Your total guide to planning and responding to a data breach

Interactive practical, and immersive workshop

CYBER MANAGEMENT ALLIANCE

GCHQ-CERTIFIED CYBER INCIDENT PLANNING & RESPONSE

BUSINESS PROCESSES & OPERATIONAL STRATEGIES FOR RESPONDING TO A DATA BREACH

Is your organisation able to detect a data breach?

Are you prepared to respond and swiftly resume business operations?

INTERACTIVE SESSIONS

WITH OPTIONAL EXAM

GCHQ Certified Training

- 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 management.
- How to use threat intelligence and international frameworks to create a robust and effective incident response plan.
- Orchestration in Incident Management: Understand its significance. Participants create their own incident management orchestration playbook.
- 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, OODA and the Diamond Methodology. 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 https://cm-alliance.com +44 203 189 1422 @cm_alliance

Interactive Group Activities
- Breach notification Templates
- Before the Incident Mind Map
- After the Incident Mind Map
- Checklists
- Crown Jewels
- Process Workflows
- The Cyber Kill Chain
- Go Destroy
- Log Data Analysis
- Press Interview Scenarios
- Crisis Comms Plan
- Client and PR Communication Templates

Understanding Threat Actors
- Threat Actors in Detail
- Threat Agents Intent & Attributes
- Detection and Response Strategies

Automating Incident Management & Response
- What is incident orchestration
- Using incident orchestration to significantly reduce time to - respond to data breaches
- How to semi-automate and fully automate incident management
- Using incident orchestration to empower and up skill existing staff
- Incident orchestration as Force Multiplier
- Using orchestration to increase compliance to regulations like GDPR

Defining Normal
- Identifying Critical Systems and Assets
- Understanding and Building the Organisational Baseline
- Interactive session on applying these principles
- Strategies in understanding operational weaknesses
- Defining high level cyber response process work-flows

The Technologies
- Understanding the technologies that underpin an effective breach ready organisation.
- Analysis of core technology requirements

The Cyber Kill Chain
- Methods of Attack
- Analysis of the Cyber Kill Chain
- Review of Recent High Profile Attacks
- Strategies to counter the Cyber Kill Chain

Triage, Detection & Monitoring
- OODA Loop
- The Golden Hour
- Log Management

The Checklist
- Creating/ adopting the checklist
- Incident management checklist
- Using the check list to beat the hackers!

Intelligence Led Incident Response
- Detailed why and how
- Actionable Threat intelligence

Forensics & Investigations
- Integrity
- Forensic Principles
- Seizing Evidence

Public Relations
- Crisis Comms Plan Management
- Social Media & PR Key Steps
- PR Case Study
- Breach notification

Building the Team
- Stakeholders - Who are they?
- Legal, Compliance and Notifications

COURSE CREATOR AND TRAINER AMAR SINGH

- UK Government GCHQ certified trainer and creator of GCHQ 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.

Free Download - our incident response mind map
http://hubs.ly/H01VWvt0

> 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 Team