



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

7.1.4 Cyberresilience

Concepts (extracted from automatically generated subtitles):

Microsoft office macros. Good example. Components of the controls. Best results. Team game. More useful frameworks. Multi-factor authentication. Cis critical controls framework. Organisational structures. Good luck. Reference frameworks. Ability of microsoft documents. Control access. Following controls. Patch applications.



[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/>

LEADERSHIP IN CYBERSECURITY

LEADERSHIP, BEST PRACTICES AND CYBER HYGIENE

Cyber Hygiene

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



...

notes

summary

0m 0s



Cyber Hygiene (CIS 8.0)



As we all know, working in the humanitarian field means that we do not have infinite resources and funding to apply in any context, let alone in cybersecurity. Of course, if you don't work in the humanitarian context, you also have constraints, but they are typically less severe. We at last come to the question of how to prioritise your resources and finances. Luckily, there are some reference frameworks that can be used.

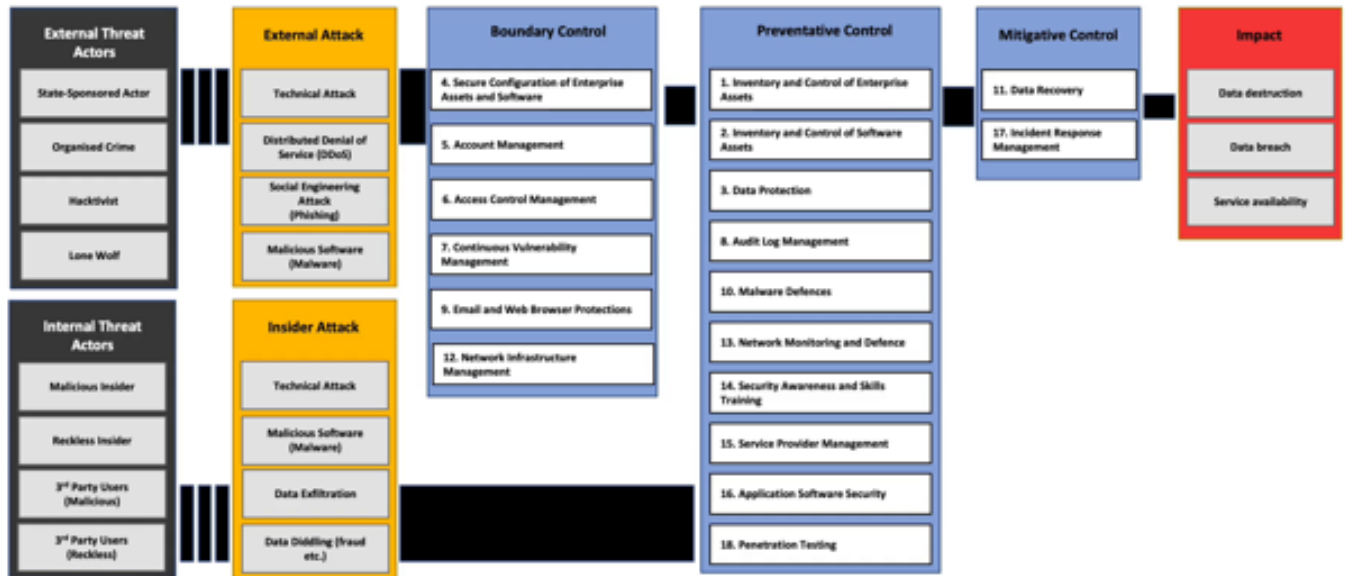
notes

summary

0m 4s



Control Model (CIS 8.0)



One of the more useful frameworks is the CIS Critical Controls Framework that we discussed in the last section, which divides up the components of the controls, which are called safeguards, and can be thought of as specific processes, into three implementation groups. This is an approach that allows an organisation to get progressively better as they mature. I recommend that you have a look at it when you get a chance.

notes

summary

0m 38s



The Essential Eight

by the Australian Cyber Security Centre



1. **Patch applications** - apply the fixes that application vendors provide
2. **Patch operating systems** - apply the fixes that OS vendors provide
3. **Multi-factor authentication** - ensure that access requires more than an identity and password
4. **Restrict administrative privileges** - limit by default the number of people and systems with admin rights
5. **Application control** - only allowing authorized applications to operate
6. **Restrict Microsoft Office macros** - restrict the ability of MS documents to automatically execute code
7. **User application hardening** - controlling the configuration of web and common productivity platforms
8. **Regular backups**

But which of these provides the most value? Or in other words, which are the ones you absolutely have to have in place? Once again, guidance exists through many national cyber security centres. A good example of which is the Essential Eight,

notes

summary

1m 7s



The Essential Eight

by the Australian Cyber Security Centre



1. **Patch applications** - apply the fixes that application vendors provide
2. **Patch operating systems** - apply the fixes that OS vendors provide
3. **Multi-factor authentication** - ensure that access requires more than an identity and password
4. **Restrict administrative privileges** - limit by default the number of people and systems with admin rights
5. **Application control** - only allowing authorized applications to operate
6. **Restrict Microsoft Office macros** - restrict the ability of MS documents to automatically execute code
7. **User application hardening** - controlling the configuration of web and common productivity platforms
8. **Regular backups**

which is published by the Australian Cyber Security Centre, and it lists the following controls: patch applications, i.e., apply the fixes that the application vendor provides.

notes

summary

1m 25s



The Essential Eight

by the Australian Cyber Security Centre



- 1. Patch applications** - apply the fixes that application vendors provide
- 2. Patch operating systems** - apply the fixes that OS vendors provide
- 3. Multi-factor authentication** - ensure that access requires more than an identity and password
4. Restrict administrative privileges - limit by default the number of people and systems with admin rights
5. Application control - only allowing authorized applications to operate
6. Restrict Microsoft Office macros - restrict the ability of MS documents to automatically execute code
7. User application hardening - controlling the configuration of web and common productivity platforms
8. Regular backups

Patch operating systems: apply the fixes that operating system vendors provide, think Windows and Linux. Multi-factor authentication: ensure that access to your systems and information requires more than an identity and password,

notes

summary

1m 39s



The Essential Eight

by the Australian Cyber Security Centre



1. **Patch applications** - apply the fixes that application vendors provide
2. **Patch operating systems** - apply the fixes that OS vendors provide
3. **Multi-factor authentication** - ensure that access requires more than an identity and password
4. **Restrict administrative privileges** - limit by default the number of people and systems with admin rights
5. **Application control** - only allowing authorized applications to operate
6. **Restrict Microsoft Office macros** - restrict the ability of MS documents to automatically execute code
7. **User application hardening** - controlling the configuration of web and common productivity platforms
8. **Regular backups**

think biometrics or challenge and response systems. Restrict administrative privileges: limit by default the number of people and systems that have administrative privileges in your systems. Application control: this used to be called whitelisting.

notes

summary

1m 55s



The Essential Eight

by the Australian Cyber Security Centre



1. **Patch applications** - apply the fixes that application vendors provide
2. **Patch operating systems** - apply the fixes that OS vendors provide
3. **Multi-factor authentication** - ensure that access requires more than an identity and password
4. **Restrict administrative privileges** - limit by default the number of people and systems with admin rights
5. **Application control** - only allowing authorized applications to operate
6. **Restrict Microsoft Office macros** - restrict the ability of MS documents to automatically execute code
7. **User application hardening** - controlling the configuration of web and common productivity platforms
8. **Regular backups**

It means only allowing authorised applications to operate. Restrict Microsoft Office macros: this restricts the ability of Microsoft documents to automatically execute code. User application hardening: this is controlling the configuration of web browsers and common productivity platforms. Regular backups: make sure you can recover from a security breach by backing up your information.

notes

summary

2m 13s





Don't forget the absolute basics:

- Control access to the network (firewall).
- Install anti-virus (AV) software.
- Control physical access to IT resources (physical security).

This describes the most useful hygiene measures, but it assumes a certain level of capability for an organisation. It's missing the absolute basics like control access to the network (a firewall),

notes

summary

2m 43s





Don't forget the absolute basics:

- Control access to the network (firewall).
- Install anti-virus (AV) software.
- Control physical access to IT resources (physical security).

install anti-virus software

notes

summary

3m 0s





Don't forget the absolute basics:

- Control access to the network (firewall).
- Install anti-virus (AV) software.
- Control physical access to IT resources (physical security).

and control physical access to IT resources (physical security). Between us, let's call that the Essential 11. If you at least start with this list and then adopt a control framework to build out your cybersecurity controls over time, then you'll be heading in the right direction.

notes

summary

3m 1s





In order of appearance

PICTURE1 : Picture named Darkened air by touseef from Adobe Stock
PICTURE 5 : diagram provided by Paul Hume

That brings us to the end of the chapter. In conclusion, you should remember that cybersecurity is a team game that gets the best results from organisational structures and individual accountability working hand in hand, and you should take a structured approach to understand that the threat, vulnerabilities, and solutions that you put in place. Good luck on your cybersecurity journey. In the next chapter, we will dig into what to do when all the controls you have put in place did not work, and that you have to deal with a security incident.

notes

summary

3m 24s