SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Cyber-Security Executive Foundation 2-day course (Including a look at FinTech cyber-security and a Hacking Demo)

Cyber-security is not always about esoteric, scary, big-heist cases like what we see in the media reports and in movies, though such a likelihood is not zero. But cyber-security is not always about the bad guys, hackers or malware. Neither is it about technology. There is a clear human factor as well (hence the concept of "social engineering").

How and why do they succeed in breaking into our network and/or spilling our data in the first place? Are we missing something or doing something to inadvertently let them? We can never be 100% secure (short of cutting the electricity or signal) but we need to go about our business, so how do we best achieve optimal balance between security and productivity, by having a baseline cyber-security posture, hygiene and governance. What do we look out for to do so?

The second half of Day 2 of the course treats the participants to a live demo of some of the hacker's typical tricks and techniques, on some of the various IT domains, eg, network and applications, beginning with various information-gathering and reconnaissance processes. The purpose is to make the course participants aware of such risks so as to try to minimise them. (It's not all about technology.)

Objective, knowledge & understanding, key skills to be gained & participants' requirements

This 2-day course is built for business and work officers and tertiary-level students who do not have the time or interest to attend a 40-hour technical or certification cyber-security program, but would appreciate a comprehensive, real-world, high-level and policy view of various domains and issues of an organizational IT infrastructure, some idea of where our risks and pitfalls lie, and various practical risk mitigation solutions and best practices.

No cyber-security or advanced IT knowledge is required as a prerequisite, though basic IT knowledge and that of an organization's IT infrastructure and operations would be helpful, though not compulsory.

As our internet world and life becomes increasingly inter-connected over time, and with faster lines, more powerful devices, more services and more powerful ones, it appears that the cyber-security issue correspondingly does not seem to get any better. We need to focus on our business and work, instead of trying to play cyber-cop.

We need in place a succinct yet comprehensive base reference level of knowledge and awareness, but without having to become technical geeks (not today), so as to help maintain the cyber-safety and governance posture of our respective organizations and communities. This course offers a comprehensive high-level overview of the various aspects and domains of cyber-security, some key solutions, and why we continue to fall prey to hackers.

The majority of hacking and malware attacks occur opportunistically and randomly, as opposed to targeted. Most of the time they succeed because of some innocent, non-malicious human mistake akin to leaving a door or window open, or an inherent weakness that a hacker or virus finds and exploits to come into the organization's network and steal data or compromise services.

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Topics / Course Agenda

Day 1

Time	Agenda
Day 1	
09:00 – 09:15	2-Day Course Overview
09:15 – 10:30	Introduction to key cyber-security concepts, mantra, domains, issues; (its not always about the bad guys, its not always about technology)
10:30 – 11:45	Break
11:45 – 11:30	Building the CIO view of the enterprise IT infrastructure
11:30 – 12:30	Some Basic cyber-security solutions
12:30 – 14:00	Lunch
14:00 – 15:00	A look at policy, audit, standards, frameworks
15:00 – 15:30	A look at SG-PDPA and Data Security
15:30 – 15:45	Break
15:45 – 16:30	Web application & mobile app security
16:30 – 17:15	Cloud security
17.15 – 17.30	Wrap-up, recap, Q&A
Day 2	
09:00 – 09:30	Recap from Day 1, Q&A
09:30 – 10:30	FinTech cyber-security considerations
10:30 – 10:45	Break
10:30 – 11:45	Block-chain cyber-security considerations
11:45 – 12:30	Course Assessment
12:30 – 14:00	Lunch
14:00 – 15:30	Hacking – live demo * operation system and network * inherent weakness of Microsoft Windows
15:30 – 15:45	Break
15:45 – 17:00	Hacking – live demo * web applications and mobile apps
17:00 – 17:30	Wrap-up, recap, Q&A

Duration: 2 days

Venue: Singapore University of Social Sciences (formerly known as SIM University)

Minimum number to run: 25 participants

Certificate of participation is awarded upon 75% attendance for the course
(As the university was renamed recently on 17 March 2017, we will be reprinting our course certificates to incorporate the new name and logo. As such, you will receive your certificate at a later date.)

SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

Trainer's Profile

Anthony Lim is pioneer and veteran in the Asia Pacific cyber-security space, with over 20 years' professional experience as a business leader, advocate, consultant, auditor and instructor. He has helmed inaugural Asia Pacific security business units at IBM, CA Technologies, Check Point and a few other US vendors. He has been involved in building, advocating and teaching of two international professional technical certifications (for application development security and cloud security), helped build and teach professional and academic program modules for cyber-security management and policy for some higher education institutions, and conducts trainings for staff of government, financial and other organizations, in Singapore and the region.

Anthony is a long-time well-known speaker, instructor and content provider for many business, industry, government and academic conferences, workshops, courses, executive roundtables, committees and media (print, broadcast, internet). He is interviewed often in press and TV news (including CNBC and BBC), and has presented at Stanford, TsingHua, NATO, Washington DC and ITU seminars, on associated matters like IT policy, governance, smart cities and cloud securities.

He also holds an MBA, ITIL certification, 3 other international technical cyber-security professional certifications and is an ISO-27001 lead auditor. He is a life alumni member of the University of Illinois, Urbana-Champaign. Anthony is a Singapore Director of international non-profit NGO Cloud Security Alliance and a Principal Consultant for Asia Pacific for American security solutions vendor Fortinet Inc.