CYBER MANAGEMENT ALLIANCE

NCSC-Certified Training

Cyber Incident Planning & Response

Learning Objectives

Version 1.01 15th June 2020

Module 1: Cyber Resiliency

After this module students will be able to:

- Describe the importance of "Starting with Why".
- Discuss what cyber resiliency means for a modern digital business.
- List the four constituents of a cyber-resilient organisation.
- Explain why 100% security is a fallacy with examples.

Module 2: Threat Actors & Privileged Users

After this module students will be able to:

- Recount the importance of knowing your threat actors and how they operate.
- Describe how knowing your threat actors can help in risk identification and risk management.
- Describe effective ways to determine threat actors and refer to specific resources to support in the objective.
- Be able to participate and contribute in identifying threat actors during assessment workshops and describe the key attributes of a threat actor.
- Articulate the different forms of threat to, and vulnerabilities of, information systems and assets and support and participate in activities that
    - Threats and threat actors to critical assets.
    - Explain how threat agents exploit vulnerabilities.
    - Start to assess the level of threat posed by potential threat agents
- Comprehend and manage the threats and risks relating to information systems and assets from cyber-attacks and threat actors.

Module 3: Define Normal

After this module students will be able to:

- Describe the importance of Defining Normal and explain its role in
    - Significantly improving accuracy of attack detection capabilities.
    - Improving and or creating fit-for-purpose organisation cyber and IT related policies.
    - Materially improving incident-alert accuracy and consequently having an appreciable impact on staff efficiencies.
- Host and or participate in Define Normal workshops.
- Explain the challenges with implementing defining Normal.
- Describe the technologies that can help in automating Define Normal.
- Support investigations into information security incidents.
- Define the need for and of implementing processes for establishing business continuity.
- Define and support the implementation of processes and procedures for detecting breaches of security policies.

Module 4a: The Attack Process

After this module students will be able to:

- List the two attack frameworks that attackers use as the baseline of their attack strategies.
- Explain how you can use these frameworks to help identify an organisation's readiness in dealing with specific cyber-attacks.
- Explain and discuss the primary objective of cyber-attackers after they enter a digital network. Furthermore, you will be able discuss the importance of this goal.
- Explain an organisation's core objective when constructing a cybersecurity strategy.
- Discuss the various attack-vectors that criminals use when launching a cyber-attack.
- Name and discuss some of the tools that hackers use when they are planning and launching their cyber-attack.
- Describe, based on real cyber-attacks, the key steps attackers took and the reasons why they succeeded. You will be able to relate these attacks back to the methodologies and the tools.
- Explain what Threat-Intelligence and its significance is in keeping organisations cyber-resilient. Discuss how threat-intel can aid in rapid-detection of advanced threats.
- Discuss the various steps you can take and technologies an organisation can deploy to ensure they are more cyber-resilient.
- Understand the Core principals of and actively contribute by
    - Contributing to the creation of your organisation's cybersecurity strategy.
    - Participating in the selection of credible providers of threat intelligence.
    - Evaluating an organisation's readiness against specific scenarios.
    - As part of wider group, challenging and interrogating decisions on technology stack investments.

Module 4b: Tools & Techniques

After this module students will be able to:

- Name some of the tools and describe the purpose of the tools.
- Describe how specific tools fit in to the attack methodology.
- Understand the importance of and the impact hacking tools can have if used without supervision.
- Understand and explain the importance of up-skilling staff in the use of such tools and the benefit of using these tools for protection.

Module 4c: Case Studies

After this module students will be able to:

- Discuss the specific cases studies in detail.
- Explain the importance of cyber-resilience, the need for rapid detection and rapid response by referring to key events in the case studies.
- Apply the knowledge and lessons-learnt from real-world attacks to your own organisation.
- Understand the Core principals of and actively contribute by
    - Articulate the different forms of threat to, and vulnerabilities of, information systems and assets.
    - Better manage the risks relating to information systems and assets.

Module 4d: Threat Intelligence

After this module students will be able to:

- Understand the importance of scenarios in cyber-resilience.
- Explain the key ingredients to create effective scenarios.
- Discuss how threat intelligence helps in early and more accurate detection.
- Discuss the various types of threat intelligence.
- Management of Risk
    - Participate in the development of information risk management strategies to reduce business risk.
    - Gain management commitment to the support of the information risk elements of business risk management.
    - Adapt the risk management strategy to address changes in the threat environment.

Module 5: Visibility

After this module students will be able to:

- Explain the importance of focusing on visibility in your cyber-resilience and risk management strategy.
- Have a good grasp of the core concepts and terminology of log management in relation to visibility.
- Outline the key terms and requirements for visibility infrastructure.
- Understand and be able to organise workshops to help better identify "Crown Jewels".
- Explain the connection between log management and transparency and forensics.
- Discuss the benefits of monitoring and auditing for violations of relevant security policies. (e.g. acceptable use, security, etc.)

Module 6a: The Golden Hour & Incident Management

After this module students will be able to:

- Understand and discuss the concept of the Golden Hour and explain its significance in cyber incident management.
- Explain the importance of the Golden Hour and what actions an organisation should do in this timeframe.
- Understand and explain
    - The importance and key benefits of accurate triage.
    - The disadvantages of unreliable triage and its impact on organisational resiliency.
    - Examples of triage activity that can be carried out in a cyber-attack.
- Discuss with examples the consequence of bad triage.
- Understand the benefits of technology and automation in assisting accurate triage.
- Defining the need for and of implementing processes for establishing business continuity.
- Engage with the overall organisation on incident management process to ensure that security incidents are handled appropriately.
- Define and implement processes and procedures for detecting breaches of security policies.

Module 6b: Incident Management

After this module students will be able to:

- Describe the various stages / categories of incident response and the key activities associated with each phase.
- Discuss the importance of and benefits of understanding and following incident management procedures in relation to cyber resiliency.
- Explain the reasons to have clear incident definitions and describe the benefit this brings to an organisation's overall cyber-resilience posture.
    - In addition, you will be to Contribute to the review and or definition of and apply the knowledge to:
- Incident management policies and standards.
- 3rd party / supply chain contracts specifically related to the various stages of incident management.
- Discuss the benefits of having easy to understand and integrate process workflows.

Module 6c: Incident Response Playbooks

After this module students will be able to:

- Explain the role playbooks play in incident response.
- Describe the benefits of having structured response playbooks.
- List the four key phases a playbook must cover.

Module 6d: Creating an Incident Response Plan

After this module students will be able to:

- Describe the various stages / categories of incident response and the key activities associated with each phase.
- Discuss the importance of and benefits of understanding and following incident management procedures in relation to cyber resiliency.

Module 7: Building the Team

After this module students will be able to:

- Describe and explain the key attributes of a cybersecurity incident-response team member.
- Help outline and contribute to improve an existing cyber-incident response team or creating a new one.
- Outline key team structures in incident response and describe the links between other functional teams in the business.
- Establish and maintain a Computer Security Emergency Response Team or similar to deal with breaches of security policies.

Module 8: Forensics & Investigations

After this module students will be able to:

- Understand the basic concepts of forensics integrity.
- Discuss the necessity of an evidence-based approached to cyber resilience.
- Explain the necessity for an executive mandate on forensics and the need to preserve evidence to underpin transparency.
- Explain the important of seizing evidence in accordance with legal guidelines and in the most effective manner to minimise disruption to the business and maintaining evidential weight and integrity.

Module 9: Regulations & Standards

After this module students will be able to:

- Understand and explain the primary requirement of privacy regulations, like the EU-GDPR, in the context of cyber incident response and cyber resilience.
- Participate and raise awareness, with support from legal counsel, in supply-chain contract reviews.
- Explain the key areas to focus on to ensure better conformance to regulations.
- List some of the global regulations and describe their recall their key requirements in the context of incident planning, response and notification.
- Explain in some detail what the GDPR breach-notification requirements mean for an organisation and discuss the importance of the need for maturity in four key phases of incident management.
- As part of a wider group of informed professionals and with the support of legal counsel, contribute to better compliance with incident management related regulations and standards.
- Describe the relevant incident management section of ISO 27001:2013 and PCI-DSS and explain some of the key controls to effectively manage the incident lifecycle.
- Explain the four key phases of managing an incident according to US-NIST and discuss the importance and role of each phase in ensuring better and effective incident response.
- Be able to explain how to and determine if a cyber-attack's impact is in GDPR's reportability-scope and consequently be able to actually report a data breach to the UK supervisory authority (the ICO).
- Discuss the legal and regulatory requirements that could affect organisation security policies, and where to turn for specific detail as needed.
- Ensure security policies align with and better comply with personal data protection laws and regulations relevant to the business.
- Ensuring security policies support compliance with corporate governance.

Module 10: The Technology Stack

After this module students will be able to:

- Recognise the key role technology plays in effective incident response.
- Understand and explain the concept of and the benefits of a coherent technology stack plays in relation to cyber incident response.
- Understand the limitations of and the connection between technology and staff and describe the value of targeted staff up-skilling.
- Recognise the potential strategic application of technologies in information security.
- Discuss and support the development of innovative methods of protecting information assets, to the benefit of the organisation and the interface between business and information security.

Module 11: Communications & PR in Incident Management

After this module students will be able to:

- Recognise the need for effective internal and external communications.
- Discuss the importance of accurate but rapid communication with stakeholders.
- Recognise and explain the link between facts and transparency how focusing on this duo can uplift an organisations compliance, client trust and overall brand reputation during and after a cyber crisis.
- Discuss and support in the development, coordination and evaluate plans to communicate with internal stakeholders, external stakeholders and the media.

CYBER MANAGEMENT ALLIANCE

Author: Amar Singh

info@cm-alliance.com https://cm-alliance.com +44 203 189 1422 @cm_alliance