University of Applied Sciences Northwestern Switzerland
School of Business

D4 Data and Ethics

Autumn 2022 | Lecture 2 – Coaching

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

© Picture Raphael Stöckli, MT cover 2018

Agenda

Part I -- Intro: data & more → SD1

Part II -- From yesterday until today → SD2

Part III -- Organization Layer: preconditions → SD3

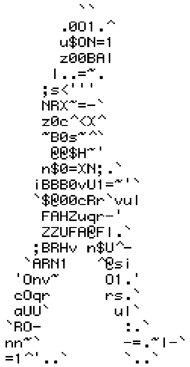
Part IV -- Organization Layer: GRC & Management → SD4

Coaching Session #2 → SD5

→ SD = Slide Deck

Today ---

And now?



Lets discuss coaching session #2

The theme is "be informed"

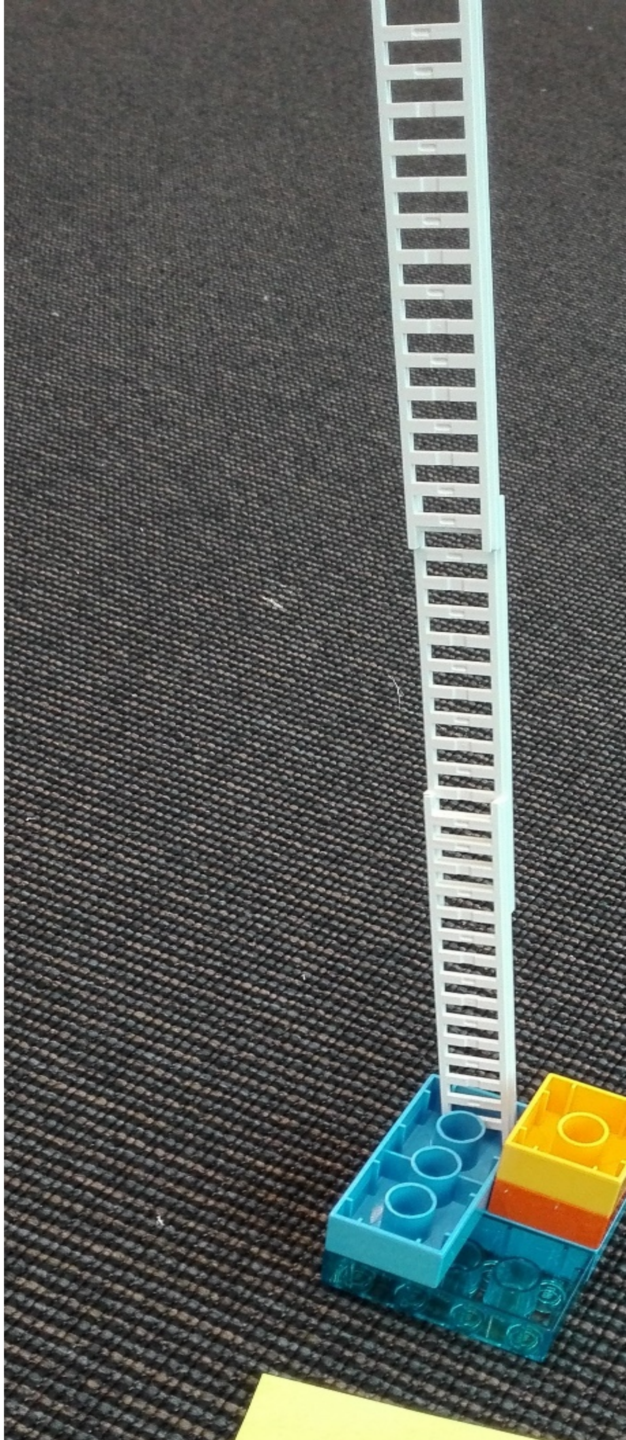
You have three (or four) tasks described in the following, which you should work on in a team of 2-3 students during your coaching session.

The aim is that you

a) “**be informed**” about events - formative and recent ones in relation to cybercrime

b) get an experience of how cyber risks can be identified and which technical terms (-> taxonomy of security) are used. If you are not familiar with any term used, please look it up (e.g. here: https://www.isaca.org/resources/glossary or https://csrc.nist.gov/glossary)

Note: There will be a FAQ, if any, from after the coaching sessions – on Moodle



Cyber Risk Index (CRI) Calculator

Calculate the CRI for a fictitious firm

Overall question: How prepared is your organization against a cyberattack?

Task 1

Find out

With the following instrument:
https://go.trendmicro.com/new-web/security-intelligence/cyber-risk/calculator.html

Your Learning:

Company-relevant questions regarding potential cyber risks and their level of detail; in turn, companies need to prepare for these issues and can improve based on the report.

Please perform the assessment for a fictive (or any other) company.
Note: You will receive the final report (pdf) only if you provide an email address address (and a (fictitious or other) company).

Relation to L1 & more examples

The 2010' -- major breaches

Task 2

- **Yahoo** - Records compromised: 3 billion / 500 million
  (1) Breach date: August 2013 -- Disclosure date: December 2016
  (2) Breach date: Nov/Dec 2014 -- Disclosure date: Sept 2016
- **Aadhaar** - Records of Indian citizens compromised: 1.1 billion
  Breach date: Unknown -- Disclosure date: January 2018
- **First American Financial** - Records compromised: 885 million
  Breach date: Unknown -- Disclosure date: May 2019
- **Facebook** - Records compromised: 533 million
  Breach date: Unknown -- Disclosure date: April 2021
- **Twitter** - Number of records: 330 million
  Breach date: Unknown -- Disclosure date: May 2018
- **Microsoft** - Records compromised: 250 million
  Breach date: December 2019 -- Disclosure date: January 2020

Discuss in your team of two or three:
How could those cases have been prevented?
Select in your team one of the breaches and analyse a.) the damage and b.) how this could have been prevented (create a list of potential prevention tasks)

The 2015' -- major breaches in Pharma

Coaching Session

Task 3

- 2014: Targeted attacks on Pharma Suppliers
  (Dragonfly/Energetic Bear attacks)
- 2017: Attacks on Merck
  infected around 30K computers across sales, manufacturing, research
- 2018: Attacks on Bayer
- 2019: Attacks on Roche
- 2020: Attacks on Dr Reddy's Laboratories
- 2020: Attacks on Pfizer/BioNTech and AstraZeneca
- 2022: Attacks on Novartis
- 2021/2022: others (you find)?

Discuss in your team of two or three:
How could those cases have been prevented?
Select in your team one of the breaches and analyse a.) the damage, and
b.) was it easy to find informative information about the event?, and
c.) how this could have been prevented (create a list of potential prevention tasks)

Self Learning
"Be informed"

Recommended Literature

Task 4

Cybercriminals launch new phishing schemes COVID-19 related: "COVID-19 Phishing Update: Voicemail Attacks Surface Targeting Office 365 Users," https://www.phishlabs.com/blog/covid-19-phishing-update-voicemail-attacks-surface-targeting-office-365-users/.

Lucian Constantin, "Attacks against internet-exposed RDP servers surging during COVID-19 pandemic," CSO (May 8, 2020), https://www.csoonline.com/article/3542895/attacks-against-internet-exposed-rdp-servers-surging-during-covid-19-pandemic.html

Tamara Scott, "Cybersecurity Trends in 2020: BYOD and Mobile," Technology Advice (Jan. 7, 2020), https://technologyadvice.com/blog/information-technology/cybersecurity-trends-2020-byod-mobile/.

David Lukic, "Target Data Breach, How Target Almost Lost Everything," ID Strong (Sep. 22, 2020), https://www.idstrong.com/sentinel/that-one-time-target-lost-everything/

Scott Ikeda, "Marriott Hit With Second Major Data Breach in Two Years; Over Five Million Guests Compromised," CPO Magazine (Apr. 13, 2020), https://www.cpomagazine.com/cyber-security/marriott-hit-with-second-major-data-breach-in-two-years-over-five-million-guests-compromised/

Raphael Satter, Jack Stubbs, and Christopher Bing, "Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike," Reuters (Mar. 23, 2020), https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN

Andrew Jeong, "North Korean Hackers Are Said to Have Targeted Companies Working on Covid-19 Vaccines," The Wall Street Journal (Dec. 2, 2020), https://www.wsj.com/articles/north-korean-hackers-are-said-to-have-targeted-companies-working-on-covid-19-vaccines-11606895026

Lucian Constatin, "SolarWinds attack explained: And why it was so hard to detect," CSO (Dec. 15, 2020), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

This is your self learning area: it is recommended that you walk through the provided publications to achieve an understanding about the current situation, in particular under the light of Covid19.