D4 Data and Ethics

Autumn 2022 | Lecture 3 - Part IV

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

© Picture Raphael Stöckli, MT cover 2018

Agenda

Part I -- Repetition L1 → SD1

Part II -- Organization Layer: Relevant References → SD2

Part III -- Organization Layer: First control - IS Policy → SD3

Part IV -- Organization Layer: Selective control - GEIGER → SD4

Coaching Session #3 → SD5

→ SD = Slide Deck

Our topic --
Information Security and Cybersecurity (I&CS)

Cyber risk remediation for small businesses …

GEIGER

Cybersecurity solution for small businesses

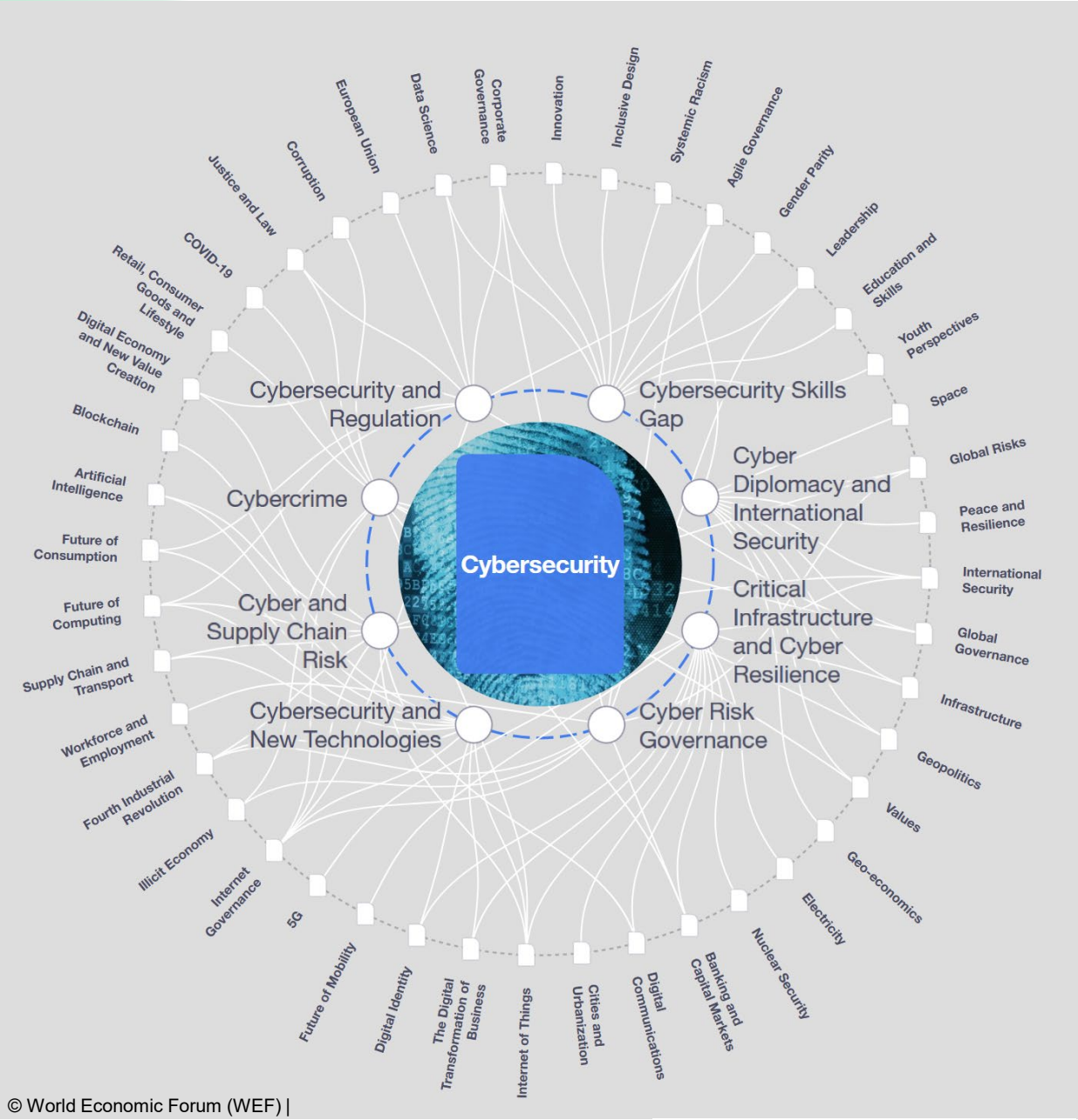
Twitter: https://twitter.com/cybergeiger/status/1273559453871341570?s=20
LinkedIn: https://www.linkedin.com/feed/update/urn:li:activity:6679327670146252800/
Facebook: https://www.facebook.com/cybergeiger/posts/126094359123895
Instagram: https://www.instagram.com/p/CBks7GOJh8x/?utm_source=ig_web_copy_link

Overall Motivation: Global threats

Attackers use malware for cyber-criminal mass attacks on private individuals, companies, authorities and other institutions, but also for targeted attacks on selected victims ...

There are several vulnerabilities in software products, some of which are critical, which attackers have been able to exploit for malware attacks or data theft …

The attackers increasingly used the "human factor" as a gateway, based on social engineering methods ...



© World Economic Forum (WEF) |

https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

Note: new version July 2022

European Union Motivation: Global threats

ENISA Threat Landscape for Ransomware Attacks -- July 2022

file:///C:/Users/petra.asprion/Downloads/ENISA+Threat+Landscape+for+Ransomware+Attacks.pdf

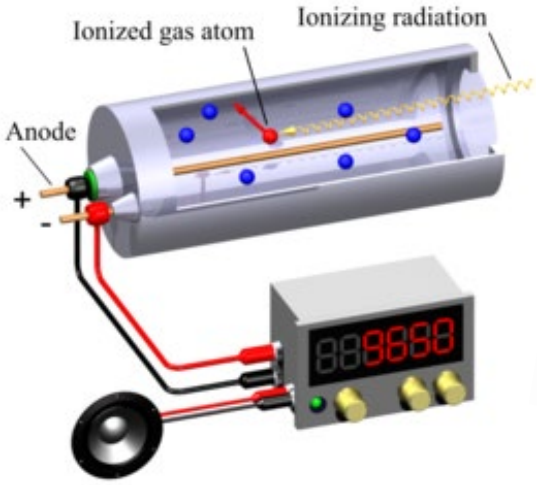
Executive summary: During the last decade ransomware has become one of the most devastating types of attacks, impacting organisations of all sizes worldwide. Quickly adapting to new business models with advanced threat actors leveraging the cybercrime ecosystem for a better distribution of labour, ransomware has managed to increase its reach and impact significantly.
No business is safe!

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

ENISA Threat Landscape for Ransomware Attacks -- July 2022

file:///C:/Users/petra.asprion/Downloads/ENISA+Threat+Landscape+for+Ransomware+Attacks.pdf

Reality of the risk ...



Hans Geiger
1882–1945
Invented Geiger
Conter in 1911

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

Motivation: Cybersecurity is too complicated …

There are plenty of tools, recommendations, and “solutions” available …

Most of them are complicated and costly ...

They don’t match the needs of small businesses!

Therefore - what I don't see (hopefully) doesn't affect me!

Or?

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

It shouldn’t be!

Think about radiation –
is invisible
to our eyes.

But even though you
can't see it,
it's life threatening!

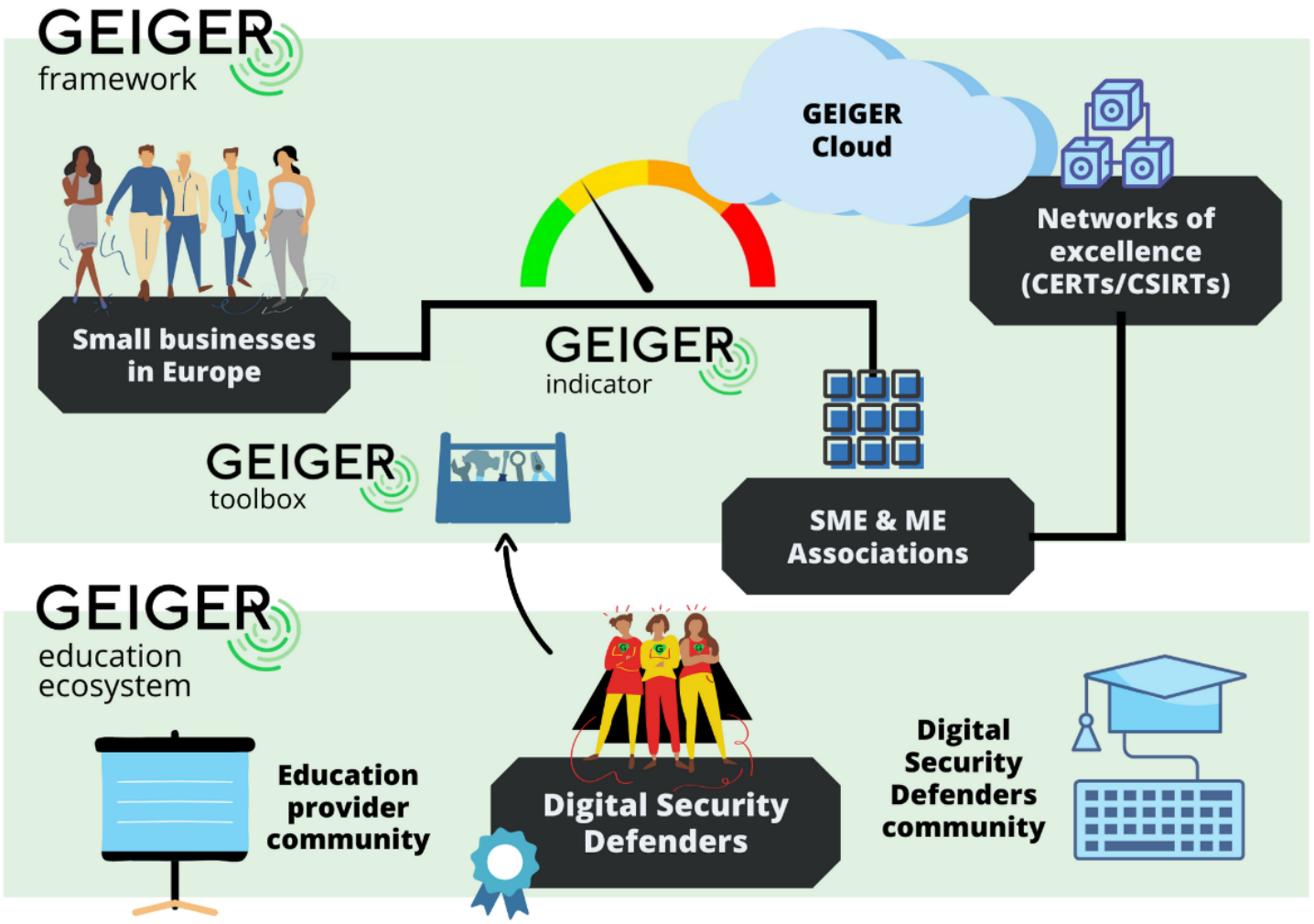
But with the right tools,
it's easy to detect.

Couldn't detecting cybersecurity
risks be as easy?

GEIGER

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

This is why we have GEIGER



University of Applied Sciences and Arts Northwestern Switzerland
School of Business

GEIGER - The ecosystem

Learning Tools

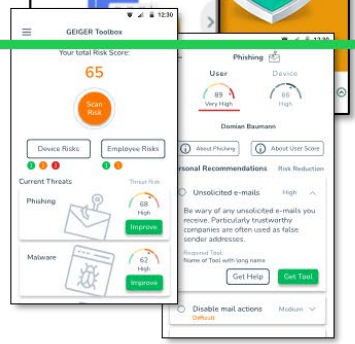
Protection Tools

xAPI

GEIGER API

Micro and Small Enterprises

GEIGER Toolbox



digital trust center.

enisa

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

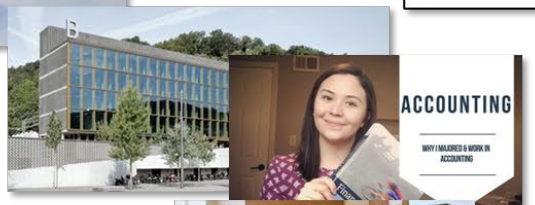
NCSC

Multipliers

Security Defenders

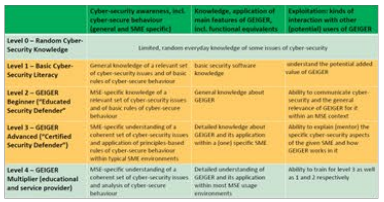
SKV Association Suisse des PME
Associazione Svizzera delle PMI
Schweizerischer KMU Verband

ffure SUISSE
hweizer Coiffeurgeschäfte
suisse de la coiffure
Imprenditori parrucchieri svizzeri



Education Providers

GEIGER Cloud



GEIGER Security Defenders Education

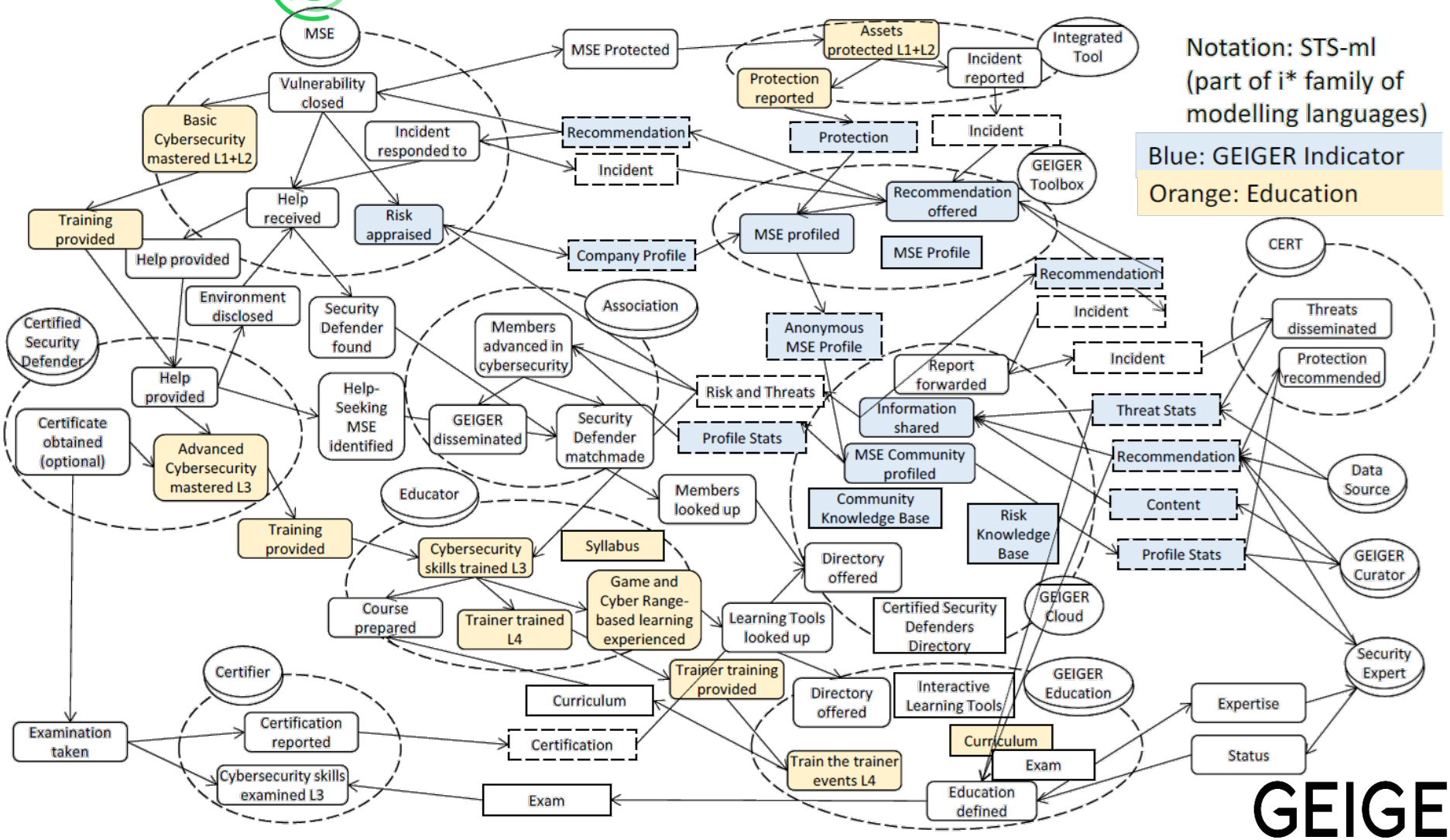
MISP Threat Sharing

CERTs/CSIRTs

GEIGER

University of Applied Sciences and Arts Northwestern Switzerland
School of Business

GEIGER - The ecosystem



University of Applied Sciences and Arts Northwestern Switzerland
School of Business

GEIGER education and exchange

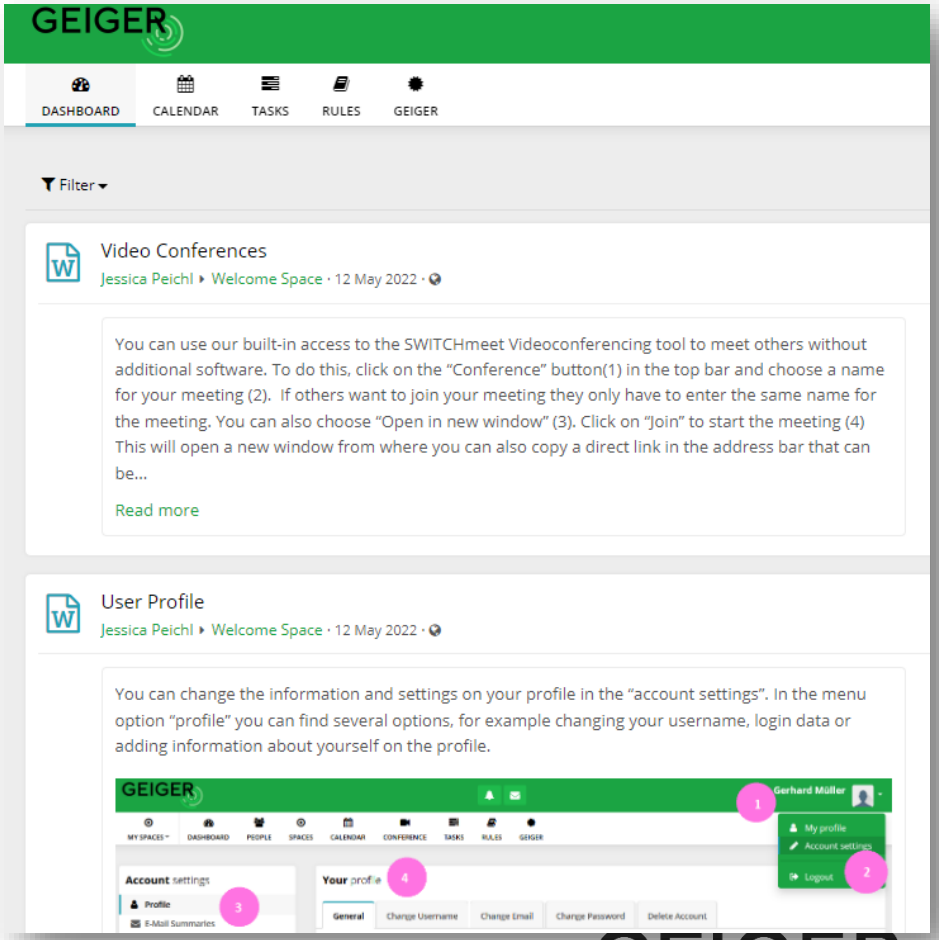
GEIGERedu

- Education for laypeople → reach MSEs that have little knowledge about cybersecurity.
- 'Reverse Mentoring' → education of (young) digital natives (e.g., apprentices) which then train ('mentor') MSE employees/owners.

GEIGERcommunity

- 'Social Media' platform for cybersecurity.
- Community building for Cybersecurity Defenders and people interested in cybersecurity.

→Join here: https://community.cyber-geiger.eu/

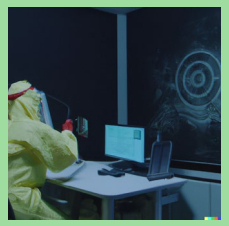


University of Applied Sciences and Arts Northwestern Switzerland
School of Business

GEIGERedu – 12 nuggets

1 **GEIGER to improve cybersecurity**

3 **Radiant Personalities**



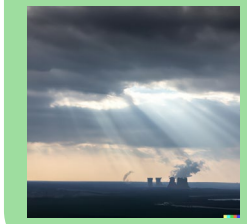
5 **Contamination**

7 **Safe transport for dangerous goods**

9 **Safe storage and disposal**

11 **Rules and Regulations**

2 **From power plants to cosmic rays**



4 **Fencing your power plant**

6 **Entangled Hostages**

8 **Danger Zone**

10 **Keeping track of dangerous goods**

12 **Become a Defender**

GEIGER

What have we discussed so far?

Relevance of global threats and ransomware
→ WEF report and ENISA threat landscape (as two further examples)

Cyber risks are invisible!

Cybersecurity is too complicated … easy solutions are necessary
in particular for small businesses

Concept of GEIGER – GEIGER Framework

and as conclusion ...

To mitigate cyber risks - an ecosystem is needed!