DeepSec, 18-19 November 2021, Vienna

Building a Cybersecurity Workforce: Challenges for Organizations

Matthieu J. Guitton, PhD, FRAI
Full Professor, Université Laval, Canada

matthieu.guitton@fmed.ulaval.ca
@matthieuguitton

I. The Nature of Cybersecurity

“Information Gathering Game”

- Spy ⇨ **obtain** the information
- Spied ⇨ **protect** the information

defense	security
diversion	disinformation

“Information Gathering Game”

- Spy ⇨ **obtain** the information
- Spied ⇨ **protect** the information

defense cybersecurity

diversion “fake news”

Technology does not change
the “principles” of intelligence.

However, technology change both
the **quantity** and the **nature** of the information
that have to be protected.

Managing Cyberthreats

- **Technical** aspects
- **(Cyber)behavior**

➪ *If you take into account only technical aspects,* ***you are not protected****.*

➲ The weakest link in the cybersecurity chain, is the **Human factor**

What do we need to protect?

➲ Protecting the “individuals”, particularly what is related to their “identity”

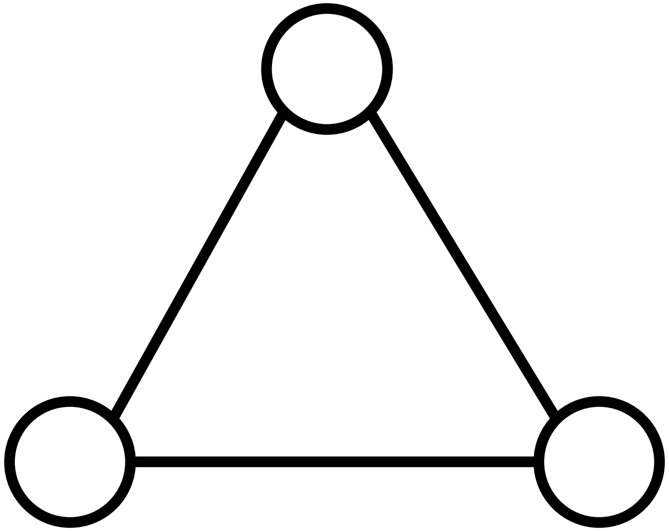
➲ But what we actually have access to are not the “individuals”, but the **data** related to the individuals

➲ So, at the end, cybersecurity is **protecting the data**

The “Triad Nature” of Cybersecurity

Data

(nature of data relevant to the organization)



Technical
aspects

Psychology
Cyberbehavior

II. Challenges for Organization

Formation Challenge

“Getting people who are trained”

- Cybersecurity is an emerging field
  - Very few academic formations existing and available
  - Typical cybersecurity formations are focusing on IT

Conceptual Challenge

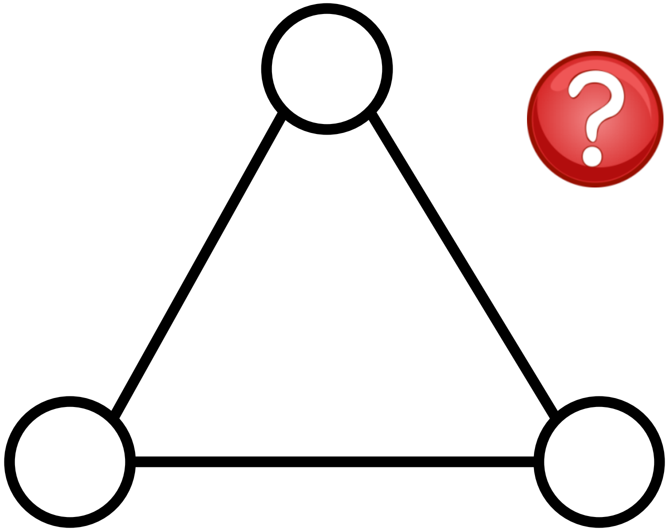
"Getting people who are trained for the right thing"

Technical aspects

Conceptual Challenge

Data

(nature of data relevant to the organization)



Technical aspects

Psychology
Cyberbehavior

➲ *Practically, how to make that happen in your organization?*

Organization Chart Challenge

"Getting people to the right place in your organization"

"cybersecurity"

➲ IT department

➲ Security service

How do we "negotiate" the relations and interactions between these two poles?

➲ *Typically, very poorly…*

Threat Evolution Challenge

“Getting people to react appropriately to new threats”

⇨ Cybersecurity

…so are the threats

- ➲ New cyberthreats are constantly emerging
- ➲ Cybersecurity workforce needs to stay state-of-the-art

III. Paths to Solutions

Optimizing the Workforce Training

Realistically, most cybersecurity personals are IT experts

“superimposed” training (supplementary layer of training)

➲ **psychology / cyberpsychology**

vulnerability, mental health, etc…

➲ **nature of the data of the organization**

you are a biopharma, you need someone who understand a pharmacological graph…

Optimizing the Workforce Training

Alternative solution…

If you can not have 3 in 1, then go for 3 in 3

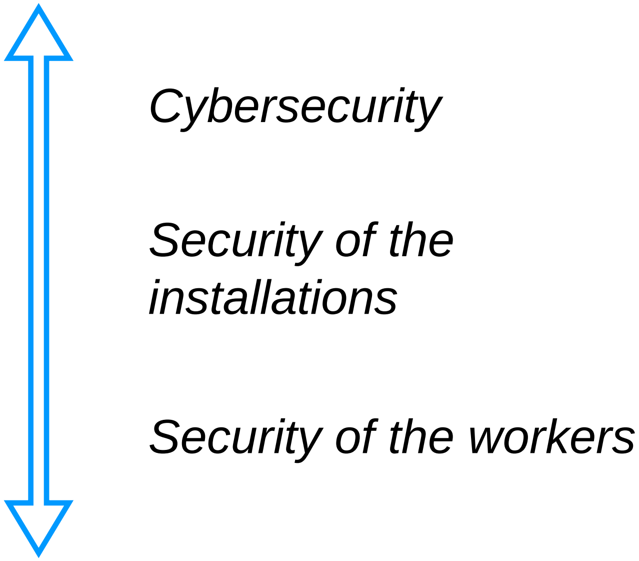
⇨ Structure your cybersecurity unit as a “**team**” consisting of three people:

- 1 **IT cybersecurity person**
- 1 **psychologist / cyberpsychologist**
- 1 **content expert** (of organization’s data)

Integrating Cybersecurity within Security

- ➲ Integrate cybersecurity within the global security strategy of the organization

- ➲ Integrate cybersecurity in a security and data protection continuum



Cybersecurity

Security of the installations

Security of the workers

Interacting with the Academia

- **Initial training** of cybersecurity professionals
- Dialog to **inform academic community** of the **needs** of organizations
- Allows to **stay state-of-the-art**
- Even better: If you feed researchers with the new forms of attack, they can **develop countermeasures faster**, and **integrate them within education cursus**

Conclusion – "Take-Home Messages"

- Challenges
  - Formation Challenge
  - Conceptual Challenge
  - Organization Chart Challenge
  - Threat Evolution Challenge

Conclusion – “Take-Home Messages”

- Operational Recommendations

  - ⇨ Get personals expert in IT, cyberpsychology, and organization-specific data
  - ⇨ If not possible, provide expertise in cyberpsychology and organization-specific data to your IT cybersecurity people
  - ⇨ If not possible, get three-man teams to cover all these three expertise

Conclusion – “Take-Home Messages”

- Operational Recommendations

⇨ **Integrate** your cybersecurity workforce within your security department, not just your IT department

⇨ **Increase the interactions with the academia**
For continuous training / professional development

matthieu.guitton@fmed.ulaval.ca

@matthieuguitton

Further Readings

- Guitton MJ (2019).
  Facing cyberthreats: Answering the new security challenges of the digital age.
  Computers in Human Behavior, 95:175-176

- Guitton MJ (2020).
  Using biotechnology to build a workforce for intelligence and counterintellgience.
  International Journal of Intelligence and Counterintelligence, 33:119-134

matthieu.guitton@fmed.ulaval.ca

@matthieuguitton

?

Got a question?

⇨ matthieu.guitton@fmed.ulaval.ca