



Course material

Course:

**Understanding the digital supply chain and its stakes for humanitarian actors**

Video:

## **7.2.2 Cyberresilience - Anatomy of an incident**

Concepts (extracted from automatically generated subtitles):

**Cybersecurity incident. Cyber incident. Incident management. Technical lead. Operational incident. Threat actors presence. Forensic evidence. Most important element. Brief time period. Recovery phase. Capability of the team. Roles. Given incident. People's well-being. Technical leads.**



[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/>

page 1/13

# LEADERSHIP IN CYBERSECURITY

## HANDLING A SECURITY CRISIS

### Anatomy of an Incident and Crisis Response

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



...

notes

summary

0m 0s



# Anatomy of an Incident and Crisis Response



A cybersecurity incident is like any other operational incident except in the need to collect and retain forensic evidence.

notes

---

---

---

---

---

---

---

---

---

---

summary

0m 4s



---

---

---

---

---



## Retention of forensic evidence

A cyber incident is a crime, and evidence might be needed to prosecute.

Data needed to ensure that the threat actors presence is eliminated in your systems.

To help understand what happened to detect and prevent incidents in the future.

Retention of forensic evidence is about three things. A cyber incident is a crime, and it requires evidence to be collected in the case that you, or the authorities want to prosecute.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

0m 13s



---

---

---

---

---

---

---

---

---

---



## Retention of forensic evidence

A cyber incident is a crime, and evidence might be needed to prosecute.

Data needed to ensure that the threat actors presence is eliminated in your systems.

To help understand what happened to detect and prevent incidents in the future.

You need the data to ensure that the recovery phase, that you have eliminated the threat actors presence in your systems, and it's important to understand what happened during the lessons learned activity to understand what happened so you can detect and prevent it in future.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

0m 26s



---

---

---

---

---



## Incident taxonomy

- **Identify**
- **Analyse**
- **Contain**
- **Diagnose**
- **Resolve**
- **Recover**
- **Close and review**

Back to incident management. As I just stated, a cyber incident is no different to any other operational incident, and the response has an identical taxonomy, which is identify, you must first determine there is a problem. Analyse, determine how big the problem is. In IT operations, we then assign a priority to the response. Contain, stop the problem getting worse. Diagnose, identify the specific problems. It is at this point that you may escalate the incident

### notes

### summary

0m 45s





## Incident taxonomy

- **Identify**
- **Analyse**
- **Contain**
- **Diagnose**
- **Resolve**
- **Recover**
- **Close and review**

to the crisis response while continuing to work on the incident. Resolve the problem. Recover your data and services. Finally, close and review. This is the lessons learned activity, so you can improve from a failure. In this case, a cyberattack.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

1m 25s



---

---

---

---

---



## Roles in a crisis

If at any point it gets beyond the capability of the team to manage the incident or its impact to operations is significant escalated to your crisis team. To successfully manage an incident, perhaps the most important element is to define roles. Obviously, for a given incident, who's filling those roles? This way, you can have clear leadership and direction. The roles in a crisis are as a minimum. Incident controller.

notes

## summary

1m 45s







## Roles in a crisis

- **Incident controller** – Leader of the incident response, exercise command and control to ensure that the response is efficient.
- **Technical lead** – Multiple roles depending on the event (technical cyber lead, network lead and applications lead).
- **Communications** – Responsible for communications with internal and external stakeholders.
- **Health and wellbeing** – Ensure people wellbeing is maintained.

This is the leader of the incident response. In reality, this role does not need to be deeply technical,

notes

summary

2m 18s





## Roles in a crisis

- **Incident controller** – Leader of the incident response, exercise command and control to ensure that the response is efficient.
- **Technical lead** – Multiple roles depending on the event (technical cyber lead, network lead and applications lead).
- **Communications** – Responsible for communications with internal and external stakeholders.
- **Health and wellbeing** – Ensure people wellbeing is maintained.

but it must have a sufficient manner or presence and the ability to exercise command and control to ensure that the response is efficient. Technical lead. You will have multiple technical leads depending on the event. As an example, you should have a technical cyber lead as the incident controller should not be the one fulfilling this role

### notes

---

---

---

---

---

---

---

---

---

---

### summary

2m 25s



---

---

---

---

---

---

---

---

---

---



## Roles in a crisis

- **Incident controller** – Leader of the incident response, exercise command and control to ensure that the response is efficient.
- **Technical lead** – Multiple roles depending on the event (technical cyber lead, network lead and applications lead).
- **Communications** – Responsible for communications with internal and external stakeholders.
- **Health and wellbeing** – Ensure people wellbeing is maintained.

a network lead, and an applications lead. Communications. You must also appoint someone who is responsible for communications to deal with the internal and external communications and as the interface with other teams if it becomes a crisis.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

2m 49s



---

---

---

---

---



## Roles in a crisis

- **Incident controller** – Leader of the incident response, exercise command and control to ensure that the response is efficient.
- **Technical lead** – Multiple roles depending on the event (technical cyber lead, network lead and applications lead).
- **Communications** – Responsible for communications with internal and external stakeholders.
- **Health and wellbeing** – Ensure people wellbeing is maintained.

Health and well-being. Many incidents are not resolved in a brief time period, so you may well need to work in shifts. This role exists and is often combined with another one, but is there to ensure that your people's well-being is met maintained, and more importantly, to ensure that you don't have heroes. These are people who want to work around the clock to solve the problem. After a long shift, this starts to negatively impact the individual and the incident response as a whole.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

3m 5s



---

---

---

---

---

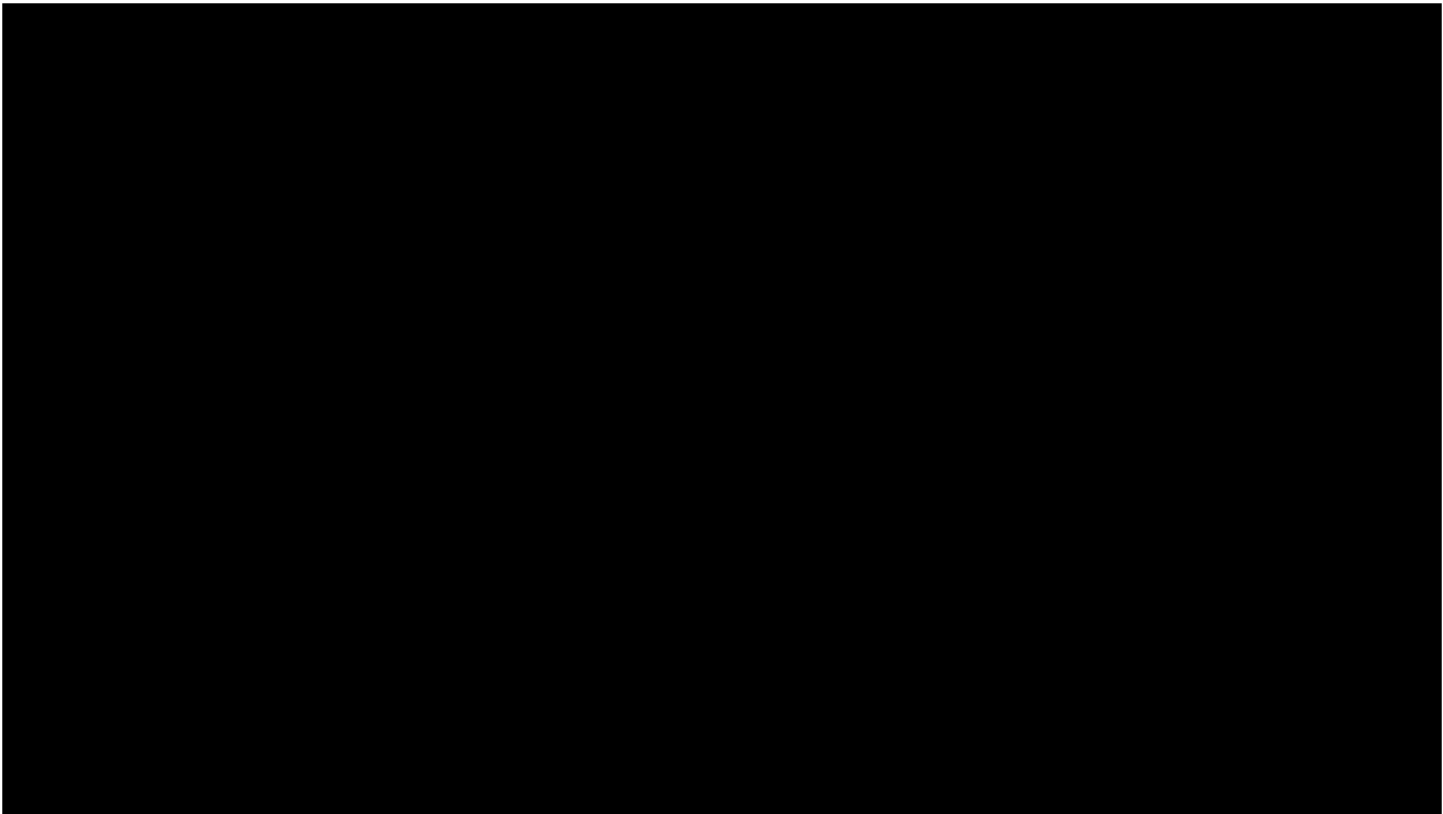
---

---

---

---

---



Now that we went through the anatomy for an incident and how to answer it, we will now go through what can be done beforehand to help manage the situation when it happens. This is the topic of our next video

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

3m 39s



.....

.....

.....

.....

.....