Strengthening Hemas Hospitals' Cybersecurity

By Anjula Meegalla

Agenda

1. Information Assurance Concepts & Mitigation (P5)
2. Enhancing Cyber Resilience through IA (M3)
3. Security Standards, Regulations, and Consequences (P6)
4. Types of Response to Cybersecurity Threats (P7)
5. Role of Legislation in Deterring Cybercrime (M4)
6. Evaluation of Organizational Responses (D2)
7. Conclusion & Recommendations

Information Assurance Concepts & Mitigation

- # Key IA Concepts (The CIA Triad & Beyond):

Confidentiality:

Mitigation: Encryption (data at rest/in transit), access controls (Principle of Least Privilege), data anonymization.

Eg: Encrypting patient data on datacenter servers and during VPN connections; strict role-based access for clinic administrators to patient records.

- # Key IA Concepts (The CIA Triad & Beyond):

Integrity:

Mitigation: Hashing, digital signatures, strong change management processes, robust backup & recovery.

Eg: Implementing checksums for patient financial records, using digital signatures for critical medical reports, ensuring regular and verifiable data backups.

- # Key IA Concepts (The CIA Triad & Beyond):

Availability:

Mitigation: Redundancy (servers, networks), robust backup & recovery, DDoS mitigation, disaster recovery planning.

Eg: Implementing redundant servers for critical applications, subscribing to DDoS mitigation services to overcome the 10 concurrent connection limit.

- # Key IA Concepts (The CIA Triad & Beyond):

Accountability/ Non-Repudiation:

Mitigation: Comprehensive logging, audit trails, multi-factor authentication, digital certificates.

Eg: Centralized logging of all VPN logins and datacenter access attempts, recording all modifications to patient records with user timestamps.

- # Key IA Concepts (The CIA Triad & Beyond):

Authenticity:

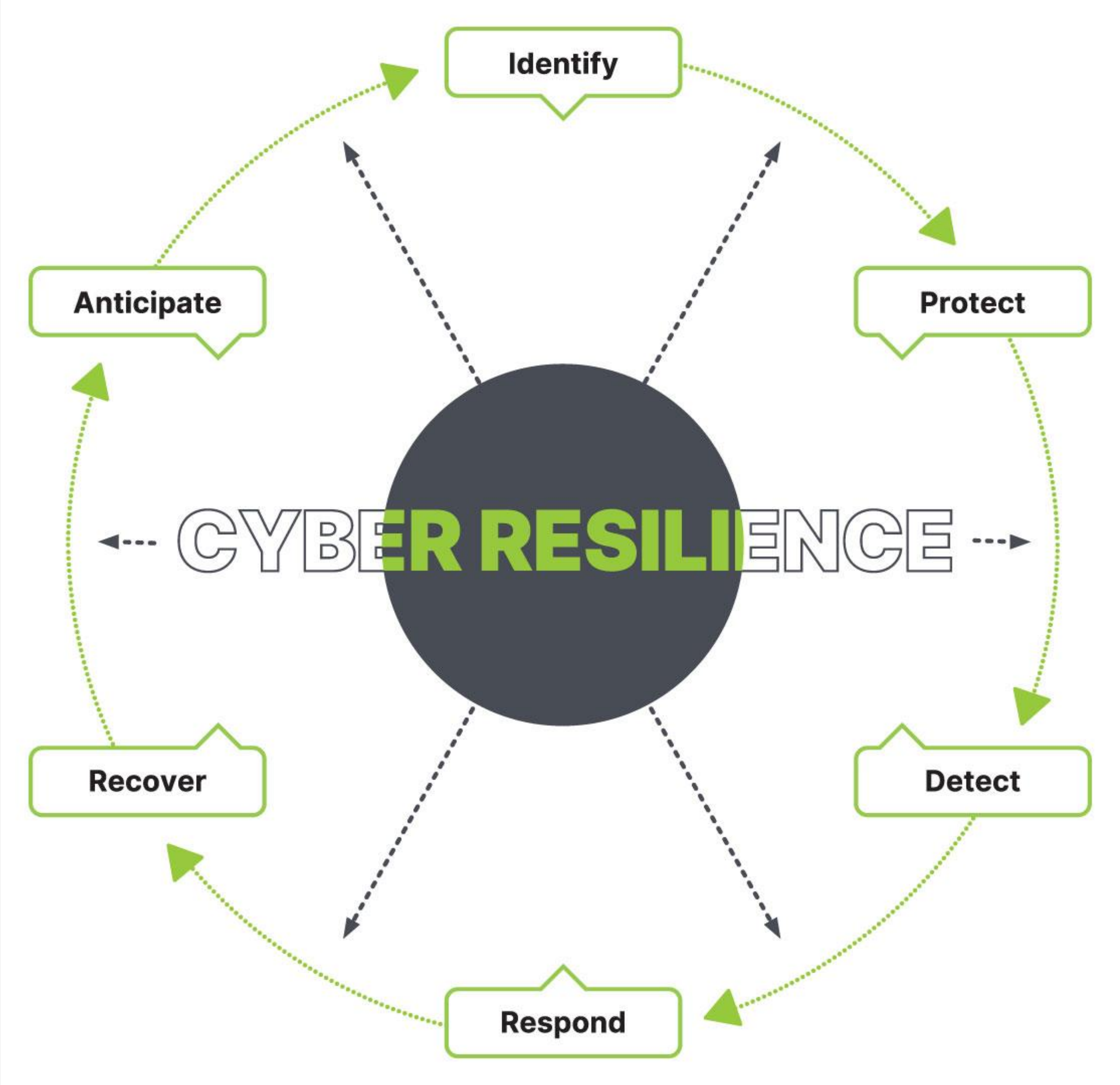
Mitigation: Strong authentication (MFA), digital certificates, biometric verification.

Eg: Implementing MFA for all VPN logins and administrative access to the datacenter, beyond just a single password per clinic.

Enhancing Cyber Resilience through IA

The Concept of Cyber Resilience

The ability to continuously deliver the intended outcome despite adverse cyber events.



How IA Enhances Resilience?

Anticipate

IA principles help proactively identify weaknesses.

Eg: Prioritizing patching efforts based on threat intelligence (from IA's influence), leading to fewer successful initial compromises.

Withstand

Strong IA controls act as barriers during an attack.

Eg: Encrypted patient data withstands exfiltration attempts; segmented networks prevent ransomware from spreading globally.

Recover

Robust IA practices enable faster and more complete recovery post-incident.

Eg: Offline, immutable backups ensure rapid restoration after a ransomware attack, directly improving recovery time.

Evolve

Continuous monitoring, auditing, and review (IA principles) ensure lessons learned from incidents lead to stronger future defenses.

Eg: Post-incident analysis identifies gaps in VPN login security, leading to the implementation of MFA and individual user accounts, improving future resilience.

Security Standards, Regulations, & Consequences

Sector 1 - Healthcare

Regulations:

Sri Lanka: Personal Data Protection Act, No. 9 of 2022 (PDPA), Computer Crime Act, No. 24 of 2007.

International: GDPR (EU), HIPAA (US)

Consequences of Non-Compliance:

Financial Penalties

Reputational Damage

Legal Action

Operational Disruption

- A major hospital in the US faced millions in fines for HIPAA violations following data breaches due to inadequate security (Eg: Anthem Inc.).

Sector 2 - Finance

Regulations:

Sri Lanka: Central bank regulations

International: PCI DSS (Payment Card Industry Data Security Standard), Dodd-Frank Act in US, PSD2 in EU

Consequences of Non-Compliance:

Heavy Fines

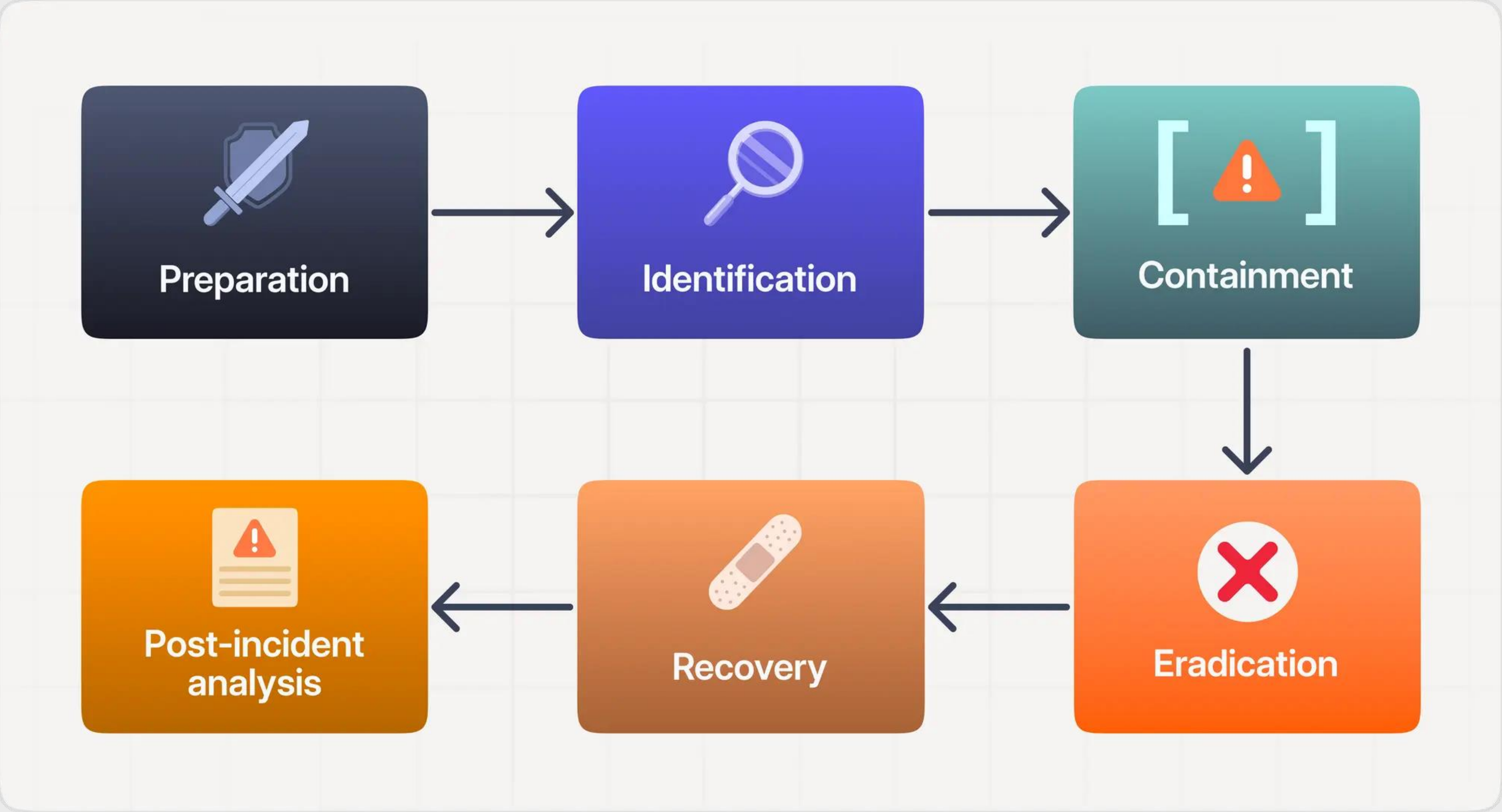
Loss of Operating Licenses

Reputational Harm

- A financial institution faced significant regulatory fines and suspension of certain operations after repeated failures to protect customer data (Eg: Capital One breach).

Types of Response to Cyber Security Threats

Common Response Phases (NIST/SANS)



Preparation

Developing policies, plans, teams, tools, and training before an incident.

Eg: Hemas preparing an incident response team, reviewing SLAs for network administration, conducting cybersecurity awareness training.

Detection & Analysis

Identifying abnormal activity, determining scope, nature, and severity.

Eg: Hemas's SIEM system flagging unusual VPN logins or large data transfers from the datacenter; clinic administrator reporting suspicious emails.

Containment

Limiting the damage and preventing further spread of the attack.

Eg: Isolating infected systems, blocking malicious IP addresses at the firewall, shutting down compromised VPN connections.

Eradication

Limiting the damage and preventing further spread of the attack.

Eg: Isolating infected systems, blocking malicious IP addresses at the firewall, shutting down compromised VPN connections.

Recovery

Restoring affected systems and data to operational status, ensuring integrity.

Eg: Restoring patient data from offline backups after a ransomware attack, bringing segmented systems back online, verifying data integrity.

Post-Incident Activity

Documenting, analyzing, and improving processes for future incidents.

Eg: Hemas reviewing its incident response plan after a simulated DDoS attack, updating VPN security protocols based on findings.

Real-World Example – Maersk (NotPetya, 2017)

Attack: NotPetya ransomware disguised as a wiper.

Response: Massive, global containment effort (pulled cables), rebuild from clean backups, extraordinary recovery efforts across 400 offices in 130 countries.

- **Key Takeaway:** Demonstrated the importance of having isolated, tested backups and strong crisis management. They prioritized recovery over immediate detailed forensics in the heat of the moment.

Role of Legislation in Deterring Cybercrime

Criminal Legislation

Mechanism: Defines cyber offenses (unauthorized access, data theft, malicious software, DDoS attacks) and prescribes penalties (imprisonment, fines).

Impact: Creates legal risk for cybercriminals, making certain activities punishable. Facilitates law enforcement action against perpetrators.

Other Legislation (Data Protection)

Mechanism: Focuses on responsibilities of organizations to protect data, notify breaches, and adhere to security standards.

Impact: Motivates organizations to invest in robust cybersecurity. Creates legal pathways for victims to seek redress. Fosters a culture of accountability for data protection.

Challenges to Deterrence

- **Jurisdictional Complexity:** Cybercrime crosses borders, making prosecution difficult.
- **Anonymity:** Tools for anonymity (Tor, cryptocurrencies) aid criminals.
- **Evolving Techniques:** Laws struggle to keep pace with rapid technological advancements.

Evaluation of Organizational Responses to Cyber Threats

By analysing 3 real-world cases

Maersk (NotPetya, 2017)

Response: Extraordinary rebuild from clean backups (over 4,000 servers, 45,000 PCs in 10 days). Emphasized quick decision-making and pre-existing, isolated backups.

Lesson for Hemas: Prioritize the SLA review for data backups; ensure they are off-site, immutable, and regularly tested. Invest in robust recovery infrastructure.

Colonial Pipeline (Ransomware, 2021)

Response: Shut down operations (pipeline) to contain the spread. Paid ransom (later partially recovered). Collaboration with FBI.

Lesson for Hemas: Develop clear policies for dealing with ransomware: never pay if robust backups exist. Understand the cascading impact of operational shutdowns on healthcare services.

Equifax (Data Breach, 2017)

Response: Delayed public disclosure, initial poor communication, inadequate patching of known vulnerability.

Lesson for Hemas: Emphasize stringent patch management, rapid detection, clear communication protocols, and a robust data breach notification plan (aligned with Sri Lankan PDPA).

SolarWinds Supply Chain Attack, 2020

Response: Involved broad industry collaboration, extensive forensic analysis, and complex remediation across affected organizations.

Lesson for Hemas: Implement strong vendor risk management for outsourced services and cloud/IoT providers. Assume breaches and focus on detect-and-respond capabilities.

Conclusion & Recommendations for Hemas

1. Prioritize Core IA Principles
2. Maintain Resilience via Backups
3. Strengthen Access Management
4. Invest in Detection & Containment
5. Focus on Proactive Compliance
6. Continuous Training & Threat Intelligence
7. Review and Refine Incident Response Plan

Thank you

Q&A