

Module D4 – Local Session 2 (Cybersecurity I)

Instructions for students

Task 1 – Application of Cyber Risk Index (CRI) Calculator

- ➔ Team building: 2-4 students (the solve all tasks together)
- ➔ Time allocated: around 60 min
- ➔ Setting: At the beginning, please discuss in the team which company you want to evaluate. It can be the company where (one of you) works or a fictitious company (that you know). Setting adjustment: You can also do the assessment twice - for two different companies. But then you have to manage your time well.

Objectives and Conversion:

1. Become aware of cyber risks and how to assess (in general) them within an organization
2. You will be able to assess certain organizational cyber risks based on a (pre-defined) tool – **the Cyber Risk Index (CRI) Calculator** -- <https://go.trendmicro.com/new-web/security-intelligence/cyber-risk/calculator.html>

Relevant sources: see provided presentation in lecture 2 -- 02.5 Coaching Session II.pptx or below the excerpt of the slide deck with the selected cases.

Excerpt presentation:

Cyber Risk Index (CRI) Calculator

Calculate the CRI for a fictitious firm

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

Find out

Task 1

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).

Task 2 – The 2010' -- major breaches

- ➔ Team building: 2-4 students (they solve all tasks together)
- ➔ Time allocated: around 15-30 min
- ➔ Setting: Setting: At the beginning, please discuss in the team and decide which case you want to examine and discuss in more detail.

Objectives and Conversion:

1. Become aware of cyber risks that can affect any organization (you work for)!
2. Discuss: Select in your team one of the cases/breaches and analyze
 - a.) the damage (can you find concrete figures?), and
 - b.) why are these large organizations so severely affected (any idea?), and
 - c.) how the incident could have been prevented (create a list of potential prevention tasks)

Relevant sources: see provided presentation in lecture 2 -- 02.5 Coaching Session II.pptx or below the excerpt of the slide deck with the selected cases.

Excerpt presentation:

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)

Task 3 – The 2015' -- major breaches in Pharma

- ➔ Team building: 2-4 students (they solve all tasks together)
- ➔ Time allocated: around 15-30 min
- ➔ Setting: Setting: At the beginning, please discuss in the team and decide which case you want to examine and discuss in more detail.

Objectives and Preparation:

1. Become aware of cyber risks that can affect an organization
2. **Discuss:** How could those cases have been prevented?
Select in your team one of the breaches and analyze
 - a.) the damage
 - b.) was it easy to find informative information about the event? (May you discuss, why potentially not or which sources were meaningful), and
 - c.) how this could have been prevented (create a list of potential prevention tasks)

Relevant sources: see provided presentation in lecture 2 -- 02.5 Coaching Session II.pptx or below the excerpt of the slide deck with the selected cases.

Excerpt presentation:

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)