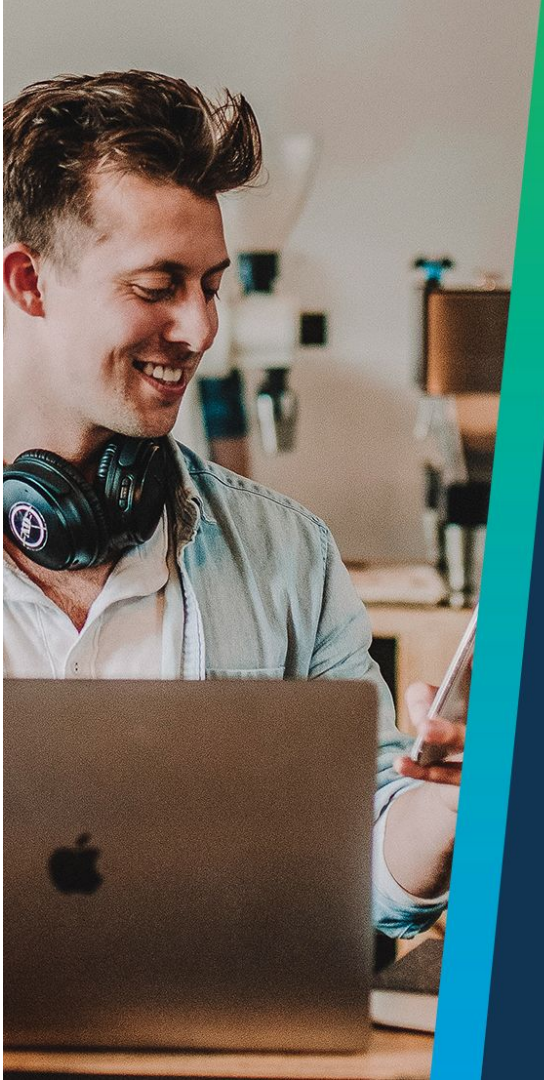


Cyber Security Bootcamp

Hyperiondev

Cyber Crimes, Governance and Incident Responses

Lecture - Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly.
- No question is daft or silly - ask them!
- There are Q/A sessions at the end of the session, should you wish to ask any follow-up questions.
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: http://hyperiondev.com/safeguardreporting

Objectives

1. Define Cybersecurity and its four main categories.
2. Explore different types of attacks .
3. Understand the role of governance and risk management in relation to security

Poll

What is Cybersecurity?

- Measures to ensure the confidentiality, integrity, and availability of information.
- Protection of digital systems and data from unauthorized access or attacks.
- Strategies to defend against hacking, malware, and cyber threats.
- Safeguarding personal and financial information online.

Poll

What does C.I.A stand for?

- Central Intelligence Agency
- Confidentiality, Integrity, Availability
- Customer Intelligence Analysis
- Certified Internal Auditor

Cybersecurity & Attacks

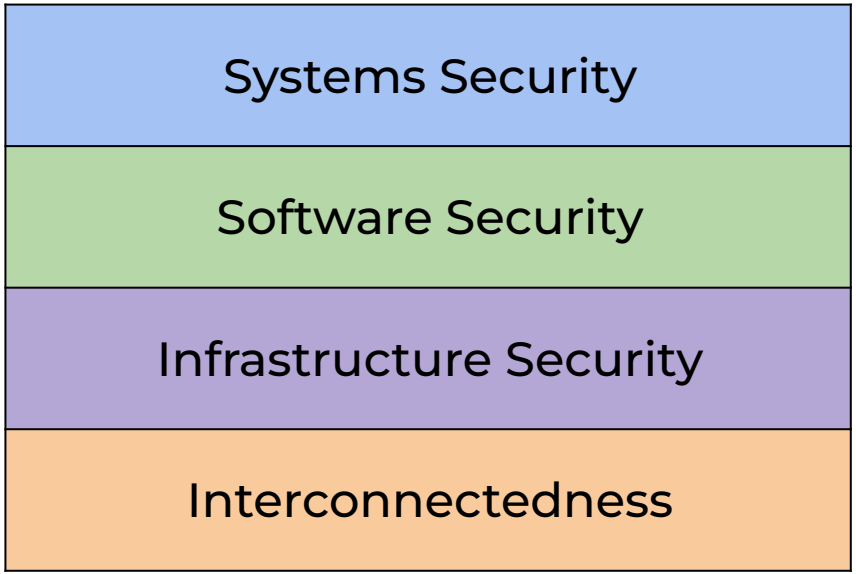
Cyber Security

Cybersecurity is the practice of protecting systems, networks, and data from digital **attacks**, **theft**, or **damage**.

In a world increasingly reliant on digital systems, cybersecurity is crucial for protecting personal data, corporate secrets, and national security.

Cybercrime has a significant economic cost, with global damages estimated at over $600 billion annually.

Categories of CyberSec



Understanding the CIA Triad

STATIONX

CIA

Confidentiality

Ensuring that sensitive information is accessible only to those authorized to view it. Techniques include encryption, access controls, and data masking.

Integrity

Maintaining the accuracy and trustworthiness of data. This involves protecting data from unauthorized alterations and ensuring that data is reliable.

Availability

Ensuring that systems and data are accessible to authorized users when needed. This includes maintaining hardware, upgrading software, and backing up data to prevent loss during incidents.

CIA

The CIA Triad		
What Is the CIA?		
Confidentiality	**Integrity**	**Availability**
The information is safe from accidental or intentional disclosure.	The information is safe from accidental or intentional modification or alteration.	The information is available to authorized users when needed.
Example		
I send you a message, and no one else knows what that message is.	I send you a message, and you receive exactly what I sent you (without any modification)	I send you a message, and you are able to receive it.
What's The Purpose of the CIA?		
Data is not disclosed	Data is not tampered	Data is available
How Can You Achieve the CIA?		
e.g., Encryption	e.g., Hashing, Digital signatures	e.g., Backups, redundant systems
Opposite of CIA		
Disclosure	Alteration	Destruction

Types of Attacks

Email Spam & Phishing

Unsolicited emails that often contain malicious links or attachments designed to trick the recipient into providing personal information. **Examples:** Fake emails claiming to be from a bank asking for login details.

Financial Malware

Purpose: Designed to steal financial data, such as credit card information or bank account credentials.

Examples: Trojans that log keystrokes or redirect users to fake banking sites.

Click Fraud & Cryptocurrency Mining

Click Fraud: Fraudulent clicks on online ads to generate revenue.

Cryptocurrency Mining: Using compromised computers to mine cryptocurrency, often without the user's knowledge.

Compliance & Risk Management

Compliance

- Compliance frameworks set mandatory standards for protecting data and reducing risks.
- Common frameworks:
  - NIST: Enhances collaboration to manage cybersecurity threats.
  - GDPR: Protects EU citizens' data rights.
  - IoTSF: Focuses on IoT security across industries.
- Compliance ensures adherence to legal and regulatory standards, protecting against significant legal and financial consequences.

Compliance Frameworks

Ensuring that organizational activities are operated in accordance with the laws and regulations impacting those systems.

- ISO 27001/27002
- NIST Cybersecurity Framework
- PCI DSS
- HIPAA
- GDPR

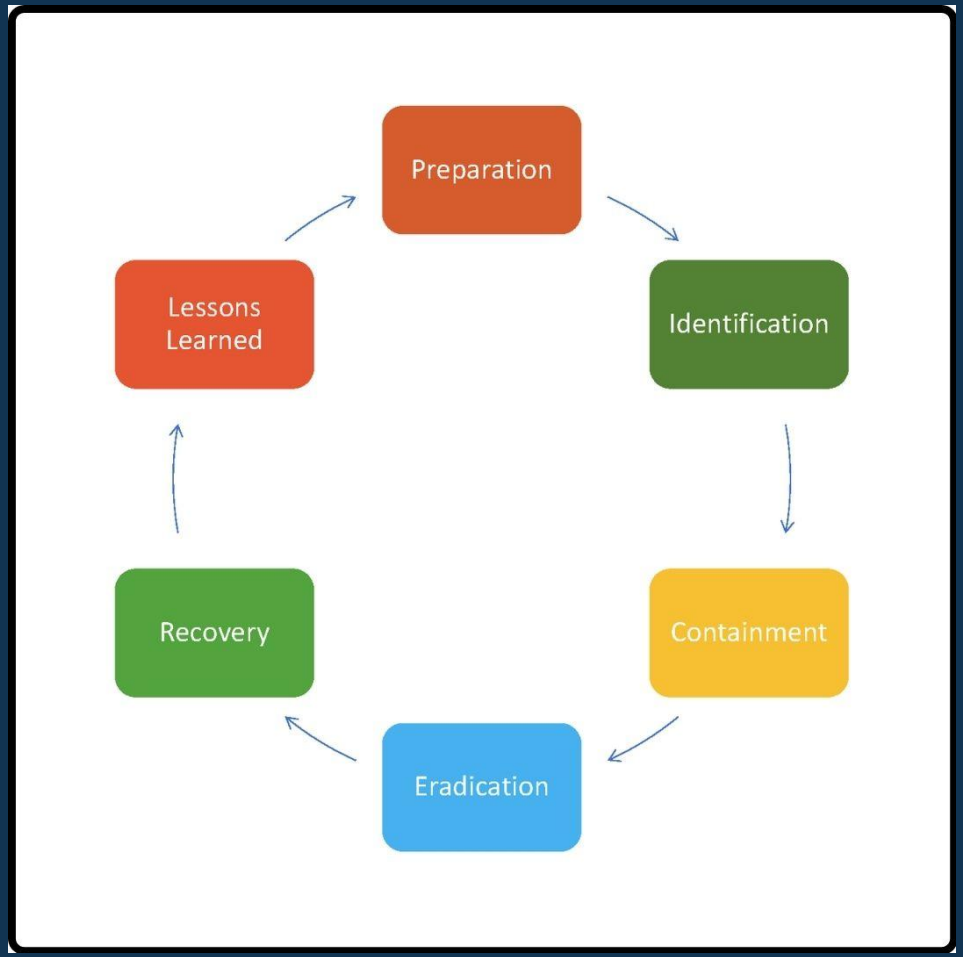
Governance

- Cybersecurity governance provides a strategic framework for enforcing security, assessing risks, and assigning responsibilities.
- Principles-based governance allows companies to adapt standards like ISO to their specific needs.
- Benefits include efficient incident response, rapid risk identification, and fostering a security-aware culture.

7 Steps

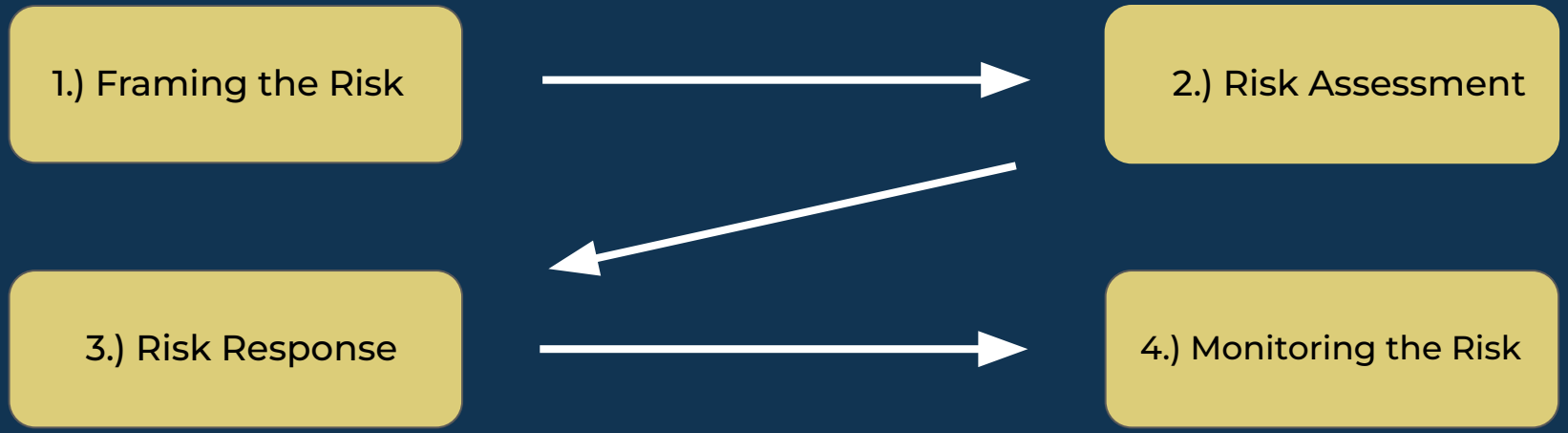

7 Steps to Build a Cybersecurity Governance Program
1
Establish a Clear Governance Structure
2
Conduct a Comprehensive Risk Assessment
3
Develop and Implement Policies
4
Implement Security Controls
5
Prioritize Employee Training and Awareness
6
Develop and Test Incident Response Plans
7
Implement Continuous Monitoring and Improvement
SC

Incident Response



Risk Management

The formal process of continuously identifying and evaluating risk in an effort to reduce the impact of threats and vulnerabilities is known as risk management. You cannot completely eliminate risk, but you can set acceptable levels by comparing the impact of a threat with the expense of putting controls in place to lessen it. Never let the price of a control exceed the worth of the asset it is intended to safeguard.



Risk Management Process

Risk Management Process

1. Determine the risks' rising threats. Processes, products, attacks, potential service failure or interruption, negative perception of an organization's reputation, potential legal liability, or loss of intellectual property are all examples of threats.

2. Find out how serious of a threat each one is. For instance, some threats might have the power to paralyze an entire organization, whereas others might only cause minor annoyances. Risk can be ranked according to its potential financial impact (quantitative analysis) or scaled operational impact (qualitative analysis).

3. Create a plan of action to lessen the overall risk exposure of the organization, outlining the areas where risk can be eliminated, mitigated, transferred, or accepted.

4. Continuously review any risk reduced through elimination, mitigation or transfer actions. Remember, not all risks can be eliminated, so you will need to closely monitor any threats that have been accepted.

Lesson Conclusion and Recap

- Principles-Based Security Governance and Compliance Frameworks provide a solid foundation for effective security practices.
- By incorporating key principles and leveraging compliance frameworks, organizations can establish robust security governance and meet regulatory requirements.
- Organizations can lessen the impact of security incidents, safeguard crucial assets, and resume normal operations by putting in place a strong incident response plan.
- To ensure effective incident management, it is crucial to constantly stay up to date on incident response frameworks, methodologies, and best practices.
- While we cannot completely eliminate risk, we can set acceptable levels by comparing the impact of a threat with the expense of putting controls in place to lessen it.

Hyperiondev

Q & A Section

Please use this time to ask any questions relating to the topic explained, should you have any

Hyperiondev

Thank you for joining us

Take regular breaks.
Stay hydrated.
Avoid prolonged screen time.
Remember to have fun :)