How to prepare a defined and managed approach

Highly interactive practical and immersive one day workshop

CYBER MANAGEMENT ALLIANCE

MANAGEMENT BEST PRACTICES IN CYBER SECURITY & DATA PRIVACY

HOW DO YOU REDUCE CYBER RISK WITHOUT INCREASING THE BUDGET?

How to reduce business risk exposure and actually reduce costs

Increase your security posture on budget and with existing resources

INTERACTIVE SESSIONS

Criminals are leveraging the connectivity of the Internet and actively engaging in corporate espionage to steal intellectual property, engineering designs, customer sensitive data and other business and financial confidential information.

When it comes to increasing IT and cyber budgets accounting and finance professionals are increasingly being asked to referee and opine on cyber security spending. There is a way to reduce the risk exposure but simply opening the purse strings and increasing the budget is not the solution. For example, a leading international bank, despite spending over $500 Million dollars annually on cyber security, suffered a major data breach.

Cyber Managements Alliance's one day session will equip attendees with practical knowledge about cyber risk, attacks, their real world effect on brand reputation and the financial impact on business.

This course will enable you to prepare a defined and managed approach when responding to a data breach or attack of an information asset. The content is intended for senior management and business executives who wish to gain a better understanding of cyber security and the real threats to their organisation.

TARGET COMPETENCIES

- **Information Risk Management, policies and standards.**
- **Strategies to protect business reputation, brand image and bottom line.**
- **Data Breach Response – strategy, planning and management.**
- **Basic awareness on cyber and breach regulatory and legal issues.**

Cyber Management Alliance are approved by APMG the only Certification Body licensed and approved by GHCQ to deliver this scheme.

> “Overemphasis on technological (as opposed to management, behavioural and cultural) aspects weakens cyber defensive capabilities.”
>
> *Bank of England and FCA – 2015*

WHO SHOULD ATTEND

An awareness level, non technical, program intended for those who would like to gain a better understand of information risk, cyber attacks, and how to protect their businesses against cyber criminals.

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

COURSE OBJECTIVES

Identify, evaluate and treat cyber-risk and improve their organisation's security posture and undertake responsive measures to reduce business risk exposure to within risk appetite, with constrained resources and within budget.

Explain the key differences between the various types of attacks and discuss mitigating strategies.

Understand the business benefits of complying with international standards including the UK Government's Cyber Essentials scheme, NIST and ISO 27001:2013.

MODULES

Information Risk Management

- Understand the concepts of and establish an Information Risk Management program (Risk identification, risk assessment and risk treatment, Risk monitor)
- Understand how to produce and implement an effective Cyber Information Governance Strategy
- Understand the concepts of cyber resilience, business governance and cyber governance

Information Security Strategy

Information Security Policies

- Understanding the role of policies in an effective strategy and creating an effective policy framework
- The CIA principles and their relationship to the information security strategy model

Understanding the international standard in Information Security ISO 27001:2013

- Building an Information Security Management System (ISMS)
- IT security policies, procedures and IT security framework
- Type of controls including procedural, technical, physical
- Key elements of an effective ISMS
- Interactive session – learn how to create your own ISMS
- Understanding the UK Cyber Essentials framework and the NIST frameworks and how to use them in your business strategy

Understanding the Adversary

- The five types of attackers
- Understand cyber-attack motives, opportunities and threats.
- How cyber criminals select and target businesses
- Business case studies of recent cyber attacks and impact on the businesses
- The Business Cyber Kill Chain and how it can be used to stop most attacks
- Practical demo of cyber-attacks

Innovation in Information Security Strategy

- Review and discuss most current and innovative ways in cyber-security
- Encourage and adopt innovative methods to secure your business and its employees

Legal & Regulatory Issues Cyber Security & Data Privacy

- Understand the impact of global regulations in data privacy and how it can impact your business
- Discuss the relevant case studies in data breach and incident response
- Discuss how to manage and engage media outlets during and after a breach

The Checklist

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

Public Relations

- Crisis Comms Plans Management
- Social Media & PR Key Steps
- PR Case Study
- Breach notification

Building the Team

- Stakeholders – Who are they?
- Legal Considerations, Compliance and Notifications
- Building an effective & agile stakeholder
- Third Parties

Workshop duration: One Day

COURSE CREATOR AND TRAINER AMAR SINGH

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

- *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.*

> “Ideal introduction course for non technical senior executives.”
>
> Naomi Climer
> *President of The Institute of Engineering & Technology (IET)*

> “I was coming from a very low knowledge base and am not a "techie" so it was perfectly pitched to increase my awareness.”
>
> Susan Cordingley
> *Director of Planning & Communications, National Council for Voluntary Organisations (NCVO)*