The adage that there are only two types of companies – those who have experienced a breach, and those who do not realise they have been breached – is very true. So, how do Senior Executives and Organisational Directors take the appropriate actions to defend their shareholders?

Data breaches and malicious attacks from both external and internal sources continue to be the highest priority for senior executives and organisational boards. They reinforce three facts. First, the protection of critical company and customer data is essential to protect revenue, reputation and enterprise value. Second, attacks against customer/employee information or intellectual property are being directed at all sectors of the Australian economy. Finally, even the best programs will experience failure and expose some information the company would like to protect.

ABOUT THE WORKSHOP

Bringing together world leading experts, this one-day workshop will cover an overview of what’s happening out there and provide the knowledge and frameworks to help you execute your obligations. The University of Queensland Australian Leadership Cybersecurity Workshop will cover the most significant and wide-spread threats facing IT today, with real-world examples and responses illustrating steps and precautions you can take to keep your enterprise on top of current and emerging threats. Cyber-security is NOT just a technology question. It is a cross-functional issue that must be addressed at the CEO/Board level and made a part of critical business decisions.

PRESENTERS

This workshop will be presented by two world renowned experts. Colonel Jeff Arsenault, the former head of the “ethical hacking team” of the US National Security Agency, and Dr Paul Twomey, former CEO of both ICANN, the body responsible for coordinating the global Internet, and the Australian National Office for the Information Economy.

WHAT WILL YOU EXPERIENCE?

A Live Demonstration of how a Skilled Hacker Penetrates an Enterprise. Witness technical demonstrations of what an attack actually looks like and how easy it is to move around inside an organisation and steal data.

Observe how a hacker can:

- Open Source Research (how to find out about your target using free resources)
- Finding credentials for sale on the Dark Web
- Phishing/Spoofing to get into the network
- Escalating through Access Privileges
- Moving Laterally throughout a computer network
- Data Identification
- Data Exfiltration.

Along with each of these steps you will also gain insight into how to detect such activity from the defender’s point of view.

Plus, with the experts, work through a Risk Management Framework which seeks to optimize the limited resources of every enterprise has for cyber security. The reality is that Enterprise leaders shape their cyber opportunities and risks. You must balance openness, innovation, privacy, security & safety down to data assets, people and process level.
WHAT YOU’LL LEARN

• The old model of leaving security to the IT team is dead — Corporations have to adopt approaches to cyber-security very different from the ones used to date in order to protect business information and systems without slowing business innovation and growth.

• The Data Revolution is increasing risk — As well as traditional Intellectual Property, corporations looking to mine data – transaction and customer information, results of product launches, market information – create valuable IP that is also an attractive target for cyber-criminals. Corporations are finding new ways to interact with their customers, agents and counterparties, performing customer care online and providing an ever-richer set of digital services. As a result, access points onto corporate networks are multiplying. Today’s organizations are more networked with vendors and partners than ever before, requiring them to share a wide variety of valuable data and intellectual property, often in real time. Outsourcing functions to a vendor does not mean that the risk or the liability goes away – a business’s supply chain is only as secure as its most vulnerable link.

• Malevolent Actors are increasingly sophisticated: Disgruntled employees, “hactivists,” organised criminal enterprises and, in many cases, state actors can tap a growing arsenal of techniques and tools.

• The Best take a Data-centric and Risk Management Approach — Businesses need to start by identifying the most valuable intellectual property and information assets to protect, and then developing a strategy that aligns the level of protection against the risk. The most sophisticated organisations are beginning to model the “value at stake” in cyber-attacks to make better trade-offs – they classify data by criticality and apply different tools and access policies based on criticality. In some cases, cybersecurity also represents a business opportunity, as corporations find ways to create end-to-end customer experiences that are both convenient and secure.

• Cybersecurity is not a problem to be “solved;” rather, it’s an ongoing battle — The threats are evolving rapidly, along with technology and business processes. New digital assets and mechanisms for accessing them simply mean new types of cyber-attacks. In addition to evolving security, corporations need to conduct realistic, cross-functional simulations of cyber-events in order to surface unexpected vulnerabilities and build organisational capability for managing a fast-moving situation.

CONTACT

Email: cpd@eait.uq.edu.au
Web: www.eait.uq.edu.au
ABN: 63 942 912 684

REGISTRATION DETAILS

Dr Mr Mrs Ms           First name_________________________  Last name_________________________

Organisation_________________________

Address_________________________

Phone_________________________  Email_________________________

I have dietary requirements. Details__________________________________________

☐ Please add my contact details to the ITEE CPD enews so I can receive updates on upcoming events.