
KÖRBER
KÖRBER HUNGÁRIA
GÉPGYÁRTÓ KFT.

Andreas Gaetje

Körber AG - CISO

Career

- Unilog: Software developer, Process Consultant
- ZURICH: IT & Security Audits
- GENERALI: Head of IT Audit Germany; Group Head of IT Risk and Security; Head of Security Operations
- KÖRBER: Group Chief Information Security Officer

Gergely Székely

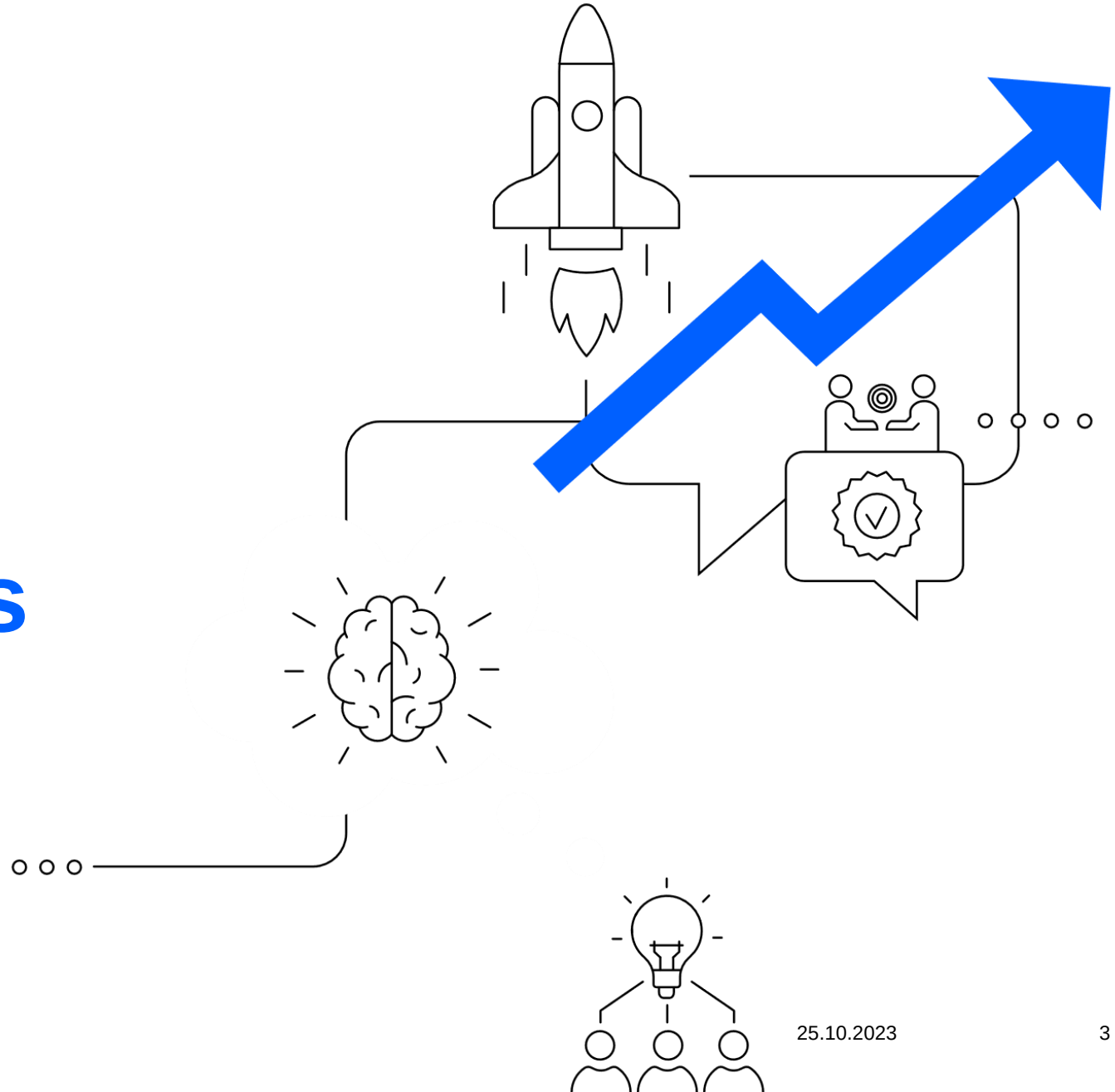
Körber Hungária – Head of IT

Career

- PÉCSI TUDOMÁNYEGYETEM Műszaki és Informatikai Kar: Electrical enginner, major in IT; Quality engineer
- ELCOTEQ: 2000 - 2011; From IT staff to CISO
- IBM: 2012 - 2014; IT Security Program Manager
- IT SERVICES HUNGARY Member of T-Systems: 2014 - 2018; Team Leader
- KÖRBER: 2018 – 2022: IT Department Leader; 2023 – Head of IT

Our purpose

We turn entrepreneurial thinking into customers' success



more than

100

locations worldwide

We

13,000

experts
















Our vision

Market leadership through technology leadership

2.5
billion euros
sales 2022

169
million euros
for research and development

2.9
billion euros
order intake 2022

Ecosystems
for holistic solutions

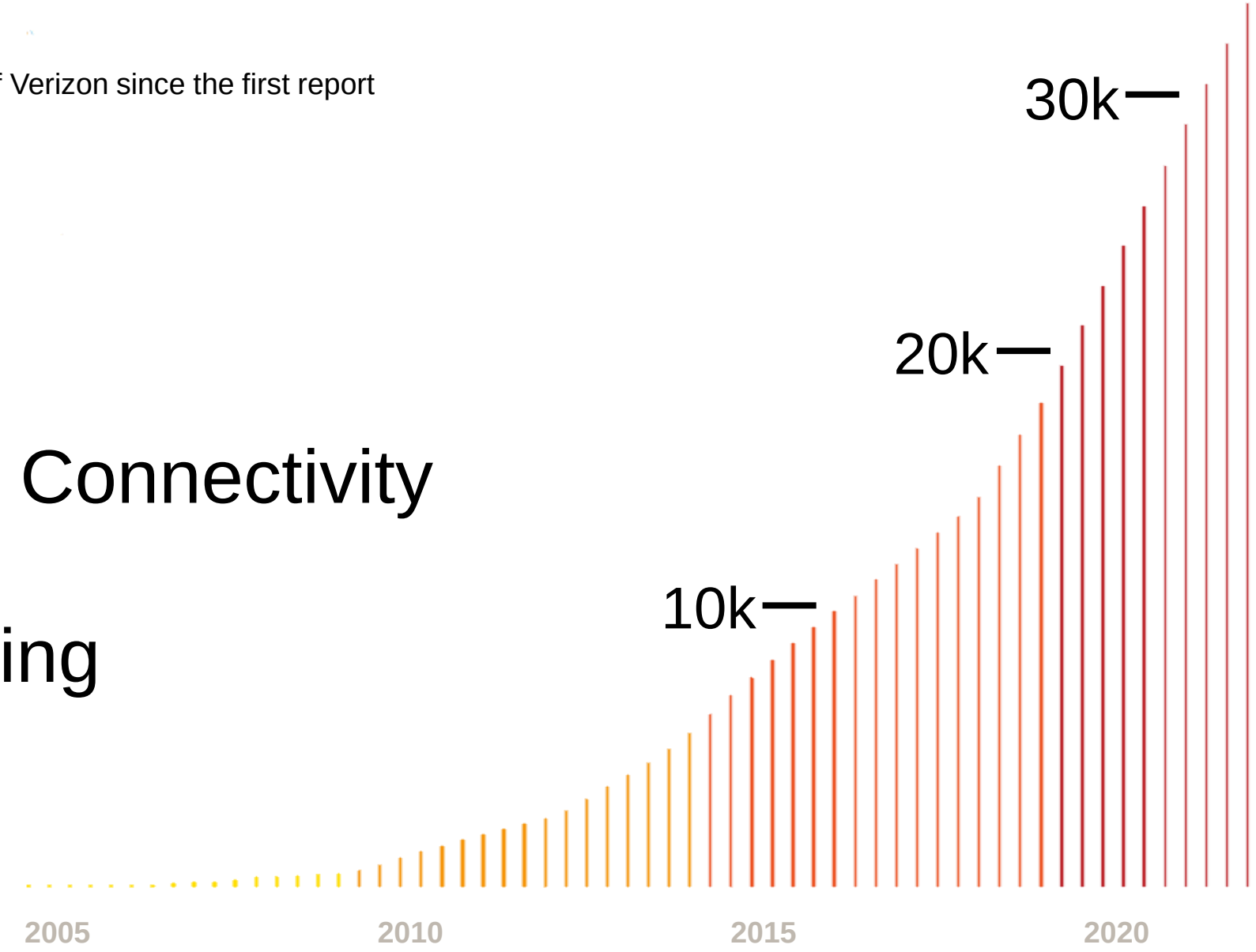
Drivers for data breaches

Number of breaches worldwide in the dataset of Verizon since the first report

Value of data

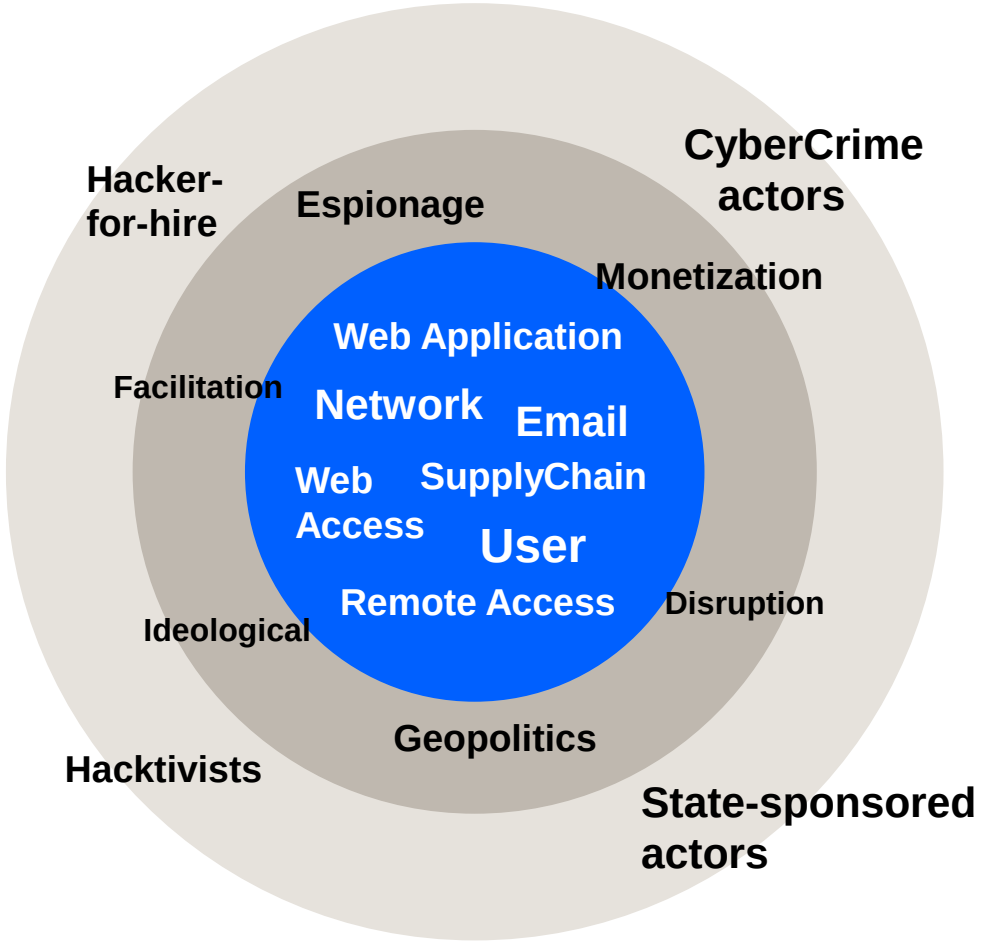
Complexity and Connectivity

Social engineering



Source: 2023 Data Breach Investigations Report – Verizon

Threat actors and attack vectors from Körber perspective



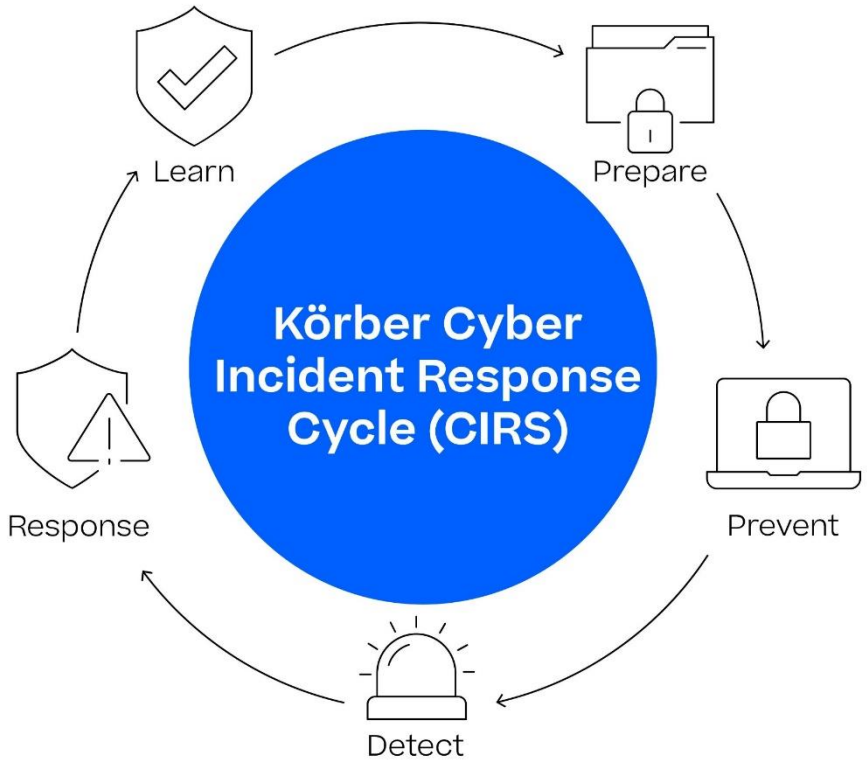
- **CyberCrime actors** are still the most relevant threat actor for Körber.
- **Monetization of attacks (i.e. ransomware)** remains the most important motivation for attacking manufacturing companies.
- **Espionage** of state-sponsored actors is another high risk that especially when it comes to internal IP transfer.
- Based on observations of Körber systems, the risk resulting from the **conflict in Ukraine** can be considered as low, but not negligible.
- Network and Remote Access are the most **critical attack vectors** for Körber due to the heterogeneous IT environment.

Threat actor | Motivation | Attack vector

Source: Threat actors and motivations – Enisa Threat Landscape 2022

Source: Attack vectors – Barracuda blog

Körber‘s Cyber Incident Response Cycle



Prepare
Set up all prerequisites to perform the following steps of prevention, detection, response and learning.

Prevent
Manage incoming threats and vulnerabilities, circulate them, and conduct all the steps needed to avoid potential incidents.

Detect
Manage security events to identify and communicate offences caused by malicious/abnormal behavior, network communication and/or transactions.

Response
Investigate on potential incidents (offenses) and react properly in terms of technical countermeasures.

Learn
Verify that the incident has been mitigated, the adversary has been removed, and additional counter measures are being implemented.

Awareness is the core of everything in information security

Security is the safeguard and the enabler for your business

WE PROTECT
WHAT WE CREATE.
Information Security

Legal disclaimer