Your total guide to planning and responding to a data breach

Interactive practical, and immersive workshop

CYBER MANAGEMENT ALLIANCE

NCSC-CERTIFIED CYBER INCIDENT PLANNING & RESPONSE

BUSINESS PROCESSES & OPERATIONAL STRATEGIES FOR RESPONDING TO A DATA BREACH

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

Certified Training

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 on a strategic and operational level.
- Learn 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- resiliency 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 informaton risk management approach to incident management.
- Discover the "golden hour" and its significance in effective incident response and management.
- How to use threat intelligence and international frameworks to lower your overall organisational risk.
- Understand Rapid Response in Incident Management and how to design IR frameworks to achieve rapid detection and rapid response in cyber-attacks.
- Working together, 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-resiliency and 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

info@cm-alliance.com www.cm-alliance.com +44 203 189 1422 @cm_alliance

Interactive Exercises, Group Activities & Takeaways
- 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 Resilience
- 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 & Their Business Impact
- Threat actors, Intent and Attributes
- The TAL or threat actor library and its purpose
- Building the Threat Actor Profile

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' in an organisational context

Module 4 - The Cyber Kill Chain (Cyber Attack Process)
- The different phases of attack methodologies
- Analysis of the Cyber Kill Chain
- The importance of knowing the attack process flows
- Understanding specific threat models & methodologies
- Strategies to counter the Cyber Kill Chain

Module 5 - Visibility
- Its importance in cyber resilience strategy
- Log data & its relationship to cyber resilience
- The strategies for increasing visibility in an organisation
- Crown jewels - the concept & relationship to visibility
- Interactive review – applying the visibility principle to critical asset management

Module 6 - The Golden Hour & Incident Management
- The 'Golden Hour' & it's relevance in cyber resilience
- Triage, concepts & significance in rapid detection and rapid response
- Standards and incident management processes
- Planning for a cyber response - interactive exercise

Bonus - Threat Intelligence Based Incident Response
- Threat intelligence & its role in cyber incident response
- Awareness of the Bank of England Framework
- Creating a threat intel based attack scenario – the basics

Module 7 - Building the Team
- Identifying stakeholders
- Defining the key skills & activities of the team
- Designing an ideal Incident Response Team

Module 8 - Forensics & Investigations
- Introduction to forensics principles
- Importance of protecting evidence & forensic integrity
- Forensics policy & key constituents

Module 9 - Regulations & Standards
- Legal, financial & reputational impact
- A look at common regulations and standards
- Breach notification & how it's defined in the GDPR
- GDPR fines and strategies to lower the risk

Module 10 - The Technology Stack
- The common mistakes organisations make while buying technology and building a technology stack
- The problems a disorganised and incoherent technology stack can create for the business in case of an incident
- Understanding the technologies that underpin an effective breach-ready organisation
- Analysis of core technology requirements

Module 11 - Communications & PR
- The basic principles of public relations
- Crisis Comms Plans management
- Social media and PR - key steps

COURSE CREATOR & TRAINER - AMAR SINGH

– UK Government NCSC-certified trainer and creator of NCSC-certified courses.
– Experienced cyber, information security and data privacy practitioner.
– Global Chief Information Security Officer, expert in information risk management.
– Mentor and trusted advisor to FTSE 100 Firms.

"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