NUS National University of Singapore

Strategic Technology Management Institute
School of Computing

Modern Cyber Security Technologies for Senior Managers

www.stmi.nus.edu.sg

COURSE OVERVIEW

This course updates senior cyber security professionals in an urgent and compact manner on all key cyber security developments, e.g. how the landscape has changed very quickly and which would be the best solution to attack the many "hot" and pressing problems that the organisation is now facing. By making sense of new trends and attack incidents that often appear confusing, it creates Eureka moments to resolve conflicting requirements with urgent deadlines via a methodology that makes the complex easy to understand. More importantly, it explains how the implementation strategy could be quickly internalised, communicated and then converted into fast action. Its powerful narrations will highlight the new types of cyber security opportunities, exposing many such well kept secrets. Interestingly, many are with almost no cost. A key take-away will be its comprehensive coverage of all strategic transformations in the cyber security industry today, e.g. the need for automation, non-signature defences, the rise of cloud security and Docker containers, big data security, mobile security, new cryptography and new hardware like Intel's security instruction sets and GPUs.

Duration
3 days

Course Fee
$2407.50 (incl. GST)

Venue
STMI@NUS
ICube, Level3
21 Heng Mui Keng Terrace
Singapore 119613
stmi@nus.edu.sg

Contact Us
Tel: +65 6601 1040
Fax: +65 6776 2856
Email: stmi@nus.edu.sg

WHO SHOULD ATTEND

The course is for Chief Information Security Officers, Chief Information or Chief Data Officers and those who are senior cyber security professionals, e.g. security consultants, architects and designers, product developers and integrators, requiring a highly condensed technology refresh and an update of the latest cyber security technologies, now ready and available for urgent problem solving.

PRE-REQUISITES

3 years of cyber security experience and 3 years of infocomm background

PROGRAMME BENEFITS

The course addresses continual learning and the shortfall in knowledge and experience regarding latest developments, as many busy executives have been struggling to keep up with new solutions and the high complexity of today's digital revolution. Critically, it provides key insights and advice for practical and much needed problem solving, which will build up confidence for decision making. This will protect the organisation from the menace of organised cyber crime and advanced state attackers, avoiding massive losses or even company closure when successfully attacked (no longer if, but just when). By providing guidance on the latest or pending future products, a large part of the cyber security expenditure will be saved or the money will be better spent. In addition, it helps the student to communicate the urgency required, not only when in crisis but also in everyday planning.

TOPICS COVERED

- Introduction to the latest developments and its DNA
- New forms of cyber attacks
- The offensive industry, how new cyber weapons are emerging
- Biggest shortfalls and gaps when defending
- What the enemy fears most and their greatest weaknesses
- Key Trends for problem solving
- Cyber Security automation, AI and Deep Learning
- Cost Improvements and Project Operationalisation Strategy
- New Cryptography and its latest problem solving
- Security for collaboration systems
- Big Data security
- Isolation technologies such as data diodes, RDP etc.
- Mobile Security and BYOD
- Hybrid Cloud
- Managing Shadow IT
- Critical Infrastructure security and IoT
- Improvements in point solutions:
  - ◊ Anti-leakage
  - ◊ Anti-Exploit (signatureless anti-malware)
  - ◊ Whitelisting
  - ◊ Win10 security
  - ◊ Data Diodes
  - ◊ New Biometrics
  - ◊ Patching
- Liquid Defence Framework that is agile and self-organising
- Defeating Advanced Attacks and getting the Board to know this
- How to develop own capabilities to better exploit the industry providers
- Smart Spending

SPEAKER

Prof Yu Chien Siang

Prof Yu Chien Siang is the Chief Innovation Officer (CIO) of Certis Cisco and previously, of a department in the Ministry of Home Affairs. Prior to this, he was the most senior Computer Security Consultant at the Singapore government. He was awarded the Carl Duisberg Gesellschaft Scholarship to pursue his studies at a German university and graduated as a Data Systems Engineer. During his study, he received training at the Siemens Research Laboratory and IBM R&D Laboratory in Boblingen. He has been working in the Civil Service since 1981 and was awarded National Day Honours, the Public Administration Medal (Silver) in 1993 and (Silver) Bar in 2004.

He has been active in the fields of IT leadership, innovation development and its related cultural transformation and IT Security for more than 30 years. During this time, he led numerous national-level IT projects in information security such as the Electronic Road Pricing (ERP), Standard Operating Environment (SOE) etc., IoT security via the ANSES project and homeland security, developing workflow and people identification operational systems. He was instrumental in evolving many advanced systems architecture used in the public service and the fundamental mechanisms required for their large systems rollout. He invented unique low cost smart card readers, strong cryptographic systems, more efficient protocols and fault tolerant designs.

In addition, he teaches the course on "Introduction to Cyber Crime", but now renamed as "Introduction to Cyber Security" in his capacity as Adjunct Associate Professor at the Department of Mathematics of the National University of Singapore. He was an ex-President of the Singapore Microcomputer Society, a pioneer in the exploitation of microcomputers and a regular speaker at government events, being the founder of the Governmentware show. He has also been one of the judges for the RSA Innovation Sandbox since 2014. He is currently a member of ITSC, worked on ISO security standards and was involved in the early days of the AISP.