THE GLOBAL CYBER SECURITY WORKFORCE - AN ONGOING HUMAN CAPITAL CRISIS

Leon Fourie, Abdolhossein Sarrafzadeh, Shaoning Pang, Tamsin Kingston
Unitec Institute of Technology, New Zealand

Hinne Hettema
University of Auckland, New Zealand

Paul Watters
Massey University, New Zealand

ABSTRACT

Cyber threats pose substantial risk to government, businesses and individuals. There is an alarming shortage of trained professionals and academic programs to train and produce these professionals. Many countries including the US and New Zealand see this as a human capital crisis. This paper discusses the severity and various dimensions of this crisis. An analysis of data from a cyber security research centre collected on cyber attacks is presented, practical solutions are proposed and examples from New Zealand are detailed in this paper. The paper draws conclusions based on the comparative data collected on New Zealand and Japan.

Keywords: Cyberspace, security, workforce.

INTRODUCTION

Insufficient attention paid to cyber security is a major risk internationally, nationally, to businesses and to individuals. The shortage of cyber security professionals to address this risk, and a lack of education programs to train these professionals, has led to a "human capital crisis in cybersecurity" (Evans & Reeder, 2010, p.1). This has serious implications due to the increased reliance on the services and information that make up cyber space. This is especially true with Small to Medium Enterprises who, due to a number of reasons, may be less protected, making this even more significant in New Zealand where 97.2 of businesses fit this category (Ministry of Business, Innovation and Employment, 2013). Cybersecurity may be defined as

> "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets"

based on ITU-T Recommendation X.1205 (International Communications Union, 2008).

Cyber crime is bigger than the global black market in marijuana, cocaine and heroin combined. Globally in 2012, consumer cybercrime cost 110 billion US dollars and was experienced by 556 million people – that is 1.5 million people per day (2012 Norton Cybercrime Report). In 2012 cybercrime is estimated to have cost New Zealanders 463 million dollars (Halls, 2013), and the Norton Report on Cybercrime (Palmer & Merritt, 2012) suggested that 72% of adults in Australasia were victims of cybercrime. However, many New Zealanders do not take cyber security seriously, and are unaware of major cyber security risks that they might encounter or to which they might expose themselves – distance has partially protected New Zealand from organised crime in the past, but cyber crime has no borders. This is a global issue, with many consumers having poor or no security on their computers, cell phones and other digital devices (Palmer & Merritt, 2012). These monetary figures do

©Copyright 2014 by the Global Business and Technology Association

not take into account the damage to reputations of both individuals and companies, or the risk to governments, that malicious cyber activity can cause.

Cyber criminals also target governments and governmental infrastructure. In May 2013, Amy Adams, New Zealand's Communications and Information Technology Minister, outlined that in 2012 New Zealand's National Cyber Security Centre incident summary reported an increase of about 50 per cent in serious cyber intrusions when compared to 2011. These serious incidents met a threshold of putting New Zealand government information or critical national infrastructure at risk. There were 134 of these incidents in 2012 and by May 2013, 149 had occurred, showing the trend of rapid acceleration continuing.

Governments have recognised the seriousness of cyber attacks, with the UK governments National Security Strategy classifying cyber attacks as being at the same level as terrorism (Association of Records Managers and Administrators, 2013) and the US President recently stating "cyber threats pose one the gravest national security dangers that the United States faces." (The White House, Office of the Press Secretary, n.d.). Although this has been recognised for some time (Reppert, 2005) governments have been slow to respond with formal cyber security strategies being developed as late as the late 2000's ((UK, USA and Australia in 2008/9) or early in this decade (New Zealand in 2011)

Businesses are also under attack from cyber criminals. "A recent study of UK organisations revealed that 83% experienced a data security issue last year [2012]" (Association of Records Managers and Administrators, 2013). Companies are investing in cyber security education and technology to protect themselves from cyber threats. Target in the US for example is "investing US$5 million in a multi-year campaign to educate the public on the dangers of scams, after the company disclosed that up to 110 million people may have been affected by a data breach at the retailer's U.S. stores" (Ribeiro, 2014). IBM have expanded their Cyber Security Innovation Program, where they work with universities to develop programs and fund research in cyber security (Lemos, 2013). Business is also having to grapple with the issues that bring-your-own-device are causing, with many staff accessing company IT with their own phones and computers, which are often considerably less secure than those overseen by IT departments.

CYBER THREATS, CYBER SECURITY EDUCATION AND WORKFORCE IMPLICATIONS

There has been a recognition that cyber security research is an increasingly important area in the field of computing, however it has been suggested that this is an area that has been neglected (McGettrick, 2013) and only in recent years has there been an increased focus in the field. There is global recognition by industry (Lemos, 2013), academia (York, 2013; Platt, 2013; Dodge, Toregas & Hoffman, 2011; Assante & Tobey, 2011)) government (Evans & Reeder, 2010; NZ Government, 2011; Cabinet Office, 2009; Homeland Security, 2011) and industry organisations that there is a need for people who are experienced in cyber security, and that this need is not being filled. Four years ago the following was stated "the cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal government" (Evans & Reeder, 2010, p.1), however progress on addressing this issue has been slow. There is also a perception amongst some that "the evolution of a university-level cybersecurity curriculum is being stunted by the culture and values in universities as well as by our ignorance" (Schneider, 2013) and that there is fragmentation in the training (Hoffman, Burley and Toregas, 2012), to the detriment of the development of the cyber security profession. Hoffman, Burley and Toregas (2012) suggest that cyber security as a field is very new, and that it benefits from a more cross functional approach from other disciplines, rather than the siloed approach that many universities take. Bagchi-Sen, Rao & Upadhyaya (2009) agree that cyber professionals need to merge IT knowledge with other fields such as physical security, privacy management, business contingency and legal matters They also suggest that credentialisation has not developed enough prestige in the US.

Cyber Threats and their proliferation

 ©Copyright 2014 by the Global Business and Technology Association

There are many types of cyber threats which include cyber crime, cyber espionage, hacktivism, cyber terrorism, cyber bullying and phishing (Ma, Ofoghi, Watters & Brown, 2009; McCombie, Watters, Ng & Watson, 2008). Some of the broad categories are outlined below.

Botnets are a collection of compromised computers which may be used to generate and distribute spam, viruses and other harmful programs. They have become more widespread, resilient and camouflaged, with an increasing reliance on the use of the 'Darknet' (Sophos, 2013). Recent public examples of the use of botnets is ransomware such as Crpytolocker where "once your data has been encrypted by the bad guys, the only way to retrieve it is with the private key stored on their server – for which you have to pay the criminals" (Sophos, 2013, p 5). Android malware, first detected in 2010 (Sophos, 2013) is proliferating, and infiltration by botnets and other malware is used to ransom phone owners, steal their data, and prevent their full usage of the phone. Google is fighting back, but Sophos found over 300 malware families focussed on androids alone in their 2013 research. Operating systems such as Linux and MacOS X have also been found to have vulnerabilities that are being exploited by cyber criminals, allowing them access to users of these systems. Web based malware is becoming more prevalent as the internet pervades all aspects of our lives, and compromised web servers deliver "some exceptionally serious malware" (Sophos, 2013, p.17) to computers that access web sites. Older software is also likely to become riskier to use, and with some Windows and Office support finishing in April 2014 this could be a serious target. And scams and spams of varying levels of seriousness continue to be used by cyber criminals.

Cyber Security Risks to Countries and Individuals

National infrastructure is an area of considerable concern. Our reliance on IT to run most infrastructure systems make them vulnerable to cyber attacks. These systems include power grids and water supplies – cyber criminals could take control of the power grid, or of government IT systems. Cyber theft can also be from organisations – attempting to steal money or gather information that can be used to steal money (for example credit card numbers). Banking systems have been attacked requiring ongoing responses from the banking sector (Motley, 2012). Theft of personal information and of identities of customers of targeted organisations that can be used by cyber criminals is also increasing – the attack on Target which occurred in the US is evidence of how much information can be stolen relatively easily (Perlroth, 2013). On a more personal basis, on a daily basis individuals are convinced by emails to give strangers money, enter their online banking passwords, or allow cyber criminals access to their computers and pay for software that is not required to "fix" their computer.

Cyber bullying can occur through IT devices (including cell phones) and IT tools such as email, Facebook, and ask.fm. Tragic outcomes of this bullying include people taking their lives. Interfering with electronic medical devices, for example pacemakers which could be externally controlled, could be fatal. Cyber ransom is the practice of taking exclusive control of IT devices and the individuals or companies whose devices are blocked being required to pay a ransom in order to regain access to their devices. The easy availability and transferability of information brought by the reliance on electronic storage and electronic communications has also enabled activities of a political nature, such as hacktivism, which may have harmful consequences.

THE HUMAN CAPITAL CRISIS AND CYBER SECURITY JOB OPPORTUNITIES

The rise in concern over cyber security issues, particularly at governmental and organisational level, has resulted in concern about the number of cyber security graduates and cyber security professionals available to protect the cyber sphere. There is a recognised international shortage of cyber security professionals.

Governments have reacted to this demand with a variety of strategies. A key part of the 2011 New Zealand Cyber Security strategy is to work with educators to meet the demand for cyber security graduates (NZ Government, 2011). The US government has developed the National Initiative for Cybersecurity Education.

> "A nationally-coordinated effort comprised of over 20 Federal departments and agencies, academia, and industry. The mission of this initiative is to enhance the overall cybersecurity posture of the United states by accelerating the availability of educational and training resources designed to improve the cyber behaviour,

©Copyright 2014 by the Global Business and Technology Association

skills, and knowledge of every segment of the population, enabling a safer cyberspace for all" (Homeland Security n.d.) .

This initiative has four components, one of which is the Formal Cybersecurity Education component, which "aims to strengthen the academic pipeline leading to cybersecurity careers" (Homeland Security n.d.). Other components of this initiative support the workforce structure, cybersecurity awareness, and training and professional development in cyber security. In the United Kingdom the government is working with higher education institutions to develop cyber security programmes, with two universities being funded by the UK's Department for Business, Innovation and Skills and the Engineering and Physical Sciences Research Council Association of Records Managers and Administrators, 2013). In Australia one of the strategic priorities stated in their cyber security strategy is to promote the development of the cyber security workforce (Australian Government, 2009).

Many countries now have a cyber security strategy and a government department responsible for cyber security – in NZ this is the National Cyber Security Centre (http://www.ncsc.govt.nz/). There is also a recognition that there is a lack of cyber security expertise and government agencies are working with the education sector to address this (Lemos, 2013),. However the gap between the need for trained cyber security professionals and the supply of these professionals is still wide. The US Occupational Outlook Handbook predicts that IT security jobs will grow 37% between 2012 and 2012 (Bureau of Labor Statistics). The competition for cyber professionals remains strong as demand outstrips supply (Lemos, 2013; Fitzpatrick, 2012A) – this seems likely to be the case for some time. Many educational institutions are developing programs to fulfil this need. Internationally cyber security programs in higher education are booming (Chang, 2013; York, 2013; Association of Records Managers and Administrators, 2013) and alternative ways of becoming qualified such as certification and credentialing are being explored, particularly as many cyber security professionals emerge from hacker culture (Platt, 2013) and may not have formal qualifications from traditional institutions.

Cyber security education in New Zealand

Several tertiary institutions in New Zealand have now realized the need for developing cyber security programs. For example Unitec Institute of Technology in Auckland developed a co-ordinated response to this skills gap by developing a number of programs at all levels of higher education starting as early as 2011. These programs are supplemented by the research undertaken in the Centre for Computational Intelligence for Cyber Security at Unitec. These programs include:

Undergraduate degree pathway in cyber security
Graduate Diploma in Cyber Security
Master of Computing – cyber security endorsement
Doctor of Computing (professional doctorate)
Joint badged PhD - NAIST, Unitec, and NICT.

A number of courses have been introduced through these programmes, and students start taking courses related to cyber security in their first year of studies. These courses include advanced concepts in cyber security at undergraduate level and cloud and mobile security at postgraduate level.

Other New Zealand institutions have limited offerings and these include a range of courses in the University of Auckland, a new University of Waikato Master's program, and offerings by WelTec in Wellington. Massey University has also recently strengthened its cyber security capability and other universities including AUT University are actively pursuing similar initiatives.

This is however by no means sufficient for a country like New Zealand, where an ultrafast broadband service has been introduced as one of the government's election promises. The security of fast internet would require a much larger workforce than can be provided through these limited programme offerings. This has been recognised by government and tertiary providers and is being addressed by institutions throughout the country. Closer collaborations and some joint offerings supported by industry is a necessity if this workforce is to expand to meet demand.

 ©Copyright 2014 by the Global Business and Technology Association

RESEARCH INITIATIVES

There is only one established centre for cyber security research, and a newly established cyber security lab, at tertiary institutions in New Zealand, although many institutions have realized the need for such centres and have taken initial steps towards setting up research facilities for cybersecurity. Established in 2011, the Computational Intelligence for Cyber-Security (CICS) facility at Unitec is a joint venture between Unitec Institute of Technology New Zealand and National Institute of Information and Communications Technology (NICT) Japan.

This centre provides cutting edge cyber security monitoring capability, aiming to build human and technological capital in New Zealand and explore opportunities to engage relevant stakeholders and an alert system that is able to provide security to NZ including our businesses. This centre aims to:

- Serve as a cyber security hub
- Conduct and foster applied, high impact cyber security research
- Provide cyber security education to develop highly productive talent
- Produce highly employable graduates
- Help create public awareness
- Sponsor, coordinate, and provide cyber security information and training to the public

International research collaboration is essential to fight the global threat posed by cyber crime. Recognizing this need, a partnership with NICT in Japan has provided us with both a cyber security monitoring system and an attack alert system which form some of the tools used in the cyber security research centre. Collaboration with Nara Institute of Science and Technology in Japan (NAIST) has further strengthened the centre's research capability and doctoral level education through the development of a joint PhD focussed mainly on cyber security.

This research facility is researching ways to help prevent future attacks. It will help create a safe, secure and resilient cyber environment for New Zealand. We are providing advanced and up-to-date training and education for students wanting to pursue a career in cyber security. In 2013, the University of Waikato launched a cyber security laboratory to strengthen their cyber security capability. It is hoped that this centre will be able to help other institutions develop similar facilities both nationally and internationally.

Research Centre for Computational Intelligence for Cybersecurity (CICS)

The centre based at Unitec is modelled on Japan's headquarter centre and has technology which monitors cyber traffic coming in and out of New Zealand. The two centres share their data and information in order to help analyse and control the situation of cyber attacks.

As cyber security is becoming a rapidly developing profession, the centre provides advanced and up-to-date training and education for students wanting to pursue a career in cyber security. Commentators suggest that if you want job security, look to cybersecurity (Fitzpatrick, 2012B). The centre also allows students to gain hands-on experience with working on a number of current cyber security projects, and will give these students access to opportunities to travel to Japan and work on cutting edge equipment. The centre is working to increase the security capable workforce in New Zealand.

The collaboration between Unitec and NICT also aims to increase awareness with the public about the risks of going online, to develop and maintain a globally competitive cyber security workforce, and to encourage and engage people to become interested in science, technology and cyber security. The centre will in future offer short courses and seminars to increase public awareness and help combat cyber security risks to the public.

The Cybersecurity Lab – technical aspects

©Copyright 2014 by the Global Business and Technology Association

The lab is part of CICS and consists of sophisticated hardware and software some of which was imported from Japan through NICT. The equipment includes serves, terminals, sensors, networking equipment and specialised software. The hardware includes the following equipment:

a) 6 x Dell Poweredge R210-II Servers
b) 2 x Dell Powerconnect 5548 Switches
c) 2 x 50" Monitors
d) 2x 30" LED Screens
e) Rackspace as required
f) Fortinet 110C Firewall
g) Dlink DMC-300SC Media Converter for fibre connection to Building
h) Core BigIron RX16
i) Switch-ports to Cisco 3560g Other equipment

Currently, the centre hosts three network monitoring systems
(1) Network Incident analysis Centre for Tactical Emergency Response (NICTER) - see Figure 1. The system deploys several analysis engines taking advantage of data mining techniques to analyse the monitored traffic.
(2) The NIRVANA system (see Figure 2). The system visualizes the Unitec campus network traffic following through a network in real time, which allows a network administrator to promptly check the network for proper connections, fault detection, congestion, and setting errors.
(3) The Daedalus Alert System (see Figure 3). The system monitors computers of Unitec campus network for any suspicious activity and can visualize the progression of an attack as it moves through the network.

Figure 1. Network Incident analysis Centre

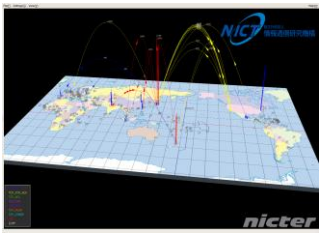

Figure 2. The NIRVANA system

Figure 3. The Daedalus Alert System

Key research topics currently being undertaken at the Centre include:

- Agent-based network intrusion detection
- Real time Darknet and Livenet traffic monitoring
- Malicious software and email spam analysis and detection
- Firewalls vulnerability assessment
- Decentralized network security
- Federated network traffic analysis
- Multi-agent coordination mechanisms and platforms

Monitoring of Attacks

The centre currently monitors 2000 Darknet IP addresses in New Zealand and 4000 in Japan. Figure 4. below shows a daily comparison of the number of attacks on those IP addresses in New Zealand and Japan over a period of 12 days, and Figure 5. provides an annual comparison.

Given that the number of IP addresses monitored in Japan is double the number that are monitored in New Zealand it would be expected that the number of packets detected would reflect the same ratio. However looking at the total number of packets received it seems that there are considerably more attacks on the New Zealand IP addresses.

©Copyright 2014 by the Global Business and Technology Association

Figure 4 Daily comparison of attacks – NZ and Japan

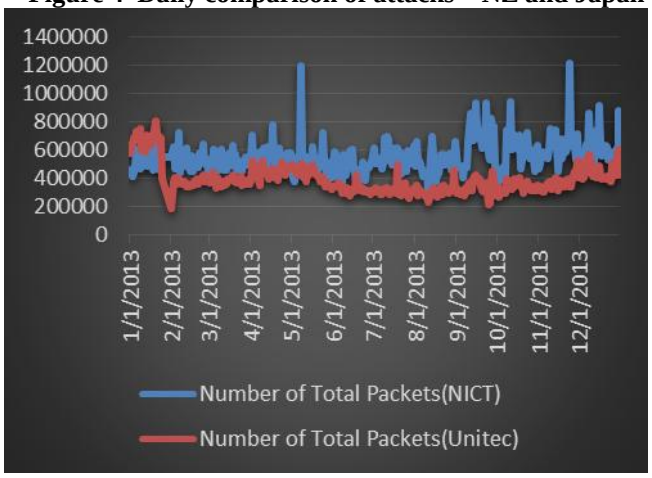

Figure 5. Annual Comparison of six different types of packets detected in the Darknet space

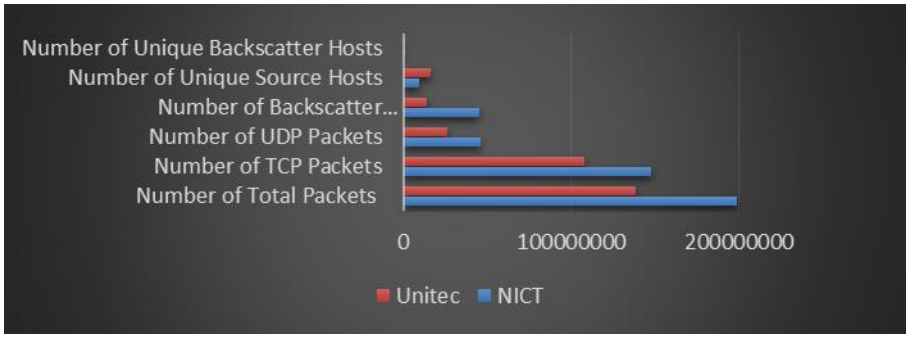

Table 1. Number of attacks in 2013

Measurements (2013)	NICT	Unitec
Number of Total Packets	199207181	138312346
Number of TCP Packets	148010207	107727061
Number of UDP Packets	46017305	25830316
Number of Backscatter Packets(SYN_ACK)	45299988	13499502
Number of Unique Source Hosts	9153129	15793291
Number of Unique Backscatter Hosts	234086	191907

Table 1 shows that threats to security are not proportional to the population, nor are they dependent on the extent of the use of the Internet. A possible explanation for the discrepancy is that the incidence of attack depends on how vulnerable attackers believe a country is, and the perceived vulnerability of systems and infrastructure in that country. Moreover, 'vulnerability' has a network effect. Vulnerabilities present in one country may translate to increased attacks on the infrastructure in related countries dependent on the nature of their interconnectedness. It is important for every nation to keep their communications and network infrastructures safe, and this can only be done with a highly trained workforce.

©Copyright 2014 by the Global Business and Technology Association

A SOLUTION TO THE SHORTAGE OF CYBER SECURITY PROFESSIONALS

To address the problem, higher education institutions can provide responses at different levels, including providing options for people with different skill levels for example:

Short courses covering particular security issues/skill needs for people already working in IT but needing further security training

Certification preparation programmes to formally certify the presence of cyber security skills

Graduate diplomas giving graduates from related IT areas opportunities to retrain in a new field in a cost- and time-effective manner

Bachelors programmes providing well qualified security professionals

Postgraduate programmes provide the opportunity for highly technical cyber security research and interaction with industry

Quick Response

Short courses can be offered for IT staff and managers, which may be heavily technical or strongly informational depending on the audience. Less technical courses may be best for the home user or small business owner wishing to protect their business. New Zealand is dominated by small businesses, with over 90% employing fewer than 20 people (Ministry of Business Innovation and Employment, 2013), and it is unlikely that a security specialist will be one of the employees, so this is particularly important in the New Zealand context.

Certification is another option for those who have existing skills and seek a credential, without the need for a long period of study to get it. More formal programmes can also offer a quick upskilling opportunity to graduates. Graduate Diploma programmes help graduates to move into cyber security from other careers. Many institutions in New Zealand offer Graduate Diplomas that allow students to focus on particular pathways depending on their interest. The Graduate Diploma in cyber security offers students the opportunity to focus on cyber security as a separate career, or to introduce cyber security awareness into their current career.

Longer Term Considerations

It will be important for industry, academia and the government (at national and regional levels) to conduct workforce planning exercises, and then collaborate to implement these plans. A similar broad multi-sector approach will be necessary to highlight cyber security issues in the community, as many cyber crimes affect individual users of IT. Academia will need to be proactive in collaborating with industry to ensure that the skills graduates are being taught remain relevant to the cyber security issues faced by industry – a decade ago who could have comprehended the challenges that bring your own device would cause.

As a result of this cross sector collaboration to develop the cyber security workforce, local responses may emerge to the cyber threats. However much the nature of this education may vary according to regional and local needs, it is important that areas such as ethics, policy, and governance are not neglected in the education of cyber security professionals. No matter how technical the programme may be, these areas are too important to neglect.

CYBER PROTECTION FOR BUSINESSES AND INDIVIDUALS

At a nation level, there is a need for increased cyber security awareness at an organisational level and a personal level. Organisations and individuals can do a lot to protect themselves from cyber attack. Following the following recommendations will significantly reduce the chances of exposure to cyber attacks, or will mitigate the effects of these attacks.

 ©Copyright 2014 by the Global Business and Technology Association

Organisational recommendations

One of the main challenges in the organisational setting is dealing appropriately with the multi-faceted nature of cyber security, especially for small organisations. The issues surrounding cyber security are complex and result from an interplay between human, legal, technical and business factors. Many organisations, especially small organisations, are not ready to take on this challenge.

A particularly pressing issue is that an adequate response to cyber security threats requires trust in, and collaboration with, other organisations that are competitors in a business sense. Hackers are primarily driven by financial motives, and tend to be specialised on particular industries. As a result, there is a significant benefit in competitors sharing cyber security intelligence data, such as malicious IP addresses, malicious URLs and attack tactics used. As an example, in the practical investigation of phishing URLs it is often possible to determine attack pages aimed at other related organisations. Hackers make mistakes too, and are sometimes not that careful about limiting access to the directories on their web server. This allows investigating security teams to discover attack sites that have been used against others or – more importantly – are about to be used against others.

The following broad recommendations should help small organisations get on the path towards an improved cyber security posture:

1. Instigate a cybersecurity task force with management, technical and legal, audit and compliance representation. The cyber security task force is responsible for driving the cyber security strategy of the organisation. For small organisations, it is possible to pool efforts in this area, for instance through utilisation of business associations.
2. Have a technical representative join a trust based network, such as the NZITF in New Zealand. In these networks, security professionals share details and solutions for cyber security problems, which are relevant to most organisations.
3. Ensure that an appropriate incident response plan and capability is in place. With the increase in both number and sophistication of cyber attacks, for most organisations the occurrence of an incident is no longer a question of 'if' but 'when'. Being able to plan and determine a response without the added pressure of having to deal with an incident is an opportunity too precious to waste.
4. Instigate a number of technical controls, such as the following
    a. Have a secure firewall with protection controls
    b. Ensure the network has up-to-date virus software, and that anti-virus scans are undertaken after every update of this software
    c. Ensure all accounts are password protected with strong passwords, and regular compulsory changes
    d. Ensure password expiry mechanisms are in place
    e. Have robust cyber security policies, and enforce these policies at all levels
    f. Consider multi-factor authentification
    g. Ensure this policy covers mobile devices and includes password protection and encryption of strategic information
    h. Ensure automated back-ups of all information occur daily (thus information cannot be held for ransom)
    i. Have a robust BYOD (bring your own device) policy including enforcing password protection to your network
    j. Restrict staff who have administrative privileges to trusted few
    k. Secure WIFI access, ensuring it is encrypted and hidden, with password protection of routers
    l. Ensure security patches are applied in a timely fashion
    m. Only allow those with administrative privileges to download software onto the network

Individual recommendations

©Copyright 2014 by the Global Business and Technology Association

Like organisations, individuals can also take some small beneficial steps to improve their personal cyber security posture. One of the most pressing issues for individuals is the development of a sense of digital hygiene, and prevent the leakage of personal data from heavily consumerised devices.

Some simple technical recommendations are

1. Do not use the same password for all logins, and ensure that the passwords used are strong
2. Password protect all devices – mobile and home based
3. Do not open emails from strangers – or if you accidentally do, do not open any attachments or click on links in these emails
4. Secure WIFI access, ensuring that it is not open, and with password protection of the router, and uses WPA encryption
5. If an online offer seems too good to be true, it probably is – delete the email!
6. Do not respond to online requests for Personally Identifiable Information (PII); most organisations – banks, universities, companies, do not ask for your personal information over the Internet, and will definitely not ask you to reveal your password to a third party
7. Review the privacy settings on social media accounts regularly, to ensure access to your personal information is limited

Some more complex technical remediations are

1. Use JavaScript whitelisting while in a browser session. With the exception of Internet Explorer, most browsers now support easy to use JavaScript whitelisting mechanisms. The smart use of JavaScript whitelisting prevents so-called 'drive-by' attacks.
2. Install and use the Microsoft Enhanced Mitigation Toolkit (EMET), which is a free add-on to the Windows Operating system. This tool prevents many advanced attacks.

CONCLUSION

As seen in the figures and tables above, the comparative data outlined above regarding attacks on New Zealand and on Japan reveal that the New Zealand takes considerably more attacks than are made on Japan. This confirms that a cyber security crisis exists, and New Zealand is not immune from this crisis. Superhighways are created in the new virtual world, and they are growing exponentially. Like real highways, there is a need for designers, for legislative controls, and for a police force to make sure that all those using the virtual superhighway remain safe and protected from harm. Momentum is gathering at the governmental level and at the institutional level to increase education programmes at all levels of society, and to increase the numbers of graduates in cyber security, however currently insufficient programmes shows there needs to be a wider national response to the human capital crisis in cyber security that exists. It is the responsibility of educators to accelerate this progress.

REFERENCES

Association of Records Managers and Administrators (2013). U.S. and UK Universities: Welcome to Cybersecurity 401, *Information Management Journal*, July/August 2013.

Assante, M.J., Tobey, D.H. (2011) Enhancing the Cybersecurity Workforce. IT Pro, January/February 2011, 12-15

Australian Government, Cyber Security Strategy. Retrieved from http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

Bagchi-Sen, S., Rao, H.R., & Upadhyaya, S. (2009) Women in Cybersecurity: A Study of Career Advancement, IT Pro, September/October 2009. IEEE Computer Society, 46-52.

 ©Copyright 2014 by the Global Business and Technology Association

Bureau of Labor Statistics, U.S. Department of Labor. (2014) Information Security Analysts Occupational Outlook Handbook, 2014-15 Edition. Retrieved from http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Cabinet Office (2009). Cyber Security Strategy of the United Kingdom – safety, security and resilience in cyber space. June 2009. TSO.

Center for Strategic and International Studies, Securing Cyberspace for the 44th Presidency, December 2008, p. 72. Retrieved from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Chang, J. M. (2013) New Trends in Cybersecurity. ITPro. July August 2013. IEEE, 2-3.

Dodge, R.C., Toregas, C., & Hoffman, L. (2011) Cybersecurity Workforce Development Directions, Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance. 1-12.

Evans, K. & Reeder, F. (2010). A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency. Centre for Strategic and International Studies: Washington. Retrieved from http://csis.org/files/publication/101111_Evans_HumanCapital_Web.pdf .

Fitzpatrick, A. (2012A) Cybersecurity experts needed to meet growing demand, The Washington Post. Retrieved from http://www.washingtonpost.com/business/economy/cybersecurity-experts-needed-to-meet-growing-demand/2012/05/29/gJQAtev1yU_story.htm

Fitzpatrick, A. (2102B) For Job Security, Try Cyber Security, Experts Say, Mashable. Retrieved from http://mashable.com/2012/05/29/cybersecurity-career/

Halls, C. (2013) Identifying the real cost of cyber crime to New Zealand. Netsafe. Retrieved from http://blog.netsafe.org.nz/2013/05/16/identifying-the-real-cost-of-cyber-crime-to-new-zealand/

Hoffman, L.J., Burley, D.L. & Toregas, C. (2012) Holistically Building the Cybersecurity Workforce. *IEEE Security and Privacy.* March/April 2012, 33-39.

Homeland Security (2011). Blueprint for a Secure Cyber Future – The Cybersecurity Strategy for the Homeland Security Enterprise. Homeland Security. Retrieved from http://www.dhs.gov/blueprint-secure-cyber-future

Homeland Security. About the National Initiative for Cybersecurity Education. Retrieved from http://niccs.us-cert.gov/footer/about-nice

International Telecommunications Union. 2008, X1205: Overview of Cyber Security. Retrieved from http://www.itu.int/rec/T-REC-X.1205-200804-I

Lemos, R. (n.d). Cyber-Security Training a Top Priority for Industry, Government. Retrieved from http://www.eweek.com/security/cyber-security-training-a-top-priority-for-industry-government.html

Ma, L., Ofoghi, B., Watters, P., & Brown, S. (2009, July). Detecting phishing emails using hybrid features. In *Ubiquitous, Autonomic and Trusted Computing, 2009. UIC-ATC'09. Symposia and Workshops on,* 493-497.

McCombie, S., Watters, P.A., Ng, A. & Watson, B. (2008). Forensic characteristics of phishing – Petty theft or organised crime? *Proceedings of the 4th International Conference on Web Information Systems and Technologies* (WEBIST), Madeira, Portugal, 149-157.

McGettrick, A. (2013). Toward Effective Cybersecurity Education. *IEEE Security and Privacy*. November/December 2013, 66-68.

©Copyright 2014 by the Global Business and Technology Association

Ministry of Business, Innovation and Employment (March 2013). Small Businesses in New Zealand – how do they compare with larger firms. Retrieved from http://www.med.govt.nz/business/business-growth-internationalisation/pdf-docs-library/small-and-medium-sized-enterprises/Small-business-stats-factsheet.pdf.

Motley, A. (2012). Cyber Sentries. ICBA Independent Banker. November, 38-41.

NZ Government. (2011) New Zealand's Cyber Security Strategy. Retrieved from http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf

The White House, Office of the Press Secretary. (2014) Statement by the President on the Cybersecurity Framework.[Press release]. Retrieved from http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework

Palmer, A., Merritt, M. (2012) 2012 Norton Cybercrime Report. Retrieved from http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Peltroth, N. 2013 Target Stuck in the Cat-and-Mouse Game of Credit Theft. The New York Times. December 19 2013. Retrieved from http://www.nytimes.com/2013/12/20/technology/target-stolen-shopper-data.html?pagewanted=all&_r=0

Platt, J.R. (2013) Cybersecurity Careers – An International Priority. Ieee-usa today's engineer. June 2013. Retrieved from http://www.todaysengineer.org/2013/Jun/career-focus.asp

Reppert, B. (2005). United States Facing Cyber Security Crisis, Experts Tell Capitol Hill Briefing, As IEEE-USA Prepares New Position Statement. *IEEE-USA Today's Engineer Online*. Retrieved from http://www.todaysengineer.org/2005/Aug/cybersecurity.asp

Ribeiro, J. (2014). Target to invest $5 million in cybersecurity education. CIO Magazine. Retrieved from http://www.cio.co.nz/article/535833/target_invest_5_million_cybersecurity_education/

Schneider, F.B. (2013). Cybersecurity Education in Universities. IEEE Security and Privacy. July/August 2013, 3-4.

Sophos (2013). *Security Threat Report 2014 – Smarter, Shadier, Stealthier Malware*. Retrieved from http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf

The White House (n.d.). The Comprehensive National Cybersecurity Initiative. Retrieved from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

York, T. (2013). School Programs Aim to Meet Demand for IT Security Experts, San Diego Business Journal. June 24, 2013.

 ©Copyright 2014 by the Global Business and Technology Association