



Valuable Advice From Workshop 2

Cyber Security - Safe-guarding Your Business In A Hostile Connected World Held on Wednesday 6 July 2016

Chaired by [Greg France](#), Corporate and Commercial Principal at Lowndes, the workshop's three speakers were:

- [Paul Ash](#), Director of the National Cyber Policy Office at the Department of the Prime Minister and Cabinet;
- [Scott Bartlett](#), CEO of Kordia New Zealand Limited; and
- [Michael Wallmannsberger](#), Chief Information Security Office at Wynyard Group



(L-R) Paul Ash, Scott Bartlett and Michael Wallmannsberger with Greg France (Chair)

Greg France

Greg opened the workshop by noting that we live in an increasingly online and connected world. He gave various examples to illustrate the extent and pace of the technological advances in the past 20 years, from the launching of the World Wide Web to the iPhone. These changes have had a profound effect on our working lives and businesses are becoming more reliant on technology for their business operations, to communicate with their customers and to deliver goods and services. Greg discussed businesses he has advised here and in London as their business models transformed to take advantage of this technology.

These changes have meant that cyber security is no longer a concern only for those companies that were traditionally viewed as technology businesses. He gave as examples the recent high profile hacking of a law firm in the Panamanian Papers scandal and of builders' emails here in New Zealand. The increasing value and sensitivity of the data held and shared online means that it is becoming increasingly important for businesses to focus on safeguarding their and their customers' data. The aim of today's workshop is to close the gap between the awareness of this issue and knowledge of what we can do about it.

Paul Ash

Paul began by explaining that traditionally people think of cyber security as a risk. However, it also presents an opportunity for New Zealand. If cyber security is managed well, New Zealand will be positioned well in the world. Paul noted that there are standards being introduced in key export markets such as the EU and US and it will be important for businesses to be able to demonstrate that they meet these standards not just to safeguard their businesses, but in order to be able to continue to export services to these markets. Paul gave an overview of New Zealand's Cyber Security Strategy and Action Plan.

New Zealanders rely on the Internet everyday. In fact, 90 percent of New Zealand businesses use the Internet on a daily basis. Connectivity is embedded. Paul stated that if New Zealand businesses made more effective use of the Internet offers, 34 billion dollars could be added to our economy.

Paul encouraged businesses to think about what cyber risk might look like for their businesses, which could include loss of intellectual property, client details, legal liability, direct financial cost, third party risk, interruption of service or non-fulfillment, damage to reputation and remediation costs. To address this risk, Paul



recommended that businesses have an action plan, which is updated every year to address technological changes. Businesses could sit down with an insurer, who would have considered risks and value, and discuss the cyber risks.

Paul then discussed the role of the board when it comes to cyber security. Paul noted that a recent survey reported that only 23% of boards actively participate in cyber security policy. He stated that boards have a key role to play in this issue. Boards need to ask sensible questions to their IT security people and need to consider how their business can move from risk to opportunity. Paul stated that boards can do this by using risk frameworks they can understand. They need to first understand the risk, treat or minimise the risk (e.g. educate people, in-house capability, managed security services), transfer the risk (cyber security insurance), and accept that there will always be some risk (but understand what you are accepting and ensure you have adequate business continuity planning for when that risk arises).

Paul ended by mentioning resources boards could refer to and use, such as the [Institute of Directors' Cyber Risk Practice Guide](#) and the [ConnectSmart website](#).

Scott Bartlett

Scott addressed three topics:

- The threat is escalating;
- The board's perspective; and
- Real life examples.

Scott noted that people are being attacked on the Internet all the time but most people are unaware that it is happening or has happened. According to PWC statistics, the average time attackers were on a network before detection was 229 days, and 67 per cent of victims were notified by an external entity. He stated that a key goal for businesses should be to reduce the time taken to detect, investigate and remediate incidents.

Scott stated that most of the time cyber security was talked about on a technical level and this was bad. We need to increase awareness of the issue. The weakest link in businesses is not the technical environment but the cultural environment. Scott emphasised the importance of educating the workforce on how to be cyber safe.

Scott also emphasised the importance of the role of boards. In his view, a failure to manage cyber security will have as serious a consequence for directors as a failure to manage health and safety. The duties of directors are wide and far reaching. There are already examples overseas of directors being legally unstuck due to cyber security failures.

Scott stated that traditional thinking was that the board goes to the Chief Information Security Officer (CISO) or other technical person and asks whether they have it under control because cyber security is viewed as a technical thing. However, it is far wider reaching than that. Cyber security needs to be part of the board's risk narrative and strategy; it needs to be a recurring theme. Boards need to direct and send reviews of cyber strategy for the business, and need to have clear line of sight to the CISO or security adviser. Businesses need to invest in technology, education, awareness and training

Scott then provided two examples of cyber breach. The first example was a fast-growing company with a younger workforce. People in the company wanted to bring their own electronic devices. The company allowed this. Their policy was well intentioned and incredibly flexible, but lacked proper controls, such as strong passwords for devices. One day one of the employees lost his phone. The phone was picked up by someone and given to a competitor of the company. The phone allowed access to the employee's emails, which provided access to the company's plan and acquisition targets. This was incredibly damaging to the business. The company could have mitigated the risk by having responsible policies in place, e.g. a requirement that devices are encrypted, strong passwords are used and the ability to remote wipe devices.

The second example was a New Zealand business that had a lot of success in online sales in New Zealand but wanted to go global. They engaged a firm to redevelop their website for international markets. The firm was relatively inexperienced and the website was not tested. The website was hacked and the site became completely disabled. The business lost details of all sales and revenue, and there was reputational damage, which was difficult to salvage as it was a niche market. Since all of the company's revenue was coming from online, the company should have had a cyber risk management policy to address these risks. It should have made sure that there was a security infrastructure that would have meant the site could have been quickly restored without the loss of data and reputation. Scott noted these were examples we were seeing frequently these days, which emphasised the importance of cyber security.

Michael Wallmannsberger

Michael began by setting out the defender's problem. He noted that businesses are confronted with threats from everywhere and they need to keep pace with that. The cyber security problem is unsolvable, in the same way as marketing isn't a "solvable" issue – if we stop doing marketing we will go out of business. Michael stated that a risk-managed approach is best practice. However, with a number of low probability but high consequence risks, it is difficult to prioritise. Businesses should also be having this conversation at a board level.

Michael noted that to manage cyber security it is necessary to:

- Pick a standard of security;
- Achieve that standard of security and maintain that standard across time; and
- Validate it.

He emphasised that businesses cannot win until they validate or maintain the standard of security. Michael noted that New Zealand is relatively lightly regulated when it comes to cyber security. He compared New Zealand to overseas countries where there are strong cyber standards. It is important that New Zealand improves this aspect to meet international standards.

Michael noted that businesses first need to know what they have and decide what matters most (that is, identifying your assets). Policy is the basic instrument of information security management. Without assurance, it is difficult to give effect to policy and defend assets. If you have not tested security, it is usually safe to assume your systems and assets are vulnerable. Michael stated that without the foundations of assets, policy and assurance, many other security efforts will fail to deliver.

Cyber security involves achieving an adequate and balanced attention to various elements of the process. People, process and technology all need to be considered in a strategy. There is a balance to be struck based on the company's risk appetite, its strategy and the available resources, which is a challenge for CISOs. This makes cyber security a multi-disciplinary matter and it is important that CISOs are involved in these discussions so that they understand the context in which they are making decisions. It is important also to focus not only on prevention, but also on detection and correction of breaches. The correction phase is often split into two phases, focusing on the immediate response and business recovery.

Michael stated that security is a fast-moving discipline and it is really important that we are open to others outside the security industry and participating in this issue. It is crucial to know there is vulnerability. Understanding what we do not know is as important as what we do know. He noted that it is easy for well-resourced criminal groups to buy attack methods that were, until recently, considered to only be available to nation-states. Continuing to learn about the problem as it relates to your business is important. To illustrate, Michael highlighted the differences between an expert and non-expert's top 5 security practices, which essentially showed the non-experts had absorbed messages but were 10-15 years behind on best practice.

To end, Michael noted the following lessons. When there is a cyber security incident keep calm and call a CISO and provide him/her with context. The board's job is to articulate risk appetite and ask to be kept informed about how the board's risk compares to that. Ensure you know what assets you have and what matters most, in business terms. Aim for adequate across the board rather than awesome, as balance is more important. Lastly, ensure resources are available for security and that you manage out-of-date infrastructure.

Conclusion

Greg France ended the workshop by noting the interesting threads brought up. Cyber security is not just a threat but can be opportunity for those who get it right. The issue is one that needs to be addressed at a board level and there is an emphasis on getting the culture right – people and culture are as important as the technology aspects. Businesses need to accept there will always be some risk, but make sure they are in a position to make informed decisions about those risks. Importantly cyber security is a moving field so it is crucial for businesses to stay current.

The session concluded after Greg thanked the panel for sharing their passion, knowledge and experience on this topic, and thanking all of the participants and supporter organisations of the second Business Intelligence Work Shop for 2016.



Watch video interviews with our speakers, [click here](#).

For information on or to register for upcoming workshops in the Business Intelligence Series, please visit:
<http://www.business-intelligence.co.nz>.

Hosted by:



Supporters:



Business Intelligence Series PO Box 7314, Auckland | Phone +64 9 373 7712 | info@business-intelligence.co.nz

