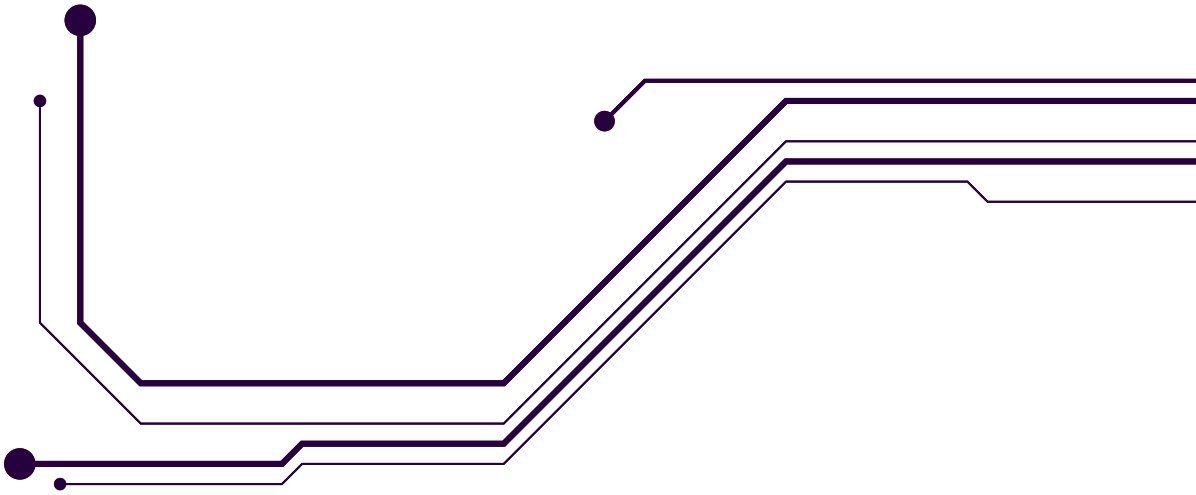
IS YOUR ORGANISATION **READY FOR A CRISIS?**

THE FUTURE OF SECURITY IN AUSTRALIA. A THINK TANK REPORT BY BLACKBERRY.

BlackBerry



3 Foreword

4 Introduction

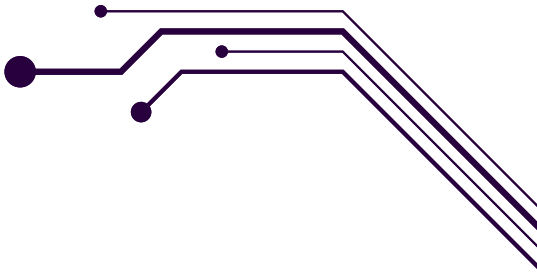
5 Participants

6 Collective Response

8 Arms Race

10 Vulnerabilities

12 Human Factors



Foreward by
Jeffrey Bleich

Partner at Dentons, former US Ambassador to Australia and advisor to the Obama government on cybersecurity

Jeffrey Bleich

At the close of 2016, I had the pleasure of participating in a critical discussion in Sydney about trends in cyber and mobile security. Together with BlackBerry and other leaders in various fields of information and people security, this 'Think Tank' explored the threat impact today upon organisations in the private and public sectors in Australia and around the world.

It goes without saying that cybercrime and cybersecurity were high on the agenda. As a former advisor to the Obama government on the subject, this is an area I am passionate about. It was clear that it's a challenge for everyone, from C-levels to boards to IT managers, who are grappling with these challenges every day with different strategies. However, beyond this, we also heard first-hand how it impacts technology and people strategies, including how roles and organisational responsibilities are changing and solutions are evolving to help manage citizen and employee safety.

The changing security threat outlook continues to be a challenge and 2017 will be no different in how we tackle its problems. The landscape will only continue to evolve, threats will grow and become more complex. This discussion among some of Australia's leading experts aimed to examine how organisations and governments can better ready themselves for a crisis and mitigate risks in the future. However, this is just a starting block.

We hope the themes in this report help to encourage ongoing dialogue about cybersecurity, holistic strategies for staff and people safety – and importantly, what can be done to mitigate and survive cybercrime's destructive path.

Introduction

Australia's cyber risk profile is changing.

Once primarily the concern of IT departments, digital attacks now threaten to disable critical infrastructure, bring entire cities to their knees and steal billions of dollars from the economy.

In 2015, the number of digital attacks increased 38% on the previous year.[1] The coming year is expected to see even bigger growth in cybercrime, with the number of potential targets, agents and vulnerabilities all continuing to diversify and expand.

It's a problem with a hefty price tag.

Today in Australia, cybercrime is a significant financial problem. In the first quarter of 2015, more than A$234 million worth of financial loss was self-reported by victims of cybercrime to the Australian Cybercrime Online Reporting Network (ACORN), whilst a report by the Attorney General's office suggested the potential national cost at around $2 billion a year.[2]

The rising threat tide is understandably causing an increasing level of concern amongst business leaders. A recent survey of more than 1,000 IT executives found nearly nine out of 10 executives (86%) are nervous that their company's security won't be enough to keep out hackers or malware.[3]

Cybersecurity today is charged not only with protecting technology, but also critical infrastructure and even people. Recent crisis scenarios such as the 2016 South Australian power blackout saw technology playing a lead recovery role – from messaging impacted residents about the disaster to routing energy to critical services such as hospitals and maintaining networks.

The BlackBerry Future of Security Think Tank brought together a select group of experts to explore the increasingly complex Australian security environment – both on and offline. The goal was to establish dialog amongst public and private sector experts, in order to better understand the varied challenges facing cities in the future and how best to develop more comprehensive and collaborative risk management strategies.

[1] BlackBerry Security Summit reporting, http://fleetowner.com/technology/your-biz- may-be- compromised-long-you- know-it- if-you- ever-do

[2] https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/national-plan- to-combat-cybercrime.pdf

[3] http://blogs.blackberry.com/2016/07/survey-nearly- 9-out- of-10- executives-worry- their-companys- security-is-too- weak-to- deter-hackers/

Future of Security Think Tank participants

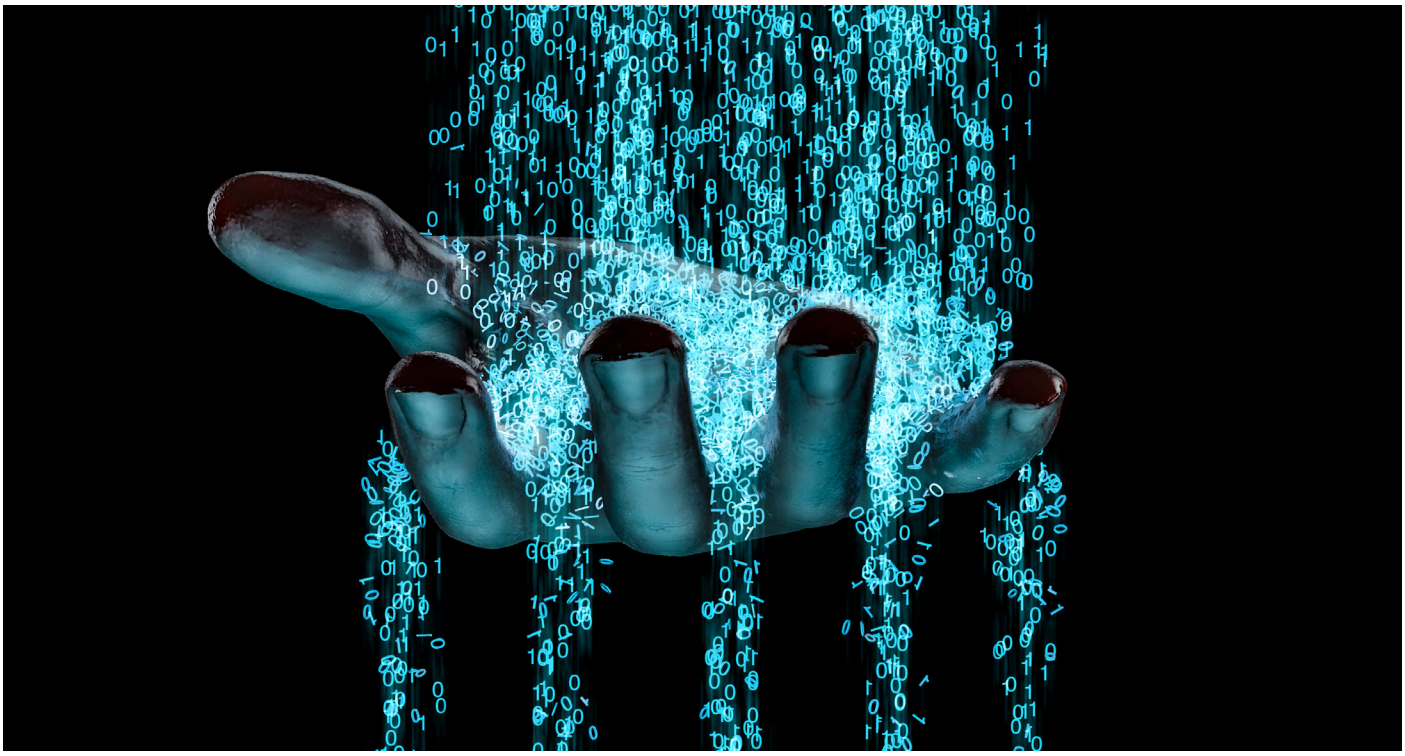
The Think Tank brought together participants from a wide-range of security backgrounds – including fraud, cybersecurity and terrorism. Importantly the sectors they work in are incredibly diverse, from professional services, government departments, financial services, security agencies, utility and telecommunications and academia.

The Think Tank was moderated by industry commentator and freelance journalist Brad Howarth. He was joined by:

- Sinisha Patkovic – *Vice President, BlackBerry Government Solutions*
- Jeffrey Bleich – *Group CEO and Partner, Dentons; Former US Ambassador to Australia*
- John Durbridge – *Head of Campus Security, Macquarie University*
- Berys Amor – *Director for Technology, Corrs Chambers Westgarth*
- Rex Stevenson – *Director, Signet Group International; Former Director General for Australian Secret Intelligence Service*
- Claudine Ogilvie – *Chief Information Officer, Jetstar Airways*
- Craig Davies – *CEO at Australian Cybersecurity Growth Network Ltd*
- George Reinoso – *Security and Services Consultant, Ericom*
- Derek Chen – *Regional Head of IT Security, British America Tobacco*
- Dr Liming Zhu – *Research Director, Software and Computational Systems, DATA61 | CSIRO*

The discussion unlocked a number of themes pertinent in the security landscape – above and beyond just cyber. There were four key take outs that reflected what cities in Australia and businesses within them should be thinking about moving into 2017 and beyond. These included:

- The need for a collective response
- The attack arms race
- Changing vulnerabilities
- Overcoming the human factor



Need for a collective response

The need for a nationally integrated response to cyber threats remains the single most important goal for addressing cybercrime in 2017, according to the Think Tank members.

Almost all of the group suggested that changes to the threat landscape have created an overlapping responsibility between governments, private enterprise and industry bodies.

For example, last financial year, peak government body CERT Australia responded to 14,804 cybersecurity incidents affecting Australian businesses, 418 of which involved systems of national interest and critical infrastructure.

With an increasing number of occurrences, it was agreed collaboration was key. There are numerous examples of where a joint effort has proved critical in staving off a digital threat.

In 2012, a foreign criminal syndicate used some 30,000 Australian credit cards to make unauthorised transactions of more than $30 million. It was only because of the combined efforts of the Australian Financial Police, many Australian banks and technology providers in identifying the threat, that the sum didn't run into the hundreds of millions of dollars.

Yet historically, such deep and large scale cooperation has been rare and it was the strong view of the Think Tank that it was an area that needed immediate emphasis. Participants agreed that there is too little formal information sharing, and no clear lines of responsibility in terms of what an organisation should do to defend itself, and where the government's role starts and ends.

Jeffrey Bleich, the former US Ambassador to Australia and now Group CEO and Partner at Dentons, said such collaboration required a level of openness not previously found in the sector.

"Only a few years ago many companies were loath to share any information or disclose details about security for fear of conceding a competitive edge. This position is changing but needs to do so even more if we're to more effectively combat cybersecurity threats in the coming year," Mr Bleich said.

Mr Bleich's comments were echoed by many other Think Tank participants, who felt that while organisations could cooperate when seeking to extinguish a specific threat, ongoing collaboration continued to be problematic.

There were a number of potential barriers to facilitate more open exchange such as commercial sensitivity, however the most prevalent concern was a lack of a singular head administrative entity.

On the government side, there are dozens of bodies focused on improved security and information sharing. Within the private sector, the number of formal and informal bodies and initiatives involved in digitally protecting our cities runs into the hundreds.

Many of the participants said the plethora of conflicting priorities and approaches amongst these businesses could be confusing to individual organisations. Even a seemingly simple task such as a shared definition of 'cybercrime' could be problematic. In a recent threat report from the Australian Cybersecurity Centre, the body said "The Government's definition of a cyberattack can be at odds with what the information security community, the public and the media envisage cyberattacks to be."

Nonetheless the requirement for a nationally coordinated approach remains, even if the structure of this relationship remains still undecided.

BlackBerry Think Tank representative, Sinisha Patkovic who is BlackBerry's Vice President of Government Solutions said, "There are some considerable challenges in bringing government and private enterprises together when it comes to cybersecurity. Everyone has a slightly different expectation and view about what a nationally coordinated approach would look like. Fortunately, I think Australia already has a lot of the right foundations in place for such collaboration, it's now about taking the next steps."

Although full cooperation may be a work in progress, the Future of Security Think Tank agreed that there were four key factors that could determine the success of future collaborations:

- Helping educate Australians about how to better protect themselves
- Improved dialogue between government and private enterprise on cybersecurity – particularly in the area of breach reporting
- Better intelligence provided by government about emerging and likely cyberattacks
- Closer collaboration amongst those businesses in the private sector

[4] http://webcache.googleusercontent.com/search?q=cache:clNj5DQivWsJ:www.aph.gov.au/DocumentStore.ashx%3Fid%3Da03cf049-7f2b- 43bd-846c- 9eb7bd2f59ef%26subId%3D253039+&cd=3&hl=en&ct=clnk&gl=au

[5] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

[6] https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf

The attack arms race

One of the big drivers between improved public/ private cyber collaboration was that many Think Tank participants felt companies were struggling to keep pace with an ever-changing range of threats.

Even the cyber criminals themselves are morphing. The term ‘cyber criminal’ is a catchall category that now includes a vast range of nation states, groups and individuals engaged in online crime from all corners of globe. Their drivers are as distinct as their backgrounds, from pure financial gain through to disrupting critical infrastructure.

However, there is one trait that almost all share – they can move at the speed of light. Criminals are able to absorb and take advantage of new vulnerabilities within days or even hours.

The ability to prepare for, or even respond to, such a rapidly changing threat landscape was much discussed by the Think Tank members.

Dr Liming Zhu, Research Director of Software and Computational Systems at CSIRO, gave some interesting insight into how this created a sense of pressure amongst those charged with protecting the networks.

“At times it really does feel like an arms race. The better we get at finding countermeasures, those countermeasures then become a training ground for adversaries to find better exploits. As a company, you need be methodical about removing classes of threats completely. Keeping focused on the root cause is very important,” Dr Zhu said.

George Reinoso, a Security and Services Consultant at Ericom, agreed with Dr Zhu's thoughts. Rather than getting overwhelmed he said, "The companies that weather an unexpected crisis the best are the ones that are meticulous with their planning. They may not know the nature of the threat but they know, down to the smallest degree, what their response approach will be. When working in an environment where things change so quickly, it's important not to get too swept up and instead focus on preparedness. At the end of the day it's the details that matter."

Another way of alleviating the burden of protecting a network is to seek outside experts to help better understand and address rapidly changing threats. As Head of Campus Security at one of Australia's leading education organisations, John Durbridge from Macquarie University said academic insight should play a key role in shaping industry security strategy. "Keeping ahead of the game is key when it comes to cybersecurity. We have access to some of Australia's brightest minds here at Macquarie enabling us to draw on their expertise and stay one step ahead. It's important that organisations are flexible and open minded in who is the 'expert' when it comes to security."

Whilst the industry pushes towards drawing on more security experts, those behind cybercrimes are often at the other end of the spectrum.

Underpinning the 'attack arms race' is an increasingly business-like approach taken by digital crime organisations – offering products and services to the less technology savvy. Hackers for hire are likely to offer round-the-clock support desk services, money laundering expertise and readily packaged cybercrime 'kits' .

The so-called 'script kiddies' armed with off-the-shelf DDoS products were widely suspected to be behind the Dyn attacks in October 2016, which brought down services such as Twitter, Spotify, Netflix and Paypal.

> ***"At times it really does feel like an arms race. The better we get at finding countermeasures, those countermeasures then become a training ground for adversaries to find better exploits. As a company, you need be methodical about removing classes of threats completely. Keeping focused on the root cause is very important"***

The hackers infected common IoT devices, such as DVRs and webcams, with a malware named Mirai that turned these devices into a powerful botnet army that jammed up traffic to a domain name system (DNS) server.

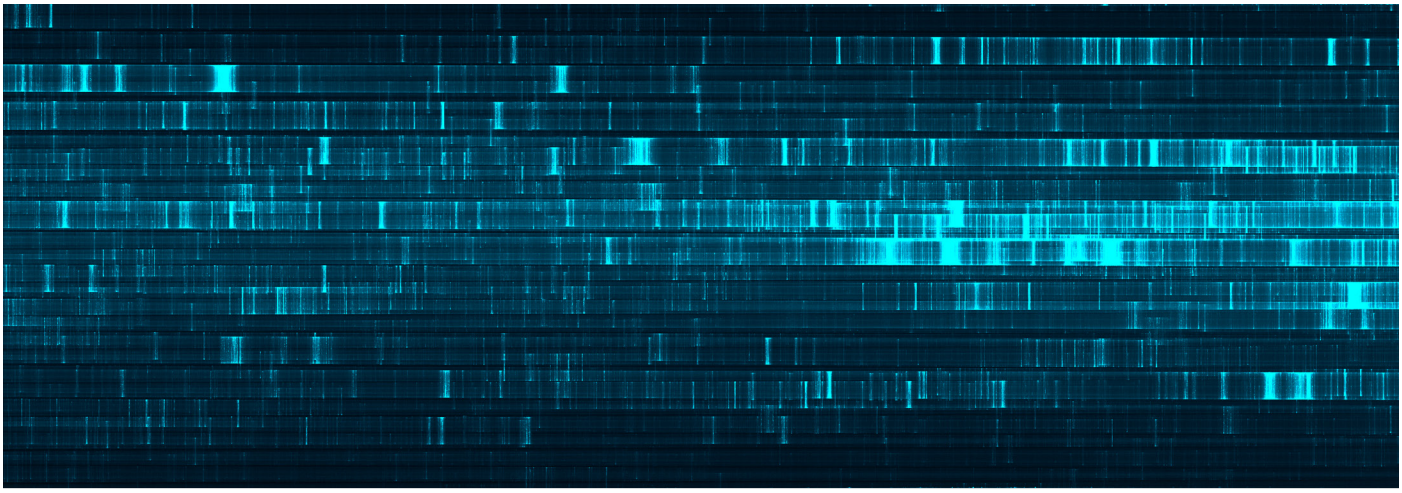
While most Think Tank participants weren't specifically concerned about the threat from less sophisticated attackers, it did raise concerns about the need for constant vigilance.

Craig Davies, the former Director of Security at Atlassian and now Chief Executive Officer at the Australian Cybersecurity Growth Network Ltd said, "We need to be continually testing and helping our organisations on security to deal with an almost constant threat. Every company has a security strategy and plan, but too many of them just sit in a desk drawer somewhere. Organisations need to stop asking 'What could possibly go wrong?' and accept that constant attack is the new normal."

[7]http://www.pcworld.idg.com.au/article/599997/cybercriminals-increasingly- embracing-sophisticated-business-model- approach/

Changing vulnerabilities

However, it is not just the rate and sophistication of attacks that is changing, vulnerability areas are also shifting. The Think Tank believed that technology security professionals needed to widen their view of what needs to be protected.



The potential vulnerability of the Internet of Things, infected Artificial Intelligence engines and even people themselves were amongst some of the potential concerns raised by the group.

Most pointed to the potential impact of targeting these emerging areas. The 2015 attack on Ukraine power stations via connected plant control equipment provided a sobering example. In this instance cyber terrorists shut down 30 substations throughout the country – leaving hundreds of thousands of residents without electricity for hours. Authorities believe more than six months of planning went into the attack using a combination of spear phishing, keylogging and data exfiltration.

However, participants were quick to point out that it wasn't just large-scale utility infrastructure that was at risk. During the past 12 months, researchers have hacked everything from hospital insulin pumps to humble electric kettles.

Think Tank participants said they expected to see increasing connections between the technological and physical worlds in a bid to better protect cities.

Jeffrey Bleich felt that an integrated approach is paramount to success, "The notion that people think differently in the virtual and physical world is a fiction. We need to observe human nature and apply this to both spheres, where we are now operating simultaneously."

[8]http://blogs.blackberry.com/2016/11/how-hackers- could-draft- connected-cars- into-their- botnet-armies/

> ***"Looking specifically at IT security, with larger organisations there can be different maturity levels across the business - what is accepted in one part of the business, may not be embraced in others. You can't simply look at an organisation as a single environment. There are many individual, yet overlapping needs."***

Craig Davies, Chief Executive Officer at Australian Cybersecurity Growth Network Ltd, echoed Mr Bleich's comments, adding, "It's critical to our organisations that we have good overlap between the protection of physical assets and the IT world. Most organisations in the past have tended to do one area well, but not necessarily the other. In such an integrated future we need to be able to do both really well."

Derek Chen, Regional Head of IT Security at British America Tobacco, added, "We're operating in a new world. We have had to find new ways of working, with a number of teams working together whenever there is a risk highlighted in our organisation to get the best outcome. An integrated approach is necessary with fighting sophisticated threats."

Claudine Ogilvie, Chief Information Officer at Jetstar further commented, "It is indeed a new world with the risk of human factors a big threat – just as much as technology. A big part of a company's strategy should be to help staff understand the risks and what to look out for. To do this you need to bring people on the journey, putting methods in place to help change behaviours and be more vigilant. Together with enhanced technology, it's important to create that culture of education across different lines of business – and that is often overlooked in an organisation."

"Looking specifically at IT security, with larger organisations there can be different maturity levels across the business, may not be embraced in others. You can't simply look at an organisation as a single environment. There are many individual, yet overlapping needs."

In reference to the 'new world' of security, this is also where people, as well as information and data, are subject to threats. The Think Tank participants discussed the changing role of the CIO and the wider threat landscape where partner organisations, friends and families were an increasingly targeted vulnerability. These parties were often seen as the weakest link in the security chain, providing a stepping stone to the organisation or high value individual.

"As an organisation we don't only think about security as something that happens within our internal systems," said Berys Amor, Director of Technology at Corrs Chambers Westgarth. "Sometimes the easiest way to get to a company might be through a partner organisation and as an industry we're increasingly seeing cyber criminals go after executives through their personal assistant, friends or even families."

Overcoming the human factor

In an environment of ever evolving technology threats, it's somewhat ironic that amongst the biggest problems in digital safety is the 'human element'. Every member of the Think Tank was able to provide extensive examples of how people could unravel even the most well-thought security strategy.

Undoubtedly, the key concern amongst businesses was that security was often perceived as a barrier to productivity, rather than a critical safeguard. Many participants believed that increased security was inseparably linked to sluggish performance or administrative red-tape.

Research suggests this belief is right on the money.

A recent BlackBerry security survey found that 82% of global executives felt that security precautions, specifically in mobile working, caused at least some frustration amongst their employees. Incredibly, 44% of employees felt too much security could stop employees from doing their job altogether.

Against this backdrop, many in the Think Tank believed that a better approach for businesses was to deploy security solutions that better matched existing employee behaviours.

According to Derek Chen, Regional Head of IT Security, British America Tobacco, "a lot of issues come down to people, they absolutely shape the risk profile. As an industry we need to build our solutions from the people perspective up. The challenge is that behaviours, like technologies change all the time, you have to constantly monitor how people are or aren't using security and adjust your strategy accordingly. It's not just about ticking off boxes and thinking you're done."

It's this kind of accommodating approach that Berys Amor, Director of Technology at law firm Corrs Chambers Westgarth has been using with some success. The firm has developed an ongoing internal communications program to help employees to better understand the importance of security.

"Five years ago employees were not as aware of the security threats and we've slowly been able to turn that around through ongoing awareness activity and making sure our approach fitted the needs and expectations of the business. Today we have a lot of interaction with the business to check that partners and staff are doing the right thing."

Companies are highly aware of employees circumventing security measures. BlackBerry's recently commissioned research into mobile working practices found 62% of Australian businesses are worried about the risks of errant employees storing sensitive information on cloud services. Rather than driving to force employees to use company-provided storage, 75% of companies within the survey said they were working towards delivering an enterprise-grade file sharing service – that would accommodate both employee workflow and company needs.

"The challenge is that behaviours, like technologies change all the time, you have to constantly monitor how people are or aren't using security and adjust your strategy accordingly. It's not just about ticking off boxes and thinking you're done."

The Think Tank said executive support was critical in creating a successful security culture. Rex Stevenson, the former Director General for the Australian Secret Intelligence Service and now Director of Signet Group International said, "Unless security is driven from the very top of the organisation, you're not going to get any real change. The CEO needs to get behind it and push it, otherwise all of your effort trying to change the rest of the organisation is lost. You need the commitment right through the organisation, but it needs to start with the most senior executives."

What can sometimes be an overlooked factor, the Think Tank believed there are three critical steps in overcoming the 'human element' challenge:

- Constantly test adherence and educate; being vigilant around both is the centrepiece of a successful security strategy
- Design strategies and programs within organisations for the people, not for the product
- Behaviour changes constantly; be aware of how working and social patterns evolve within an organisation over time

The BlackBerry view

by Sinisha Patkovic, Vice President, BlackBerry Government Solutions

I've said it before, and I'll say it again – mobile, in all its forms has changed the way the cybersecurity landscape needs to operate. The Internet of Things will require further changes to how we all think and act about cybersecurity in the enterprise and beyond. This is why we have accelerated our efforts to address these emerging issues, with what BlackBerry calls – "The Enterprise of Things."

By this, we mean the network of intelligent connections and end points within the enterprise that enables products to move from sketch to scale. It's the devices, computers, sensors, trackers, equipment and other "things" that communicate with each other to enable smart product development, distribution, marketing and sales.

A Future without vulnerabilities?

At BlackBerry, we know that mobile has brought a series of challenges to organisations – from BYOD to end user data in the cloud, the convenience of mobile is marred by the security risks it presents. Today, as companies continue to grapple with securing their mobile workforces, they are also looking to the future and how to manage all the other end-points that are sharing unsecured data.

As shared on our blog, Inside BlackBerry, when individuals buy electronic devices or use online services, they generally assume that they're secure and that they will protect our private information. But all too often, these assumptions turn out to be wrong, as highlighted by the constant news stories on major cyberattacks and data breaches. The root of the problem is the typical industry approach to security: build products, ship them, and hope they don't get hacked.

We know that a future without vulnerabilities is one of the world's biggest challenges. So, at BlackBerry, we're working day and night to turn this security model on its head. Rapid patching is critical to product security, but the reactive approach gives the attacker the opening move. Formal methods have the potential to proactively improve security design standards and certifications, giving us the ability to prove that products and services are secure – including the obscure details that even the experts sometimes overlook. With the cybersecurity battle raging on, formal methods can change the battlefield over the long term and give us the best possible chance to win the war.

Organisations therefore need to take a more strategic look at how they comprehensively protect themselves from end to end. The right approach to achieving sustainable results rests on three pillars: making the decisions at the right level through Governance of IT and Security, having a big picture with a comprehensive security program, and ensuring effective use of the security tools. Software plays a vital role as it is a core building block of a modern enterprise. It needs to mitigate both the current threats as well as be resilient against challenges still to come.

For BlackBerry, it is vitally important that we not only create great software but that we are able to help organisations at a strategic level understand the threat landscape and take appropriate action. This is why information-sharing initiatives like this 'Think Tank' are very important – because collaboration, at every level, is key to combatting the ever changing threat. Without dialogue, we are limited in our understanding and therefore deficient in our solution. Our enemy listens, learns and adapts with swiftness and precision. We must do the same.

Closing Thoughts by Think Tank moderator

Brad Howarth

The changing cybersecurity threat landscape demands greater clarity regarding the roles and responsibilities both within and between those organisations under threat. At the same time, the group which should consider itself under threat is constantly adding new members, while the threats they face are growing more complex and broadening in scope.

Faced with such a complex and potentially confusing scenario, it is incumbent upon all organisations to not just consider the threats they face and their potential impact, but to also be actively planning for the seeming inevitability that one day their fears will be realised.

It is not enough for an organisation to simply maintain a defensive perimeter, especially as the insider threat – be it accidental or malicious – has proven to be so devastating to so many organisations. So too organisations must accept that the goals of unscrupulous attacks today are wider than just financial windfalls – intellectual property, customer records, staff data, and so many other information types all have value and can all be used to inflict damage at an organisational or even personal level.

And it is not just the actions of malicious actors that organisations must be prepared for. The heavy dependency of organisations on digital systems and communications means natural occurrences can have a devastating impact on business continuity.

It is essential that all organisations be well drilled in what to do once an incident occurs – for the protection of staff as well as for its reputation, intellectual property, and financial assets. So too it is vital that mechanisms exist so that information regarding attacks can be quickly shared amongst those most vulnerable.

Because the enemy is multitudinous, well-armed, and has very little to lose. The same cannot be said of their targets.