Asia Masters Center

Introduction to Information Security

Asia Masters Centre (AMC), Suite 2 B, level 6, Office Block, Grand Millennium Hotel, Bukit Bintang Street,
55100 Kuala Lumpur, Malaysia. | Tel: +60327326992|Mobile: +601 8909 0379 | Fax: +60327326992
Website: http://www.asiamasters.org/ | Email: info@asia-masters.com

Introduction to Information Security

Course Objective

- select appropriate techniques to tackle and solve problems in the discipline of information security management
- understand why security and its management are important for any modern organisation
- understand how an information security management system should be planned, documented, implemented and improved, according to the BSi standard on information security management.

Target Audience

- This course is designed for students who have a basic knowledge of computers and technology but no prior knowledge of cyber security. The hands-on, step-by-step teaching approach will enable you to grasp all of the information presented even if some of the topics are new to you. You'll learn the fundamentals of information security that will serve as the foundation of your InfoSec skills and knowledge for years to come.

Course Outline

- **Day 1**
- Security's Foundation
- Overview
- Every good security practitioner and every good security program begins with the same mantra: learn the fundamentals. SEC301 starts by instilling familiarity with core security terms and principles. By the time you leave the classroom after the first day, you will fully understand the Principle of Least Privilege and the Confidentiality, Integrity, and Availability (CIA) Triad, and you'll see why those principles drive all security discussions. You will be conversant in the fundamentals of risk management, security policy, authentication/authorization/accountability, and security awareness training.
- Exercises
- Lab 1 – Introducing the www.sec301.com Website: Establish a user account on that site to use in later labs (access to the site also provides access to lab videos that walk you through all of the labs).
- Lab 2 – Building Better Passwords: We'll use a tool that shows how long it takes to compromise various passwords via a brute force attack.

- **Day 2**
- Computer Numbers and Cryptography
- Overview
- This course day begins with an explanation of how computers handle numbers using decimal, binary, and hexadecimal numbering systems. It also provides an understanding of how computers encode letters using ASCII (American Standard Code for Information Interchange). We then spend the remainder of the day on cryptography – one of the most complex issues faced by security practitioners. It is not a topic you can explain in passing, so we will spend some time on it. Not to worry, we won't take you through the math behind cryptography, but we'll look at basic crypto terminology and processes. What is steganography? What is substitution and transposition? What is a "work factor" in cryptography and why does it matter? What do we mean by symmetric and asymmetric key cryptography and "cryptographic hash", and why do you need to know? How are those concepts used together in the real world to create cryptographic systems?
- Exercises
- Lab 3 – Crypto by Hand: Apply the knowledge and skills you've learned to encrypt information using mono and poly alphabetic ciphers and gain a better understanding of triple encryption (as used by Triple DES).
- Lab 4 – Visual Crypto: Observe the encryption process that occurs by turning plaintext (what you can read) into cyphertext (what you cannot read) in real time. Increase your understanding of what "randomness in cyphertext" really means and why it matters. See the cyphertext turned back into plaintext.

- **Day 3**
- Networking and Network Security
- Overview
- All attacks or exploits have one thing in common: they take something that exists for perfectly valid reasons and misuse it in malicious ways. Always! So as security practitioners, to grasp what is invalid we must first understand what is valid – that is, how things like networks are supposed to work. Only once we have that understanding can we hope to understand the mechanics of malicious misuse of those networks – and only with that knowledge can we understand how security devices such as firewalls seek to thwart those attacks. Day three begins with a nontechnical explanation of how data move across a network. From there we move to fundamental terminology dealing with network types and standards. You'll learn about common network hardware such as switches and routers, and you'll finally grasp what is meant by terms like "protocol" and "encapsulation". We'll give a very basic introduction to network addressing and port numbers and then work our way up the Open Systems Interconnection (OSI) protocol stack, introducing more detail only as we proceed to the next layer. In other words, we explain networking starting in non-technical terms and gradually progress to more technical detail as students are ready to take the next step. By the end of our discussions, you'll have a fundamental grasp of any number of critical technical networking acronyms that you've often heard and never quite understood: TCP/IP, IP, TCP, UDP, MAC, ARP, NAT, ICMP, and DNS. We will close out our day learning how to secure those networks using firewalls, intrusion detection systems, intrusion prevention systems, and others.

- Exercises
- Lab 5 – Networking: Use several network tools that are built into the Windows Operating System or the Mac Operating System to determine your network settings, and discover if Network Address Translation (NAT) is being used inside the classroom.

- **Day 4**
- Host Security
- Overview
- Our fourth day in the classroom is devoted primarily to securing host computers and similar devices. We begin with wireless network security (WiFi and Bluetooth), and mobile device security (i.e., cell phones). We follow that with a brief look at some common attacks. We then move into a discussion of malware and anti-malware technologies. From there we move into several data protection technologies and look at email encryption, secure remote access, secure web access, secure file transfer, and Virtual Private Network technologies. We will then look into the basics of securing endpoint computers via Operating System hardening, patch management, and application security. Of course, we spend some time on the critical topic of backups as well. We end the day with a look at web and browser security, one of the most common attack vectors.
- Exercises
- Lab 6 – Phishing IQ Quiz: Use an online site to look at several potential spam messages and determine which are legitimate and which are not. Students will see the results of their quiz with an explanation of why each message is either legit or spam.

- Lab 7 – Validating Browser Security: Use a tool that scans your browser and browser plugins to determine if they are up to date and secure. If they are not, the tool will also help you to fix those problems.

- **Day 5**
- Protecting Assets
- Overview
- The final day of our SEC301 journey is all about protecting assets, mostly with a physical security theme but with some logical security included as well. We begin with the "meta security" discipline of operations security that looks at security issues throughout the organization, not just in the IT area. We then introduce the topic of safety and physical security. Students will become familiar with the concepts of data classification and data loss prevention. From there we move to an introductory look at incident response, including business continuity and disaster recovery planning. We'll close out with a brief discussion of social engineering so that students understand what it is and why it's so difficult to defend against.
- Exercises
- Global Information Security Fundamentals (GISF) Practice Exam: We end the course with an (optional) truncated GISF practice exam. We'll go through 20 exam questions together and answer them as a group, giving students an idea of the types of questions they might see on the real exam. We'll focus on some of the tougher questions students might struggle with.
- Optional Advanced Labs

- Three optional advanced labs are available to students in the lab workbook. These labs require administrative access on Windows computers:
- LastPass – A password management utility
- MalwareBytes – A malware scanning utility
- SyncBack – A backup and file synchronization utility
- These are not testable for the GISF exam, but are provided for advanced students looking for more of a hands-on challenge.

➢ The Feature Of Asia Master Training And Development Center

- we pick up the customer from the airport to the hotel.
- we give the participant training bag includes all the necessary tools for the course.
- Working within groups to achieve the best results.
- All our courses are confirmed and we do not postpone or cancel the courses regardless of the number of participants in the course.
- We can assist you in booking hotels at discounted prices if you wish to book through us.
- We offer the certificate from Asia Masters Center for Training and Administrative Development.

➡ The Cost Of The Training Program Includes The Following:

1) Scientific article on flash memory.
2) Training Room.
3) Training.
4) Coffee break.
5) The training bag includes all the tools for the course.

Price (USD)
Communicate with the training department to know the participation fees ➢ There are offers and discounts for groups
<u>The details of the bank account</u>
Bank name: CIMB Bank Berhad Account name: Asia Masters Center SDN. BHD Bank account number: 80-0733590-5 Swift code: CIBBMYKL IBAN: Null