D4 Data and Ethics

Autumn 2022 | Lecture 2 - Part III

Focus: Information security & cybersecurity | Author: Prof. Dr. Petra Maria Asprion | FHNW

Agenda

Part I -- Intro: data & more	→ SD1
Part II -- From yesterday until today	→ SD2
Part III -- Organization Layer: Be informed!	→ SD3
Part IV -- Organization Layer: Be prepared -- GRCM	→ SD4
Coaching Session #2	→ SD5

→ SD = Slide Deck

Conclusion and resulting consequence

Data becomes a valuable commodity

Data must be professionally protected -- confidentiality, integrity and accessibility are now a must!

Go back to L1 major threats

- Edward Snowden copied and leaked classified information from the National Security Agency (NSA), he leaked that the government was ‘spying’ on the public. He is controversially thought of as a hero to some, and a traitor to others (https://www.bbc.com/news/technology-54013527)
  - In 2020, the NSA surveillance of millions of Americans' telephone records was ruled unlawful by the US Court of Appeals. Mr Snowden said afterwards that he felt vindicated by the ruling.
  - *BBC news (2022-09-26): Putin grants Russian citizenship to Edward Snowden - https://www.bbc.com/news/world-europe-63036991*

Source and enhanced information: https://www.whistleblowers.org/whistleblowers/edward-snowden/

Excurse – Whistleblowing (1/2)

Trigger -- Compliance -- Regulatory Requirements

EU Directive 2019/1937 *(in force as of 17 Dec 2021)*

"On the protection of persons who report breaches of Union Law"

Companies must establish internal reporting channels guaranteeing confidentiality and diligent follow-up

Legal framework to protect whistleblowers from retaliation	Applies to companies with more than 50 employees	~40% of companies have no reporting channel in place *DE, FR, UK, and CH (Whistleblowing Report 2021)*

Mission -- Vision -- Objectives

Mission: Protect the privacy (→ focus on the **anonymity**) of internal informers (whistleblowers) and allow businesses to adequately resolve the misconduct in view of the public interest.

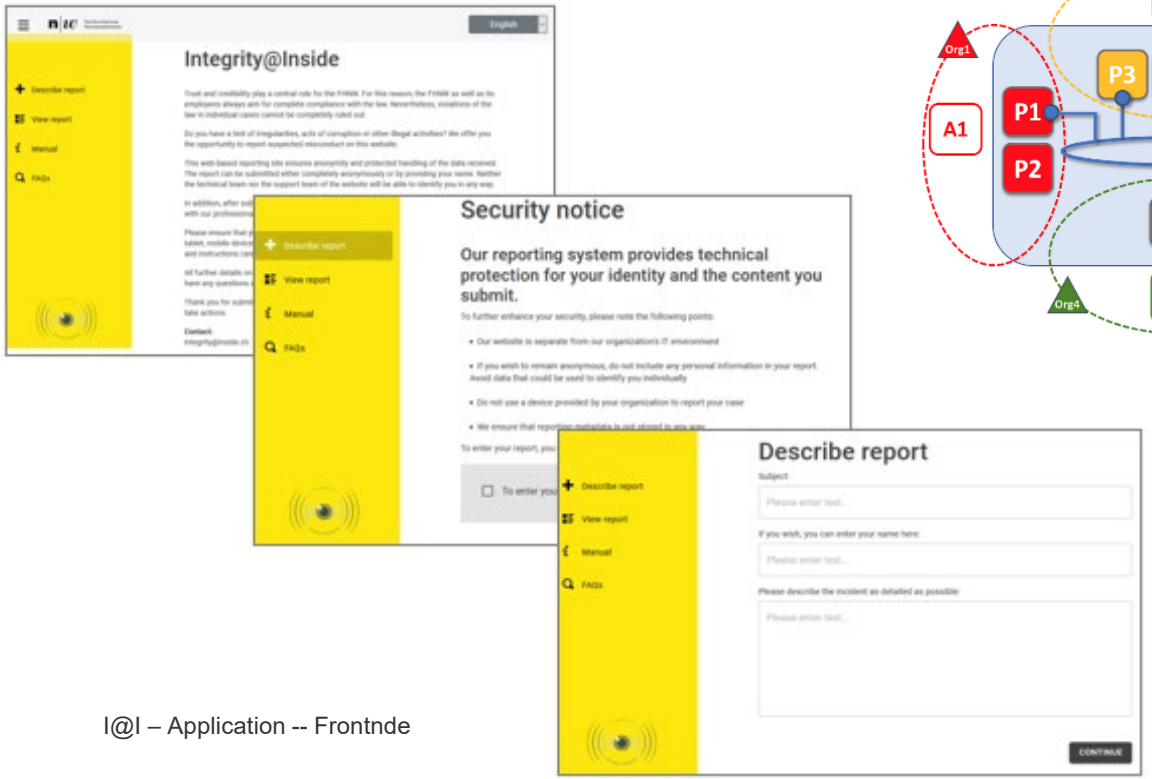
Vision: Use the characteristics of blockchain like "immutability", "transaction tracing", "pseudonymous accounts", and "smart contracts" to develop a resilient solution that offer whistleblowers unconditional anonymity whilst securing with certainty that the reported misconduct will be followed-up upon by the organization.

Objectives:

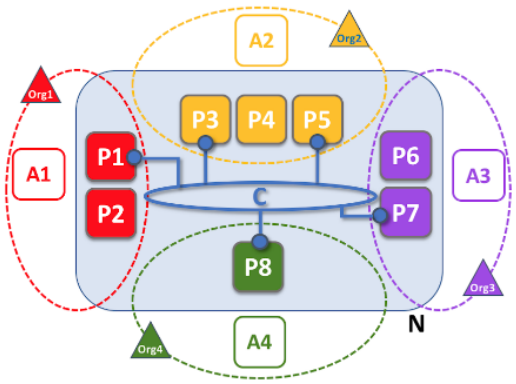
- ✓ Enable whistleblowers to report misconduct as they appear without the fear of retaliation.
- ✓ Increase "**trust**" in the digital solutions to encourage employees to do the right thing.
- ✓ Allow organizations to adequately manage and resolve reported cases.

Excurse – Whistleblowing (1/2)

A Blockchain-based Whistleblower Plattform



I@I – Application -- Frontnde



N	Blockchain Network	L	Ledger
C	Channel	A	Application
P	Peer	PA	Principal PA (e.g. A1, P5) communicates via channel C.
		Org	Organization
A1 P1 P2			Organization R owns application A1 and peers P1, P2.

I@I -- Underlying Architecture

FHNW HSW:	IWI Competence Center Blockchain Lead: Petra Maria Asprion
Funding:	KBA-NotaSys Integrity Fund, Lausanne
Duration:	2021-05 – 2022-03
Consortium:	FHNW HSW, CC Blockchain
Website:	https://whistleblowersystem.herokuapp.com/
Contact Person:	Frank Grimberg, Hermann Grieder
Student participation:	TOBIT (4 students) | BSc Praxis Project MSc BIS Master Thesis

Sources.
(1) Asprion, P.M., Grieder, H., Grimberg, F. (2022): Blockchain-basierte Meldesysteme. Vorstellung des Pro-jekts Integrity@Inside. In: comply. Fachmagazin für Compliance Verantwortliche, Jhrg. 7, 3/2022, S.18-22.
(2) Asprion, P.M., Grieder, H., Grimberg, F. (2023): Building Digital Trust to Protect Whistleblowers - A blockchain-based Reporting Channel. HICCS56, 2023. Accepted.

Resulting consequences

What do we learn from
security issues and data breaches?

Be informed –
and try to jump …

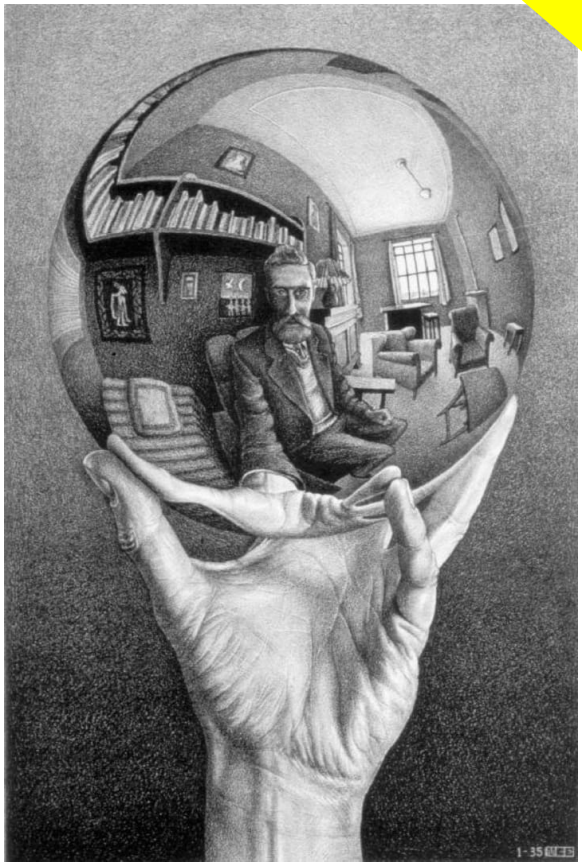
First – try jump over the four walls …

Today' – in 2022 – the dynamic geo-political and regulatory landscape shows that traditional cybersecurity approaches are no longer sufficient enough.

Practices established when IT infrastructure components were located within a company's **four walls** are not sufficient in the light of covid and in an era of **Cloud Computing** (CC), **Internet of Things** (IoT), **Internet of Everything** (IoE), **Artificial intelligence** (AI) and **Advanced Analytics**.

The threat situation or cyberattack risks faced by companies using outmoded security methods have increased dramatically during the COVID-19 pandemic. With most employees working remotely, sensitive data needs to be shared outside a company's walls.

This includes **employee data**, **intellectual property, corporate financial data**, and **other proprietary information**. It also includes the **supply chain**, data on suppliers, customers, their purchases, and the performance of products in the field.



'Hand With Reflecting Sphere' – M.C. Escher, 1935

The reflection of a mirror, plus the geometric properties of a sphere, makes for a unique self portrait by Dutch artist M. C. Escher

Assessment of your current situation

- **Practitioner approach:** Use established instruments to be informed and to get an initial overview
- **First idea**: Use an easily accessible tool, like …
  - the **Cyber Risk Index** (CRI)* -- **to be informed**
  - this comprehensive index aims to measure an **organization's readiness** to respond to different types of cyber threats or cyber attacks

The CRI is composed of two individual indices:

Cyber preparedness index: Representing an organization's readiness to defend against cyber attacks.

Cyber threat index: The state of the threat landscape at the time the CRI was determined.

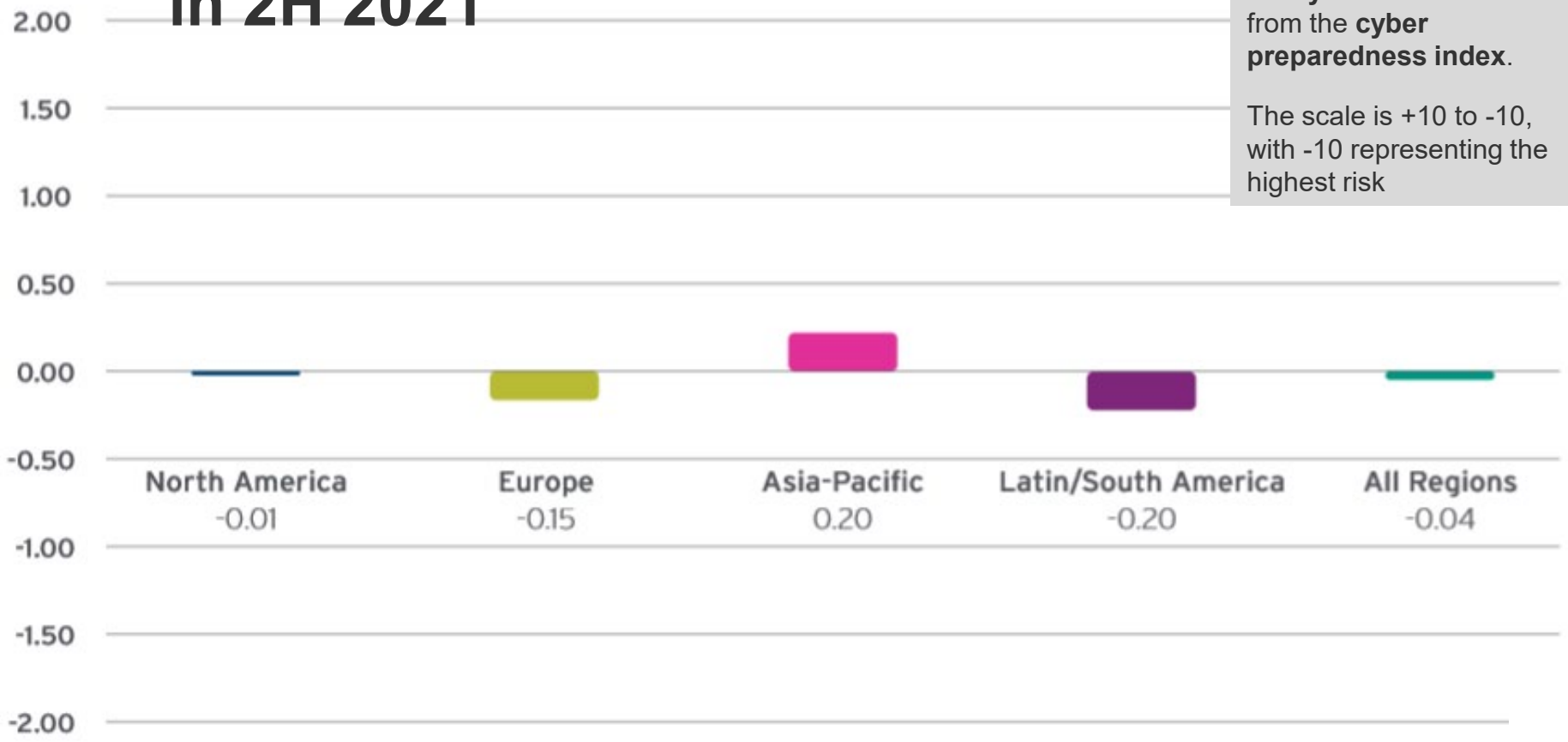
* We use the 5. edition of the **Cyber Risk Index** (CRI) from Trend Micro. The 2H'2021 version was developed in conjunction with the Ponemon Institute* and includes more than 3,400 CISOs, IT practitioners and managers across the regions of North America, Europe, Latin/South America, and Asia-Pacific.

* Have a Look: https://www.ponemon.org/

THE CYBER RISK INDEX (CRI) (1/6) in 2H'2021

Note: The CRI is calculated by subtracting the **cyber threat index** from the **cyber preparedness index**.

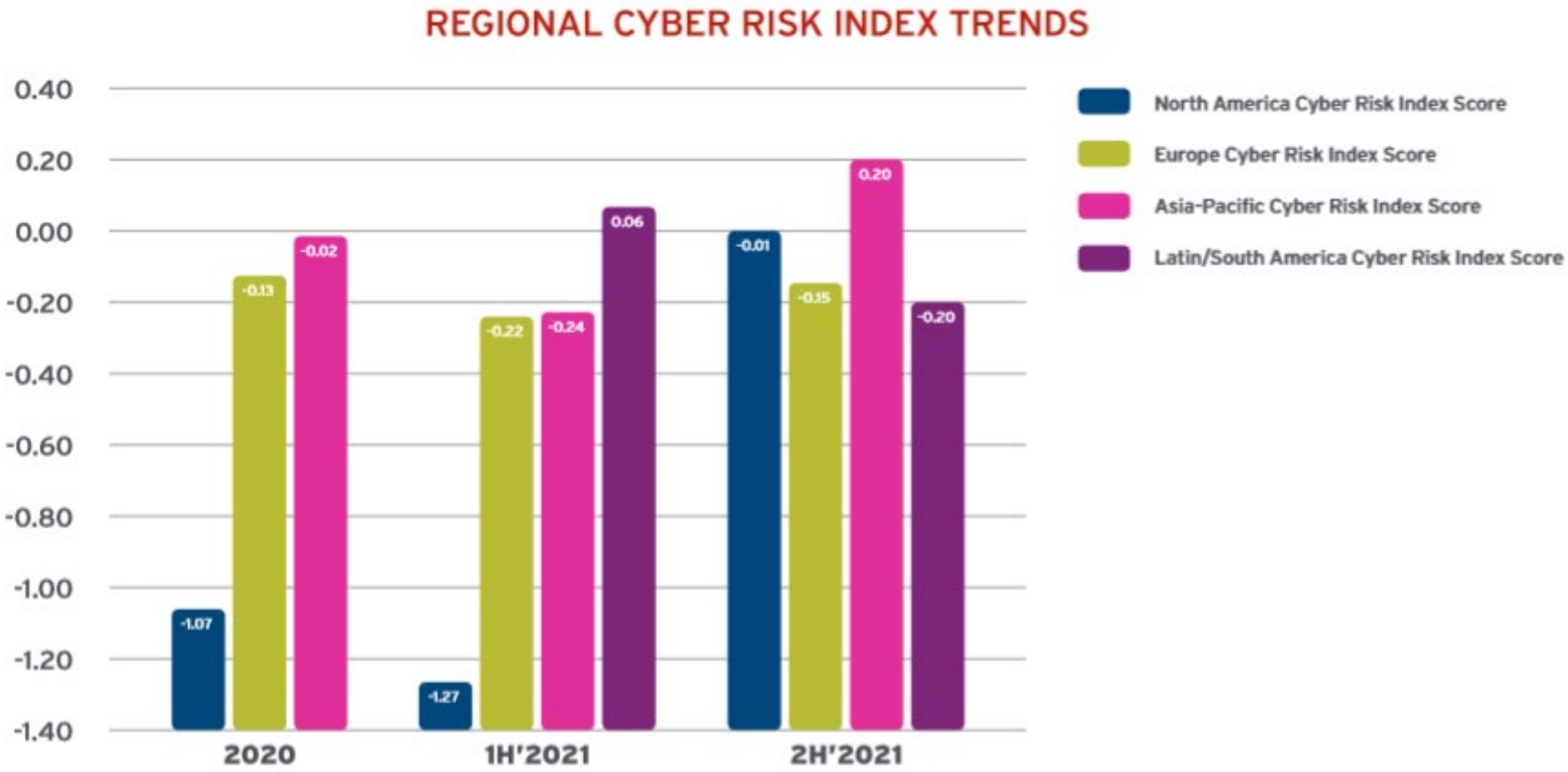
The scale is +10 to -10, with -10 representing the highest risk



Three of four regions show an elevated risk (negative CRI number), with Latin/South America having the highest risk level compared to the other three regions. This is due to Latin/South America having a lower perceived readiness than the other regions. Asia/Pacific has a positive CRI (moderate risk) due to improved preparedness and perception that the threat landscape has improved

https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

THE CYBER RISK INDEX (CRI) (2/6) in 2H'2021



https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

THE CYBER RISK INDEX (CRI) in 2H'2021 (3/6)

THE PRIMARY BUSINESS RISKS

The top cybersecurity risk factors businesses face can be broken down into five categories, based on the top concerns from respondents across the four regions:

Top five cyber threats

1. Ransomware
2. Phishing and social engineering
3. Denial of service (DoS)
4. Botnets
5. Man-in-the-middle attack

Top five data types at risk

- "My organization is not well prepared to deal with data breaches and cybersecurity exploits"
- "My organization's enabling security technologies are not sufficient to protect data assets and IT infrastructure"
- "My organization's IT security function is not able to contain most cyber attacks"

Human capital risk

- "My organization's IT security leader (CISO) doesn't have sufficient authority and resources to achieve a strong security posture"
- "My organization's IT security leader does not report to senior leadership (such as the CEO, COO, or CIO)"
- "My organization's IT security personnel do not have sufficient knowledge, skill, and expertise to protect data assets and IT infrastructure"

Top five infrastructure risks

1. Mobile/remote employees
2. Cloud computing infrastructure and providers
3. Across third-party applications
4. Malicious insiders
5. Mobile devices, such as smart phones

Operational risk

- "My organization's IT security function lacks support of security in the DevOps environment"
- "My organization's IT security function does not strictly enforce acts of non-compliance to security policies, standard operating procedures, and external requirements"
- "My organization's IT security function lacks compliance with data protection and privacy requirements"

https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

THE CYBER RISK INDEX (CRI) in 2H'2021 (4/6)

WHAT BUSINESSES STAND TO LOSE

While any information a business possesses is prone to data loss or theft, these five information types are the ones that present the greatest risk for an organization-based on results from the survey.

1. R&D information
2. Financial information
3. Business communication (email)
4. Company-confidential information
5. Trade secrets

In looking at the above results, it is clear that organizations put the most emphasis on the data that could cause repercussions for the business if it was stolen or compromised.

Top concerns (negative consequences) of a successful cyber attack are:

- Stolen or damaged equipment
- Cost of outside consultants and experts
- Customer turnover
- Reputation or brand damage
- Regulatory actions or lawsuits

Key takeaways for businesses

Our findings show that global businesses have a very high chance of being affected by a cyberattack (Note, these are all down from the previous CRI survey in 1H'2021).

- Likelihood of a data breach of customer data in the next 12 months: **67%**.
- Likelihood of a data breach of critical data (IP) in the next 12 months: **71%**.
- Likelihood of one or more successful cyberattacks in the next 12 months: **76%**.

https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

THE CYBER RISK INDEX (CRI) in 2H'2021 (5/6)

THE GREATEST CYBERSECURITY CHALLENGES FOR BUSINESSES

The polled organizations determined their risk factors based on the effectiveness of their security functions. Based on the global survey results, these are the greatest preparedness areas of concern for businesses:

- **People**: "My organization's IT security leader (CISO) does not have sufficient authority and resources to achieve a strong security posture"
- **Process**: "My organization's IT security function lacks enforcement on acts of non-compliance to security policies, standard operating procedures, and external requirements"
- **Technology**: "My organization does not make appropriate investments in leading-edged security technologies, such as machine learning, automation, orchestration, analytics, and/or artificial intelligence (AI) tools"

https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

THE CYBER RISK INDEX (CRI) in 2H'2021 (6/6)

PROTECTING BUSINESSES FROM CYBER THREATS

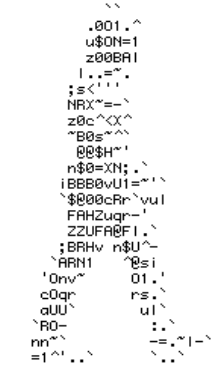
Taking the current threat landscape into consideration and based on the CRI findings, global businesses can still effectively minimize their risks by implementing security best practices. These include:

- Identifying and building security around critical data by focusing on risk management and the threats that could target this data
- Implement attack surface discovery to identify both internal and external systems, accounts, devices that you have
- Minimizing infrastructure complexity and improving alignment across the whole security stack
- Getting senior leadership to view security as a competitive advantage
- Improving the ability to protect the business environment, including properly securing, bring your own device (BYOD), internet of things (IoT) and industrial IoT devices (IIoT), and cloud infrastructure
- Investing in both new talent and existing security personnel to help them keep up with the rapidly evolving threat landscape, as well as improve retention
- Reviewing existing security solutions with the latest technologies to detect advanced threats like ransomware and botnets
- Improving IT security architecture with high interoperability, scalability, and agility
- Discuss with your security partner how a unified cybersecurity platform that includes extended detection and response (XDR) capabilities to improve your visibility and response to attacks

https://www.trendmicro.com/de_de/security-intelligence/breaking-news/cyber-risk-index.html

Today ---

And now?
What is with your learnings?



Lets walk to the coaching session #2