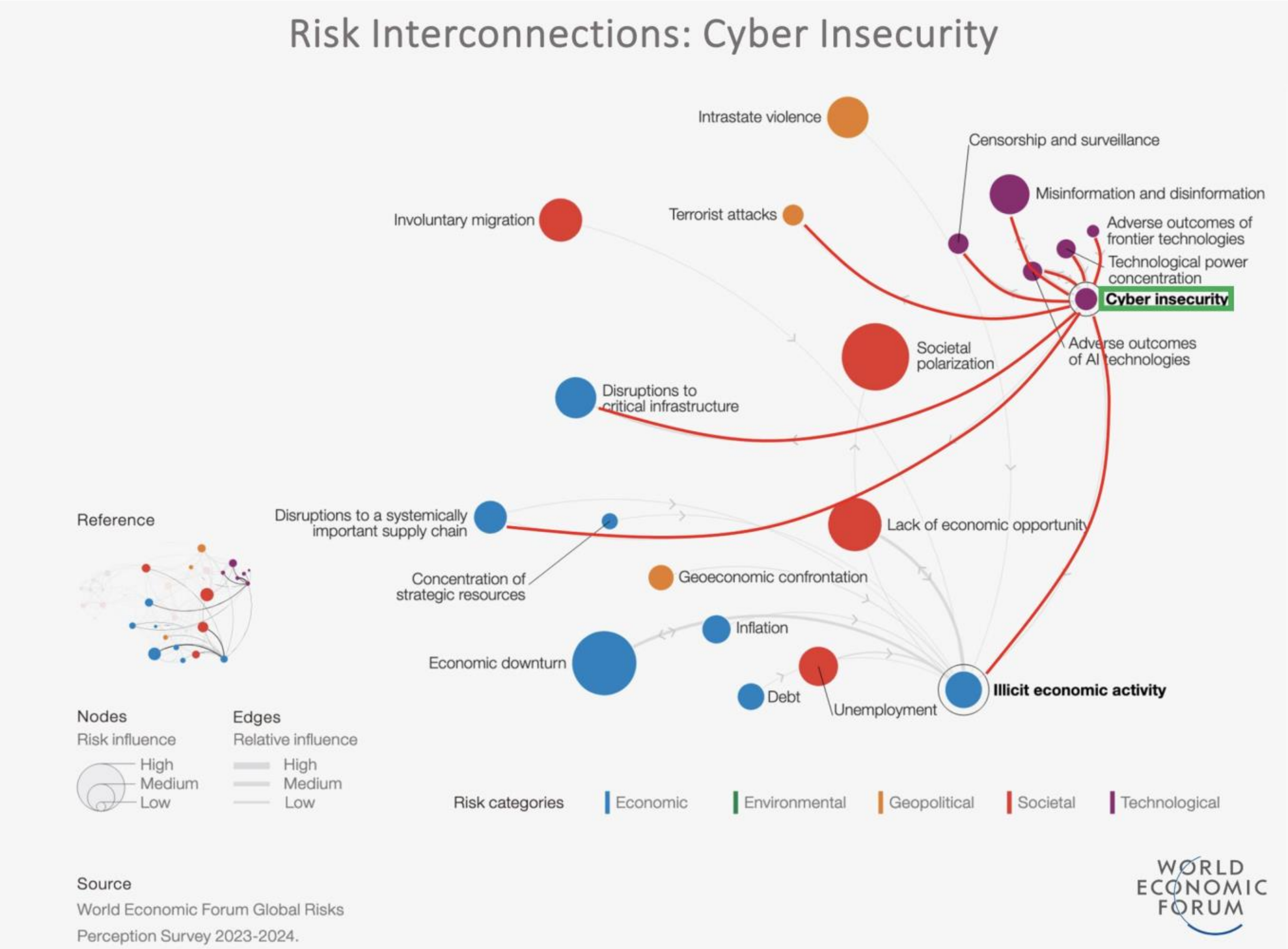


INTERNAL USE ONLY

# Risk Interconnections from Cyber Insecurity

## WEF Risk Report shows what “systemic risk” means

- World Economic Forum in collaboration with Zurich Insurance and Marsh McLennan
- Captured insights from nearly 1'500 global experts
- Technological and Environmental are top global risks ranked by severity over the next 2 and 10 years.
- Mis- and Disinformation takes the top spot on the short-run
- Cyber Insecurity takes the 4th rank on the short-run and 8th rank on the long run.
- Interconnectivity shows the “systemic risk” character


Risk Interconnections: Cyber Insecurity
Intrastate violence
Censorship and surveillance
Misinformation and disinformation
Adverse outcomes of frontier technologies
Technological power concentration
Cyber insecurity
Adverse outcomes of AI technologies
Involuntary migration
Terrorist attacks
Societal polarization
Disruptions to critical infrastructure
Reference
Disruptions to a systemically important supply chain
Lack of economic opportunity
Concentration of strategic resources
Geoeconomic confrontation
Inflation
Economic downturn
Debt
Unemployment
Illicit economic activity
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological
WORLD ECONOMIC FORUM

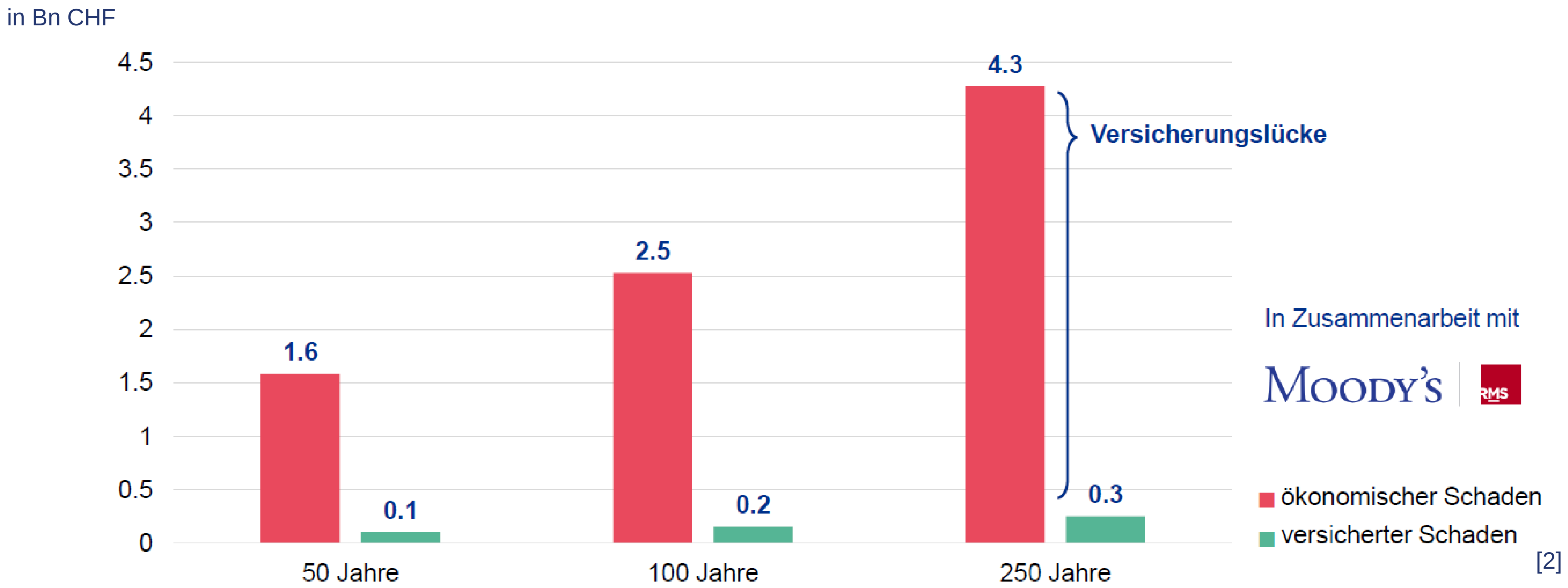
Source
World Economic Forum Global Risks Perception Survey 2023-2024.

[1]

[1] World Economic Forum Global Risks Report 2024

# Modeled loss events in Switzerland

## Risk Model by SVV in collaboration with Moody's RMS



- Economic and insured damage compared for 50-year, 100-year or 250-year events
- Systemic risks are not included (natural hazards, infrastructure failure, war, etc.)
- Most important financial risks directly resulting from cyber attack are included
- Data from the estimated economic damage

[2] Schweizerische Versicherungsverband (SVV)

# Insights from Cyentia – IRIS-Report

## Based on Advisen – leading provider of data, technology, events, and media for insurance professionals

- World-wide real data on challenges of managing cyber risks
- Over 77,000 cyber events
- USD 57 billion in reported losses
- USD 72 billion compromised data sets
- Insurers experiences are confirming these numbers
- Comparison of impact between "big enterprise" and "small shop"
- Comparison of impacts from major loss events between primary sectors

[3]

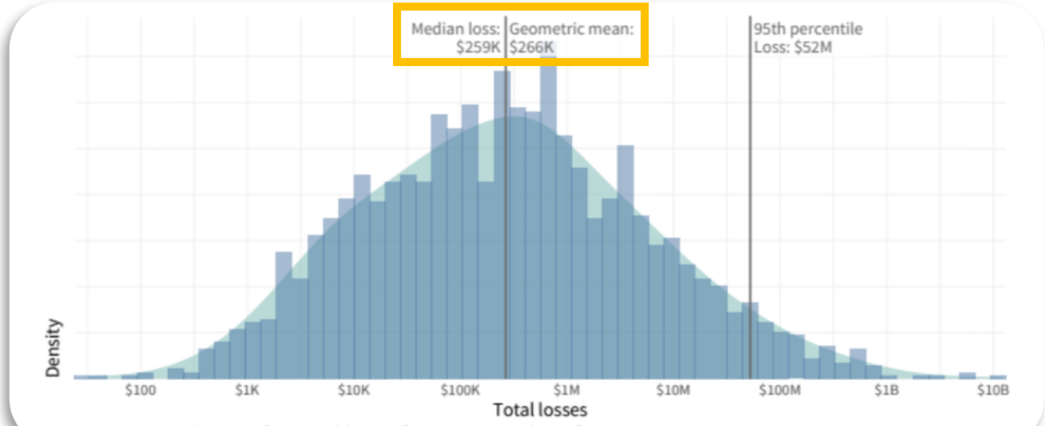


Figure 6: Distribution of reported losses for security incidents from 2012 to 2021

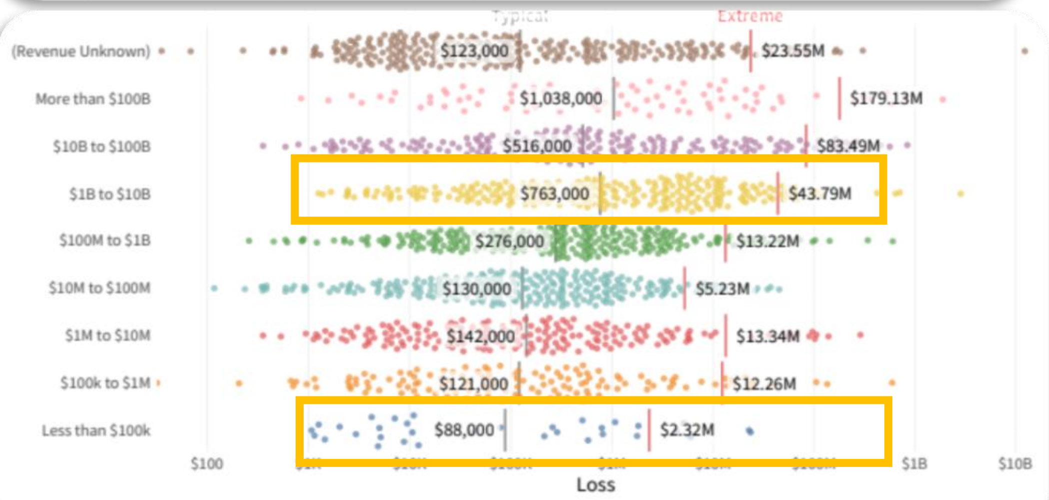
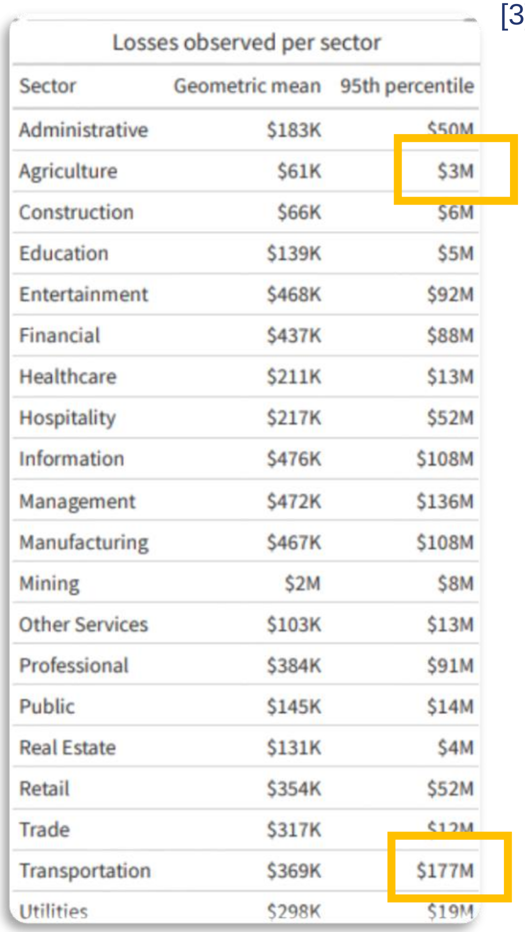


Figure 7: Distribution of reported cyber event losses by firm size (in revenue)



Losses observed per sector

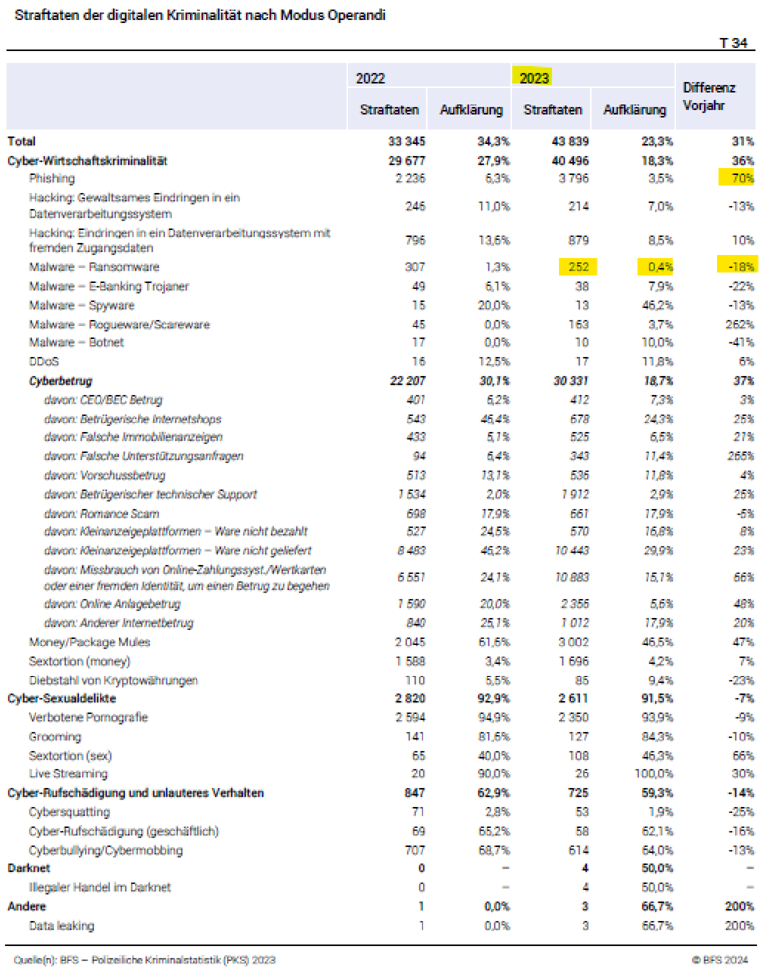
| Sector | Geometric mean | 95th percentile |
|---|---|---|
| Administrative | $183K | $50M |
| Agriculture | $61K | $3M |
| Construction | $66K | $6M |
| Education | $139K | $5M |
| Entertainment | $468K | $92M |
| Financial | $437K | $88M |
| Healthcare | $211K | $13M |
| Hospitality | $217K | $52M |
| Information | $476K | $108M |
| Management | $472K | $136M |
| Manufacturing | $467K | $108M |
| Mining | $2M | $8M |
| Other Services | $103K | $13M |
| Professional | $384K | $91M |
| Public | $145K | $14M |
| Real Estate | $131K | $4M |
| Retail | $354K | $52M |
| Trade | $317K | $12M |
| Transportation | $369K | $177M |
| Utilities | $298K | $19M |

Table 4 (Right): Loss magnitude summary statistics by sector

[3] Cyentia Institute - Information Risk Insights Study 2022

# Update 2023 – Digital Crime Police Report

## Jahresbericht 2023 der polizeilich registrierten Straftaten



**Straftaten der digitalen Kriminalität nach Modus Operandi**

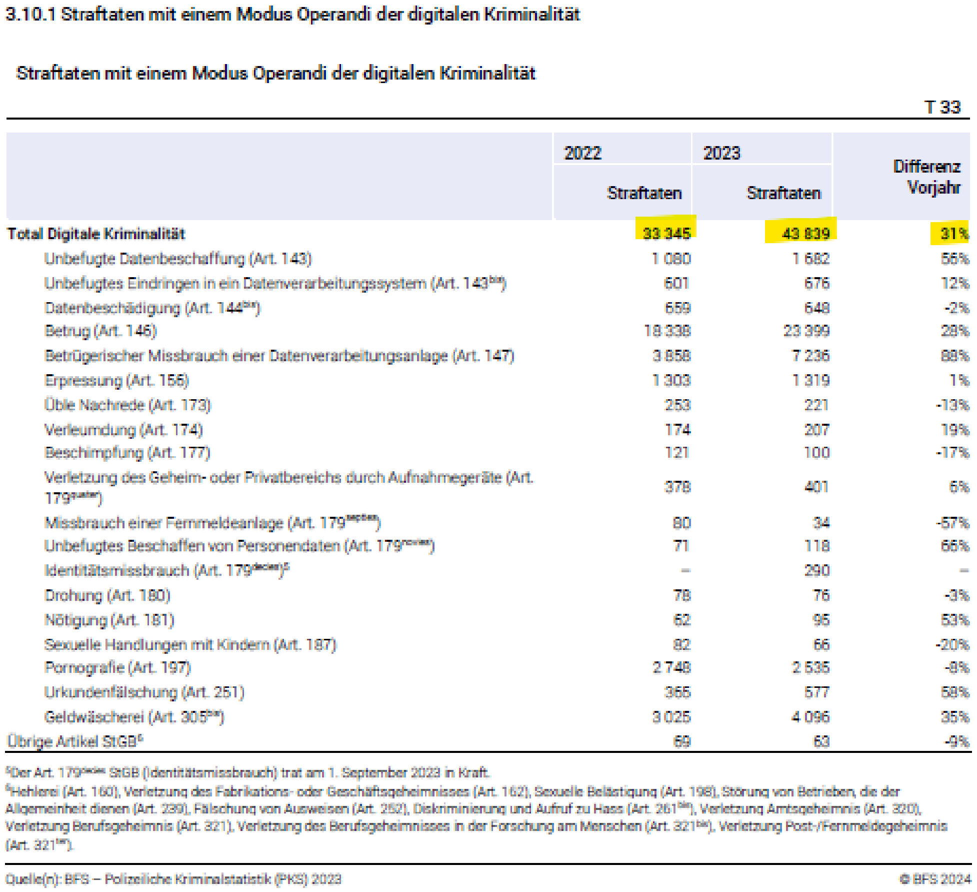
T 34

| | 2022 | | 2023 | | Differenz Vorjahr |
|---|---|---|---|---|---|
| | Straftaten | Aufklärung | Straftaten | Aufklärung | |
| **Total** | **33 345** | **34,3%** | **43 839** | **23,3%** | **31%** |
| **Cyber-Wirtschaftskriminalität** | **29 677** | **27,9%** | **40 496** | **18,3%** | **36%** |
| Phishing | 2 236 | 6,3% | 3 796 | 3,5% | 70% |
| Hacking: Gewaltsames Eindringen in ein Datenverarbeitungssystem | 246 | 11,0% | 214 | 7,0% | -13% |
| Hacking: Eindringen in ein Datenverarbeitungssystem mit fremden Zugangsdaten | 796 | 13,6% | 879 | 8,5% | 10% |
| Malware – Ransomware | 307 | 1,3% | 252 | 0,4% | -18% |
| Malware – E-Banking Trojaner | 49 | 6,1% | 38 | 7,9% | -22% |
| Malware – Spyware | 15 | 20,0% | 13 | 46,2% | -13% |
| Malware – Rogueware/Scareware | 45 | 0,0% | 163 | 3,7% | 262% |
| Malware – Botnet | 17 | 0,0% | 10 | 10,0% | -41% |
| DDoS | 16 | 12,5% | 17 | 11,8% | 6% |
| ***Cyberbetrug*** | ***22 207*** | ***30,1%*** | ***30 331*** | ***18,7%*** | ***37%*** |
| *davon: CEO/BEC Betrug* | *401* | *6,2%* | *412* | *7,3%* | *3%* |
| *davon: Betrügerische Internetshops* | *543* | *46,4%* | *678* | *24,3%* | *25%* |
| *davon: Falsche Immobilienanzeigen* | *433* | *5,1%* | *525* | *6,5%* | *21%* |
| *davon: Falsche Unterstützungsanfragen* | *94* | *6,4%* | *343* | *11,4%* | *265%* |
| *davon: Vorschussbetrug* | *513* | *13,1%* | *536* | *11,8%* | *4%* |
| *davon: Betrügerischer technischer Support* | *1 534* | *2,0%* | *1 912* | *2,9%* | *25%* |
| *davon: Romance Scam* | *698* | *17,9%* | *661* | *17,9%* | *-5%* |
| *davon: Kleinanzeigeplattformen – Ware nicht bezahlt* | *527* | *24,5%* | *570* | *16,8%* | *8%* |
| *davon: Kleinanzeigeplattformen – Ware nicht geliefert* | *8 483* | *46,2%* | *10 443* | *29,9%* | *23%* |
| *davon: Missbrauch von Online-Zahlungssyst./Wertkarten oder einer fremden Identität, um einen Betrug zu begehen* | *6 551* | *24,1%* | *10 883* | *15,1%* | *66%* |
| *davon: Online Anlagebetrug* | *1 590* | *20,0%* | *2 355* | *5,6%* | *48%* |
| *davon: Anderer Internetbetrug* | *840* | *25,1%* | *1 012* | *17,9%* | *20%* |
| Money/Package Mules | 2 045 | 61,6% | 3 002 | 46,5% | 47% |
| Sextortion (money) | 1 588 | 3,4% | 1 696 | 4,2% | 7% |
| Diebstahl von Kryptowährungen | 110 | 5,5% | 85 | 9,4% | -23% |
| **Cyber-Sexualdelikte** | **2 820** | **92,9%** | **2 611** | **91,5%** | **-7%** |
| Verbotene Pornografie | 2 594 | 94,9% | 2 350 | 93,9% | -9% |
| Grooming | 141 | 81,6% | 127 | 84,3% | -10% |
| Sextortion (sex) | 65 | 40,0% | 108 | 46,3% | 66% |
| Live Streaming | 20 | 90,0% | 26 | 100,0% | 30% |
| **Cyber-Rufschädigung und unlauteres Verhalten** | **847** | **62,9%** | **725** | **59,3%** | **-14%** |
| Cybersquatting | 71 | 2,8% | 53 | 1,9% | -25% |
| Cyber-Rufschädigung (geschäftlich) | 69 | 65,2% | 58 | 62,1% | -16% |
| Cyberbullying/Cybermobbing | 707 | 68,7% | 614 | 64,0% | -13% |
| **Darknet** | **0** | **–** | **4** | **50,0%** | **–** |
| Illegaler Handel im Darknet | 0 | – | 4 | 50,0% | – |
| **Andere** | **1** | **0,0%** | **3** | **66,7%** | **200%** |
| Data leaking | 1 | 0,0% | 3 | 66,7% | 200% |

Quelle(n): BFS – Polizeiliche Kriminalstatistik (PKS) 2023

© BFS 2024

[4]



### 3.10.1 Straftaten mit einem Modus Operandi der digitalen Kriminalität

**Straftaten mit einem Modus Operandi der digitalen Kriminalität**

T 33

| | 2022 | 2023 | Differenz Vorjahr |
|---|---|---|---|
| | Straftaten | Straftaten | |
| **Total Digitale Kriminalität** | **33 345** | **43 839** | **31%** |
| Unbefugte Datenbeschaffung (Art. 143) | 1 080 | 1 682 | 56% |
| Unbefugtes Eindringen in ein Datenverarbeitungssystem (Art. 143$^{bis}$) | 601 | 676 | 12% |
| Datenbeschädigung (Art. 144$^{bis}$) | 659 | 648 | -2% |
| Betrug (Art. 146) | 18 338 | 23 399 | 28% |
| Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Art. 147) | 3 858 | 7 236 | 88% |
| Erpressung (Art. 156) | 1 303 | 1 319 | 1% |
| Üble Nachrede (Art. 173) | 253 | 221 | -13% |
| Verleumdung (Art. 174) | 174 | 207 | 19% |
| Beschimpfung (Art. 177) | 121 | 100 | -17% |
| Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte (Art. 179$^{quater}$) | 378 | 401 | 6% |
| Missbrauch einer Fernmeldeanlage (Art. 179$^{septies}$) | 80 | 34 | -57% |
| Unbefugtes Beschaffen von Personendaten (Art. 179$^{novies}$) | 71 | 118 | 66% |
| Identitätsmissbrauch (Art. 179$^{decies}$)[5] | – | 290 | – |
| Drohung (Art. 180) | 78 | 76 | -3% |
| Nötigung (Art. 181) | 62 | 95 | 53% |
| Sexuelle Handlungen mit Kindern (Art. 187) | 82 | 66 | -20% |
| Pornografie (Art. 197) | 2 748 | 2 535 | -8% |
| Urkundenfälschung (Art. 251) | 365 | 577 | 58% |
| Geldwäscherei (Art. 305$^{bis}$) | 3 025 | 4 096 | 35% |
| Übrige Artikel StGB[6] | 69 | 63 | -9% |

[5] Der Art. 179$^{decies}$ StGB (Identitätsmissbrauch) trat am 1. September 2023 in Kraft.

[6] Hehlerei (Art. 160), Verletzung des Fabrikations- oder Geschäftsgeheimnisses (Art. 162), Sexuelle Belästigung (Art. 198), Störung von Betrieben, die der Allgemeinheit dienen (Art. 239), Fälschung von Ausweisen (Art. 252), Diskriminierung und Aufruf zu Hass (Art. 261$^{bis}$), Verletzung Amtsgeheimnis (Art. 320), Verletzung Berufsgeheimnis (Art. 321), Verletzung des Berufsgeheimnisses in der Forschung am Menschen (Art. 321$^{bis}$), Verletzung Post-/Fernmeldegeheimnis (Art. 321$^{ter}$).

Quelle(n): BFS – Polizeiliche Kriminalstatistik (PKS) 2023

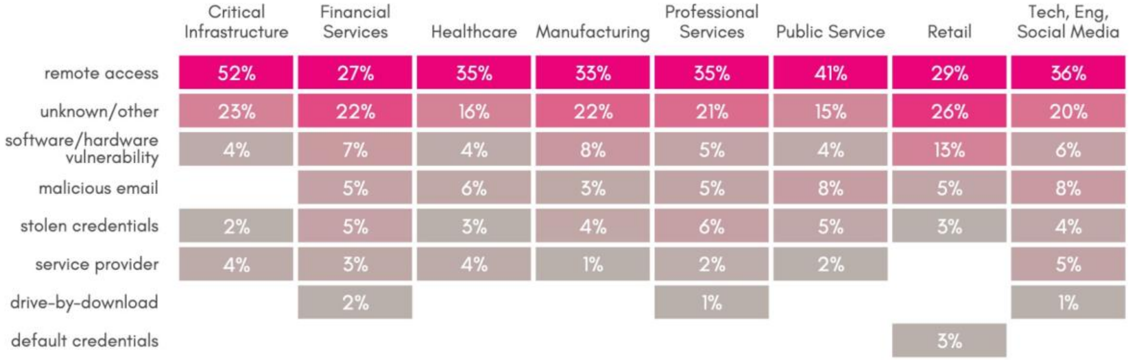
© BFS 2024

[4] Polizeiliche Kriminalstatistik (PKS) - Jahresbericht 2023

# Spotlight: Ransomware

- We mostly worry **about financially motivated ransomware** actors
- Benefit over costs is **high**
- **Low** level of persecution
- **High** level of volume
- **Potentially high** level of impact
- Trends are similar in Europe and USA
- Implementation of **MFA** and a solid **back-up strategy** were the main drivers to reduce likelihood of an attack and increase chances of full recovery
- Pre-defined **incident response strategies** were the main drivers behind loss mitigation
- Avoid being **"low hanging fruit"**

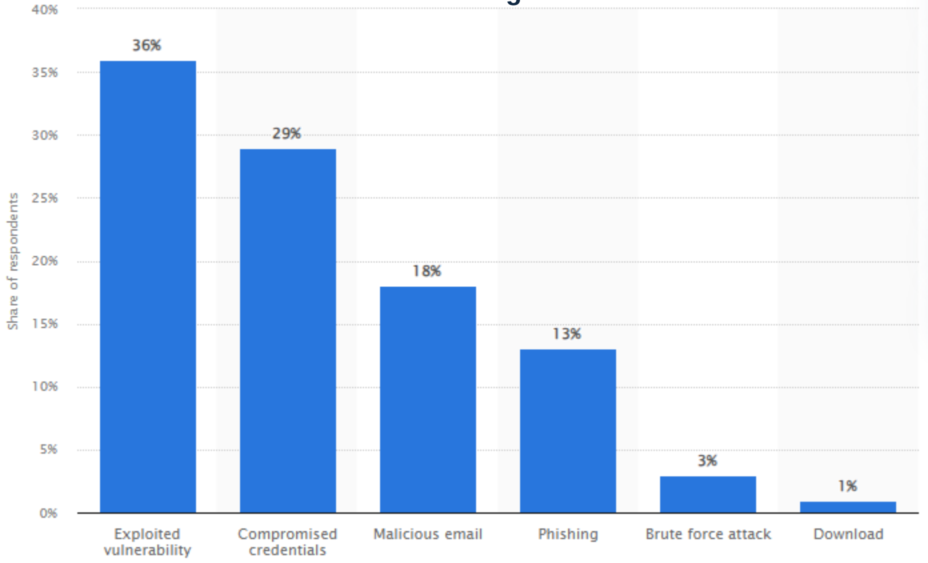
**Intrusion methods used in ransomware attacks by industry 2023**



[5]

| | Critical Infrastructure | Financial Services | Healthcare | Manufacturing | Professional Services | Public Service | Retail | Tech, Eng, Social Media |
|---|---|---|---|---|---|---|---|---|
| remote access | 52% | 27% | 35% | 33% | 35% | 41% | 29% | 36% |
| unknown/other | 23% | 22% | 16% | 22% | 21% | 15% | 26% | 20% |
| software/hardware vulnerability | 4% | 7% | 4% | 8% | 5% | 4% | 13% | 6% |
| malicious email | | 5% | 6% | 3% | 5% | 8% | 5% | 8% |
| stolen credentials | 2% | 5% | 3% | 4% | 6% | 5% | 3% | 4% |
| service provider | 4% | 3% | 4% | 1% | 2% | 2% | | 5% |
| drive-by-download | | 2% | | | 1% | | | 1% |
| default credentials | | | | | | | 3% | |

**Root causes of ransomware attacks in organizations worldwide as of March 2023**



[6]

[5] Arete / Cyentia

[6] Statista

ZURICH

# Conclusion

**(How) can we assess the realistic real-life impact of claimed security vulnerabilities?**

- Insurance approach:
  - Define and frame covered scenarios, which aim to insure the most demanded risk transfer requests
  - Within this frame, assess the risk based on data and loss experiences.

- A “realistic real-life impact” can be quantified with direct financial loss from a security or privacy incident.
- Reinsurers, have an excellent view on the vulnerabilities and incidents that cause most damage (or “impact” so to say)
  - Insight into events covered as well as uncovered by insurance
  - Broad geographical insurance exposures in many diversified industries

- Historic data-sets not enough to have high confidence with estimated maximum losses and risk quantification
- Highly volatile information security environment makes this even less predictable

  → reflected in risk management of insurance carriers

**Why are some vulnerabilities not addressed?**

- Low-hanging fruit:
  - poor privileged account management,
  - bad back-up strategies
  - overall lack of security awareness
- Vulnerabilities need to be exploited for harm to happen
- Relatively easily exploitable; otherwise next company/target
- Biggest vulnerability → people
- Immediate recall or replacement affects availability of business activities
- Impact on profits and potentially requires additional investments

# Thank you for your Attention!

## Any Questions?