



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

7.1.1 Cyberresilience

Concepts (extracted from automatically generated subtitles):

Field of cybersecurity. Chief information security officer. Formal roles. Cybersecurity incidents. Full-time. Part-time role. Cybersecurity people. Context of humanitarian organisations. Best use of resources. Second chapter. Topic of leadership. Organisations. Chief security officer. Cyber function. Best results.



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

UNDERSTANDING THE DIGITAL SUPPLY CHAIN AND ITS STAKES FOR HUMANITARIAN ACTORS

EPFL
EssentialTech
Centre



EPFL
**Center for
Digital Trust**

...

notes

summary

0m 0s



LEADERSHIP IN CYBERSECURITY

LEADERSHIP, BEST PRACTICES AND CYBER HYGIENE

Introduction

Paul Hume,
Chief Information Security Officer (CISO), ICRC



What is leadership in the field of cybersecurity?

notes

summary

0m 6s



Introduction



What is leadership in the field of Cybersecurity?



Does it depend on organizations or individuals?

How to make the best use of resources?



How do we manage Cybersecurity incidents?

Does it depend on organisations or individuals? How to make the best use of resources

notes

summary

0m 13s



Introduction



that are available in your organisation in this field? How do we manage cybersecurity incidents? Hello, my name is Paul Hume, and in this module, we will try to answer these questions together.

notes

summary

0m 25s



Introduction



A little bit about myself first. I'm the Chief Information Security Officer for the International Committee of the Red Cross, or the ICRC. I've worked in many sectors and countries for many years,

notes

summary

0m 37s



Introduction



more years than I care to admit. I'm going to help you unpick the topic of leadership in cybersecurity in the context of humanitarian organisations.

notes

summary

0m 49s



What We Will Learn



Leadership in Cybersecurity



**Understanding Threats
and Vulnerabilities**



**Handling a Cybersecurity
Incident**

Hopefully, to provide some useful tips along the way. In this video, we will start by speaking about what is leadership in this context. In the subsequent videos, we will speak about understanding threats

notes

summary

1m 1s



What We Will Learn



Leadership in Cybersecurity



Understanding Threats and Vulnerabilities



Handling a Cybersecurity Incident

as well as vulnerabilities. That will be it for this first chapter. In the second chapter, we will look into how to manage cybersecurity incidents.

notes

summary

1m 13s





Leadership in Cybersecurity

- Combination of organizational and individual levels.
- What works best is contextual.

Let's talk about leadership now. Let me first state that leadership in cybersecurity must be viewed both at an organisational level

notes

summary

1m 22s





Leadership in Cybersecurity

- Combination of organizational and individual levels.
- What works best is contextual.

and for you as an individual.

notes

summary

1m 32s





Leadership in Cybersecurity

- Combination of organizational and individual levels.
- What works best is contextual.

It's a combination of both that will yield the best results. In addition, what works best for you and your organisation is entirely contextual. Let's start with the organisational perspective.

notes

summary

1m 37s



Organizational Perspective



Cybersecurity officers are often perceived as the “people that always say NO” BUT the cyber function is a service that helps the organization to operate and innovate safely in the digital world.

If you have a cybersecurity people working in your organisation, you need to understand that while they may be known as the guys that always say no and may be perceived as blockers for innovation or prevent you from delivering the services that you want to your beneficiaries, it's a misperception.

notes

summary

1m 49s



Organizational Perspective



Cybersecurity officers are often perceived as the “people that always say NO” BUT the cyber function is a service that helps the organization to operate and innovate safely in the digital world.

The cyber function is indeed a service that helps the organisation to operate and innovate safely in the digital world. In the end, by managing the risks related to cybersecurity, they help you deliver on the long-term goals and aspirations of your organisation.

notes

summary

2m 8s



Formal Role for Managers



Formal roles for managers of these functions include titles

notes

summary

2m 24s



Formal Role for Managers



such as Chief Information Security Officer, Chief Security Officer, Information Security Officer, Information Security Manager, Cybersecurity Manager, etc.

notes

summary

2m 25s



Formal Role for Managers



In the end, it doesn't matter what the title is. As long as someone in a full-time or part-time role in an organisation is the focal point for the organisation.

notes

summary

2m 37s





Key Responsibilities for such role:

- Understanding the governance, compliance and technical elements of keeping the organization safe.
- Define strategy to improve the security capabilities and maturity.

This is someone who has the role of understanding the governance, compliance, and technical elements of keeping the organisation safe. It's also someone who has the responsibility or accountability to ensure that there is a strategy to improve the security capabilities and maturity and dependent on the seniority in the organisation to seek funding for those activities.

notes

summary

2m 48s





The Role of Individuals in Cybersecurity:

- **Cybersecurity as a team job.**
- Behave in ways that does not put people and information at risk.
- Management of infrastructure, applications development and information by complementary teams.

Speaking about the role of individuals, good cybersecurity requires teamwork, and in this case, the team is not just the cybersecurity function. You and every other individual in the organisation

notes

summary

3m 14s





The Role of Individuals in Cybersecurity:

- Cybersecurity as a team job.
- Behave in ways that does not put people and information at risk.
- Management of infrastructure, applications development and information by complementary teams.

actually has the responsibility to ensure that you and the people around you behave in ways within the organisation that does not put the people and information at risk.

notes

summary

3m 27s





The Role of Individuals in Cybersecurity:

- Cybersecurity as a team job.
- Behave in ways that does not put people and information at risk.
- Management of infrastructure, applications development and information by complementary teams.

Additionally, in nearly all cases, the cybersecurity team needs other teams that manage infrastructure, applications, development, and information management to put in place and maintain what the organisation needs to operate safely.

notes

summary

3m 37s



The Role of Individuals in Cybersecurity



If your organisation does not have a formal cyber role, then this might be your opportunity to shine.

notes

summary

3m 55s



What Do You Need to Understand to be in a Cybersecurity Leadership Role



This brings us to the question of what you need to understand to be in a cybersecurity leadership role, regardless of whether you are in a formal role or showing leadership as an individual.

notes

summary

4m 1s





Risk Management

Priorization based on risk

- Understand the threats
- Understand the vulnerabilities ... and how to control both!

Note that you do not need to be a technical genius to be a cybersecurity leader. The number one thing is to understand that it is all about risk management.

notes

summary

4m 13s





Risk Management

Priorization based on risk

- Understand the threats
- Understand the vulnerabilities ... and how to control both!

I say this because it's impossible to prevent every threat to your organisation. You need to be able to prioritise where you put your effort, time, and resources.

notes

summary

4m 25s



Image reference



In order of appearance

PICTURE1 : robin-worrall-FPt10LXK0cg-unsplash
PICTURE2 : Kras99from Adobe Stock
ICON1 : Created by Sharon Showalter from Noum Project
ICON2 : Created by Chalwat Kinkaew from Noum Project
ICON3 : Created by IconField from Noum Project
ICON4 : Created by Good Wife from Noum Project
PICTURE3 : Picture named Darkened air by touseef from Adobe Stock
ICON5 : Cybersecurity by Baim Icon from Noum Project
ICON6 : Cyber Threat by. Ahmad Musyaffa from Noum Project
ICON7 : Vision Problem by Nithinan Tatah from Noum Project
PICTURE4 : Tech staff monitor by Maryna from Adobe Stock

In other words, prioritise based on risk. To be able to do this, you need to understand that the threats to your organisation are. You also need to understand the vulnerabilities that your organisation has. Finally, you need to understand what you can do to control the threats and vulnerabilities. This will be the topic of the next video. See you there.

notes

summary

4m 37s

