Recap: Security Management

Lecture – Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment - please engage accordingly.
- No question is daft or silly - **ask them!**
- There are Q/A sessions midway and at the end of the session, should you wish to ask any follow-up questions.
- You can also submit questions here: hyperiondev.com/sbc4-cs-questions
- For all non-academic questions, please submit a query: www.hyperiondev.com/support
- Report a safeguarding incident: hyperiondev.com/safeguardreporting
- We would love your feedback on lectures: https://hyperionde.wufoo.com/forms/zsgv4m40ui4i0g/

Previously:

- Understand the process of incident response.
- Explored Some Career paths

Objectives

- Recap on:
  - Governance
  - Compliance
  - Risk management
  - Incident Response

Security Governance & Compliance Frameworks

- Security Governance: Ensures effective management and oversight of security within an organization that are aligned in a way that supports the organization's business goals.

- Compliance Frameworks: Established guidelines and standards for meeting legal, regulatory, and industry requirements.

Principles-Based Security Governance

Flexible approach focusing on guiding principles rather than rigid rules.

1.) Risk-Based decision Making

2.) Accountability and Responsibility

3.) Transparency & Communication

4.) Continuous Improvement

5.) Integration and Alignment

6.) Resilience and Adaptability

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

Hyperiondev

Benefits and Considerations of Principles-Based Security Governance

Benefits:

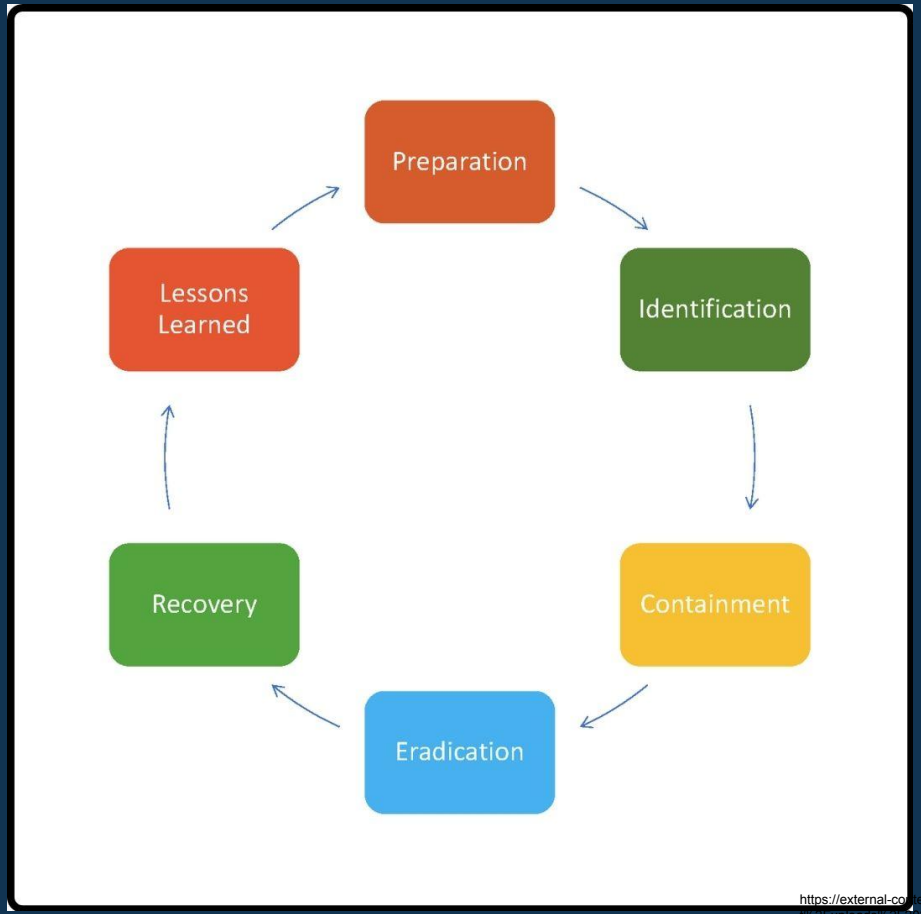
- Flexibility and adaptability to evolving threats and needs.
- Alignment of security measures with business objectives.
- Enhanced risk management and accountability.

Factors that require consideration:

- Balancing compliance requirements with organizational needs.
- Sustaining security governance and compliance.

Questions and Answers

Incident Response Process



https://external-content.duckduckgo.com/iu/?u=https%3A%2F%2Fisea.utoronto.ca%2Fwp-content%2Fuploads%2F2021%2F05%2FIncident-Response-Graphic.jpg&f=1&nofb=1&ipt=083605c369c8773665efb44bca0918eeed3aef4bf5b4687582c68fb577aad96e&ipo=images

Fundamental British Values

1.) Democracy: Participating in democratic processes when making decisions during incident response activities

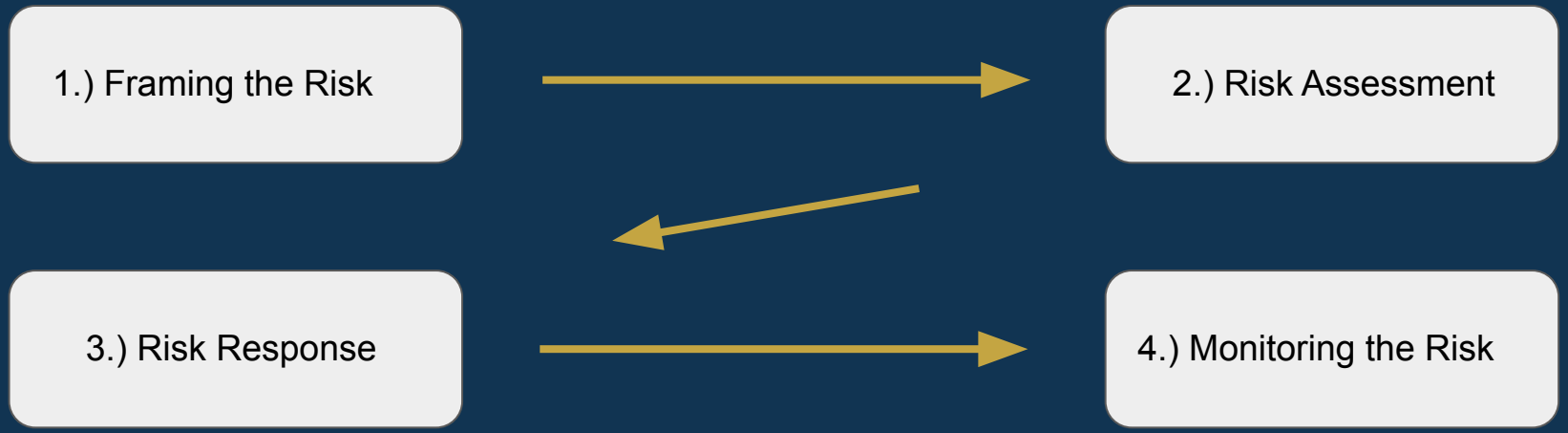
2.) Rule of Law: Respecting the law and following regulations when responding to incidents

3.) Individual Liberty: Juggling incident response procedures to reduce interference with individual rights and privacy

4.) Mutual Respect: Communication and cooperation with incident response teams, stakeholders, and affected parties out of mutual respect

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

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.

Wrapping Up

- 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.

Next up

- Berkeley Sockets API in Python

Questions and Answers

Hyperiondev

Thank you for joining us

1. Take regular breaks
2. Stay hydrated
3. Avoid prolonged screen time
4. Practice good posture
5. Get regular exercise

"With great power comes great responsibility"