



Course material

Course:

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

Video:

### 7.1.3 Cyberresilience

Concepts (extracted from automatically generated subtitles):

**Mitre att&ck; framework. Useful way. Legitimate user. Cybersecurity professional. Known vulnerability. Zero-day. Organisation harm. Complex view. Primary takeaway. Comprehensive list of cybersecurity controls. Thriving business. Primary threat. Cybersecurity defenses. Participants of this course. Particularly useful way.**



[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 1/18

A hand holding a small, light-colored wooden circle with the word "OOPS!" printed on it. The background is a solid, bright yellow. The hand is positioned at the bottom left, with the thumb and index finger gripping the edge of the circle. The circle is slightly tilted, and the text "OOPS!" is centered on its face. The lighting is even, and the overall composition is simple and direct.


**Most attacks occur  
through human failure:**

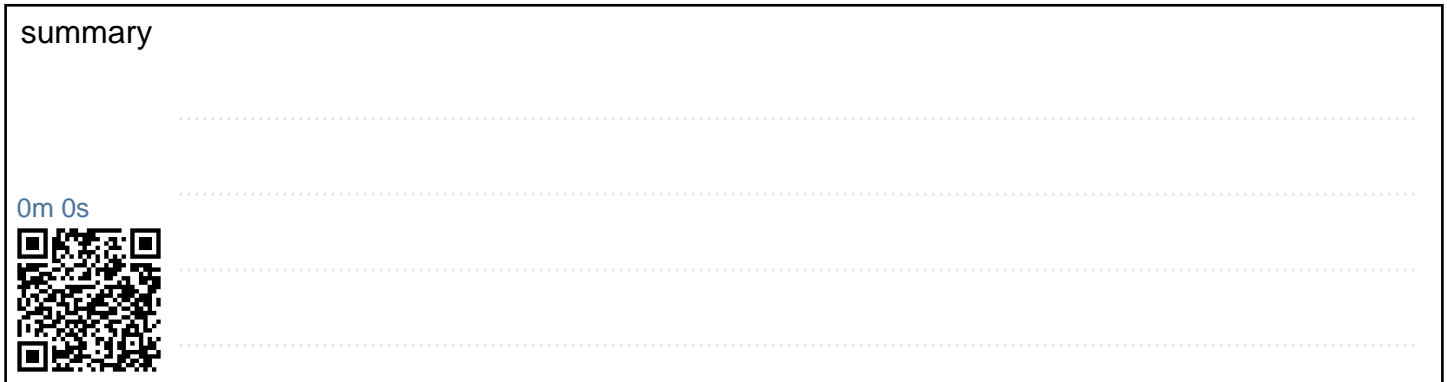
Now that you understand the who and why someone may wish your organisation harm, it's time to think about how each of them could attack you. Similarly to where we started this module, it can be both simple and complex. The complex view is represented by the MITRE ATT&CK framework, which describes the technical paths that an attacker can take when attacking an organisation. For a cybersecurity professional, this is extremely useful for informing you how to structure your cybersecurity defenses, what we call controls, and conducting forensics after the event. The term forensics here is the activity of examining all the evidence of how an attack has occurred. A simpler, more useful way to think of this for the participants of this course, is to understand it like this.

[illegible]

summary

0m 0s







## Most attacks occur through human failure:


- Sharing credentials through phishing email or fake websites.
- Installing malware on computer.

Most attacks occur through human failure. This typically occurs in two ways. A person gives up their credentials, meaning their account and password, through a phishing email, or signing up to a website using their work credentials because many people reuse their passwords. This allows the attacker to become a legitimate user in your network,

notes

summary

1m 1s





## Most attacks occur through human failure:

- Sharing credentials through phishing email or fake websites.
- Installing malware on computer.

or a person installs malware on the computer as a result of being phished, or it is embedded in what appears to be a legitimate programme,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....


.....

.....

.....

.....

1m 24s





# The attack is technical in nature and exploits:

- An unknown weakness (zero-day) in your systems.
- A known vulnerability (security weakness) in your systems that has not been patched.

or the attack is technical in nature,

notes

summary

1m 34s





# The attack is technical in nature and exploits:

- An unknown weakness (zero-day) in your systems.
- A known vulnerability (security weakness) in your systems that has not been patched.

and exploits an unknown weakness in your system, a zero-day, meaning that it has not been seen before, or more likely, a known vulnerability,

## notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

## summary

1m 37s





# The attack is technical in nature and exploits:

- An unknown weakness (zero-day) in your systems.
- A known vulnerability (security weakness) in your systems that has not been patched.

or a security weakness in your system that has not been patched.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....


.....

summary


.....

.....

1m 49s







# Zero-Day

**What is a "zero-day" vulnerability?**

**A vulnerability in software or hardware typically unknown to the vendor and for which no patch or other fix is available.**

You have probably heard of the term zero-day. More specifically, it is a vulnerability in software or hardware that is typically unknown to the vendor, and for which no patch or fix is available. The vendor has zero days to prepare a patch. As the vulnerability has been described and/or exploited. The identification and sale of zero-days is a thriving business, with accessible websites such as Zerodium,

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....


.....

.....

.....

.....

1m 52s







## Controls need to be put in place to:

- Prevent or limit the risk of your users making poor decisions.
- Reduce vulnerabilities of the systems that you use.

or the Deep and Dark Web providing a platform for their sale. There are, of course, many rumours of Nation-State actors also purchasing these vulnerabilities for their exclusive use. From this, you can immediately tell that the things that you need to ensure are in place are the controls. That one, prevent or at least limit the risk of your users making poor decisions, and two, that minimise the vulnerabilities of the systems that you use.

### notes

---

---

---

---

---

---

---

---

---

---

### summary

2m 25s



---

---

---

---

---

---

---

---

---

---



# Expert Frameworks for Security Controls

International Standards  
Organization - (ISO) 27001:2022

Center for Internet Security  
(CIS) - Critical Security  
Controls 8.0

National Institute of Standards  
and Technology (NIST) –  
Cybersecurity Framework  
(CSF) 2.0

Luckily, for you, there are frameworks that have been created by experts for you to use.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

2m 54s





## Expert Frameworks for Security Controls

**International Standards  
Organization - (ISO) 27001:2022**

**Center for Internet Security  
(CIS) - Critical Security  
Controls 8.0**

**National Institute of Standards  
and Technology (NIST) –  
Cybersecurity Framework  
(CSF) 2.0**

These frameworks all describe similar security controls, but present them in different ways. The best-known ones are ISO 27001,

notes

summary

3m 1s





# Expert Frameworks for Security Controls

**International Standards  
Organization - (ISO) 27001:2022**

**Center for Internet Security  
(CIS) - Critical Security  
Controls 8.0**

**National Institute of Standards  
and Technology (NIST) –  
Cybersecurity Framework  
(CSF) 2.0**

CIS Security Controls 8.0, and the NIST Cybersecurity Framework, which is now up to 2.0. There are others, of course, but these are the three most popular. These frameworks provide a comprehensive list

notes

summary

3m 14s





# Expert Frameworks for Security Controls

**International Standards  
Organization - (ISO) 27001:2022**

**Center for Internet Security  
(CIS) - Critical Security  
Controls 8.0**

**National Institute of Standards  
and Technology (NIST) –  
Cybersecurity Framework  
(CSF) 2.0**

of cybersecurity controls for you to use. When I say comprehensive, I mean there are a lot of controls

notes

summary

3m 30s



# Understanding the Vulnerabilities



that should be in place to effectively manage the cyber risk to the organisation. This step at the highest level is surprisingly easy. If you think about your assets being surrounded by defenses, what we call defense-in-depth. I have found a particularly useful way of understanding this is to use a modified risk bow tie.

## notes

---

---

---

---

---

---

---

---

---

---

## summary

3m 37s



---

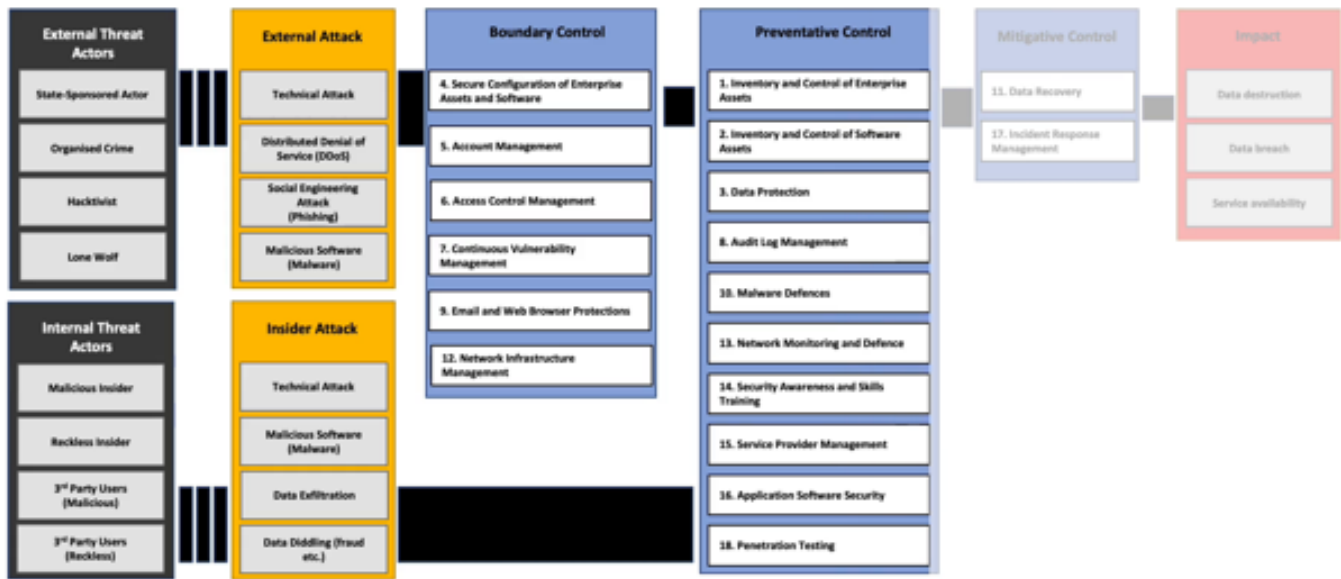
---

---

---

---

# Control Model (CIS 8.0)



You start from the left-hand side of the bow tie, where your attack is located,

notes

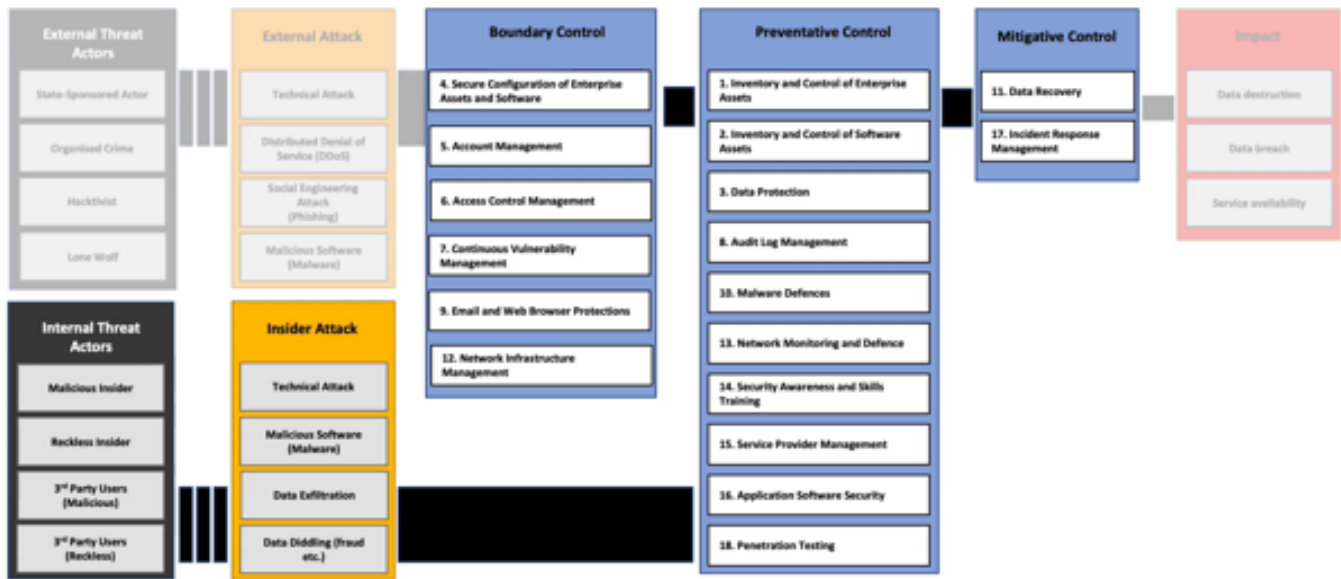
summary

4m 2s





# Control Model (CIS 8.0)



and move through the attacks to the controls that are shown here in blue, to the impacts in red. This is particularly useful when you divide your controls up into boundary, preventative, and mitigative controls. Your primary takeaway from this slide is that people inside your organisation bypass some of the more well-known controls, such as firewalls, and system vulnerability management. In other words, patching.

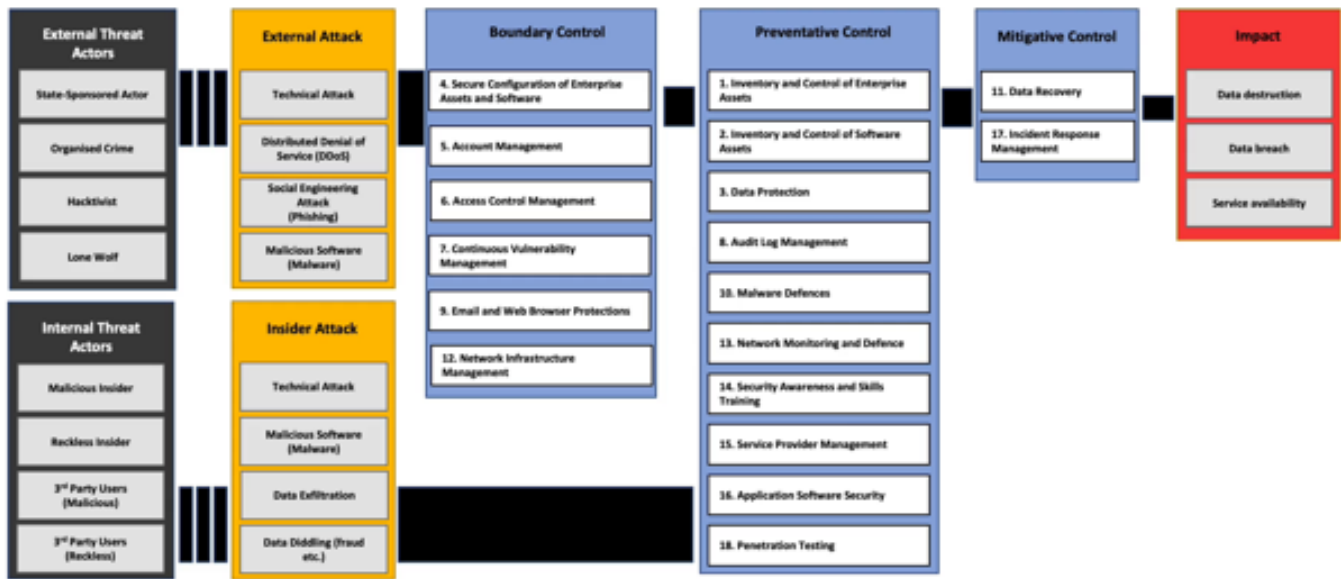
notes

summary

4m 13s



# Control Model (CIS 8.0)



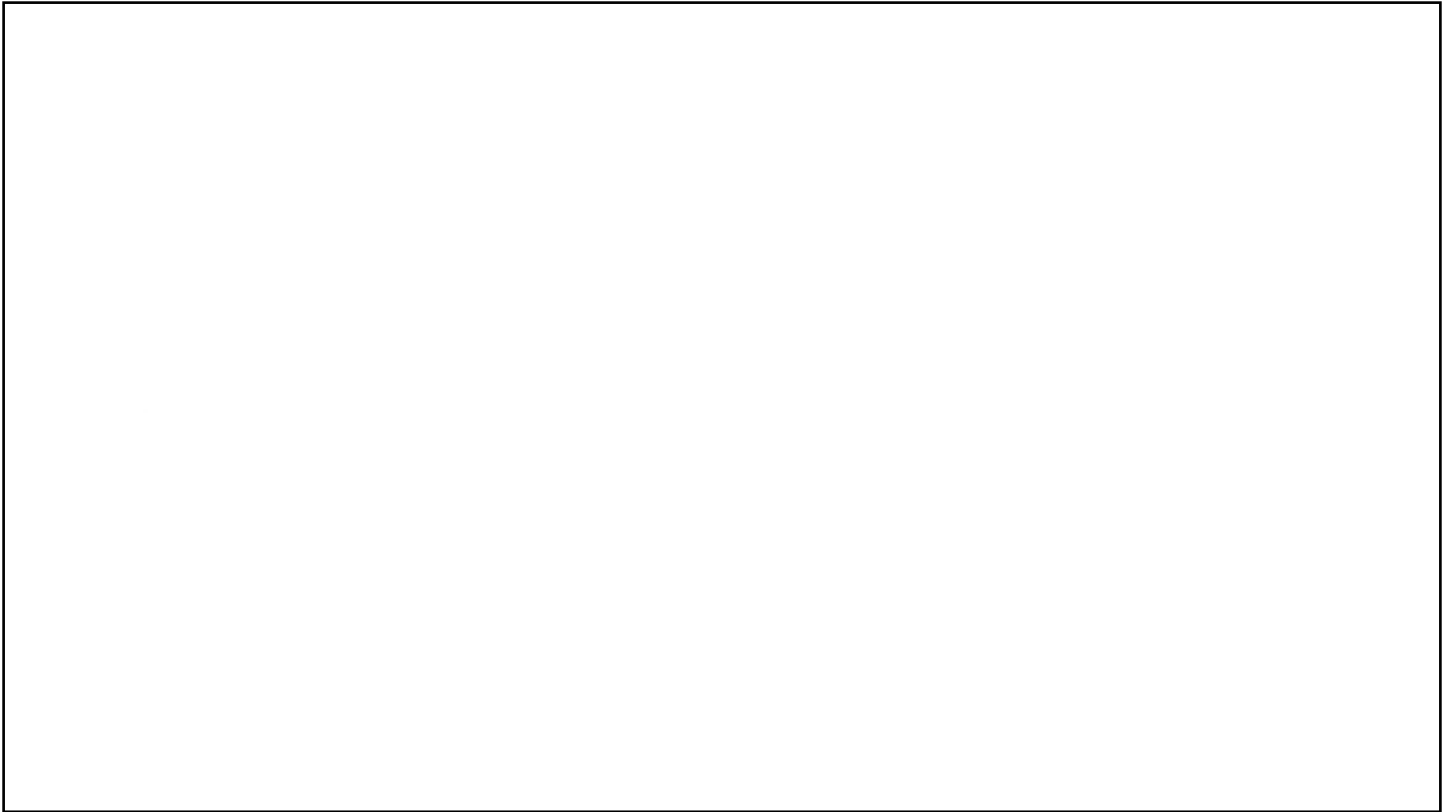
As they have legitimate access to your systems and information, this does not necessarily mean that your primary threat is internal, but you are most vulnerable to the internal threat.

notes

summary

4m 37s





How we prioritise our controls in organisations that do not have the resources or maturity to have comprehensive protection is the subject of the next video.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

4m 50s

