

Cyber Security Bootcamp

Establish And Maintain Protection Against Cyber Attacks



Led by **Steve Blais**

Key Benefits Of Attending:

1. **Identify** the cyber threats your organisation faces and the countermeasures against those threats
2. **Prepare** and maintain an effective security policy for your organisation
3. **Perform** security assessments and audits (using methods such as penetration testing) of the organisation's processes, technologies, communications and perimeters to determine the vulnerabilities
4. **Review** the latest threats (including ransomware) and what your organisation can do to fight them
5. **Design** security architectures that will protect your organisation and prevent cyber attacks

22 – 25 October 2018*

Conrad Hotel, Dubai, UAE

OFFER

3 FOR 2

Save up to **\$1000**
by booking early!

Cyber Security Bootcamp

22 – 25 October 2018* | Conrad Hotel, Dubai, UAE

Course Timings

Registration will be at 08:00 on Day One. The course will commence at 08:30 and conclude at 14:30. There will be two breaks for refreshments and lunch will be served at the end of each day's sessions.



Corporate Member

The CPD Certification Service

About CPD

Established in 1996, The CPD Certification Service is the independent CPD accreditation centre working across all sectors, disciplines and further learning applications and supports policies of institutional and professional organisations globally.

CPD is the term used to describe the learning activities professionals engage in to develop and enhance their abilities and keep skills and knowledge up to date. This course is an accredited Continuing Professional Development (CPD) training which means it meets CPD standards and benchmarks. The learning value has been scrutinised to ensure integrity and quality.



Course Overview

Securing your organisation from those who wish to harm or steal from your business has never been more critical. As the Internet evolves and reaches into more and more of our everyday lives, there are more opportunities for criminals and others to invade our organisations and wreak havoc.

This course provides an intensive, interactive exploration of the potential dangers lurking in the connected world and the methods to protect your organisation from those dangers.

Course Methodology

This is a highly interactive course that will use a case study organisation. Participants will work individually and in groups to perform the course exercises using the case study organisation.

Course Assessment

Assessment will be ongoing and based on class participation.

Course Outline

Day One

Surveying The Cyber Threat Landscape

- What are the threats?
- Threat classification: interception, modification, masquerade, Denial-of-Service (DoS)
- What are the countermeasures?
- Standard threats to the organisation
- New threats to the organisation: ransomware, "hacktivism", data leakage, cyber espionage
- New organisational security risks: cloud storage, Everything-as-a-Service (XaaS), virtualisation
- Mobile security: wireless access, mobile phone hacking and security, public Wi-Fi availability
- Other security risks: phishing, social engineering, Internet of Things (IoT)

Exercise: Determine general threats

Exercise: Define the threats for case study organisation

Day Two

Security Concepts And The Security Policy

- Security stances
- The security model
- The security formula
- Security policies considerations: depth, breadth, enforcement, application, circulation
- Areas of concern: networks, perimeters, main storage, backups, end devices, remote devices
- People in the policy: who writes it, who implements it, the roles defined by the policy
- Creating a security policy

Workshop: Create a security policy for the case study organisation

Moving From Policy To Protection

- Threat analysis
- Risk analysis
- Define countermeasures
- Determine implementation
- Review results and adjust

Workshop: Perform threat analysis for case study organisation

Workshop: Perform risk assessment for case study organisation

Workshop: Define countermeasures for case study organisation

Workshop: Incorporate results into security policy

Day Three

Security Architectures That Will Prevent Or Protect

- Authentication approaches: passwords, biometrics
- Access approaches: firewalls, perimeter protection
- Authorisation approaches: encryption, digital signatures, certificates
- Availability approaches: virus protection, IDS (Intrusion Detection System) and IPS (Intrusion Prevention System)

Workshop: Design a security architecture for the client server organisation

Workshop: Revise the security policy to include security architecture

Verifying The Protection

- Security auditing: legal implications, ethical implications, technical implications
- Security testing: penetration testing, social engineering, ethical hacking

Workshop: Revise security policy to include verification and audit

Day Four

Future-proofing The Organisation

- IoT in the organisation
- Mobile security
- "Digital bombs" and ransomware
- Cyber warfare, hacktivism and espionage

Workshop: Add strategic policies to the security policy

Conclusion

- Best practices in security policy
- Best practices in security procedures

Who Should Attend

- Cyber Security Engineers, Specialists, Analysts, Architects, Officers, Managers, or Directors
- Information Security, Information Technology/IT Security, or Business Security: Personnel, Officers, Engineers, Specialists, Analysts, Architects, Executives, Associates, Consultants, Managers, or Directors
- Systems Administrators, Network Architects or Engineers, (Forensics) Investigators, Auditors, Strategists, Systems Engineers or Integrators, and Technology Evangelists
- Software Developers, Project Managers, General Managers and others involved in the creation, maintenance, or enforcement of the organisational cyber security policy, practices and procedures
- Anyone who needs to understand the implications of cyber security on their technology and overall business operations

Meet Your Expert Course Director



Steve Blais, PMP, PBA, is a Consultant, Author, Teacher and Coach who has nearly 50 years of experience in Information Technologies. He has worked as an IT Security Analyst, System Analyst, Programmer, Tester, and Business Analyst. He worked on the first cyber security plan

for a US Federal agency in the early '90s, and has since been in an executive position for several start-up companies, including acting as Chief Security Officer.

He writes a monthly column for Business Analyst Times and is a frequent contributor to AllpM.com, Modern Analyst and other publications. He has presented the keynote addresses at the PMI PacRim Conference in Tokyo (2012), PMI South America in Sao Paulo (2011), IPMA European Conference (2013), and many other conferences around the world. He is also the author of *Business Analysis: Best Practices for Success* (John Wiley, 2011) and co-author of *Business Analysis for Practitioners: A Practice Guide* (PMI, 2014) and a contributor to *A Guide to the Business Analysis Body of Knowledge®*, V3 (IIBA, 2015).

Read what past delegates said about Steve's courses:

"[Steve is] well experienced and [offered] a lot of practical tips."

Kameswara Shastry, Infrastructure Architect,
Community Development Authority, UAE

"Good presentation skills and pace, with practical examples. The trainer helped a lot to clear our doubts and ambiguities regarding [IT] Security."

Syed Faraz Hassan Zaidi, Senior Internal Auditor,
Dubai Electricity and Water Authority (DEWA), UAE

Would you like to run this course in-house?

customised training solutions

The in-house training division of Informa


Tel: +971 4 407 2624 Email: cts@informa.com
www.informa-mea.com/cts

Cyber Security Bootcamp


22 – 25 October 2018* | Conrad Hotel, Dubai, UAE

FOUR WAYS TO REGISTER

 +971 4 335 2437

 +971 4 335 2438

 register-mea@informa.com

 Informa Middle East Ltd.
PO Box 9428, Dubai, UAE

customised training solutions
The in-house training division of Informa Middle East

SAVE UP TO 40%

If you have 6 or more people interested in attending, and would like to customise this training course to suit your team and business, contact our **Training Consultants** on **+971 4 407 2624** or email **cts@informa.com**.

Course	Course Fee Before 13 August 2018	Course Fee Before 17 September 2018	Final Fee
Cyber Security Bootcamp 22 – 25 October 2018*	US\$ 3,995	US\$ 4,495	US\$ 4,995

Pricing excludes 5% VAT, which will be charged where applicable

*Book and pay full fee for two colleagues and the third attends for FREE.

Not applicable in conjunction with corporate discounts.

Payment to be settled before start of the course to avail the offer.

The 3 for 2 offer is valid on full price final fee registration only.

DISCOUNTS AVAILABLE FOR 2 OR MORE PEOPLE

CALL: +971 4 335 2483
E-MAIL: a.watts@informa.com

Course fees include documentation, luncheon and refreshments. Delegates who attend all sessions will receive a Certificate of Attendance.

All registrations are subject to our terms and conditions which are available at www.informa-mea.com/terms. Please read them as they include important information. By submitting your registration you agree to be bound by the terms and conditions in full.

DELEGATE DETAILS

First Name: _____ Surname: _____

Job Title: _____

Company: _____

Address: _____

Postal Code: _____ Country: _____ City: _____

Tel: _____ Mobile: _____ Fax: _____

Email: _____

PAYMENTS

A confirmation letter and invoice will be sent upon receipt of your registration. Please note that full payment must be received prior to the event. Only those delegates whose fees have been paid in full will be admitted to the event.

AVOID VISA DELAYS – BOOK NOW

Delegates requiring visas should contact the hotel they wish to stay at directly, as soon as possible. Visas for non-GCC nationals may take several weeks to process.

CANCELLATION

- If you are unable to attend, a replacement delegate will be welcomed in your place. If you cancel your registration 57 days or more before the event, you will receive a refund minus a 10% cancellation fee (plus VAT where applicable). Cancellation after 56 days before the event or if you fail to attend the event will be 100% payable. All cancellations must be sent by email to register-mea@informa.com marked for the attention of Customer Services Cancellation.
- All registrations are subject to acceptance by Informa Middle East which will be confirmed to you in writing.
- Due to unforeseen circumstances, Informa reserves the right to cancel the course, change the programme, alter the venue, speaker or topics.
- For full details, please visit www.informa-mea.com/terms-and-conditions-for-delegates

EVENT VENUE:

Conrad Hotel, Dubai, UAE
Tel: +971 4 444 7444

ACCOMMODATION DETAILS

We highly recommend you secure your room reservation at the earliest to avoid last minute inconvenience. You can contact the Hospitality Desk for assistance on:
Tel: +971 4 407 2693 Fax: +971 4 407 2517
Email: hospitality@informa.com

HK/LM

IT

© Copyright Informa Middle East Ltd



BC7211