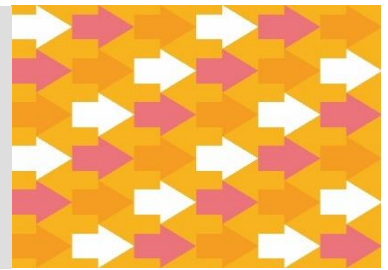




Cybersecurity for Non-CS Professionals



Next run:
Coming soon!

Time:
9am – 5pm

Venue:
PwC Singapore Office
(seminar room)

Objectives

Understand cyber risks and the pre-emptive practical measures to protect your organisational assets.

Benefits of attending

Cybersecurity isn't just about technology – it involves people, information, systems, processes, culture and physical surroundings. The key aim is to create a secure environment where businesses can remain resilient in the event of an attack. At the end of this course, you will walk away with:

- An understanding of the potential cyber attacks and preventive measures for your organisation
- Knowledge of an effective cybersecurity strategy and programme

Who should attend?

Business Directors, Management or Managers who wants to learn more about cybersecurity

*Prior knowledge of cyber security and/or IT is not required.

Key highlights

Live hacking demonstration

You will witness first-hand, a “live” hacking exercise conducted by our PwC Cyber Security experts – where it will highlight the importance of securing your data.

Game of Threats

You will get the opportunity to participate in our PwC proprietary virtual game, designed to simulate the speed and complexity of an actual cyber breach. The solution integrates elements of gamification and game theory to provide an interactive client experience where a client team playing itself tries to defend itself from a of threat actors team. For more information, please refer to

<https://www.pwc.com/us/en/industries/financial-services/cybersecurity-privacy/game-of-threats.html>



Workshop agenda

Cyber Resilience: Day 1

- Global trends in cyber security protection
- Cyber Security Architecture
- Insights into possible failures of BCM
- IT governance of Cybersecurity
- Cybersecurity and privacy strategy components
- Strategy development vs maturity assessment
- Cyber risk assessment
- Common risks and system vulnerabilities
- *Activity*: Conducting a cyber risk assessment
- Global trends in cyber security regulatory requirements
- Compliance with relevant regulator requirements
- IT security processes and procedures
- *Activity*: Effective cyber security policies and procedures

Cyber Resilience: Day 2

- Threat management concepts and terminology
- The importance of threat management to client organisation's
- Threat modelling methodology and set Incident Response KPI's
- Assessment of the business impact of the identified threats and formulate possible responses
- Component of Cyber resilience
- How to make action plan of identified control GAP
- Game of Threats

What did past participants say?

"It (PwC) explains to them through the game what a denial-of-service attack is, what a penetration test is and it just takes them through the terminology while they interact with it – it's a powerful learning tool." Telstra's Mike Burgess

"You get fast-paced gameplay that mimics the stress of a real-life data breach." CNN Money

"'Game of Threats' Teaches Executives Cyber Readiness Through Game Play" The Wall Street Journal

How to register

For any further queries, please email sg_academy_mailbox@pwc.com

