Harvard Cyber learnings

David Banger

CXO Advisor / Adjunct Professor / Author

WHAT IS CYBER SECURITY?

The balancing of priorities

Goals of information security

Adapted by Harvard – *The CIA triad refers to the three goals of cybersecurity, namely to ensure the confidentiality, integrity, and availability of information systems.*

Must address these

Is there a cybersecurity program that identifies threats & provides protection against them?

Is there a cybersecurity policy covering matters like disaster recovery planning, customer data privacy, & access controls?

How does your organisation restrict user access to data & systems?

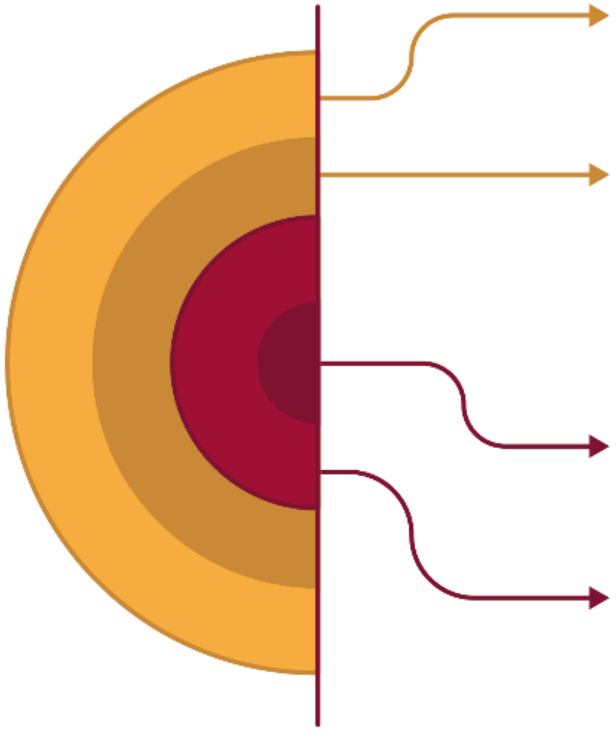
Has a Chief Information Security Officer (CISO) been appointed, or is there an equivalent arrangement?

How qualified and available are your personnel to manage cybersecurity risks?

How does your organisation report cybersecurity incidents to the appropriate authority?

Is an incident response plan in place?

Possible scenarios



Unintentional external threats: These are threats to an organization that accidentally result from the organization's relation to external actors.

Malicious external threats: A deliberate attempt by outsiders to gain unauthorized access to an organization's critical information systems. For example, hacks actioned by nation states or cybercriminals attempting to steal sensitive information, or significantly impede a business's operations.

Malicious internal threats: Deliberate acts perpetrated by insiders intending to gain unauthorized access to an organization's critical information systems.

Unintentional internal threats: Accidental acts by insiders that may negatively affect an organization's systems, networks, or data, usually resulting from negligence or human error.

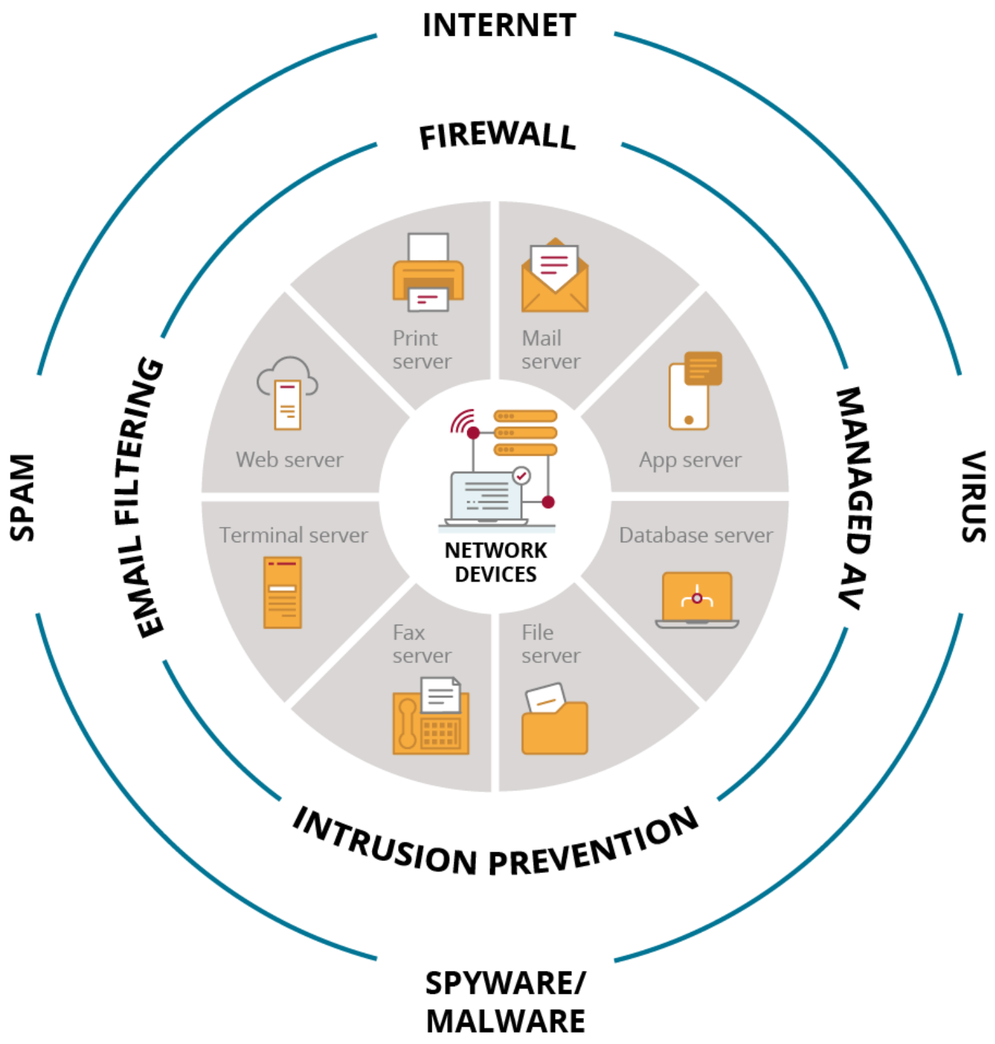
Three primary areas

Business operational risk – the potential for direct or indirect loss that results from the failure of key business systems, processes, procedures, or people.

Reputational risk – the potential for loss or damage that results from harm caused to an organisation's reputation or public image.

Legal and compliance risk – the potential for loss or damage that results from legal action being taken against an organisation for breaching the law or regulatory requirements.

WHAT NEEDS TO BE MANAGED



Actors are varied …

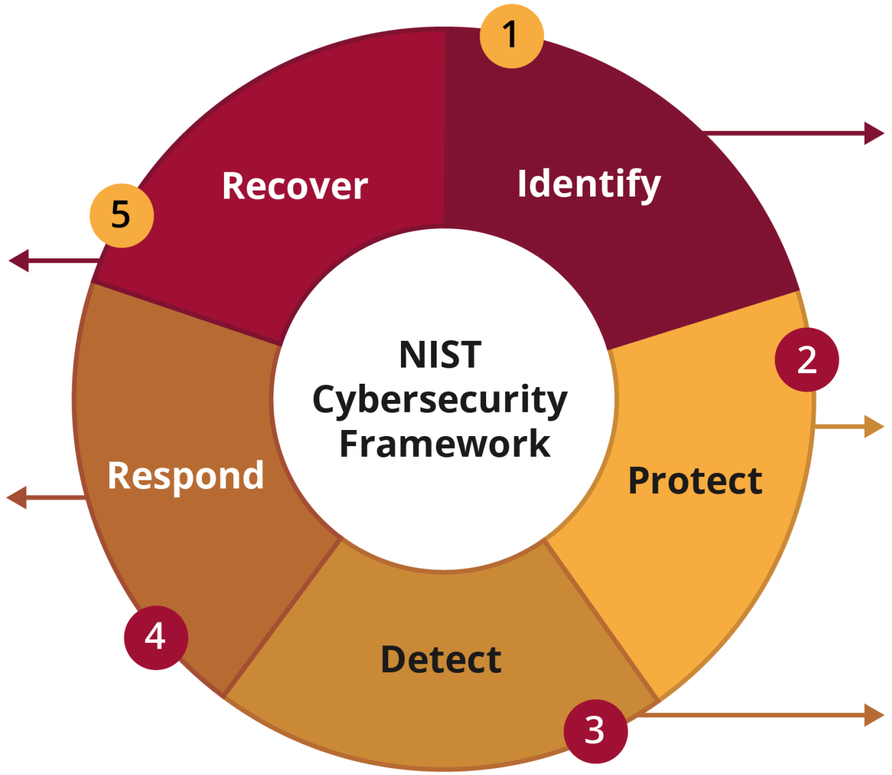
- Lone hackers
- Hacktivists
- Petty criminals
- Organised criminals
- Professional criminals
- Cyberwarfare vendors
- Criminals with military partnerships
- Nation states

MISSION CRTITICAL

Identify and protect; for business continuity;

- Systems
- Infrastructure (network)
- Data

RECOGNISED INTERNATIONAL FRAMEWORK



- AM: Asset management
- BE: Business environment
- GV: Governance
- RA: Risk assessment
- RM: Risk management strategy

- AC: Access control
- AT: Awareness training
- DS: Data security
- IP: Information protection processes and procedures
- PT: Protective technology

- AE: Anomolies and events
- CM: Security continuous monitoring
- DP: Detection processes

- RP: Response planning
- CO: Communications
- AN: Analysis
- MI: Mitigation
- IM: Improvements

- RP: Recovery planning
- IM: Improvements
- CO: Communications

Resilience

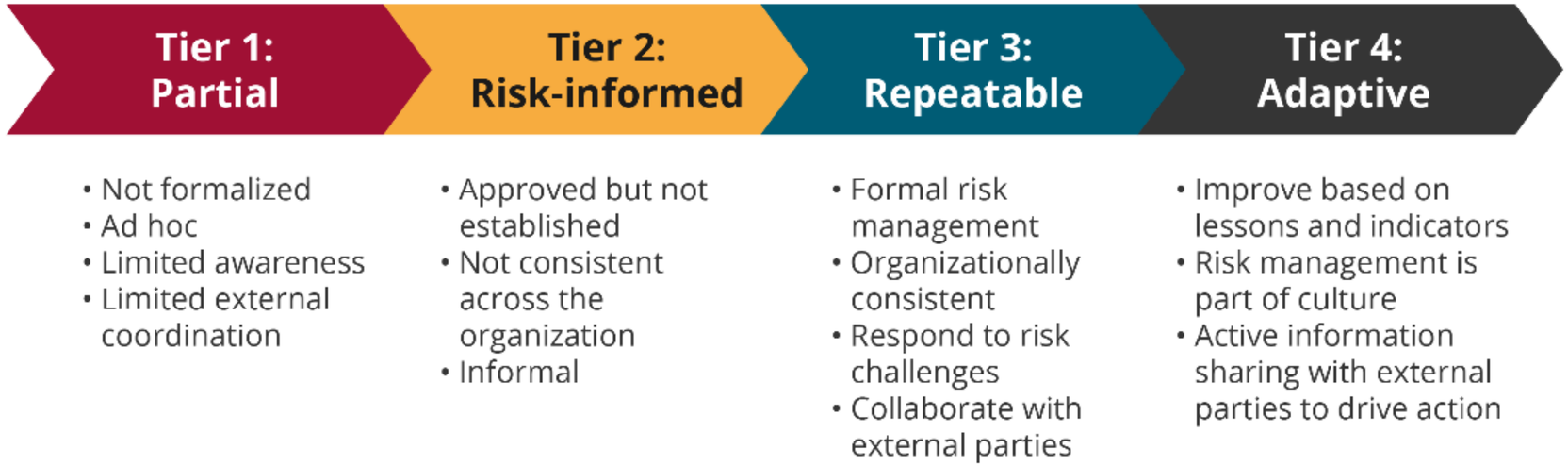
(1 to 4) being the procedures followed; measures taken to protect

Recovery

(5) the capacity to recover

NIST – US National Institute of Standards & Technology

Assess and improve



WORK THE DETAIL

Structure activities to prevent and recover from an attack

Functions	Categories	Subcategories	Informative References
IDENTIFY	• Asset management • Business environment • Governance • Risk assessment • Risk management strategy		
PROTECT	• Access control • Awareness training • Data security • Information protection processes and procedures • Protective technology		
DETECT	• Anomalies and events • Security continuous monitoring • Detection processes		
RESPOND	• Response planning • Communications • Analysis • Mitigation • Improvements		
RECOVER	• Recovery planning • Improvements • Communications		

WHERE TO START

Define Cyber vision

Link organisational values to vision

Objectives include outcomes

Actions are beyond technologies