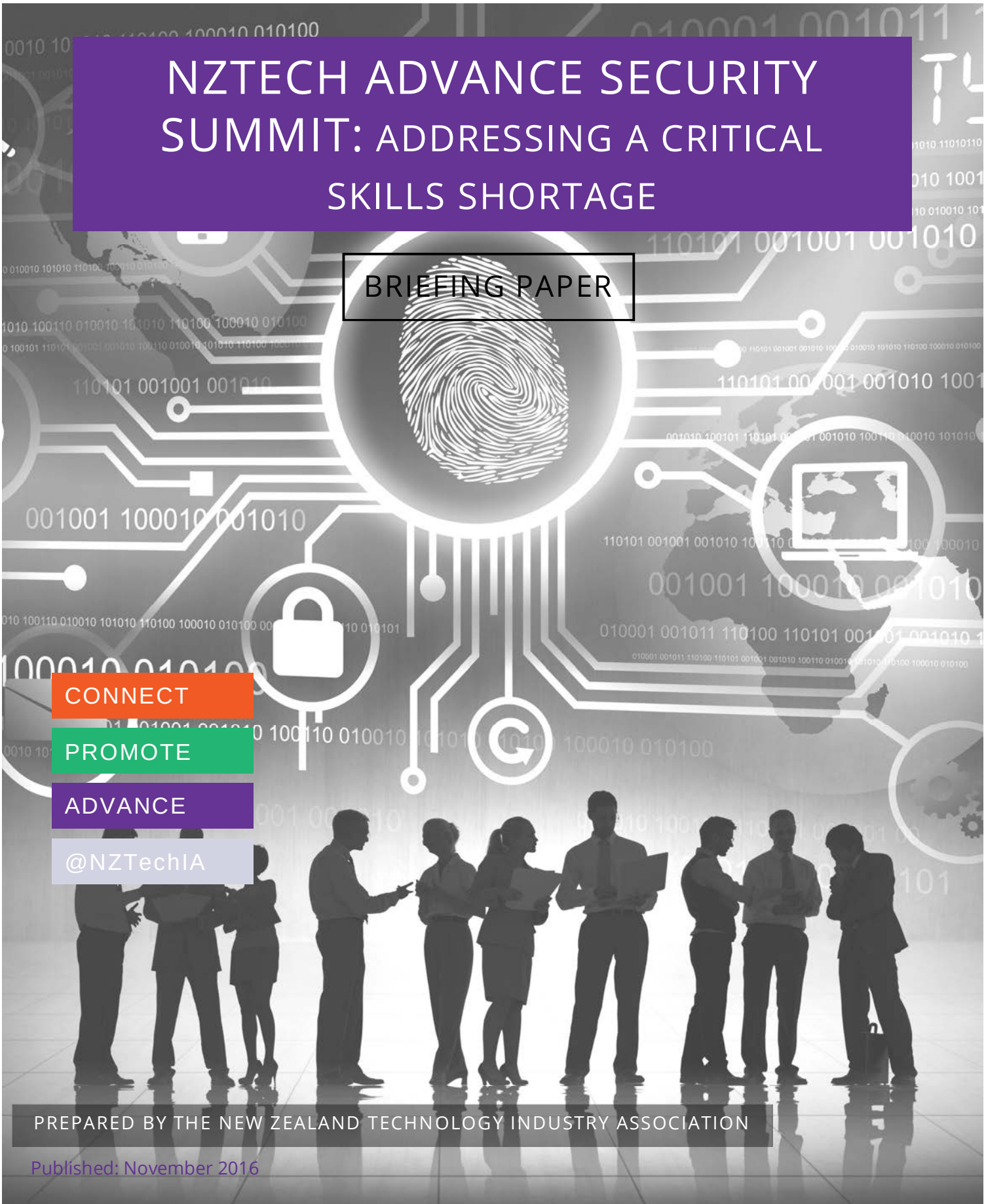
NZTECH ADVANCE SECURITY SUMMIT: ADDRESSING A CRITICAL SKILLS SHORTAGE

BRIEFING PAPER



PREPARED BY THE NEW ZEALAND TECHNOLOGY INDUSTRY ASSOCIATION

Published: November 2016

NZTECH ADVANCE SECURITY SUMMIT:

Addressing a Critical Skills Shortage

NOVEMBER 2016

This NZTech briefing paper provides insights from the recent NZTech Advance Security Summit in Wellington, an event organised and hosted as a joint venture between NZTech and Conferenz. The paper includes key observations from roundtable discussions involving senior executives and security specialists from a broad cross section of government agencies, large private corporations and the tech sector.

EXECUTIVE SUMMARY

Cybercrime is on the increase. Criminals have determined that it is safer and more lucrative to rob and extort online than via traditional methods. This realisation is driving an increasing number of criminals and criminal organisations into cybercrime. In response, there is an increasing demand for cyber security professionals. Recent reports suggest there is a global skills shortage of more than one million cyber security professionals, as government and corporations struggle to keep up with the large growth in cyber threats.

Subsequently, the New Zealand government's Cyber Security Strategy identifies the development of cyber capabilities as one of its four pillar strategies. A collaborative private-public sector taskforce has been established to proactively initiate solutions within New Zealand to help address this emerging challenge. The NZTech Leaders Forum at the Security Summit brought together another group of tech leaders to further explore the cyber skills challenge and discussion identified the following insights:

- **We need to raise awareness:** a concerted effort is needed to raise awareness of the career opportunities in cybersecurity, appealing to a diverse talent pool.
- **We need to develop education:** traditional education and existing policies are clearly not meeting current demand, let alone preparing for unprecedented future demand and a collaborative approach will be needed.
- **We need to develop a clear pathway:** a bridge needs to be created to connect the supply and demand of cybersecurity skills. An internship programme must be integrated into any specialist tertiary study to provide relevant opportunities to develop skills and to increase the work readiness of graduates.
- **We need a published skills list:** immigration was identified as a potential stop gap to the local shortage, however, cybersecurity is an emerging sector and the shortage is global. If immigration is to be considered in part to build local capability, a published skill base is required.

THE RISE AND RISE OF CYBERCRIME

In addressing the Summit, the Hon Amy Adams, Minister of Communications, expressed concern that there is a significant shortage of cybersecurity talent and that a clear way forward is required. Many businesses simply cannot fill roles that require cybersecurity skills, due to a severe lack of available talent.

At the heart of the issue is the need to have a secure nation, protecting businesses and infrastructure from attacks by cybercriminals, criminal groups and terrorist organisations. Despite our geographic isolation as an island nation, cybercrime is a borderless crime that affects us all. Cybercrime is now bigger than the global drugs trade and the local incidence of phishing emails and ransomware is only increasing. Without a secure nation, we won't have a prosperous New Zealand, said Minister Adams.

As technology accelerates at an exponential rate, so does cybercrime. Newer technologies like mobile, cloud and IoT are prime targets for cybercriminals to cause disruption through online attacks. Criminals have determined that with seemingly no physical risk, instead of robbing one person at a time, with digital tools they can rob millions in an instant. This new risk/reward ratio has seen an increasing number of both career criminals and criminal organisations turn to cybercrime.

Whilst New Zealand has been trailing our international partners in the Cybersecurity sphere, the recent establishment of a national CERT is evidence of the government's commitment. We have an excellent opportunity to learn from other nations experiences, so that in turn, we can quickly become more effective.

The Minister also encouraged organisations of all sizes to review their cyber security practices. The shortage in cybersecurity skills is effectively leaving companies and organisations highly vulnerable and at risk. As identified in the Cyber Security Strategy, it is imperative that we act quickly to defeat cybersecurity threats as they continue to grow at an alarming rate.

Figure 1. New Zealand's Cyber Security Strategy

Source: New Zealand's Cyber Security Strategy, Department of the Prime Minister and Cabinet, 2015

The recent *Digital Nation New Zealand: From Tech Sector to Digital Nation* report highlighted that the tech sector touches all of New Zealand, generates exports, creates jobs and provides the foundation for all industries. Understanding workforce development is critical to advancing and protecting New Zealand. Subsequently, the cybersecurity skills shortage is a challenge for every sector across New Zealand, however, it is more than just an IT issue as it requires a specialist skill set. High value

cybersecurity skills in short supply include breach detection and attack mitigation. Other growth roles include security analyst, security auditor, security architect, forensic analyst, information assurance and Chief Information Security Officer (CISO). With the rapidly evolving nature of cybercrime, likewise, the skills required to detect and deal with intrusions is growing at an equally fast pace. It is anticipated that demand will grow for risk assessment and management in the coming years, alongside incident response and investigation. As a result of the short supply of cybersecurity experts, available roles are commanding premium remuneration packages.

CYBERSECURITY AS A SPECIALISATION

Recent reports have announced a global cyber security skills shortage of more than one million people, as government and corporations struggle to keep up with the growth in cyber threats. In the United States, there are currently over 200,000 open cyber security jobs without candidates and cyber jobs have grown 74 percent in the last five years. Nearly 75 percent of US security professionals say they do not have enough staff to defend their organisations against current threats. As cybercrime continues to escalate, the need for skills and talent will only be more prevalent. Predictions expect global demand for a cybersecurity workforce to increase to 6 million by 2019.

Cybersecurity is a specialisation and we need to develop greater capability locally. Cybersecurity specialists need to be agile and constantly updating their skill set in alignment with cybercrime innovation. In part, the lack of standardised job titles is presenting as a common issue.

In New Zealand, the government and the tech sector have recognised this growing global problem and have created a collaborative private-public sector taskforce, including education personnel, to proactively initiate solutions within New Zealand such as the introduction of specialist tertiary degrees and the inclusion of cyber security in the new digitech curricula. The taskforce is developing a Level 6 Diploma to help develop junior security analysts to provide a pathway into cybersecurity for local students. The Diploma will connect back into year 13, include an extensive internship programme and a potential pathway onward into degree courses.

BUILDING CYBERSECURITY CAPABILITY

Traditional education and existing policies are clearly not meeting current demand, let alone preparing for unprecedented future demand. To grow a cybersecurity workforce to meet current and future demand requires a collaborative approach, bringing together multiple agencies working towards various solutions. Timing is also critical in delivering a skilled cybersecurity workforce as traditional degree courses for example, will mean a 4-6 year time delay.

The roundtable at the summit identified that building cybersecurity capability requires a twofold approach, addressing the issue of both supply and demand.

With regards to supply, general education is required to raise awareness of career opportunities in cybersecurity. This includes increasing awareness of cybersecurity as a career for children and school leavers. Pursuing a more diverse talent pool is an obvious option, as is apparent in the tech sector as a whole.

In addition, specific and relevant courses need to be designed to meet the demand. A traditional three year degree may not necessarily be the most relevant way to instil knowledge as much of the talent may already be employed and require a modular approach to learning that can be completed whilst on the job. This approach will up skill existing talent without removing them from the workforce for an extended period of time.

In the interim, a bridge needs to be created to connect the supply and demand of cybersecurity skills. It was suggested that this could take the form of internships. However, it was strongly agreed that for internships to be successful, industry needs to be actively involved to ensure their effectiveness.

While immigration was identified as a potential stop gap to the local shortage, cybersecurity is an emerging sector and the shortage is global. If immigration is to be considered in part to build local capability, a published skill base is required. This currently doesn't exist.

RECOMMENDATIONS

To close the gap between demand and supply in the newly emerging cybersecurity field, NZTech makes the following recommendations to build capability:

1. **Raise Awareness**
   - while promoting the importance of cyber security in general, the National Cyber Policy Office and its Connect Smart brand should leverage the marketing effort to also raise awareness of cybersecurity as a career option.
   - ensure that an understanding of cybersecurity is included as part of digital citizenship within the new digitech curricula in schools, then highlight the growing career options in this space.
   - take the opportunity to raise awareness across a diverse potential talent pool by ensuring all communication is broadly appealing and avoid the trap of promoting stereotypical tech roles.
2. **Develop Education**
   - review formal education offerings, especially traditional diploma and degree courses, and encourage them (where possible) to include relevant cyber security modules.
   - encourage the creation of modular courses that can be obtained in and around working hours as this will make it easier to support the upskilling of the current workforce.
   - the nature and scale of the challenge warrants the rapid development of a specialist tertiary course to develop cohorts of work ready cyber specialists.
3. **Develop a Clear Pathway**
   - integrate an extensive internship programme into any specialist tertiary study to provide relevant opportunities to develop skills and to increase the work readiness of graduates.
   - NZTech recommends taking the successful Summer of Tech internship program and integrating it into all relevant computer science, information technology and cyber security tertiary programmes to create a comprehensive nationwide pathway from tertiary studies into tech roles.

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