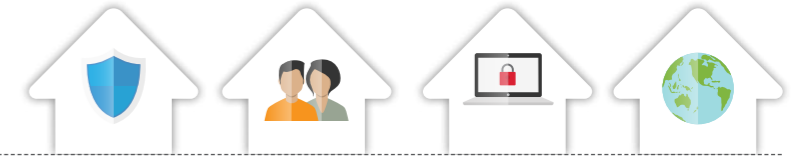


SUMMIT PROGRAMME

#CYBERNZ16



8.15AM – 9.00AM Registration

CYBER SECURITY SUMMIT OPENING SESSION

9.00AM – 9.20AM Welcome and Opening Keynote Address

KEYNOTE SPEECHES

9.20AM – 9.45AM

- **Jim Lewis**, Senior Fellow and Program Director, Center for Strategic and International Studies (CSIS)
- Q & A

9.45AM – 10.15AM

- **Matt Thomlinson**, Vice President of Security, Microsoft
- Q & A

10.15AM – 10.30AM Morning tea

SESSION 1: WHAT'S AT STAKE FOR NEW ZEALAND? UNDERSTANDING THE OPPORTUNITIES AND THREATS

10.30AM – 11.15AM **“Achieving the vision of a secure, resilient and prosperous online New Zealand means that individuals are protected online and New Zealand’s businesses can function, grow and innovate. Cyber security has the potential to be used as a point of positive, competitive advantage internationally.”**
New Zealand’s Cyber Security Strategy, December 2015

Panel discussion facilitated by Frances Valintine, Founder Tech Futures Lab; Founder and Chair of the Mind Lab by Unitec

- **Russell Stanners**, Chief Executive, Vodafone
- **Major General (Ret) Earl D Matthews**, Vice President, Enterprise Security Solutions, Hewlett Packard Enterprise Services, U.S. Public Sector
- **Dr Patrick Strange**, Chair Chorus; former Chief Executive Transpower
- **Steve Glynn**, Chief Information Security Officer, ANZ Bank

KEYNOTE SPEECH

11.15AM – 11.45AM

- **Richard Bejtlich**, Chief Security Strategist, FireEye, Non-resident Senior Fellow, The Brookings Institution
- Q & A

MINISTERIAL ADDRESS

11.45AM – MIDDAY Address by Minister for Communications, Hon Amy Adams

SESSION 2: A CALL TO ACTION: MAKING NEW ZEALAND SECURE, RESILIENT AND PROSPEROUS ONLINE

MIDDAY – 12.45PM **“The government has a role to play in cyber security – but not on its own. Close partnerships with the private sector and non-government organisations are required. Businesses drive the New Zealand economy and depend on the Internet and networked technology. They must protect the information that is critical to their commercial success. The private sector owns and operates the telecommunications systems. The private sector and technical community also have considerable cyber security expertise.”** *New Zealand’s Cyber Security Strategy, December 2015*

Panel discussion facilitated by Frances Valintine, Founder Tech Futures Lab; Founder and Chair of the Mind Lab by Unitec

- **Dr Rick Ede**, Chief Executive, Unitec Institute of Technology
- **Jo Healey**, Chief Executive, Dimension Data
- **Major General Stephen Day**, former head of the Australian Cyber Security Centre
- **Rick Shera**, Partner Lowndes Jordan (IT/IP specialist); Chair of NetSafe; Director, Network for Learning

SESSION 3: WHAT ARE THE ODDS OF GETTING HACKED?

12.45PM – 1.00PM

- **John Allen**, Chief Executive, NZ Racing Board
- Q & A

1.00PM – 1.45PM Networking lunch

SESSION 4: SUMMING UP THE KEY ISSUES FOR NEW ZEALAND

1.45PM – 2.30PM **Paul Ash**, Director of the National Cyber Policy Office, Department of the Prime Minister and Cabinet, welcomes participants to the afternoon sessions
The panel sums up the key messages from the morning’s discussions.

- **Richard Salgado**, Global Director of Information Security, Google
- **David Havercroft**, Chief Operating Officer, Spark
- **Kendra Ross**, Co-Founder, Duo NZ, 1stTuesday and iSANZ
- **Jordan Carter**, Chief Executive, Internet NZ
- **Toby Gee**, Special Counsel, Minter Ellison
- **Tony Wilson**, Head of Information Security, BNZ

WORKSHOPS 1 & 2

2.30PM – 3.15PM **WORKSHOP 1: CLOSING THE CYBER SECURITY SKILLS GAP** **WORKSHOP 2: BUILDING A CERT**

“New Zealand’s cyber security expertise needs to grow so that businesses and organisations can source the technical staff required to carry out ICT security. At the same time, the education and training system should produce ICT users at all levels with the skills to put in place basic cyber hygiene practices.”
New Zealand’s Cyber Security Action Plan, December 2015

Facilitator: **David Eaton**, Chief Technology Officer (NZ), Hewlett Packard Enterprise (NZ)

“It is proposed that a national CERT be established. This institution would act as a central reporting mechanism for the full range of cyber incidents, triaging incident response to the relevant separate organisation and ensuring technical advice gets to the organisations that need it – in real-time.”
New Zealand’s Cyber Security Action Plan, December 2015

Facilitator: **Kirk Hope**, Chief Executive, Business New Zealand

3.15PM – 3.30PM Afternoon tea

WORKSHOPS 3 & 4

3.30PM – 4.15PM **WORKSHOP 3: MAKING A DIFFERENCE TO THE CYBER SECURITY OF SMALL BUSINESSES** **WORKSHOP 4: CONNECTING SMART AND PREVENTING CYBERCRIME**

“Small and medium enterprises (SMEs) play a huge role in New Zealand’s economic growth; it is important that they are equipped to protect their business information.... A new “cyber credentials” scheme is proposed for SMEs. The scheme will promote to the SME audience the core actions that, if implemented properly, can make a big difference to their cyber security.”
New Zealand’s Cyber Security Action Plan, December 2015

Facilitator: **Ken Wallace**, New Zealand practice leader for Technology Risk and Assurance, EY

Introductory comments:
Minister for Small Business, **Hon Craig Foss**

“Achieving [the Cyber Capability] goal means that New Zealanders at all levels will have the skills and tools to protect themselves online, making it harder for malicious cyber actors to steal private data, identity information or cause damage to information systems.”

“Prevention first” is at the heart of our approach to cybercrime – giving New Zealanders the tools to change their online behaviour.”
New Zealand’s Cyber Security Action Plan, December 2015

Facilitator: **Kevin McDonald**, Chief Risk Officer, ASB

WRAP-UP: KEY OUTCOMES FROM THE FOUR WORKSHOPS

4.15PM – 5.00PM **The four facilitators sum up the key messages from the workshops.**

- **David Eaton**, Chief Technology Officer (NZ), Hewlett Packard Enterprise (NZ)
- **Kirk Hope**, Chief Executive, Business New Zealand
- **Ken Wallace**, New Zealand practice leader for Technology Risk and Assurance, EY
- **Kevin McDonald**, Chief Risk Officer, ASB

5.00PM – 6.30PM Networking drinks