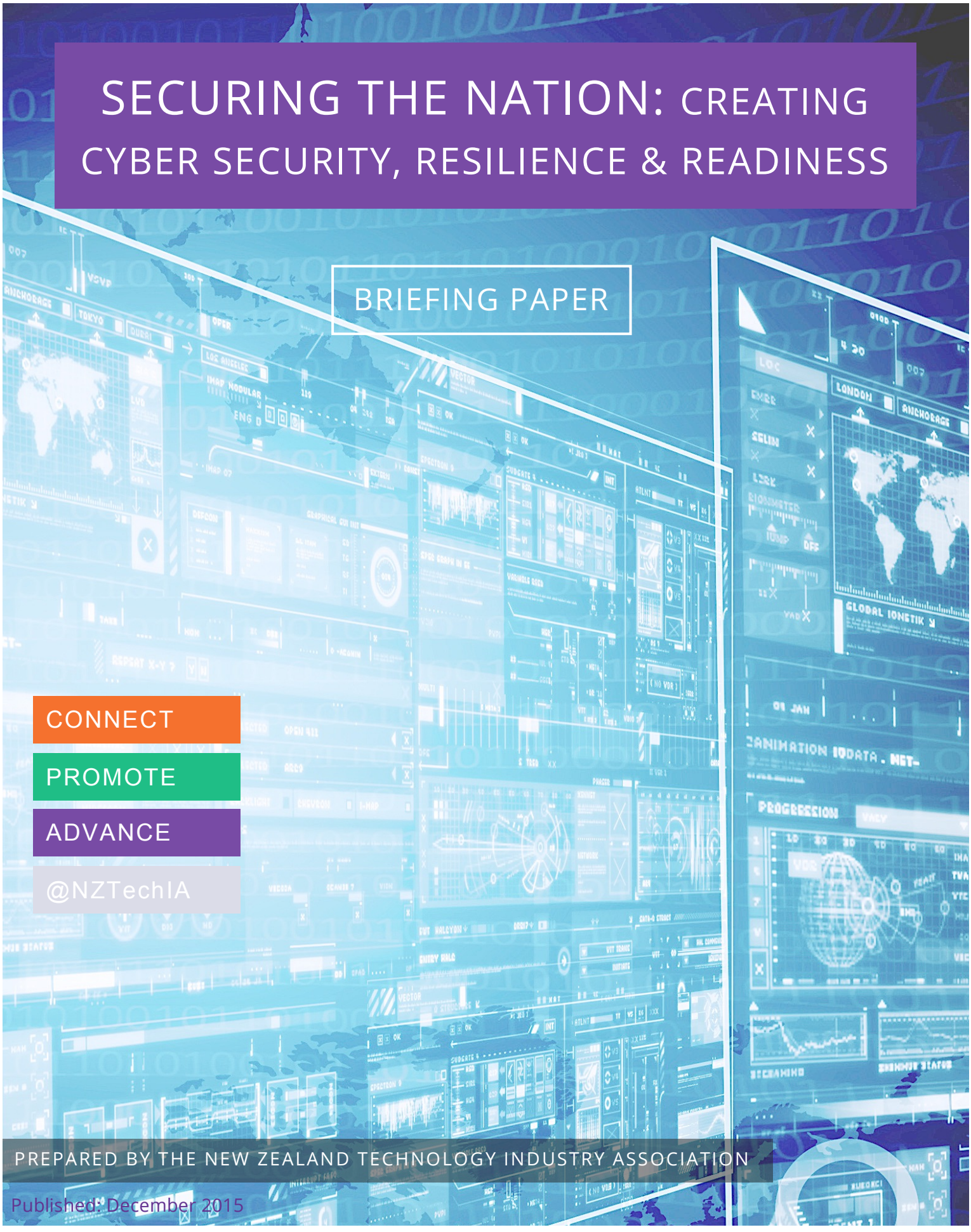
NEW ZEALAND TECHNOLOGY
INDUSTRY ASSOCIATION

SECURING THE NATION: CREATING CYBER SECURITY, RESILIENCE & READINESS

BRIEFING PAPER



CONNECT

PROMOTE

ADVANCE

@NZTechIA

PREPARED BY THE NEW ZEALAND TECHNOLOGY INDUSTRY ASSOCIATION

Published: December 2015

NEW ZEALAND TECHNOLOGY INDUSTRY ASSOCIATION

CONNECT
PROMOTE
ADVANCE

SECURING THE NATION:
CREATING CYBER SECURITY, RESILIENCE AND READINESS

DECEMBER 2015

This NZTech briefing paper provides insights from the recent NZTech Advance Security Summit in Wellington, including key observations from the Leaders Forum discussions involving senior executives and chief information security officers from a broad cross section of government agencies, large private corporations and the tech sector.

EXECUTIVE SUMMARY

The effective and safe use of information technology has the potential to deliver incredible benefits to the New Zealand economy by enabling greater efficiency and productivity. In addition, the local technology industry is fast becoming a significant source of export revenues for the country accounting for at least $6.5 billion in exports in 2015.

For New Zealand to grow its economy through digital exports, it needs to have trusted, reliable and secure ICT environments. However, there is risk of a significant impact to the economy if individuals and organisations are reluctant to engage in the digital economy or avoid using technology to its full potential due to cyber security fears. SMEs, in particular, are seen as being most vulnerable to both actual threats and fears over perceived threats.

The recent NZTech Leaders Forum at the Security Summit identified the following insights:

- Many New Zealand organisations do not yet prioritise cyber threats as a business risk, with few businesses adopting responsibility for cyber security at a board level.
- While there has been recent activity focused on keeping New Zealanders safe online and a great deal of individual effort by private organisations and public organisations, what appears to be lacking is a coordinated approach.
- Education is critical. Cyber security needs to become part of New Zealanders' DNA, much as road or fire safety have become. This requires action to integrate cyber security learning into the school curriculum and ongoing awareness campaigns for businesses.

The need to work together to keep the New Zealand economy, organisations and critical infrastructure safe was identified. This raised a set of key questions such as:

- How should New Zealand respond in a coordinated manner to cyber security incidents?
- What are the roles and responsibilities of Government, the private sector and the tech industry in keeping the New Zealand economy and critical infrastructure safe for cybercrime?
- How do these parties work together to improve the country's cyber security resilience, preparedness, education and awareness of cyber threats?

© 2015 New Zealand Technology Industry Association

THE RISE OF CYBERCRIME

The Government Chief Information Officer (GCIO) and the relevant teams in DIA, MBIE and other agencies have done an excellent job of moving toward this vision. The industry recognises the significant progress that has been made in a relatively short period of time. Yet it is apparent to the

The Summit heard how cyber risks were becoming more complex, growing in scale and reach and are now affecting a wider subset of the economy. The complexity of cyber security is increasing as the technology landscape becomes more advanced. With technologies such as the Internet of Things and machine-to-machine communications expected to further accelerate the challenges.

Cybercrime has become industrialised and can be state sponsored with well-organised enterprises able to launch advanced persistent attacks aimed at government agencies and organisations with high-value intellectual property.

Despite the rise of more sophisticated threats, the vast majority of attacks still exploit simple vulnerabilities. It is postulated that 80% of exploitable vulnerabilities could be protected with 20% more effort.

However, with the rise of social engineering attacks, organisations need to step up their security awareness and policies and implement multi-layered cyber security plans to address vulnerabilities relating to people, processes and technology.

THE COST OF CYBERCRIME

The direct cost of cybercrime is difficult to calculate since the true cost is obscured by incomplete and inconsistent reporting. According to the Ponemon Institute, an international research house specialising in privacy and security, the cost of a cyber breach is increasing. It is estimated that the cost of the average security breach is now $3.8 million, representing a 20% increase over the previous year. Meanwhile the average cost of losing personal information records, such as credit card data, is now $154 per record.

The indirect cost of cybercrime is even harder to quantify. The proportion of New Zealand firms confident in their ICT security has reduced significantly in the past year. Much of this decrease can be attributed to greater awareness about cyber security rather actual threats. But this sentiment reveals that as organisations become more aware of cyber security risks they also become more afraid of the threats. This concern could result in avoidance by organisations to use technology to its maximum potential or to engage in the digital economy, as they try to avoid cyber threats. This, in turn, can have a great impact on the New Zealand economy as organisations, especially SMEs, miss out on the efficiency and productivity gains ICT delivers.

BALANCING RISK AND OPPORTUNITY

The government's new Cyber Security Strategy highlights both the opportunities for the New Zealand economy by enabling the unbridled use of technology and the risk cybercrime poses to this opportunity.

At the Security Summit, the Honourable Amy Adams, Minister for Communications, highlighted that the tech sector is growing rapidly, accounting for a significant proportion of GDP, employing tens of thousands of people and has grown to be the country's third-largest exporter. She went on to note that the value of ICT stocks on the NZX is now worth over $7 billion representing 10% of the market.

With 96% of businesses in New Zealand now having an internet connection, the tyranny of distance, which has challenged the country's participation in global markets, is steadily eroding. As the use of

© 2015 New Zealand Technology Industry Association

ICT increases, it is delivering greater productivity benefits and enabling greater innovation, borne from New Zealanders' unique and creative mindset, and which can now easily be sold on the world stage.

However, according to Minister Adams, New Zealand organisations are not yet truly maximising their use of technology, which could deliver even greater productivity benefits. If they were to use the internet to its full potential, research from the Innovation Partnership estimates it would deliver an additional $34 billion worth of productivity to the economy.

It is suggested that one of the reasons New Zealander firms are not realising the true potential of the efficiency gains of digital technology is an element of fear about digital threats and cyber security.

EDUCATION AND AWARENESS

The need for greater education and awareness of cyber security emerged as one of the key issues at the Summit. The government appears to have a keen long-term interest in raising awareness around cybercrime and educating the public on how to stay safe online. Education has been an essential element of initiatives such as Connect Smart targeting smaller organisations.

Education initiatives also feature prominently in the new Cyber Security Strategy, particularly with the goal to ensure New Zealanders, businesses and government agencies understand cyber threats and have the capability to protect themselves online. However, experts at the Security Summit expressed the view that more needs to be done regarding both security and awareness raising.

The discussion at the Summit highlighted some key areas of concern relating to education and awareness of cyber threats, including:

SMEs – a soft underbelly?

Concerns were raised over the cyber security posture of the thousands of SMEs in New Zealand – with these organisations described as the soft underbelly of New Zealand's national infrastructure. The general lack of security awareness among smaller businesses creates the possibility that SMEs could inadvertently become a threat to the larger organisations or Government agencies they work with.

The need for ongoing education and learning

While the general education philosophy in New Zealand recognises that learning is a lifelong process, involving a number of different agencies, it was felt a similar approach is needed for cyber security. Learning about cyber safety and online threats needs to start at a young age and needs to continue through school and on into the workforce. In countries like Israel, children are taught from a young age to be creative with and explore technology, and also to understand vulnerabilities and threats.

Rewiring tech education

Developing and nurturing a pool of deeply skilled cyber security professionals in New Zealand is critical to strengthening the country's resilience against cyber threats. Work is currently being done to include information technology teaching and computational thinking in the school curricula. Elements of this rewiring must include education in cyber-security. Work needs to be done to attract more interest in security as a career and relevant tertiary options should be developed.

Engaging industry

Engaging the tech sector in education is seen as a key element in achieving greater cyber security training. The importance of having people with real-world security experience in the classroom to teach was also highlighted. The New Zealand tech sector is interested in finding ways to develop integrated teaching and internship pathways with the education sector.

© 2015 New Zealand Technology Industry Association

Reporting

Reluctance from organisations and individuals who have been breached to report incidents, creates a false sense of security among others, thereby perpetuating the belief that it won't happen to them. However, on average there is a 22% likelihood of an organisation experiencing a breach in the next two years. More focus must be placed on reporting in order to better enable understanding and education.

RESILIENCE AND PREPAREDNESS

The need for a coordinated approach to ensure New Zealand organisations, critical infrastructure and the economy as a whole are resilient against and prepared for major cyber-attack incidents was identified.

It was generally agreed that several government agencies have responsibility for ensuring large, strategic organisations and infrastructure of national significance are well prepared for major cyber security incidents and are highly resilient to attacks. However, the issue was raised on how well prepared and resilient the rest of the economy is, and what threat this lack of cyber security readiness posed to the economy as a whole.

In some ways, cyber risks could be compared to earthquake risk in that there is a high probability of a low-probability event occurring. Can we learn from our preparedness for earthquakes and develop similar systems to prepare for cyber-threats - from teaching children to duck and cover, to establishing a national insurance fund.

RECOMMENDATIONS

Addressing the cyber security issues highlighted above will require collaborative efforts between the Government, private sector and the tech sector. It is encouraging that several of the actions in the Government's new Cyber Security Strategy address many of the same issues highlighted at the Security Summit. However, there are specific areas where more work is required, particularly around education, reporting and preparedness. Below are our recommendation for addressing these, in conjunction with the actions outlined in the Cyber Security Strategy:

Improve technology education

Cyber security needs to become part of New Zealanders' DNA, much as road or fire safety have become. Teaching cyber security from a young age will better equip New Zealanders to be more innately aware of cyber threats.

- Integrate cyber security understanding into the school curriculum.
- Make computational thinking and computer studies a core subject from year one similar to the UK and other countries.
- Design cyber security courses for NCEA and tertiary education.
- Engage the technology industry into learning at both school and tertiary levels via internship programmes.

Work together to increase cyber security awareness

The Summit recognised the work the Government has done to date in raising awareness of cyber security among its agencies, crown entities, corporates and consumers. It is recommended the Government make more of its knowledge in this space available to the business sector, especially SMEs, in a more useable format.

© 2015 New Zealand Technology Industry Association

- Provide an accessible and easy-to-understand framework of the key steps organisations and individuals need to follow to ensure their cyber security
- Embedding cyber security into programmes such as the Digital Journey,
- Support the deployment of the Digital Journey tool and encourage more uptake by small businesses.

Increase cyber security resilience and preparedness

Closely associated with the requirement for greater education and awareness, the need to improve New Zealand's resilience to and preparedness for cyber threats was identified. We note that one of the four goals of the Cyber Security Strategy is to ensure New Zealand's Cyber Resilience. The aim is to ensure New Zealand's most significant assets are protected, that agencies may use cyber tools to further New Zealand's national security interests, and to ensure preparedness for major cyber incidents.

We also welcome the proposal of regular cyber security exercises involving the public, private and international partners to ensure preparedness for major cyber incidents, and to test the effectiveness of the National Cyber Security Emergency Response Plan.

- As per the Cyber Security Strategy, we agree that Government and industry should work together to create a cyber security preparedness model for New Zealand.
- Determine which parties are responsible for funding and implementing each element of the response plan.

Improve reporting mechanisms

In line with the actions outlined above to create a greater understanding of cyber security issues, sharing details on cyber threats was identified as a key strategy to help combat cybercrime. Detail gained from an incident against one organisation can provide invaluable intelligence to help protect other organisations, thereby improving New Zealand's overall cyber security resilience. However a weakness was identified in the lack of standardised national reporting of incidents since compulsory disclosure of breaches is not required in New Zealand. While the New Zealand CERT proposed in the Cyber Security Strategy would provide a single point for reporting cyber incidents, more detail is needed on how data collected through such reporting will be shared more widely.

- Enhance the role of a CERT to encourage or mandate reporting of incidents. We believe this will assist in both educating and alerting the wider community of emerging threats to help organisations better prepare against such threats.

Educate SMEs on highly effective controls

The strategy proposes a cyber credentials scheme to complement Connect Smart's SME Cyber Security Toolkit. This scheme aims to promote to SMEs the core actions required to boost their cyber security significantly. We welcome this proposed scheme as it helps to establish crucial cyber security standards SMEs can aspire to, which, as discussions at the Summit highlighted, are sorely needed for this sector. However, we believe the scope of this scheme needs to be widened to include help and support for SMEs to train their technical staff to carry out ICT security, or to access such skills easily and affordably. We look forward to seeing more detail on how these credentials will be formulated and assessed.

© 2015 New Zealand Technology Industry Association

CONCLUSION

We welcome the acknowledgement by Minister Adams at the Security Summit of the major part the technology industry can play in cyber security. We are also pleased to note this sentiment is reiterated in the Cyber Security Strategy with partnerships with industry among the four principles that underpin the strategy.

Leaders at the NZTech Security Summit identified that partnerships between the public and private sectors, and the technology industry, are critical to achieving all the recommendations presented in this paper.

The New Zealand technology industry looks forward to working with the Government to help improve New Zealand's cyber security awareness, skills, readiness and resilience.

We believe only through collaborative efforts can we create a secure, resilient and cyber safe New Zealand.

CONTACT

For any queries, discussion or feedback regarding this paper, contact the author:

Graeme Muller, CEO, NZTech

graeme.muller@nztech.org.nz | Phone 09 475 0204 | www.nztech.org.nz

NEW ZEALAND TECHNOLOGY INDUSTRY ASSOCIATION

The New Zealand Technology Industry Association (NZTech) is the national voice for the technology sector in New Zealand.

NZTech is a not-for-profit association funded by members - the technology businesses in New Zealand and associated partners - from start-ups and local IT firms through to hi-tech manufacturers, major corporations and tertiary institutes.

NZTech works to increase New Zealand's prosperity through better use of technology and strategically focuses on enhancing skills and talents, driving business growth and exports, and guiding and supporting government policy. By actively encouraging relevant initiatives and policies that stimulate and advance the use of technology, together we aim to increase New Zealand's productivity, innovation and economic growth.

DISCLAIMER

Any opinion and analysis presented in this Briefing Paper are the opinion of the author of the paper, not the opinion of the members of NZTech. Any NZTech information that is to be used in press releases or promotional materials requires prior written approval from NZTech.

New Zealand Technology Industry Association
L1 Building C, 14-22 Triton Drive, Auckland 0632, New Zealand
Ph +64 9 475 0204
www.nztech.org.nz

Copyright 2015 New Zealand Technology Industry Association.
Reproduction is forbidden unless authorised