

Your total guide  
to planning and  
responding to a  
cyber attack

Virtual Classroom,  
eLearning and  
private immersive  
workshops

# NCSC ASSURED CYBER INCIDENT PLANNING & RESPONSE

PROCESSES & OPERATIONAL STRATEGIES TO IMPLEMENT

NIST'S INCIDENT RESPONSE LIFECYCLE

& ISO 27001:2013'S ANNEX A.16.1 OBJECTIVES

**Learn how to implement NIST's  
Computer Security Incident Handling  
Guide: NIST SP 800-61 Revision 2**

**Create cyber response strategies  
and plans designed to enable rapid  
recovery of business operations**

**Produce tangible incident-response  
processes for organisation-specific  
threat-actors and scenarios**



Chartered Institute of  
Information Security

**WITH OPTIONAL EXAM**

Assured Service Provider



in association with  
**National Cyber  
Security Centre**

- Gain deeper insights on key risk-reducing controls to increase your company's ability to protect, detect and respond to cyber-attacks.
- Learn how to design an early warning system to lower discovery time from months to days.
- Develop the skills to understand and improve your company's cyber resilience by making more cost-effective, risk-based decisions.
- Gain an understanding of crisis communications, media management and how to communicate with clients, employees and journalists.
- Learn how to integrate with and benefit from an information risk management approach to incident management.
- Discover the "Golden Hour" and its significance in effective incident response and management.
- Learn how to use threat intelligence and international frameworks to lower your overall organisational risk.
- Understand Rapid Response in Incident Management and learn how to design IR frameworks to achieve rapid detection and rapid response in cyber-attacks.
- Collaborate to create usable collateral you can put to use immediately to improve your detection and response capabilities.
- Discover why risk-based profiles of cyber-attackers matter in cyber resilience and learn how to create these.
- Understand the application of incident triage in incident response. Drill down into the Cyber Kill Chain process.

“...this course and workshop that I've been through today, was amazing. I think overall, this has actually allowed me to think about lot of other things which we can achieve.”

*Suraj Singh*  
Head of Microsoft, Security Operations Centre

“...found today's course very productive. Course was very clearly presented. Looking forward to putting some of the things we learnt into practise.”

*Euan Ramsay*  
CSIRT Director, UBS Bank Switzerland

**Templates, Interactive Exercises, Group Activities designed to teach you how to implement NIST's Computer Security Incident Response Handbook & ISO 27001:2013's Annex A.16.1 Objectives**

- Mindmap: Exercise on planning for a Cyber-attack
- Process Workflows: Incident Response Strategy
- Process Workflows: Selecting Threat Actors
- Process Workflows: Breach Readiness Framework
- Process Workflows: Responding to an incident
- 5Ds & defending against the Cyber Kill Chain
- Visibility: Identifying your Crown Jewels
- Visibility: Identifying Critical Log Data
- Client and PR Communication Templates
- Worksheet: Identifying Privileged Threat Actors
- Worksheet: Defining & Baselining Normal
- Cyber Response Plan Template
- Cyber Response Checklists

**Module 1 - Cyber Resiliency**

- The "why" with relevant real-world examples
- The 'Security Fallacy' and how to work around it
- Four constituents of a cyber-resilient organisation

**Module 2 - Threat Actors & Privileged Users**

- Importance of knowing threat actors for risk identification & management
- Managing risks from cyber-attacks & threat actors

**Module 3 - Define Normal**

- With examples, learn the importance of this concept
- How to define 'normal' for your organisation based on the nature of your business, scale, operational model etc.
- Applying 'Define Normal' & challenges with implementing it at the organisational level.

**Extended Module 4 - Attack Methodology**

**Module 4 (a) - The Attack Process**

- Understanding attack frameworks that criminals use to baseline their strategy
- The importance of Threat Intelligence in keeping organisations cyber resilient

**Module 4 (b) - Tools & Techniques**

- Understanding purpose of tools & how they fit into the attack methodology
- Importance of knowing how to use these tools for protection

**Module 4 (c) - Case Studies**

- Discussing specific case studies in detail
- Understanding importance of cyber-resilience, the need for rapid detection & rapid response through specific events in the case studies

**Module 4 (d) - Threat Intelligence**

- Understanding importance of scenarios in cyber-resilience
- Discussing how threat intelligence helps in early detection
- Risk management strategy & how to adapt it to address changes in the threat environment

**Module 5 - Visibility**

- Understanding the importance of visibility in cyber-resilience & risk management strategy.

- Understanding & being able to organise workshops to help better identify "Crown Jewels".
- Understanding the connection between log management, transparency & forensics

**Extended Module 6 - The Golden Hour**

**Module 6 (a) - The Golden Hour & Incident Management**

- Understanding the concept of 'Golden Hour' & what actions should be taken within the timeframe
- Importance of accurate triage
- The benefits of technology automation in triage

**Module 6 (b) - Incident Management**

- Understanding various stages of Incident Management & their benefits for cyber resilience
- Incident Management Policy & Standards

**Module 6 (c) - Incident Response Playbooks**

- Understanding role of playbooks in Incident Response
- Benefits of having structured Response Playbooks

**Module 6 (d) - Creating an Incident Response Plan**

- Understanding stages of Incident Response
- Understanding importance of Incident Management procedures for cyber resiliency

**Module 7 - Building the Team**

- Understanding key attributes of a Cyber Incident Response team
- Outlining key team structures & describing links between other functional teams in the business.

**Module 8 - Forensics & Investigations**

- The basic concepts of forensics integrity
- Understanding importance of maintaining evidence in accordance with legal guidelines

**Module 9 - Regulations & Standards**

- Understanding primary requirements of privacy regulations like the EU-GDPR
- Ensuring better conformance to regulations
- Implementing NIST's Incident Response Lifecycle & meeting ISO 27001:2013's Annex A.16.1 Objectives

**Module 10 - The Technology Stack**

- Understanding role of technology in Cyber Incident Response
- The connection between technology & staff; Understanding the value of targeted staff up-skilling.

**Module 11 - Communications & PR in Incident Management**

- Importance of accurate & rapid communication in a crisis
- Learning how to develop, coordinate & evaluate plans to communicate with all stakeholders & media

“ A really good session, the trainer is really knowledgeable and presents it in a really understandable format that the participants really enjoyed. ”

Wayne Parkes  
Head of ICT, West Mercia & Warwickshire Police

“ I have to say I was very impressed with the course and its content. The day was packed full of information, examples and there was plenty of interaction between the group. ”

DCI Vanessa Smith  
Yorkshire and Humberside Region Cyber Crime