Legal Issues and Cyber Law (HUM 4747)

Md. Rafid Haque

Department of Computer Science and Engineering

Software Engineering Programme

Cyber security strategy guide

A document that outlines the vision, goals, objectives, and actions for enhancing the security and resilience of an organization’s information systems and networks.

Benefits of a cyber security strategy guide

Identify and prioritize	Identify and prioritize the most critical assets and risks
Align	Align the security efforts with the business objectives and values
Establish	Establish roles and responsibilities for security governance and management
Define	Define the security policies, standards, and procedures
Implement	Implement the best practices and controls for security prevention, detection, and response
Monitor and measure	Monitor and measure the security performance and effectiveness
Improve	Continuously improve the security posture and maturity

Components of a cyber security strategy guide

Executive summary: A brief overview of the purpose, scope, and main points of the strategy guide

Vision statement: A statement that describes the desired future state of the organization's security

Mission statement: A statement that describes the core purpose and function of the organization's security

Goals and objectives: A set of specific, measurable, achievable, relevant, and time-bound (SMART) outcomes that the organization wants to achieve through its security efforts

Action plan: A detailed description of the tasks, activities, resources, timelines, and responsibilities for implementing the strategy guide

Evaluation plan: A plan for assessing the progress, results, and impact of the strategy guide

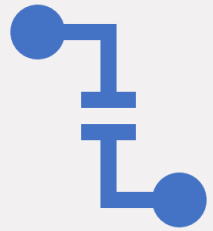
Threats to information resources

Any potential events or actions that can compromise the confidentiality, integrity, or availability of an organization’s information assets.

Types of threats to information resources

Natural threats: Threats that are caused by natural disasters or phenomena, such as floods, earthquakes, fires, etc.

Human threats: Threats that are caused by intentional or unintentional actions of people, such as hackers, insiders, competitors, etc.



Technical threats: Threats that are caused by failures or malfunctions of hardware, software, or networks, such as viruses, bugs, glitches, etc.

Examples of threats to information resources

- Phishing: A fraudulent attempt to obtain sensitive information or credentials by impersonating a legitimate entity via email or other communication channels
- Ransomware: A malicious software that encrypts the victim’s data and demands a ransom for its decryption
- Denial-of-service (DoS): An attack that overwhelms a system or network with excessive traffic or requests to disrupt its normal functioning or availability
- Data breach: An unauthorized access or disclosure of confidential or personal data to a third party
- Insider threat: A threat that originates from a current or former employee or contractor who has legitimate access to the organization’s information systems or networks

Digital Forensics

The process of collecting, preserving, analyzing, and presenting digital evidence from various sources, such as computers, mobile devices, networks, cloud services, etc.

Purpose of digital forensics

Identify the cause and intent of a cyber attack

Maintain the security posture

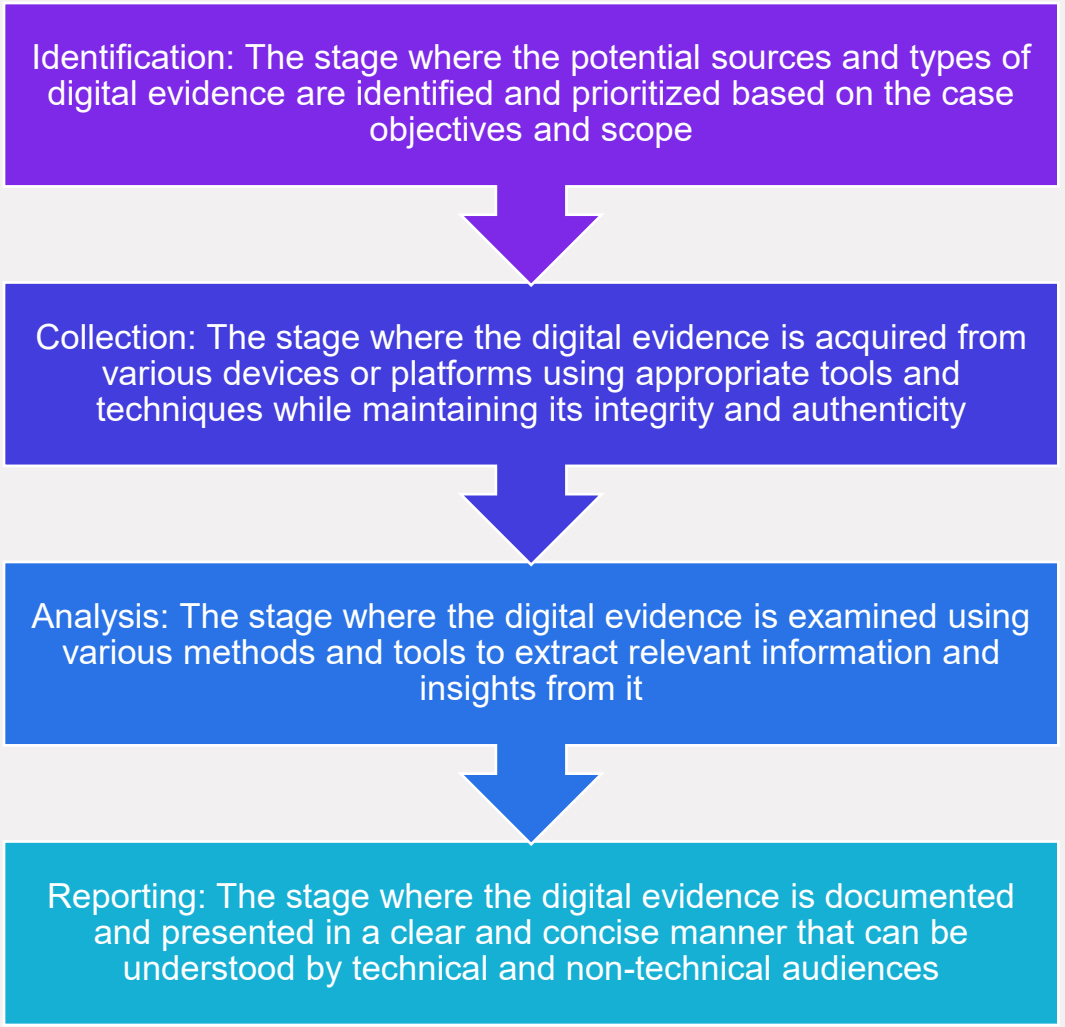
Backtrack the hacker's steps to expose attack tools

Preserve electronic evidence before it becomes obsolete

Find the source of data exfiltration or access

Geolocating and tracking the attacker

Stages of Digital Forensics



Thanks

See you in the next class