OPTUS

MACQUARIE University

Awareness and training programs

OPTUS MACQUARIE UNIVERSITY CYBER SECURITY HUB

In today's digital world, safeguarding data, intellectual property, financial information and your company's reputation is a crucial part of business strategy.

Yet, with the number of cyber threats and the sophistication of attacks increasing, it's a formidable challenge, too.

Boards and executives acknowledge cyber security is no longer a matter for the IT department alone. With an estimated 60 per cent of attacks – malicious and accidental – carried out by insiders, an effective response to cybercrime relies on developing a whole-of-business awareness. This includes education at all levels – from the board to every employee.

The best way to achieve a lasting improvement in information security is not by throwing more technical solutions at the problem – it's by training and educating everyone who interacts with computer networks and systems, and by providing information about the basics of information security to all employees.

THE IMPORTANCE OF CYBER SECURITY AWARENESS TO YOUR BUSINESS

Security culture starts at the top, and boards and executives need to have the right knowledge to lead effectively.

What people do or don't do is the number-one source of cyber breaches. Developing good practice is the best way to prevent loss.

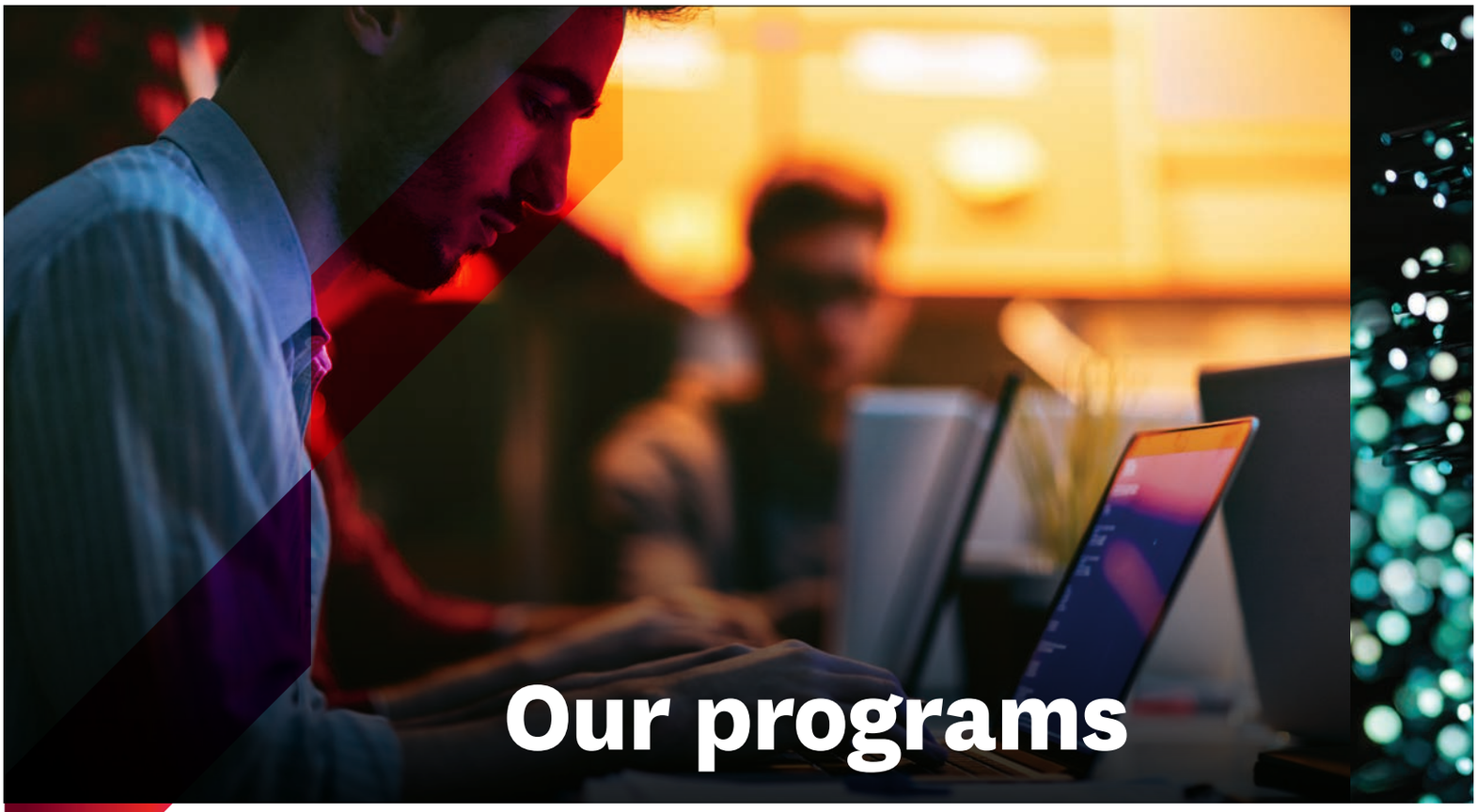
Security can't be guaranteed. We need to understand the risks and prepare ourselves to defend them. Preparation begins with understanding.

Awareness isn't just a good idea; it's the law. The Notifiable Data Breaches Bill passed in February 2017 requires businesses to notify individuals and government of any data breach that may result in serious harm.

OUR APPROACH

Our programs are:

- Tailored – our courses are designed to suit the needs of C-suite executives, technical teams, managers and all employees
- Integrated – as a suite of courses, we provide a single framework which enables all employees to speak the same language across the whole organisation
- Multidisciplinary – we provide a holistic perspective that draws on our expertise in technology, business, risk, legal and human factors
- Customised – we can tailor what we cover, how deeply and the length of our courses to meet the needs of your organisation
- Engaging and interactive – our experts facilitate discussions among participants who can then effectively learn from their collective experience.



Our programs

EXECUTIVE CYBER SECURITY LEADERSHIP

Half-day seminar for groups of 5–10 senior leaders

- Appreciate the risks and rewards of technology and cyber security
- Build awareness in the technology and cybercrime trends that impact your business
- Review national and international regulatory and legal frameworks
- Experience policy-level training in cyber security planning, management and response

This executive seminar is designed for senior managers and board members.

It demystifies the technical jargon and explains the different types of cyber threats. It addresses cyber governance and compliance frameworks, and provides practical legal guidance. As a senior leader, you will learn how to leverage best practice to proactively lead and manage the security culture and practice within your business.

The seminar format gives space for a select group of senior leaders to reflect on their own experience and be actively involved in discussions.

CYBER SECURITY MANAGEMENT

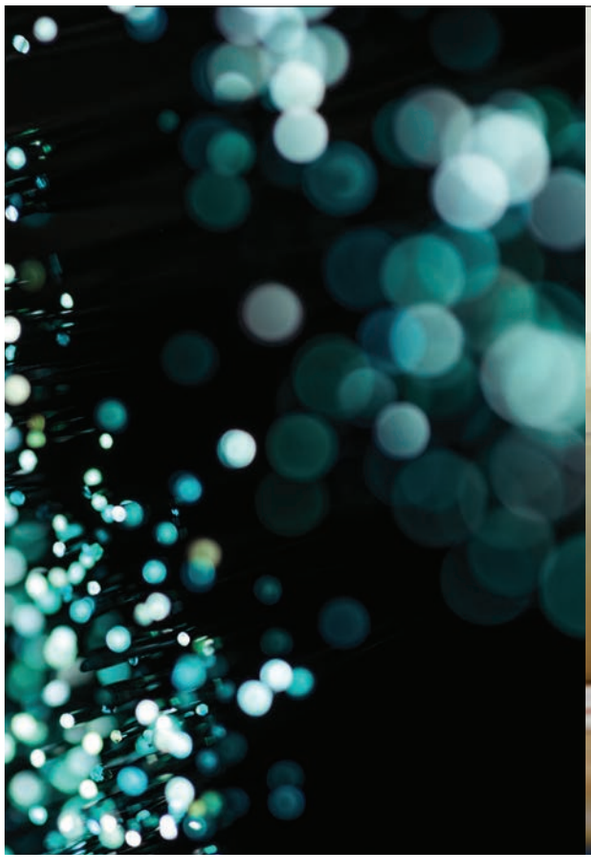
One-day workshop for 15–20 managers

- Build awareness in the technology and cybercrime trends that impact your business
- Assess organisation security culture and get insights into how to make it more resilient
- Manage and implement level training in security planning, risk management and contingency planning

This workshop offers a non-technical management perspective on cyber security.

It reviews the cyber security landscape and trends, and addresses risk management, cyber governance and the main legal and compliance frameworks.

You will acquire tools to better assess how much to spend on cyber security, as well as develop your understanding and management decisions through a true-to-life exercise based on a cyber-attack case study. As a manager, you will be armed with the ability to understand and work with your executive team to build a stronger cyber security culture and defences for your organisation.



CYBER GOVERNANCE AND RISK

Half-day workshop for 10–15 risk specialists

- Build awareness in the technology and cybercrime trends that impact your business
- Assess cyber governance and risk management practices against a compliance framework
- Link high-level governance and compliance strategies to practical cyber-risk management measures

This workshop is designed for risk management specialists and their teams.

It reviews the cyber security landscape and trends, and provides you with the tools to assess the cyber governance and security posture of your organisation against a compliance framework, such as the National Institute of Standards and Technology (NIST).

Although it tackles risk management from a non-technical perspective, it aims to enable a better understanding of IT principles and requirements. You will have the opportunity to practice your understanding and management decisions in the development of a cyber security budget.

TECHNICAL APPROACHES AND TRENDS

Two-day workshop for 10–15 technical staff

- Review information security concepts
- Gain exposure to the latest theoretical and practical advances in cyber security
- Develop a new domain of expertise

This workshop is targeted towards cyber security practitioners.

It reviews information security and network security concepts, strengthening your foundations in those areas.

It then extends your cyber security skills and knowledge by diving into the latest developments and applications of SDN, cloud computing, IoT, cryptography, machine learning and much more.

FOUNDATIONS IN CYBER SECURITY

Half-day workshop for up to 50 people

- Understand the complexity of computer systems and the foundations of information security
- Appreciate the risks to business, including information assets, reputation and privacy
- Recognise cyber threats and apply relevant tools and techniques to address those threats

This workshop is designed for every employee who wishes to increase their understanding of their role in the cyber governance framework. It also encourages the adoption of effective cyber hygiene and, as such, it contributes to strengthening organisations against cyber threats.

Our expert facilitators have strong academic backgrounds as well as vast industry experience.

Meet the team

INSPIRED BY LEADING RESEARCH, ROOTED IN PRACTICE

JOHN BAIRD

John Baird has more than 30 years of experience in information technology. He is CEO and founder of Revio Cyber Security. He has spent time as a consultant and has worked in house with some of the world's biggest financial services firms, most recently as chief technology officer for Deutsche Bank in Australia and New Zealand.

LES BELL

Les Bell is an adjunct lecturer in the Department of Computing at Macquarie. He is a Certified Information Systems Security Professional (CISSP) and teaches a preparation course for the CISSP examination for clients including IBM, Lockheed Martin, Northrop Grumman and Westpac. His research interests include secure coding techniques, probabilistic risk assessment, security culture, forensics and computational trust.

YVETTE BLOUNT

Yvette Blount is a senior lecturer in the Department of Accounting and Corporate Governance at Macquarie. She is an expert in business information systems, and has worked in the banking and IT industries. Her research interests include the use of information systems to achieve business objectives and competitive advantage with a particular emphasis on telework.

MARTIN BOYD

Martin Boyd is an adjunct lecturer in the Department of Computing at Macquarie. He is an expert in information technology systems and cyber security. He was executive manager, cyber security for CBA. His research interests include security defences and communication security.

DAMIAN JURD

Damian Jurd is an adjunct lecturer in the Department of Computing at Macquarie. He is an expert in virtualisation and software-defined networking, and has provided independent consulting services and technical training on behalf of vendors such as Hewlett-Packard and VMware. His research interests include VLSI design, systems software and distributed systems.

JOHN SELBY

John Selby is a lecturer in the Department of Accounting and Corporate Governance at Macquarie. He is an expert in internet law, and has practiced as a IT/IP lawyer at King & Wood Mallesons in Sydney, at TMI Associates in Tokyo, and as in-house counsel at Telstra. His interdisciplinary research focuses on the spillover effects of the internet on business, including internet governance and cyber security issues.

NILOUFER SELVADURAI

Niloufer Selvadurai is an Associate Professor in the Macquarie Law School. She researches and teaches in information technology law. Having formerly practiced as a solicitor in the areas of intellectual property and telecommunications, she understands the legal and compliance challenges faced by industry.

OPTUS

MACQUARIE University

OPTUS MACQUARIE UNIVERSITY

Cyber Security Hub

CRICOS Provider 00002J
CEA2894

Contact us to discuss
opportunities for collaboration
cybersecurityhub@mq.edu.au

For more information visit
mq.edu.au/cyber-security-hub