ACCREDITED TRAINING PROVIDER

RISK REWARD
GLOBAL BANKING & FINANCIAL SERVICES EXPERTS

Managing Cyber Security

A 3-Day Training Event

As economies digitise so too do the threats facing them which can be seen in the unprecedented number of cyber-attacks against financial institutions and businesses of various sizes and across various sectors in recent years.

Course Objectives

This 3-day up-to-the-minute, real life case studies-driven course will provide delegates a critical overview of cybercrime, its threats and events, UK-, USA- and EU regulation, techniques for detection, prevention, intervention and mitigation for those in the financial services industry.

Who should attend?

This qualification is appropriate for
- Compliance Officers & staff
- Money Laundering Reporting Officers & staff
- Legal professionals
- Regulatory professionals
- Trade professionals
- those involved in bi-lateral development organisations
- civil society organizations
- charities
- CISI Candidates for the Investment Operations Certificate (IOC)

Our unique 3-day classroom training course features:

- Content-rich study materials
- Up-to-date and industry relevant case studies
- In-depth analysis of course topics
- Smaller class sizes which focus more on personal attention & expert-delegate interaction
- An experienced, expert practitioner-trainer with real industry track-record & available for delegate Q&A for up to 90 days to help in exam preparation following the course.

Methodology

The expert trainer will use slides, case studies, exercises and lead workshop-style group discussion to engage the delegates in practical learning and understanding. The trainer remains available to delegates for Q&A related to the course topic for 90 days following the course dates.

Advanced Preparation: ***None***
Training Type: ***Classroom***
Learning Level 3: ***Intermediate***
Field of Study: ***Financial Crime***

This training course is scheduled for:

London UK, 3 days
June 17 - 19, 2019
October 31 – November 02, 2019

The price per delegate for this 3-day programme is £3,145.00
(+ UK VAT when applicable)

1:1 training courses available at 2x per delegate price!

For an in-house training option, alternative dates and locations are available.
We are happy to add extra content to the programme to meet additional requirements from your company. Please contact us for further information.

www.riskrewardlimited.com

Risk Reward Ltd 47 Limeharbour, 2nd Floor, London E14 9TS, UK
Tel: +44 (0)20 7638 5558 CISI@riskrewardlimited.com UK Companies House # 434 6234.

Managing Cyber Security

Course Outline

Session 1: The Background and Nature of Information Security and Cybercrime

Definitions

- The difference between the Internet and the World Wide Web
  - The Deep Web
  - The Dark Web
- Cloud computing
  - Software as a Service (SaaS)
  - Hardware as a Service (HaaS)
  - Infrastructure as a Service (IaaS)
- Co-location
- Database structure
- Internet protocol (IP) addressing versions 4 and 6
- Domain Name servers
- Routers and gateways
- Data packets
- The Financial Conduct Authority (FCA)
- The definition of electronic money
- Information security

Distinctions

- How cyber security is distinct from information security
- Cybercrime and cyber-enabled crime

Fundamental issues of cyber security:

- Policies & Standards
- Identity & Access Management
- Threat & Vulnerability Management
- Outside Service Providers
- IT Risk Management

Technical Cybercrime attacks

- Types of network level technical Cybercrime attack:
  - Denial of Service (DoS) and distributed denial of service (DDoS)
  - Man-in-the-middle attacks (MitM)
  - Sniffing attacks
  - Session hijacks
  - Botnets
  - Malnets
  - Spam
  - Remote code injection
  - Structured query language (SQL) injection
  - Cross site scripting (XXS)
  - Format string vulnerabilities
  - User name enumeration

The most common types of technical Cybercrime attack at device level:

- Device intrusions / hacking
- Password cracks
- Physical key loggers
- In-built infections at point of manufacture or sale
- Device-sharing risks
- Device disposal and maintenance-related data breaches
- Device theft

The most common technical Cybercrime attach via peripheral devices:

- Bring your own device (BYOD) risks
- Removable media risks
- Printer risks

The types of technical Cybercrime based on application exploits:

- Application hacking
- Password cracks
- Code injection
- Malicious websites
- Drive-by downloads

The main types of technical Cybercrime arising from malware exploits

- Viruses
- Worms
- Trojans
- Spyware
- Rootkits

Attack Types

- Crypto-extortion attacks
- Web attack toolkits
- Data leakage and breaches
- Online frauds and other financially motivated eCrimes

The Human Element

The most common types of technical Cybercrime stemming from user-level issues:

- Errors and accidental disclosures
- Rogue insider
- Insider frauds
- Identity theft
- Phishing

- Pharming
- Physical intrusions
- Password sharing and weak passwords
- Self-provisioning

Social media risk in relation to Cybercrime:

- Social engineering ploys
- Identity theft
- Contact network analysis
- Blackmail
- Harassment
- Stalking
- Grooming
- Data breaches
- Reputational harm and brand damage
- Target acquisition and reconnaissance

Key desktop attacks and concealment techniques

- Search engine robots ploys
- Page source edits and hidden text
- Advanced online searching and reconnaissance
- LinkedIn, Facebook and Twitter searches
- Security & privacy vulnerabilities
- Image searching methods
- Mapping & geo-location vulnerabilities
- Reputational harm and brand damage
- Target acquisition and reconnaissance

Session 2 The Legislative Environment

Legal concepts

The key concepts influencing internet law:

- Net neutrality
- Free speech on the Internet
- Internet censorship
- Privacy expectations
- Intelligence services surveillance
- Responsibilities of Internet Service Providers (ISP's)

UK legislation

What are the offences created under the Computer Misuse Act (1990)

- Offence 1: accessing computer material without permission
- Offence 2: accessing computer material without permission with intent to commit further criminal offences
- Offence 3: altering computer data without permission
- The maximum penalties applicable to Offence 1, 2 & 3

The amendment to "unauthorised access" and the 2 additional offences defined in the Police and Justice Act (2006)

- Section 36: unauthorised acts with intent to impair operation of computer
- Section 37: making, supplying or obtaining articles for use in computer misuse offences

How the Fraud Act (2006) relates to Cybercrime

- Fraud by false representation
- The maximum penalty stipulated under the Fraud Act (2006)

How the Data protection Act (1998) relates to Cybercrime

The penalties that may be imposed for failing to comply with the 8 data principles

The core principles of the Regulation of Investigatory Powers Act (RIPA) with respect to communications meta-data and message content

Relevant international legislation

- How European Union (EU) data protection law relates to Cybercrime
- The key US regulation and guidance that relates to Cybercrime
    - Homeland Security Act (2002)
    - The DHS Critical Infrastructure Cyber Community (C-cubed) Voluntary Program
    - Electronic Communication Privacy Act (1986)
    - Privacy Act (1974)
    - Federal Information Security Management Act (2002)
    - Executive Order 13636, "Improving Critical Infrastructure Cybersecurity"

Session 3 The Public-Private Interface In Combatting Cybercrime

Law Enforcement agencies

- The role and activities of the UK and EU agencies
    - The National Crime Agency (NCA)
    - The Metropolitan Police Service (Met) & SO15
    - The City of London Police
    - Regional Police forces
    - Europol

Standards and best practice

- What is the purpose and content of the main international standards for Information security management
- The purpose and content of the UK government's (GCHQ) information assurance "Cyber Essentials" scheme
- the purpose and content of the UK Government Communications Headquarters (GCHQ) guidance entitled "10 steps to cyber security"
- The role of the European Network and Information Security Agency (ENISA)

The financial services industry

- The role of UK and EU Information Commissioners in relation to Cybercrime
- The obligations of financial services firms to the Information Commissioner
- The role of the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) in relation to Cybercrime
- 'Operation Waking Shark'
- The obligations of financial services firms to the FCA and PRA with regard to a Cybercrime event

Session 4 Cybercrime & The Financial Services Industry

Recognising the threat

The importance of financial services as a component of critical national infrastructure:

- Threats and impacts at national level
- Managing cyber dependencies
- National cyber security culture
- How financial services firms are exposed to various categories of cybercriminal
- Employees and contractors
- "Hacktivists" or single-issue extremists
- Hackers and Script Kiddies
- Fraudsters
- Nation states
- Organised crime networks
- Malware developers
- Software developers
- Social engineers

Known vulnerabilities

- The typical classes of Cybercrime vulnerability affecting networks of common applications (Apps) of database systems

Cybercrime detection

- How Firewalls are used to detect cyber-attacks and vulnerabilities
- How intrusion detection systems (IDS) are used to detect cyber-attacks and vulnerabilities
- How anti-malware applications are used to detect cyber- attacks and vulnerabilities
- how logging and reporting applications are used to detect cyber-attacks and vulnerabilities
- How penetration testing and vulnerability assessment methodologies are employed to detect cyber-attacks
- How other common data sources can be utilised to identify evidence of Cybercrime
  - Customer complaints
  - Suspicious transactions
  - Internet and website usage patterns
  - Customer device profiles
  - Employee turnover statistics

Session 5 Combating Cybercrime

Proactive Governance

The goals of information security governance:

- Scope and charter organisational and third-party relationships
- Key cyber security and information security risk metrics

The information security framework:

- Strategy
- Risk management processes
- Business impact assessments
- Policies and procedures
- Compliance
- Audit methodologies
- Testing and validation
- Training and awareness

The commonly accepted cyber security control frameworks:

- Control categories
- Baseline controls
- Strengths and methods
- Components and architecture
- Inventory management and control (configuration management databases)
- User profiles and privileges management and reviews
- Key metrics
- Reporting exceptions

Selected effective due diligence techniques for:

- Customers
- Employees
- Service providers

The impact of culture on cyber security for international business

Risk management

What are the additional measures financial services firms can take to manage the risk of Cybercrime originated or enabled by an employee:

- Raising awareness
- Improving the management of privileges for joiners, movers and leavers
- Classifying and segmenting data
- Embedding ethical practice in relation to data security
- Implementing whistleblowing procedures

The implications of Cybercrime for technological procurement

- Bespoke software development
- Standards of software development
- Supplier due diligence
- Hardware and software lifecycles, including disposal with respect to corporate social responsibility and the data protection principles

How to manage the risk of Cybercrime throughout the employee lifecycle

Stress Testing

- The application of penetration testing to different types of vulnerabilities
- The correct application of prepared planning and dry-run modelling
- How firms can measure, or predict, the impact of cyber-attack Incident response

Incident response

- The role of a computer emergency response team (CERT) or computer security incident response team (CSIRT)
- The concept of recovery time objectives (RTO)
- The components of an incident management procedure
- How to develop an incident management response plan

Business continuity

- The concept of business recovery and disaster recovery planning (DRP)
- The purpose of the FCA "Business Continuity Management Practice Guide"
- FCA requirements for business continuity (SYSC 13.8) and incident response

Session 6 Trends in Economic Crime Compliance

Emerging Threats

- The key sources of information on emerging vulnerabilities
- The concept of the "Internet of Things" (IOT)
- The evolution and use of big data analytics
- The specific threats relating to cryptocurrencies such as Bitcoin
- To unregulated payment models
- To mobile payment devices
- To Cloud computing
- To co-location
- The purpose and limitations of risk avoidance through Cybercrime insurance policies

Ethical Issues

- How the use of big data relates to FCA financial promotion rules and Treating Customers Fairly (TCF)
    - Informed consent
- Ethical search engine optimisation
- Fair usage policy
- Good online practice
- The balance between employee monitoring and employee privacy:
- The implications of Californian Law A.B. 1844

Course schedule:

Full day classroom training
09:30 – 17:00

ACCREDITED TRAINING PROVIDER

RISK REWARD
GLOBAL BANKING & FINANCIAL SERVICES EXPERTS

Managing Cyber Security

Registration & Payment details

Please mark **X** in the box and complete the form with BLOCK LETTERS

Dates:

☐ June 17 - 19, 2019 ☐ October 31 – November 02, 2019

Course Fee (per person):
GBP £3,145 (+ UK VAT when applicable)

Email*

First name*

Last name*

Job title / Position

Department

Company Name

Company Address

City

Postcode Country*

Telephone (direct)* Telephone (main)

Approving Manager

Training Manager

CISI Certificate & Diploma Candidates

Please register, purchase your CISI workbook and online learning tools, and arrange to sit the exam at a testing centre directly with the professional body via www.CISI.org.

☐ Please tick that box if you don't want to be subscribing to the Global Risk Update magazine.

Data Privacy & Update of Contact Details Risk Reward Limited is fully compliant with the Data Protection Act. The information you provide will be safeguarded by Risk Reward Ltd. We do not rent, sell or exchange your details to anyone without your consent. Your details are never given to third parties. If you wish to update your details, please email: info@riskrewardlimited.com with your OLD and NEW details. Please allow 10 days to see the changes take effect. Thank you.

Terms and Conditions All cancellations must be received in writing 20 working days prior to the start of the course with acknowledgement from Risk Reward. Course fees must therefore be paid in full if a cancellation occurs within 20 working days of the start of the course. We are always happy to welcome a replacement onto the course. Kindly send us written notification of your replacement by email, fax or telephone. Written cancellations received 20 working days or more before the start date of the course receive a full refund less a charge of 20%. For any written cancellation requests that reach us less than 20 working days before the event, no refunds will be given. Risk Reward reserves the right to the final decision if any dispute arises.

Copyright © 2002-2019 All rights reserved. Risk Reward Limited reserves the right to amend the course fees, terms, course agenda, speaker or venue should the need arise. All public courses are subject to demand.

Signature Date

Investment Operations Certificate (IOC)

Progressive study pathways options

For UK Candidates the IOC is achieved by passing any three of the following units*;

(* please note that the following list only contains the IOC courses that Risk Reward offers and not the complete selection, for the full list please visit www.cisi.org

Introductory

- **International Introduction to Securities and Investment**

Regulatory

- **UK Financial Regulation**

Technical

- **Risk in Financial Services**
- **Global Financial Compliance**
- **Combating Financial Crime**
- **Managing Cyber Security**
- **Operational Risk**