

Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

3.2.3 Possible risk response strategies - Oceane

Concepts (extracted from automatically generated subtitles):

Main risk. Effective mitigation measures. Data of people. Various digital risks. Risk response plans. Technological advancement. Unethical use of technology. Data centre fails. Humanitarian operation's specific needs. Humanitarian organisations. Data leakage detection tools. Good practices. Sensitive data. Implementation of the thorough screening of employees. Such ethical dilemmas.



[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 1/19

STAKES FOR HUMANITARIANS ORGANIZATIONS

Potential Risk Response Strategies and Plans

Océane Martinoty

Risk and Assurance Manager

International Committee of the Red Cross (ICRC)



...

notes

summary

0m 0s



Potential Risk Responses



Welcome back. I'm Océane Martinoty, and I coordinate the practise aiming at managing the main risk for International Committee of the Red Cross. In our previous video, we heard from Benjamin Durieux, the CIO of the International Committee of the Red Cross, about the various digital risks that humanitarian organisations face. We will now discuss how we can effectively respond to these risks, considering humanitarian operation's specific needs.

notes

summary

0m 4s



Developing Effective Risk Mitigation Measures



Organization-wide effort : Risk mitigation requires wide cooperation, not just IT involvement.

Priorization : Focus on protecting information and systems critical to the organization's mandate and mission.

Balanced : Align on acceptable risk levels to tailor responses and maintain operational agility.

Agile : Regularly adjust strategies to evolving internal and external environments.

Developing effective mitigation measures for digital risks require collaboration across the entire organisation. It is not just for the IT department to deal with these risks and to develop risk response plans.

notes

summary

0m 31s



Developing Effective Risk Mitigation Measures



Organization-wide effort : Risk mitigation requires wide cooperation, not just IT involvement.

Priorization : Focus on protecting information and systems critical to the organization's mandate and mission.

Balanced : Align on acceptable risk levels to tailor responses and maintain operational agility.

Agile : Regularly adjust strategies to evolving internal and external environments.

As resources are limited, there is a need to prioritise measures that will reduce risks that could endanger an organisation's ability to deliver on what is at the heart of its DNA admission. This involves identifying which information and systems are directly related to an organisation's mandate and mission, and to protect them in priority. The International Committee of the Red Cross may, for example, prioritise the protection of its confidential dialogue with parties to a conflict, or the data of people affected by armed conflict, while other organisations may decide to prioritise, for example, the protection of patient's information.

notes

summary

0m 49s



Developing Effective Risk Mitigation Measures



Organization-wide effort : Risk mitigation requires wide cooperation, not just IT involvement.

Priorization : Focus on protecting information and systems critical to the organization's mandate and mission.

Balanced : Align on acceptable risk levels to tailor responses and maintain operational agility.

Agile : Regularly adjust strategies to evolving internal and external environments.

In the same vein, it is important to align on the level of risks that an organisation is willing to accept while pursuing its mission. This will contribute to tailoring risk responses and avoiding adding unnecessary layers of control that will most certainly increase costs and reduce operational agility. There is also a need to consider both internal and external environments in a very agile manner. Externally, factors such as: technological advancement, geopolitical dynamics, donor relationships, and [inaudible 00:02:03] are constantly evolving. It requires to regularly adapt risk responses to these changes to maintain and remain effective while adjusting internally associated ways of working, resources, and capabilities.

notes

summary

1m 31s





Operational Discontinuity

Measures

- Business continuity and disaster recovery plans.
- Redundancy.

Let's look at some specific examples of risks and possible mitigation strategies and plans. Possible mitigation measures, that I will present in a minute, are good practises, but are not the only set of measures that can be implemented. It is important to keep in mind that they need to be contextualised to the specific needs of your organisation. If we look at how to address risks of disruption of our operations, good practices notably involve developing business continuity and disaster recovery plans for our critical applications. If a critical system like logistics system fails, there should be a clear plan to restore it quickly. This is what is called a disaster recovery plan. As it may take some time, it can be relevant to also develop a business continuity plan so that you are prepared to manage tasks outside of the system that is down and in the meantime. Additionally, having redundant communication channels would ensure that you can maintain communication even during internet outages. Implementing redundant server support means that if one data centre fails, critical operations can continue.

notes

summary

2m 21s





Security of Information

People Centric

- Cybersecurity trainings
- Information handling trainings
- Screening of staff and consultants

Organizational

- Identity and access management
- Vulnerability management
- Third-party management

Technological

- Regular updates of antivirus
- Firewall

Physical

- Securing Access

Looking at how to secure the information and its confidentiality, there are multiple measures that contribute to it, and that should be implemented in parallel.

notes

summary

3m 39s





Security of Information

People Centric

- Cybersecurity trainings
- Information handling trainings
- Screening of staff and consultants

Organizational

- Identity and access management
- Vulnerability management
- Third-party management

Technological

- Regular updates of antivirus
- Firewall

Physical

- Securing Access

First, there are people-centric measures that notably include regular cybersecurity awareness training for all staff, as well as training on how to handle and classify information. These measures are essential to secure both the information and the systems that contain it. Another people-centric measures could be the implementation of the thorough screening of employees having extended access to information and systems, as well as screening of consultant and staff from third-party partners.

notes

summary

3m 49s





Security of Information

People Centric

- Cybersecurity trainings
- Information handling trainings
- Screening of staff and consultants

Organizational

- Identity and access management
- Vulnerability management
- Third-party management

Technological

- Regular updates of antivirus
- Firewall

Physical

- Securing Access

There are also organisational measures which could include, among others: strong policies and procedures for identity and access management, vulnerability management, and third-party risk management. Technological measures such as regularly updated antivirus software, firewalls, and data leakage detection tools are also an essential part for strengthening an organisation's cybersecurity posture. It is important not to forget key physical measures such as: securing access to critical infrastructure like server rooms to prevent an authorised entry and safeguard sensitive data.

notes

summary

4m 22s





Impartiality and Neutrality

Measures

- Tailored technological choices.
- Thorough due-diligence.
- Third-party risk management.
- Including relevant contract clauses with vendors.

Looking at how to manage the risk of being perceived as partial or one-sided, there is no easy answer. Reason why it's important to make tailored technological choices and to accept that any technological strategy will need to regularly evolve.

notes

summary

5m 1s





Impartiality and Neutrality

Measures

- Tailored technological choices.
- Thorough due-diligence.
- Third-party risk management.
- Including relevant contract clauses with vendors.

For non-sensitive tasks, using off-the-the-shelf solution from well-known tech players might be fine.

notes

summary

5m 17s





Impartiality and Neutrality

Measures

- Tailored technological choices.
- Thorough due-diligence.
- Third-party risk management.
- Including relevant contract clauses with vendors.

But for sensitive data, you may consider alternatives like open-source technologies. Conducting thorough due diligence before selecting a technology solution also contribute to ensuring that they align with your organisation's principle and are perceived as neutral.

notes

summary

5m 28s





Impartiality and Neutrality

Measures

- Tailored technological choices.
- Thorough due-diligence.
- Third-party risk management.
- Including relevant contract clauses with vendors.

Unfortunately, doing due diligence when selecting vendors is not enough, as there can be shift in vendor profile and strategy. Establishing a third-party risk management programme

notes

summary

5m 43s





Impartiality and Neutrality

Measures

- Tailored technological choices.
- Thorough due-diligence.
- Third-party risk management.
- Including relevant contract clauses with vendors.

allows for ongoing monitoring of vendors. In addition, including relevant contractual clauses in agreements, set clear terms for managing changes in vendor relationships, including conditions for exiting agreements.

notes

summary

5m 57s



Handling of personal data

Measures

- Data policies (including purpose and retention).
- Data protection by design.
- Regular assessment.



To avoid inadequate handling of personal data, it is important to define clear data policies that set specific purposes for data collection and establish a data retention policy. Additionally, you can also establish a process that will ensure that any new technology embeds data protection measures by design. You can also regularly assess the tools being used for data collection and processing to verify that they comply with applicable data protection and ethical standards.

notes

summary

6m 12s





Ethical use of technology and information

Measures

- Overarching ethical framework.
- Regular training and awareness programs.
- Platforms to discuss and align on dilemmas.

Similarly, to avoid the unethical use of technology and information, there are multiple prevention measures which include notably the definition of an overarching ethical framework, regular training and awareness programmes to help staff grasp the ethical considerations related to information and technology use. As there is no easy answer, it is also important to maintain

notes

summary

6m 46s



Misinformation and disinformation

Measures

- Internal and external stakeholders' awareness campaigns.
- Detection capability.
- Proactive communication.




a platform where such ethical dilemmas can be discussed internally and resolved. Finally, to deal with the increasing risks of misinformation and disinformation, your organisation may conduct regular campaigns to raise awareness of stakeholders and discourage attacks against humanitarian organisations. Building detection capabilities within your communication teams may also enable you to monitor and respond effectively to misinformation and disinformation. Using proactive communication strategies can also contribute to share accurate information and counter negative narratives.

notes

summary

7m 13s





As a conclusion, there is no one-size-fits-all type of response to these very complex risks, but there are good practices that we can all consider, learn from, and adapt to our specific strategic and operational needs. By implementing these measures, humanitarian organisations can protect their operations, maintain trust, and continue delivering their missions effectively.

notes

summary

7m 51s

