VICTORIA UNIVERSITY OF WELLINGTON

Te Whare Wananga o te Upoko o te Ika a Maui

The Great New Zealand Botnet: Broadband to the door an asset or security issue?

A research project presented to the

School of Information Management

Victoria University of Wellington

in partial fulfilment of the requirements for the course on

Research Project

(MMIM 590)

by

Kyle Gibson

Student ID: 300032880

24th February 2012

Abstract

This research explores the level of security awareness, of domestic Internet users in New Zealand. Awareness and online security are the top priorities of the New Zealand Cyber Security Strategy, but little research has been conducted to gauge the current level of security awareness in context with common mitigation strategies. The majority of the literature on the subject is primarily focused on organisational technology security and awareness so this had to be put in context with domestic users.

A sample set of Facebook friends of the researcher were asked to respond to an online survey. The survey explored the respondents' attitude and self-evaluated level of security awareness, and their awareness of a subset of mitigation strategies from the Australian Defence Signals Directorates' 'Strategies to Mitigate Targeted Cyber Intrusions'.

The respondents demonstrated a good level of security awareness regarding patching and anti-virus, but there is a need for more education regarding access control and social engineering.

Preface

I wish to thank my Facebook friends for their participation in my online survey and the insight they provided to the security awareness of domestic Internet users in New Zealand.

I would also like to thank my wife, Angela Gibson, and family for their support, encouragement and patience throughout my studies and, the preparation and writing of this paper.

Finally, I would like to express my appreciation for Dr David Johnstone, my supervisor at Victoria University, for his help, patience and invaluable input for this paper.

Kyle Gibson.

Table of Contents

Introduction

“Infamous hacker Mitnick says only users can stop security leaks.”
(Wasserman, 2000)

Much of the media and academic writing on computer security issues and their mitigation focuses on corporate environments. However, access to the Internet is now considered a basic human right by the United Nations (Anonymous, 2011, Pg 172), so do domestic users need to be aware of the same security issues and mitigation strategies?

This research explores a number of corporate security issues and mitigation strategies and puts them into context with domestic users. But how widespread is the problem and is there any security issue where both domestic and corporate systems play a role and have a direct impact on each other?

One example of a risk that affects both organisational and domestic, Internet connected systems is botnets.

> *“Unprotected home computers that are infected with malware can be used as a resource to build botnets. Botnets harness the computing power of thousands or even millions of individual computers to launch remote attacks on information and communications networks, commercial systems and government websites with the aim of denying the legitimate use of the service.”* (New Zealand Ministry of Economic Development (NZMED), 2011, Pg 4).

Individual infected machines are referred to as Bots or Zombies. Command and Control servers or infrastructure are what hackers use to control the botnets and target the victim system/s (Cooke, Jahanian & McPherson, 2005, Pg 1). The New Zealand Cyber Security Strategy (NZCSS) defines malware as *“Malicious software or potentially unwanted software installed without* *informed user consent, generally covering a range of software programmes designed to attack, or prevent the intended use of information and communications networks."* (NZMED, 2011, Pg 13).

> *"According to a recent report, the number of new bots observed each day rose from less than 2,000 to more than 30,000 over the first six months of 2004. The total number of bot infected systems has been measured to be between 800,000 to 900,000 and the Cyber Emergency Response Team (CERT) has described botnets with more than 100,000 members." (Cooke et al, 2005, Pg 1).*

On March 31, 2010 the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) released a security advisory for the Mariposa botnet. This advisory states that in December 2009 "authorities took down a 12.7 million strong zombie network" (ICS-CERT, 2010, Pg 1). This advisory also states that "it is not uncommon for new groups to assume control of old or abandoned botnets by compromising existing command and control or by establishing new command and control infrastructure using slightly modified malware" (ICS-CERT, 2010, Pg 1).

Mitigation and disruption of botnets is difficult due to the distributed nature of the zombie machines (Cooke et al, 2005, Pg 6) and that victims may not know their machine has been compromised (ICS-CERT, 2010, Pg 1). In order to defend against infection "There are a range of existing techniques, including anti-virus software (AV), firewalls, and automatic patching" (Cooke et al, 2005, Pg 1). This example shows that both organisations and domestic users of the Internet are vulnerable to security threats.

The New Zealand Government also define the following cyber threats:

- *Cyber Crime – Organised crime, dealing in identity theft, selling fake goods, stolen credit card details etc.*
- *Cyber espionage – attacks against government and critical infrastructure.*

- *Hacktivism - gaining control of computer systems or websites to promote a cause, make a political statement or disrupt services.*
- *Terrorist use of the Internet – with a growing dependence on networked systems and the Internet, vulnerable systems may be targeted.*

(NZMED, 2011, Pg 5)

More specifically for domestic users, the NZCSS also highlights social networking threats:

- *Cyber criminals are increasingly using social networking sites to lure victims to web sites that attempt to push malware or launch an attack on the victim's computer.*
- *Attackers exploit the profile information available on social networking sites (e.g. birth dates, phone numbers, employment details and other information) to mount targeted attacks.*

(NZMED, 2011, Pg 5)

In 2011 The National Business Review (NBR) published an article regarding one of the more widely publicised threats of hacktivism in New Zealand. The hacker group Anonymous announced their intention to attack the New Zealand Department of Internal Affairs (NZDIA). The group disagreed with the implementation of an Internet filter that blocked access to images, videos or promotion of child sexual abuse claiming it was "Internet censorship" (NBR, 2011). The group intended to attack and deny access to NZDIA's website by utilising a botnet to launch a denial of service (DoS) attack (Computerworld Staff, 2011). A DoS flooding attack is "a network based attack in which agents intentionally saturate system resources with increased network traffic' to deny access by legitimate users" (Carl, Kesidis, Brooks & Rai, 2006, Pg 82).

This attack was targeted at a government agency rather than domestic users but shows that attacks are being targeted in New Zealand and how compromised domestic systems can be used.

A recent survey showed that 54% of New Zealanders feel they know little or nothing at all about computer security risks and solutions (NZMED, 2011, Pg 4). With this little security knowledge, will the implementation of Ultra-Fast Broadband be a national asset or a high-speed platform populated with compromised domestic systems?

The New Zealand government is focused on delivering high-speed Internet connectivity.

> *"The vision of Crown Fibre Holdings (CFH) is to lead the rollout of Ultra-Fast Broadband to 75% of New Zealanders by 2019. CFH will lead the telecommunications industry in rolling out Ultra-Fast Broadband rapidly, efficiently and cost-effectively, and will enable and drive uptake of Ultra-Fast Broadband across New Zealand" (Crown Fibre Holdings, 2010).*

Internet based threats are targeting both organisational and domestic users. Both groups need to understand the relevant threats and mitigation strategies for their Internet connected systems. The government is building faster networks and recognises the need for greater security awareness by domestic users.

This research will attempt to answer the question:

What level of technology security awareness of mitigation strategies do domestic Internet users have to prevent targeted intrusions?

Literature Review

The majority of academic and practitioner literature on technology security, awareness and mitigation strategies is based on government and business systems. As a result, the majority of examples in this research have an organisational focus but are then put in context with domestic Internet users.

Organisational Security Risks

The Department of Labours' 'Survey of Information Technology (IT) Recruiters 2008', "found that 36 out of the 50 IT occupations surveyed were difficult to fill" (Department of Labour, 2008 Pg 4). The survey found the following roles to be the most difficult to fill:

- *ICT security specialist (100% of recruiters had difficulty filling vacancies)*
- *Telecommunications network planner (100%)*
- *Telecommunications technical officer or technologist (93%)*
- *ICT systems test engineer (93%)*
- *ICT support and test engineer not elsewhere counted (85%)*
- *Telecommunications network engineer (84%)*
- *Telecommunications engineer (83%)*
- *ICT quality assurance engineer (83%)*
- *Software engineer (82%)*
- *Software and applications programmers not elsewhere counted (81%)*

(Department of Labour, 2008, Pg 5)

As has been demonstrated the ICT industry has an overall lack of security skills and knowledge, and the same is also true for domestic users. In order to understand what awareness is required we must first understand the threats organisations and domestic Internet users need to defend themselves from.

Security breaches in large enterprises can impact their services and millions of domestic users. In 2011 "Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins” (Reuters, 2011).

On 17th January 2007, TJX Companies Incorporated (TJX) announced what has been characterized as the largest retail security breach in history (Shaw, 2010, Pg 546). The breach resulted in the loss of 94,000,000 credit cards data, and other personal information such as drivers license details, military and state identification numbers and names and addresses (Shaw, 2010, Pg 546). As a credit card merchant, TJX are required to be compliant with the Payment Card Industry Data Security Standard (PCI DSS). Investigations into the breach revealed that there were a number of contributing factors:

- Storing and transmitting personal information in clear text (Not encrypted).
- Failing to use readily available security measures to limit access to wireless networks and card authorization computers.
- System administrators not being required to use strong passwords.
- Insufficient measures to detect and prevent unauthorised access such as updating anti-virus software.
- Not following up on security intrusion alerts.

Although they had been assessed as compliant with the standard, many of the requirements weren’t in place. Additionally they were storing magnetic stripe data that is prohibited by the participating credit card brands.
“The U.S. Federal Trade Commission (FTC) charged, TJX engaged in a number of practises that, taken together, failed to provide reasonable and appropriate security for personal information on its networks.” (Shaw, 2010, Pg 547). This shows that even large organisations that are required to comply with governance standards have difficulty securing their systems.

Because New Zealand does not have appropriate security breach laws that require mandatory disclosure of the loss of sensitive information, it is difficult to find information on local data breaches. In New Zealand Legislation regarding mandatory disclosure of data breaches is under review as many go unreported (Scroggie, 2011).

Although it is difficult to judge how many data breaches occur in New Zealand, the media has reported some examples. In 2010 the Auckland City Councils' Downtown Car Park suffered a data breach that resulted in the loss of at least 100,000 of its customers credit card information (Vass, 2010). Queenstown's Main Street parking building also suffered a similar breach in 2010 (Bryant, 2010). Based on technology security incidents that were reported to the National Cyber Security Centre (NCSC) in 2010, nearly 25% of New Zealanders have been victims of cyber crime or cyber security incidents with an associated cost of approximately $600 million (NCSC, 2012).

Organisational Security Risk Mitigation Strategies

Due to security issues and a lack of security knowledge that have resulted in data breaches, governments and a number of market sectors have introduced security standards and governance frameworks. The NZCSS provides a high level strategy but does not go into detail regarding policy or mitigation strategies. The New Zealand Information Security Manual (NZISM) was published in 2010 and replaced the New Zealand Security of Information Technology (NZSIT) 400, 401 and 402 policies and guidelines which were published in 2008 (Government Communications Security Bureau, 2012). The NZISM is intended to be a formal guideline for government agencies. This document is publically available so it can be used as a guideline for government agencies, business and private sector organisations. It is a large complex document and would be difficult to apply to domestic users.

In 2011 the Australian Department of Defence, Defence Signals Directorate (DSD) published 'Strategies to Mitigate Cyber Intrusions', which won the National Cyber Security Award in 2011. The award is judged on four main criteria:

- It is an innovation that has not been deployed effectively before;
- It can show a significant impact on reducing cyber risk;

- It can be scaled quickly to serve large numbers of people; and
- It should be adopted quickly by many organisations.

The research done by the DSD found four controls that “must be implemented across all Cabinet-level organizations if they are to have any hope of defending their systems against targeted intrusions” (Paller, 2011). “At least 85% of the targeted cyber intrusions that the DSD responded to in 2010 could have been prevented by following the first four mitigation strategies” (DSD, 2011, Pg 1).

> *“The cost of implementing these four controls is a tiny fraction of the cost of implementing the average U.S. federal government agency cyber security program. Since the impact of this low-cost approach is much better security than what U.S. agencies are experiencing, the Australian innovation changes the game” (Paller, 2011).*

The strategy also has proven success. The DSD worked with government agencies to implement the top four strategies and as a result “the spread of targeted attacks is no longer a significant problem” (SANS, 2011).

While the Strategy is targeted at government agencies, business and private sector organisations, three of the top four mitigation strategies can be implemented by domestic users at no cost. Also rather than being a large complex document, the DSD document is a brief, ranked set of mitigation strategies. The top four strategies are shown in Table 1.

Table 1 – DSD Top Four Mitigation Strategies

Ranking	Strategy
1.	Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high-risk vulnerabilities. Use the latest version of applications.
2.	Patch operating system vulnerabilities. Patch or mitigate within two days for high-risk vulnerabilities. Use the latest operating system version.
3.	Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.

4.	Application whitelisting to help prevent malicious software and other unapproved programs from running e.g. by using Microsoft Software Restriction Policies or AppLocker.

(DSD, 2011 Pg 2)

The PCI DSS was created to provide a minimum standard of technology security for credit card merchants and service providers. The standard is created and maintained by the Payment Card Industry Security Standards Council (PCI SSC). Representatives from Visa, MasterCard, American Express, Discover and JCB formed the PCI SSC. The PCI DSS was introduced in 2004 to reduce the amount of credit card fraud that was being perpetrated. This standard is targeted at businesses; covers the three aspects of the Informal Formal Technical (IFT) model (Backhouse, Liebenau & Land, 1990) and its 211 requirements include at least the top three mitigation strategies.

Although government and industry standards may vary in their focus on what is to be protected and to what degree, they do have common requirements/ mitigation techniques. The security controls in these standards can be broken down into three types of controls; Informal, Formal and Technical controls. These three areas form the basis of the IFT security model, which shows that to achieve effective technology security the three components must be in balance and support each other (Backhouse, 1997, Pg 34).

The informal element addresses the human aspect of security. Knowledge of an organisation’s technology is often widely spread through the organisation. In current distributed architectures, ensuring employees understanding and attitude towards their security responsibilities is critical to a well-rounded and balanced security posture (Backhouse, 1997, Pg 34).

The formal element addresses the supporting security policies, procedures and processes of an organisation. The formal elements support both the technical and informal elements of the IFT model by providing formal foundations and boundaries for the informal and technical controls to operate in (Backhouse, 1997, Pg 34).

The technical element addresses the security technologies in place at an organisation. Security technologies such a firewalls, Intrusion Detection Systems (IDS)/ Intrusion Detection & Prevention Systems (IDP), access controls systems etc are examples of technical controls (Backhouse, 1997, Pg 34).

Patching and Anti-virus

The complex nature of computer programs results in regular errors and vulnerabilities being found in the programming code. Some of the errors result in unusual behaviour or instability of systems. The vulnerabilities can cause security issues that can be exploited to gain unauthorised access to systems or privilege escalation, which allows a malicious user to take control of a system (Liu, Kuhn, Rossman, 2009, Pg 49).

Software vendors such as Adobe, regularly publish bulletins advising users that updates to fix errors are available (Adobe, 2012). Microsoft also regularly releases updates to their operating systems. These updates are also referred to as patches. In 2002 Microsoft introduced the Trustworthy Computing Initiative to encourage the development of more secure code and more secure default security settings to help protect users (Microsoft, 2003).

Organisational governance policies recognise the importance of regularly updating system. The PCI DSS, for example, has a requirement to keep all systems up to date and patched (PCI SSC, 2010, Pg 11). The top two mitigation strategies to mitigate targeted cyber intrusions are:

1. Patch applications
2. Patch operating system vulnerabilities

(DSD, 2011, Pg 2)

Patching home computer systems is highly recommended for domestic Internet users. The SANS ‘Home Users PC Security: Threats To Windows Users and Countermeasures To Defend Against These Threats’ whitepaper states: "*Patch your system with Latest patches… These patches are critical to defend against vulnerabilities in Windows*" (SANS, 2001, Pg 8).

Another recommended mitigation strategy is anti-virus (AV) software. AV software is a program that is installed on a computer to defend against malware. It detects, blocks and if possible removes the malware to stop it infecting a computer. The majority of current AV products are signature based. The AV software scans the computer it is installed on looking for signatures (patterns of code in the malware) that match those in its database or dictionary of known malware 'signatures' (Zeltser, 2011, Pg 1).

One of the limitations of AV is that it can only detect known malware. As hackers are constantly developing new malware, AV signatures need to be regularly updated (or patched) to keep them current (Zeltser, 2011, Pg 1).

Once again this mitigation strategy can be found in governance policies. One of the twelve sections of the PCI DSS is dedicated to the use of AV software and keeping its signatures up to date (PCI SSC, 2010, Pg 11). The use of AV is ranked 21 in DSD's mitigation strategy (DSD, 2011, Pg 2). As can be seen from the practitioner literature substantial focus is put on AV and keeping it up to date. SANS recommend domestic use of AV in the SANS 'Home Users PC Security: Threats To Windows Users and Countermeasures To Defend Against These Threats' whitepaper (SANS, 2001, Pg 8).

Access Control

Access control systems and policies control and maintain user accounts on computer systems. These controls include who can access a computer, what they can access on the computer and what actions they can perform. Access control is considered a critical security measure in organisations (Hu, Ferraiolo, Kuhn, 2006, Pg 3-5). There is an abundance of academic and practitioner literature on access control systems and models.

The importance of access control can be seen by the emphasis put on it in practitioner literature. The PCI DSS again dedicates one of its 12 sections to the topic and other access control requirements can be found as sub-requirements in other sections (PCI SSC, 2010, Pg 15 & 17). The NZIMS states:

> *"Inappropriate use of any feature or facility of a system that enables a privileged user to override system or application controls can be a major contributory factor to failures or cyber security incidents on systems"* (GCSB, 2010, Pg 92).

Minimising the use of administrator accounts is ranked 3rd in their Strategies to Mitigate Targeted Cyber Intrusions (DSD, 2011, Pg 2). On windows systems there are three main types of user accounts, Standard, Administrator and Guest. Standard users cannot make any changes that affect other users, install software etc. while Administrator accounts have full access to the system, system functions and the ability to manage user accounts (Microsoft, 2012). The same user levels are also on Mac OS-X (Apple, 2012). Administrator user accounts are also referred to as privileged accounts (Hu et al, 2006, Pg 3).

Access control is relevant to domestic users as it controls the ability to install software and perform administrative functions. Malware can often require the use of a privileged account to cause harm. If a user is not using this type of user-account for everyday tasks it can make it more difficult for malware to spread and resist efforts to remove it (DSD, June 2011, Pg 1)

Password security is a subset of access control. Enforcement of a strong password policy is ranked 18 by the DSD mitigation strategy. It goes on to say that the policy should cover complexity, length, dictionary words and reuse of the passphrase (DSD, 2011, Pg 2).

The PCI DSS goes into greater detail. The standards definition of a strong password can be found in requirements 8.5.9 to 8.5.13. Compliance with the standard requires:

- Regular password changes (at least every 90 days)

- Minimum password length of seven characters
- Passwords must contain both alpha and numeric characters
- Users must not reuse any of the last four passwords used

As the PCI DSS is a business focused standard in addition to the password composition requirements the PCI DSS also has requirements regarding the management of passwords and formal password controls in the form of documented policies (PCI SSC, 2010, Pg 17).

The NZISM states ‘A simple six-letter password can be brute-forced in minutes by software available on the Web. Passwords with at least seven characters utilising upper and lower case, numbers and special characters have a much greater resistance to brute force attacks’ (Government Communications Security Bureau, 2010, Pg 190). The remainder of password related guidance is similar to the PCI DSS in that it focuses on password management and associated formal controls.

Fordham and, Zviran & Haga go into greater detail on the construct of a strong password and appropriate associated behaviours to protect individuals' passwords. These articles extend alphanumeric passwords to include the use of special characters and that the length of the password is also a key consideration. It also introduces the concept of a passphrase rather than a password, obfuscation, randomness and password/ phrase creation and recall techniques. (Fordham, 2008; Zviran & Haga, 1999)

The more random and longer a password the better it is. However, this may make a password the more difficult to remember. A passphrase is a combination of words to make a long password easier to remember. Alternatively the first letter from each word of a sentence can be use. Obfuscation is when letters are replaced with numbers or special characters eg #, %, ^. The use of capital and lower case letters is also recommended (Fordham, 2008, Pg 44 & 47).

Social Engineering

Social engineering is described as "…the art and science of getting people to comply with your wishes…" It has also been referred to as 'the art of deception' (Kamal & Crews, 2008, Pg 145).

On June 16, 2011 a Microsoft press release stated, 'Microsoft Survey Reveals Extent of Emerging Internet Phone Scam' which detailed a social engineering scam. The press release also stated that the criminals were targeting English-language markets, it was expected to go global and costs victims on average US$875 (Microsoft, 2011). On November 4, 2010, 5:14 pm the New Zealand police released a warning about the same scam being perpetrated in New Zealand. The scam involved the victim receiving a call from someone allegedly from Microsoft support. They victim would be told that they (Microsoft) had detected a virus or malicious software on the victims computer. In one case reported in Palmerston North the perpetrator asked the victim to run a command that returns a standard response on all Microsoft operating systems. This technique is commonly used to win the victims trust. The perpetrator then leads the victim to either a web site that gains remote access to the victims' computer or they are asked to make a payment so the virus or malicious software can be removed (Ellingham, 2011).

Mitigation of human based social engineering requires a different approach from traditional hacking protection and prevention. Technical controls cannot protect a user from this type of attack instead behavioural mitigation strategies, such as security awareness training, are required. This can be achieved through security awareness education (Kamal et al, 2008, Pg 149).

Security Awareness Training

The digital divide looks at ICT related access and knowledge gaps. These gaps include education and awareness gaps, between nations and their citizens. Education and awareness programs are also a fundamental component of Information Technology security frameworks and models. The IFT model shows that effective security can be achieved when informal controls, which look at the human element, security awareness and behaviours, are in balance with formal controls (policies and procedures) and technical controls (Backhouse, 1997, Pg 34).

Other models such as the Technology Acceptance Model (TAM) (Davis, 1989) show us that the successful adoption of technologies and related governance frameworks require top down support from senior management and an organisational wide awareness of why the technology or controls are required (Del Aguila-Obra & Padilla-Melendez, 2006, Pg 106). When this is put in context with the security and social engineering issues, as described in the previous sections, it shows the need for this balance domestically as well as in business environments

In the case of domestic users this top down support could be seen as coming from the government. The government have ‘lead by example’ by forming the Government Communications Security Bureau (GCSB) and National Cyber Security Centre (NCSC). While GCSB are focused on the protection of government agencies NCSC work with industry and critical infrastructure providers (Telecommunications companies, banks, energy companies etc) to work with these organisations and provide guidance to help them adequately protect their systems from malicious attacks. Similar agencies exist in other countries i.e. U.S. Department of Homeland Security, Australian Defence Signals Directorate.

In addition to providing the leadership from the top these agencies also help provide guidance regarding Formal and Technical security controls as described by the IFT model. This is done by the open publication of government security policies and guidelines. As well as providing templates for formal controls these documents also discuss specific cyber attacks and the technical mitigation techniques to defend against them.

Recognition of the need for appropriate security awareness training addresses the need to balance the Formal and Technical controls with appropriate Informal controls. Informal controls are included in security and governance standards like the PCI DSS but the requirements for them may only be a small percentage of the overall requirements. For example security awareness requirements only contribute 1.5% to overall compliance with the PCI DSS (PCI SSC 2010).

Security awareness training can be one of the most effective security controls an organisation can implement (Hagen, Albrechtsen & Hovden, 2008). The contribution these programs can make to the overall security profile of an organisation is far greater than the emphasis security standards like the PCI DSS put on them. How much focus, if any, is put on the security awareness of domestic users and where is the focus coming from? Although government publications and standards like the PCI DSS only have small sections of their overall framework dedicated to security awareness programs, the NZCSS put awareness and online security, as its top priority.

Priority 1 of the NZCSS is ‘Increasing Awareness and Online Security ‘. This priority states that it will partner with industry and non-government organisations to raise awareness with a long-term goal of working with Internet Service Providers (ISP) to develop appropriate solutions. However, how ISP’s are expected to address this is not clear.

The NZCSS is the New Zealand’s overarching cyber security strategy and is intended to influence government, industry, non-government organisations and academia. Government have recognised that that improving cyber security is a shared responsibility. This is why priority 1 of the strategy targets these areas in the short and long term. Although the need to raise security awareness of domestic users is identified in the strategy it would appear that the government do not intend to address this directly but rather though their partnerships with government agencies, non-government organisations, industry and academia.

Domestic Users

The digital divide refers to knowledge of information and communication technologies (ICT) and the level of Internet access of a country's citizens. Local research into the digital divide supports the existence of a knowledge and access gap in New Zealand and explores the four key barriers to the use of the Internet:

1) Physical access to ICTs
2) ICT skills and support
3) Attitudes
4) Content

(Cullen, 2003, Pg 249).

The issue of physical access appears to becoming less of an issue at the time this research was conducted. In 2001 only 37% of New Zealand homes had access to the Internet (as cited in Statistics New Zealand, 2004, Pg 7), while in 2009, 75% of New Zealand homes had access to the Internet (Statistics New Zealand, 2010 Pg 2). As can be seen by the CFH vision, ongoing focus has been put on this issue.

Statistics New Zealand also states that technology literacy and skills are influencing factors on use of the Internet and are considered key to job prospects (Statistics New Zealand, 2004, Pg 5). While these reports do not contribute to helping understand the nature of the knowledge gap, as this area was not included in their research, it does show the scale of domestic Internet access in New Zealand.

People in professional occupations can acquire ICT skills as part of their role but this is less likely for manual workers, the unemployed and people that do not have any form of tertiary education (Cullen, 2003, Pg 250). However, as has been demonstrated, the ICT industry has a substantial lack of skilled resources.

People’s attitudes can also impact their use of the Internet (Cullen, 2003, Pg 250) and successful adoption of ICT’s (Del Aguila-Obra et al, 2006, Pg 106). The attitudinal barrier includes people’s reluctance to develop ICT knowledge and skills, and “concern over the lack of security of personal information on computers and the internet” (Cullen, 2003, Pg 250).

> *"Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems,"* (as cited in Wasserman, 2000).

While the breaches that have been discussed were all perpetrated on business or government systems the same issues are relevant to the home user. The ‘Computer security risks to home users’ section of the Home Network Security document published by the Cyber Emergency Response Team (CERT) Coordination Centre confirm that these issues also relate to home networks (CERT, 2006)

Traditionally home users would access the Internet from personal computers and laptops. Smart devices including phones, television sets, IP based video telephony and gaming consoles such as the Microsoft x-box 360 also use home networks and are able to provide internet access.

In 2007, at the New Zealand hacker conference Kiwicon, two presenters using the hacker handles Oddy (Beau Butler) and Eon gave a presentation titled ‘Straight To Video: Bugging the Boardroom’. During this talk they demonstrated how to exploit vulnerabilities in video conferencing software and hardware that allowed the hacker to remotely activate the system and take control of it. Although he had not researched these technologies, Beau Butler confirmed that it is likely a motivated hacker would be able to exploit vulnerability in these systems and activate the video and voice capabilities remotely. He referenced the Sony hack as an example of a targeted attack on a vendor that produces these types of technologies. He went on to say that technologies like the x-box 360 if compromised en masse could be used to attack Microsoft using legitimate connections (Butler, Beau personal communication, January 18, 2012).

The Securityfocus.com BugTraq online security vulnerability advisory service published ‘a privilege escalation vulnerability’ (This type of vulnerability takes advantage of programming errors or design flaws to grant the attacker elevated access to the network, it’s associated data or applications (TechTarget, 2010)) for the X-box 360 in 2007. The vulnerability allowed the hacker to take control of the system and execute arbitrary code that could include malware (Anonymous Hacker, 2007). This highlights the need for security awareness by home Internet users beyond traditional access methods.

These examples show that not only are domestic internet users impacted by targeted breaches of corporate systems but that domestic users themselves are also a target.

Although the mitigation strategies that have been explored have been targeted at organisations, they have been put in context with domestic Internet users, who at no cost could implement the top three strategies from DSD.

Research method

Technology security is a broad, highly complex, and technical topic. With a population that has a highly varied level of Internet access and technology related skills, this diversity further complicates the ability to ascertain the level of technology security awareness. For the purpose of this research the sample population were people who had Internet access. According to Statistics New Zealand's survey in 2009 that was 75% of the population (Statistics New Zealand, 2010, Pg 2).

The sample selection for the research was friends of the researcher on Facebook. At the time the research was conducted the researcher had 305 Facebook friends. The response rate from the population was 32%, 107 respondents. Respondents who were not from or living in New Zealand were excluded as were any incomplete responses leaving a total population of 98 respondents in the sample set. The sample set could then be split into people who worked in IT and those who did not for comparative purposes. This was based on the assumption that people that work in IT are more likely to have a higher level of technical understanding.

Quantitative research was selected, as the data to be collected was to be objective and measurable rather than subjective (Lee, 1992, Pg 87).

Anonymous Online Survey

The data gathering method for the research was an anonymous online survey. The survey ran from 19th December 2011 to 9th January 2012. The survey consisted of 18 Questions.

The first two questions established the demographic of the respondent and if they worked in IT. The next two questions were used to ascertain how important the respondents thought technology security awareness was for New Zealand and what they believed their own level of awareness was.

Questions five to eleven were based on the DSD “Strategies to Mitigate Cyber Intrusions” document. In each case these strategies can be achieved at no cost for a domestic user and can reduce the likelihood of them becoming the victim of a cyber attack by approximately 70%. Table 1 shows how the questions were aligned with the strategies and the ranking of the strategy. In some cases questions may be related to more than one strategy and vice versa.

The Top 35 Mitigation Strategies are ranked in order of overall effectiveness. Rankings are based on DSD’s analysis of reported security incidents and vulnerabilities detected by DSD in testing the security of Australian Government networks (DSD, 2011).

Table 1 – Survey questions 5 to 11 relationship to mitigation strategies.

Strategy	Ranking	Related Survey Question
Patch operating system vulnerabilities. Patch or mitigate within two days for high-risk vulnerabilities. Use the latest operating system version.	2	Question 5: Which operating system does your computer use? (If you have more than one computer select as many as appropriate)
		Question 6: Does your computer automatically update the operating system (also known as patching)?
Patch applications e.g. PDF viewer, Flash Player, Microsoft Office and Java. Patch or mitigate within two days for high-risk vulnerabilities. Use the latest version of applications.	1	Question 7: Do your installed applications, for example, Microsoft Office, Adobe Reader/ Acrobat/ Flash, Firefox etc, get updated automatically (also known as patching)?
Minimise the number of users with domain or local administrative privileges. Such users should use a separate unprivileged account for email and web browsing.	3	Question 8: Do you control access to your computer? E.g. have different users set up on your computer and / or require passwords?
		Question 9: If you have different user logons configured on your computer what privileges/ rights/ user levels do the user logons on your computer have?
User education e.g. Internet threats and spear phishing socially engineered emails. Avoid: weak passphrases, passphrase reuse, exposing email addresses, and unapproved USB devices.	8	Question 15: Which of the following options describe social engineering? (Select all that are correct)
		Question 18: Which of the following options would be the best way to provide security awareness training to you? (Please select as many options that you think are relevant)

Strategy	Ranking	Related Survey Question
Enforce a strong passphrase policy covering complexity, length, and avoiding both passphrase reuse and the use of dictionary words.	18	Question 8: Do you control access to your computer? E.g. have different users set up on your computer and / or require passwords?
		Question 10: Please describe and give an example of a strong password. (Please, in your example, do not describe any passwords you actually use)
Anti-virus software with up to date signatures, reputation ratings and other heuristic detection capabilities. Use gateway and desktop anti-virus software from different vendors.	21	Question 11: From the following options please select all the options that best describe your understanding of anti-virus software:

Questions twelve to fifteen relate to social engineering and a scam that was current at the time the research was being conducted. The questions were included to discover how the respondents would respond to a current social engineering scam where the victim receives a call from someone impersonating Microsoft support and is specifically targeted at domestic users of the Internet.

The final three questions established who the respondents' thought was responsible for security awareness education, if they would make changes to reduce their chances of being hacked and what type of security awareness training they would prefer.

A full list of the questions can be found in Appendix A.

Findings

Demographics

The first two questions of the survey split the respondents into the following demographic.

Table 2 – Respondent Demographics

Survey Question	Response Type	No. of responses
1. Are you living in or from New Zealand	Yes	98
	No	9
2. Do you work in the information technology industry?	Yes	28
	No	78

Only 98 of the respondents from New Zealand were used for this research. 24 of those respondents worked in the information technology industry and 74 did not. For the purpose of this research the respondents were split into these groups for comparative purposes.

Security Awareness

When the survey asked about the importance of technology security awareness for the New Zealand public only one respondent from the non-IT workers group did not think it was important. When asked to rate their own level of technology security awareness the IT workers response average was 2.37% higher than that of the non-IT-workers.

Even though 99% of the respondents said that technology security awareness was important to the New Zealand public 9% of the respondents would not follow four simple steps to secure their machines if they were told the likelihood of being hacked could be reduced by approx 70%.
The results for questions 2, 4 & 16-18 are detailed in Table 3.

Table 3 – Security Awareness

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
3. Do you think that technology security awareness by the New Zealand Public is important?	Yes		99%	100%	99%
	No		1%	0%	1%
4. On a scale of 1-10 (1 being no awareness and 10 being very aware) please rate your current level of technology security awareness	Slider	Minimum	1	5	1
		Maximum	10	10	10
		Average	5.92	7.71	5.34
16. Who do you think is responsible for teaching the public about technology security practices? (Please select as many options that you think are relevant)	Multiple Answer	The Government	54%	77%	47%
		Internet Service Providers	90%	100%	86%
		Schools and educational institutes	77%	82%	76%
		Technology retailers	75%	77%	74%
		I don’t think it’s important	0%	0%	0%
17. If you were told that there were four things, that didn't cost anything and could be done in less than ten simple steps, that would reduce the chances of you getting hacked by 70% would you make those changes?	Yes		91%	79%	95%
	No		9%	21%	5%
18. Which of the following options would be the best way to provide security	Multiple Answers	Free on-line training course	69%	73%	66%
		TV program / advertisements	54%	50%	55%

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
		Reminder e-mails of security practices from your Internet service provider	63%	50%	66%
		Posters describing good security practices	25%	36%	22%
		Demonstrations of how security breaches can occur	61%	73%	58%

Patching and Anti-virus

Non-IT workers had greater diversity in the operating systems used but also IT-workers tended to use more recent operating systems. Both groups were similar when it came to patching but IT workers had a consistently better understanding of anti-virus. The details for the questions regarding Patching and anti-virus can be found in Table 4.

Table 4 – Patching & Anti-Virus

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
5. Which operating system does your computer use? (If you have more than one computer select as many as appropriate)	Multiple answer	Windows 95	0%	0%	0%
		Windows ME	0%	0%	0%
		Windows 2000	3%	0%	4%
		Windows XP	39%	29%	43%
		Windows Vista	11%	17%	9%
		Windows 7	48%	67%	41%
		Mac OSX Leopard	2%	0%	3%
		Mac OSX Snow Leopard	11%	4%	13%
		Mac OSX Lion	7%	13%	4%
		Older Mac OS	1%	0%	1%
		Linux Variant	4%	8%	3%

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
		Other	7%	13%	4%
6. Does your computer automatically update the operating system (also known as patching)?	Single Answer	No, but I apply updates manually	24%	25%	24%
		Yes, updates are done automatically	67%	71%	66%
		No, I don't update my operating system	3%	4%	3%
		I don't know what this means	5%	0%	7%
7. Do your installed applications, for example, Microsoft Office, Adobe Reader/ Acrobat/ Flash, Firefox etc, get updated automatically (also known as patching)?	Single Answer	No, but I apply updates manually	43%	46%	42%
		Yes, updates are done automatically	52%	54%	51%
		No, I don't update my applications	3%	0%	4%
		I don't know what this means	2%	0%	3%
11. From the following options please select all the options that best describe your understanding of anti-virus software:	Multiple Answer	I don't know why anti-virus software is important or what it's for	0%	0%	0%
		I have a good understanding of anti-virus software and what it's for	64%	79%	59%
		All electronic documents should be scanned by anti-virus software	66%	67%	66%
		All e-mails should be scanned by anti-virus software	75%	79%	74%

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
		All Internet traffic should be scanned by anti-virus software	68%	67%	68%
		As long as my documents aren't from the Internet they don't need to be virus scanned	9%	13%	8%
		I use anti-virus software at home	82%	83%	82%
		I make sure m y anti-virus software is up to date	70%	79%	67%
		I don't use anti-virus software at home, that I'm aware of	3%	0%	4%
		I don't use anti-virus software at work, that I'm aware of	0%	0%	0%

Access Control

Table 5 shows the results of the questions relating to access control and passwords. Only 24% of respondents had appropriate access control with multiple users that required passwords.

Table 5 – Access control and passwords

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
8. Do you control access to your computer? E.g. have different users set up on your computer and / or require	Single Answer	I don't have different users set up on my computer, but a password is required	49%	33%	54%

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
		I don't have different users set up on my computer, and no password is required	18%	8%	22%
		I have multiple users on m y computer, but they don't require passwords	6%	4%	7%
		I have multiple users on my computer, and they all require individual passwords	27%	54%	18%
		I don't know	0%	0%	0%
9. If you have different user logons configured on your computer what privileges/ rights/ user levels do the user logons your computer have?	Single Answer	All users have administrator rights	33%	5%	44%
		I restrict what individual users can do on my computer	60%	90%	49%
		I don't know what this means	7%	1%	7%

Question 8 asked users to describe and provide an example of a strong password. The responses have been correlated and the percentage of responses that mentioned each of the following components has been detailed in Table 6:

- Passphrase or obfuscation
- Random
- Mixed Case
- Alphanumeric
- Includes special characters
- Length greater than eight characters

Table 6 – Strong Password Components by Percentage

Strong password components by percentage						
All respondents						
	Phrase or obfuscation	Random	Mixed Case	Alphanumeric	Special Characters	Length
Number	58	17	70	88	32	61
Percentage	59%	17%	71%	89%	33%	62%
IT Workers						
	Phrase or obfuscation	Random	Mixed Case	Alphanumeric	Special Characters	Length
Number	21	4	21	22	17	21
Percentage	88%	17%	88%	92%	71%	88%
Non-IT Workers						
	Phrase or obfuscation	Random	Mixed Case	Alphanumeric	Special Characters	Length
Number	37	13	49	66	15	40
Percentage	50%	18%	66%	89%	20%	54%

Social Engineering

None of the respondents believed that Apple or MS would phone them regarding an issue; even so 3% of respondents would pay them money if the caller asked for it to fix an issue. Table 7 describes the responses to questions relating to social engineering.

Table 7 - Social Engineering

Survey Question	Response Type	Total Sample Set	IT Workers	Non-IT Workers
12. Do you think that Microsoft or Apple would telephone to advise you that they have detected an issue or virus on your computer?	Yes	0%	0%	0%
	No	100%	100%	100%

Survey Question	Response Type		Total Sample Set	IT Workers	Non-IT Workers
13. If you received a call from someone saying they were from Microsoft or Apple and that a problem or virus was detected on your computer would you follow the steps they ask you to?	Single Answer	Yes	1%	0%	1%
		Yes, but only if I understood what they were asking me to do	5%	4%	5%
		No	94%	96%	94%
14. If you did follow the steps the person from Microsoft or Apple gave you, and then they asked you for money to fix the problem, would you pay them (please assume that you have the money to spare)?	Yes		2%	0%	3%
	No		98%	100%	97%
15. Which of the following options describe social engineering? (Select all that are correct)	Multiple Answer	Shoulder surfing (watching what someone is typing)	26%	29%	25%
		A type of web site design e.g. Facebook	43%	24%	49%
		Shadowing, following someone through a security door	26%	33%	24%
		A way of testing web site security	17%	14%	18%
		A way of teaching good security practices	18%	19%	18%
		A type of hacking	44%	57%	40%

Discussion

Kevin Mitnick, a famous hacker, asserts that users are the biggest risk to computer systems (as cited by Wasserman, 2000).

As has been formally presented, technology security and awareness is a highly complex and technical issue. Although the majority of academic and practitioner literature is focused on organisations and their users, many of the threats and mitigation strategies for organisations are also relevant for domestic users.

Attitude and concerns about security and privacy were highlighted as a barrier for use of the Internet (Cullen, 2003, Pg 250). It would appear that it is also of concern to the respondents of the survey, all of which are Internet users. Only one of them did not think that technology security and awareness was important to the New Zealand public. This shows the perceived importance of security for domestic users.

This perception suggests that there would be a positive attitude towards the adoption of security technologies and practises. When asked if the respondents would adopt 4 things that, at no cost, could reduce the likelihood of being hacked 91% of the total sample set said they would. The most surprising result was that 21% of IT-workers would not. No research was conducted to find out why this was the case.

The self-rating of the respondents own level of security awareness were widespread with the overall average response being 5.92 out of 10 (where 10 is very aware). As expected the IT workers rated themselves higher here with the lowest response being 5 compared to 1 from the non-IT workers. This may indicate that IT–workers reluctance to adopt suggested preventative measures might be because they believe they know better. However, it does confirm that people in professional occupations acquire IT skills as part of their job (Cullen, 2003, Pg 250).

Only 3 % of the respondents used windows 2000 which is not longer supported by Microsoft. As such no patches to fix newly discovered security vulnerabilities in the software are officially created (Microsoft, January, 2012). The same respondents were also the only ones that did not update their operating system. However, 5% of the respondents did not know what patching was. None of the IT workers used unsupported operating system software.

Patching was well understood. Only 5% of respondents that had supported operating systems did not know what patching was.

This is a positive result as the number of unsupported operating systems is low and the majority of supported operating systems are patched.

The survey results regarding access control were much more concerning. By default computer users are privileged administration users. Only 33% of respondents had multiple users on their computers. Without having multiple users set up on computers it is not possible to have users without administrative privileges.

Awareness of access controls was concerning. 56% of respondents relied on passwords alone for access control. 24% did not require passwords and only 19% of the respondents had unprivileged, non-administrative users on their computers that required passwords.

As the access control results that have been discussed so far demonstrate 56% of the respondents are reliant on passwords alone so the strength of passwords is crucial. IT workers awareness of what makes a strong password was significantly higher in all areas apart from the use of random passwords where non-IT workers were ahead by 1%.

Using alphanumeric (a combination of both letters and numbers) was the most commonly strong password component, followed by the use of mixed case characters with a response of 71% overall. 54% of non-IT workers responded with or gave examples of passwords eight characters or longer. 50% of non-IT workers understood or provided examples of passphrases or obfuscation and only 20% were aware of or provided examples using special characters.

Awareness of strong passwords was also concerning. Only 2 out of 6 strong password techniques were well understood by the respondents. The four techniques that were the least understood were the components that contribute the most towards strong passwords.

82% of respondents used anti-virus software, there was little variation between the results from IT workers and non-IT workers.

Anti-virus software was the most well understood mitigation strategy. Only 3% of respondents did not use anti-virus software that they knew of at home.

The respondents' interpretation of social engineering was almost evenly split with 44% responding that it was a type of hacking. Although none of the respondents thought Microsoft or Apple would ring to advise them of an issue or virus, 5% would follow instructions the caller gave them and 2% would give them money. As technical security controls cannot address this type of behavioural-based social engineering scam a different approach is required. This scam has been acknowledged by Microsoft (Microsoft, 2011). It would therefore seem reasonable that since they invest in producing patches to address security issues in their software, that Microsoft should invest in protecting their brand and launch a campaign to educate users about this scam.

The government have recognised the need to increase awareness and online security for domestic Internet users. They intend to oversee this need by working with government agencies, non-government organisations, industry and academia, rather than addressing it directly with the users. Only 54% of the respondents believed that the government was responsible for awareness education while approximately ¾ of the respondents felt it was academia and technology retailers' responsibility. 90% of the respondents believed ISP's were responsible for security awareness training. These responses support the government's strategy.

The respondents believed that an online security awareness program would be the most effective method of delivering security awareness training. Security awareness reminder e-mails from ISP's were also thought to be an effective media. Awareness and understanding of breaches was also a popular response at 61% and was felt to be more effective than television advertisements on the subject (54%). This suggests that if New Zealand introduced mandatory breach disclosure laws this may have the unexpected benefit of increasing domestic users security awareness.

Bruce Schneier, a highly regarded security practitioner states:

> *"The real problem with computers is that they don't work well. The industry wants to have it both ways. They've convinced everyone that people need a computer to survive, and at the same time they've made computers so complicated that only an expert can maintain them. Corporate users get by because there's an IT department a phone call away; home users rely on the charity of their more sysadmin-inclined friends or suffer in silence."* (Schneier, 2006)

Microsoft introduced the trustworthy computing initiative in 2002 to develop more secure computing platforms (Microsoft, 2003). Since the commencement of this research Apple have announced the inclusion of application white listing functionality in their OS-X operating system (Apple, 2012). Application white listing helps prevent malicious software from running and is ranked 4 by DSD (DSD, 2011, Pg 2). This demonstrates both Apple and Microsoft's commitment to creating a more secure computing environment.

What level of technology security awareness of mitigation strategies do domestic Internet users have to prevent targeted intrusions?

In response to the research question, the level of awareness of mitigation strategies was good for patching and anti-virus; the majority of the respondents understood both mitigation strategies well. Social engineering was not a well-understood threat, 43% of the respondents thought it was a type of web site like Facebook rather than a hacking technique. Access control was the least understood mitigation strategy and is the area of greatest concern.

Limitations

The main limitation of this research was the size and demographic of the sample set. Only friends of the researcher were used in the sample set. As the researcher is a technology security practitioner, it is likely that a lot of the IT worker respondents were also technology security practitioners. Additionally the researcher has published security tips on Facebook that may have influenced their Facebook friends' security awareness.

This research only looked at the awareness level regarding password strength but did not differentiate between the respondents' awareness and actual practises. In their response, one of the respondents who appeared to have a thorough understanding of strong passwords commented that they did not actually use strong passwords in practise.

Although the media to deliver security awareness training was explored the most effective types of content were not.

Further Research

The research should be expanded to include a larger sample set of domestic Internet users, and include users who are not known to the researcher.

Only a small subset of technology security techniques were investigated, this should also be also be expanded to include web surfing and e-mail behaviours.

It is possible that different computing environments i.e. Microsoft and Apple, may have differing levels of security by default. This should be explored to see if this influences the security of domestic users. Also different types of devices such as mobile devices, gaming consoles and smart devices should be researched to better establish the security level of the domestic users.

Conclusions

Technology security and awareness is an issue and more focus is required to educate domestic Internet users in New Zealand. Although there is a good level of awareness regarding patching and anti-virus there is a need for further education about access control, strong passwords and social engineering as it relates to domestic users.

The government's approach increases awareness and online security, as described in the NZCSS, by working with stakeholders across government, industry (such as ISP's), non-government and academia (NZMED, 2011, Pg 6). This approach appears to be appropriate, as the survey results supported this.

The NZCSS does not go into detail regarding the media it would use to increase awareness and online security. The survey respondents' preferred methods were Internet based training and security awareness reminder e-mails from ISPs.

References

Adobe, (2012). ‘Security bulletins and advisories’. Adobe Systems Incorporated. Retrieved February 20, 2012 from http://www.adobe.com/support/security/

Anonymous, (September, 2011). ‘Newsletter on Intellectual Freedom’. United Nations, Vol 60(5), Pg 172. Retrieved February 10, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/898791497?accountid=14782

Anonymous Hacker, (February 28, 2007). ‘Xbox 360 Hypervisor Privilege Escalation Vulnerability’. Security Focus BugTraq. Retrieved February 6, 2012 from http://www.securityfocus.com/archive/1/461489

Apple, (2012). ‘Mac OS X v10.5: Working with user accounts and Accounts preferences’. Retrieved February 20, 2012 from http://support.apple.com/kb/HT3309

Backhouse, James, (1997). ‘Information @ Risk’. Information Strategy, Pg 33-35.

Backhouse, J & Liebenau, J & Land, F, (1990). ‘On the Discipline of Information Systems’. Journal of Information Systems, Vol 1, Pg 19-27.

Baker, Liana & Finkle, Jim, (April 26, 2011). ‘Sony PlayStation suffers massive breach’ Reuters. Retrieved January 3, 2012 from http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426

Butler, Beau, (personal communication, January 18, 2012)

Bryant, Grant, (September 3, 2010), ‘Card security breached in Qtown’, The

Southland Times. Retrieved December 1, 2011, from http://www.stuff.co.nz/southland-times/news/4090422/Card-security-breached-in-Qtown

Carl, Glenn & Kesidis, George & Brooks, Richard R & Rai, Suresh, (January, 2006). 'Denial-of-Service Attack-Detection Techniques'. IEEE Internet Computing, Vol 10(1) Pg. 82-29. Retrieved February 9, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/197340893?accountid=14782

CERT, (2006), 'Home Network Security'. Carnegie Mellon University. retrieved February 6, 2012 from http://www.cert.org/tech_tips/home_networks.html

Computerworld Staff, (March 24, 2011). 'Internal Affairs website down; no evidence of DoS attack so far', Computerworld web site. Retrieved December 1, 2011 from http://computerworld.co.nz/news.nsf/news/internal-affairs-website-down-anonymous-blamed

Cooke, Evan & Jahanian, Farnam & McPherson, Danny, (July, 2005). 'The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets'. University of Michigan, Electrical Engineering and Computer Science. Usenix Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI 2005), Cambridge, Massachusetts, Pg 39-44. Retrieved February 9, 2012 from www.eecs.umich.edu/~farnam/pubs/2005-cjm-sruti.pdf

Crown Fibre Holdings, (2010), 'New Zealand's Broadband Vision'. New Zealand Government. Retrieved February 8, 2012 from http://www.crownfibre.govt.nz/about-us/new-zealand%E2%80%99s-broadband-vision.aspx

Cullen, Rowena, (2003). 'The digital divide; a global and national call to action'. The Electronic Library. Retrieved January 2, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/218228255?accountid=14782

Defence Signals Directorate, (2011). “Strategies to Mitigate Cyber Intrusions”, Australian Government, Department of Defence, Intelligence & Security. Retrieved Nov 15, 2011 from http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Defence Signals Directorate, (June, 2011). “Minimising Administrative Privileges Explained”, Australian Government, Department of Defence, Intelligence & Security. Retrieved Nov 15, 2011 from http://www.dsd.gov.au/infosec/top-mitigations/minimisingadminprivileges.htm

Del Aguila-Obra, Ana R. & Padilla-Melendez, Antonia, (2006). ‘Organizational factors affecting Internet technology adoption’. Internet Research, Vol 16(1), Pg 94-110. Retrieved July 21, 2009 from http://search.proquest.com.helicon.vuw.ac.nz/docview/219844881?accountid=14782

Department of labour, (2008). ‘Survey of IT Recruiters 2008: IT jobs that are hard to find’ New Zealand Government. Retrieved February 10, 2012 from http://www.dol.govt.nz/PDFs/jvmp-it-recruit-2008.pdf

Ellingham, Jimmy, (February 21, 2011), “Fake Microsoft technicians in computer scam”. Manawatu Standard. Retrieved February 6, 2012 from http://www.stuff.co.nz/manawatu-standard/news/4682449/Fake-Microsoft-technicians-in-computer-scam

Fordham, David (May, 2008) ‘How Strong Are Your Passwords?’. Strategic Finance, Vol 89(11) Pg 42-47. Retrieved January 2, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/229775654?accountid=14782

Government Communications Security Bureau (December, 2010), ‘New Zealand Information Security Manual’. New Zealand Government. Retrieved June 6, 2011 from http://www.gcsb.govt.nz/newsroom/nzism/NZISM_2011_Version_1.01.pdf

Hagen, Janne Merete & Albrechtsen, Eirik & Hovden, Jan (June 8, 2008). ‘Implementation and effectiveness of organizational information security measures’ Information Management & Computer Security, Vol 16(4) Pg 377-397. Retrieved January 6, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/212339922?accountid=14782

Hu, Vincent C. & Ferraiolo, David F & Kuhn, D Rick (September, 2006). ‘Assessment of Access Control Systems’. National Institute of Standards and Technology. Retrieved February 2, 2012 from Http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

Industrial Control Systems Cyber Emergency Response Team (March 31, 2010). ‘ICS-CERT Advisory: ICSA -10-090-01 – Mariposa Botnet Activity’. Retrieved January 8, 2012 from www.us-cert.gov/control_systems/pdf/ICSA-10-090-01.pdf

Kamal, Mustafa & Crews, Dylan (March, 2008). ‘The Psychology of IT Security in Business’. Journal of American Academy of Business, Cambridge, Vol 13(1), Pg 145-150. Retrieved January 22, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/222867792?accountid=14782

Lee, Jean (April, 1992). ‘Quantitative Versus Qualitative Research Methods – Two Approaches to Organisational Studies’. Asia Pacific Journal of Management, Vol 9(1) Pg 87. Retrieved February 22, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/228433051?accountid=14782

Liu, Simon & Kuhn, Rick & Rossman, Hart (March, 2009). ‘Surviving Insecure IT: Effective Patch Management’. IT Professional Magazine, Vol 11(2), Pg 49-51. Retrieved January 5, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/206326512?accountid=14782

Microsoft, (June 16, 2011). ‘Microsoft Survey Reveals Extent of Emerging Internet Phone Scam’. Retrieved November 4, 2011, from http://www.microsoft.com/Presspass/press/2011/jun11/06-16MSPhoneScamPR.mspx

Microsoft, (January 15, 2003). ‘The Journey to Trustworthy Computing: Microsoft Execs Report First-Year Progress’. Retrieved February 20, 2012 from http://www.microsoft.com/presspass/features/2003/jan03/01-15twcanniversary.mspx

Microsoft, (January 19, 2012). ‘Windows 2000 End-of-Support Solution Center’. Retrieved February 20, 2012 from http://support.microsoft.com/ph/1131

Microsoft, (2012). ‘What is a user account?’. Retrieved February 20, 2012 from http://windows.microsoft.com/en-US/windows-vista/What-is-a-user-account

The National Business Review, (March 24, 2011). ‘Internal affairs down after hacker threat’, The National Business Review. Retrieved December 4, 2011, from http://www.nbr.co.nz/article/internal-affairs-down-after-hacker-threat-nn-89057

National Cyber Security Centre, (2012), ‘Some Interesting Facts’. New Zealand Government. retrieved December 3, 2011 from http://www.ccip.govt.nz/index.html#

New Zealand Ministry of Economic Development, (June 7, 2011), 'New Zealand's Cyber Security Strategy'. Retrieved December 1, 2011 from www.med.govt.nz/sectors-industries/technology-communication/pdf-docs-library/nz-cyber-security-strategy-june-2011.pdf

New Zealand Police (November 4, 2010). 'Police warn of latest phone scam', The New Zealand Police. Retrieved December 4, 2011, from http://www.police.govt.nz/news/release/25930.html

Paller, Alan (October 24, 2011). 'Australian Defence Signals Directorate wins U.S. National Cybersecurity Innovation Award'. SANS Institute. Retrieved November 15, 2011 from http://www.sans.org/press/australian-defence-signals-directorate-national-cybersecurity-award.php

Payment Card Industry Security Standards Council (October, 2010). 'Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 2.0'. Retrieved March 21, 2011 from https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf

SANS (2001). 'Home Users PC Security: Threats To Windows Users and Countermeasures To Defend Against These Threats'. SANS Institute. Retrieved February 2, 2012 from Http://sans.org/reading_room/whitepapaers/hsoffice/home-users-pc-security-threats-windows-users-countermeasures-defend-t_613

Schneier, Bruce (April, 2006). 'Is user education working?'. Retrieved February 20, 2012 from http://www.schneier.com/essay-139.html

Scroggie, Craig (September, 2011). 'Move quickly on mandatory data breach disclosure laws'. New Zealand Computer Society Newsline. Retrieved January 6, 2012 from http://www.nzcs.org.nz/newsletter/article/202

Shaw, Abraham (2010). ‘Data Breach: From Notification to Prevention Using PCI DSS’. Columbia Journal of Law and Social Problems Vol 43(4) Pg 517-562. Retrieved February 2, 2012 from http://search.proquest.com.helicon.vuw.ac.nz/docview/752061975?accountid=14782

Statistics New Zealand, (March 5, 2004). “The Digital Divide In New Zealand” New Zealand Government. Retrieved Dec 1, 2011 from http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/digital-divide.aspx

Statistics New Zealand, (April 16, 2010). “Household Ue of Information and Communication Technology: 2009” New Zealand Government. Retrieved Dec 1, 2011 from http://www.stats.govt.nz/browse_for_stats/industry_sectors/information_technology_and_communications/HouseholdUseofICT_HOTP2009.aspx

TechTarget, (November, 2010), ‘Privilege Escalation Attack’. Retrieved February 22, 2012 from http://searchsecurity.techtarget.com/definition/privilege-escalation-attack

Vass, Beck, (March 18, 2010). ‘Fraud cases hasten $4m upgrade of city carparks’ The New Zealand Herald retrieved March 20, 2010 from http://www.nzherald.co.nz/auckland-city-council/news/article.cfm?o_id=13&objectid=10632707

Wasserman, Elizabeth, (March 3, 2000). ‘Teaching the Government Hacking 101’. PCWorld, Security. Retrieved February 15, 2012 from http://www.pcworld.com/article/15560/teaching_the_government_hacking_101.html

Zeltser, Lenny, (March, 2011). ’Understanding Anti-Virus Software’. Ouch! Monthly Security Awareness Newsletter for Computer Users, SANS Institute.

Retrieved February 2, 2012 from http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201103_en.pdf

Zviran, Moshe & Haga, William j. (1999). ‘Password Security: An empirical study’. Journal of Management Information Systems, Vol 15(4), Pg 161-185. Retrieved January 2, 2012, from http://search.proquest.com.helicon.vuw.ac.nz/docview/218915955?accountid=14782

Appendix A – Survey Questions

1. Are you living in or from New Zealand?
2. Do you work in the information technology industry?
3. Do you think that technology security awareness by the New Zealand Public is important?
4. On a scale of 1-10 (1 being no awareness and 10 being very aware) please rate your current level of technology security awareness
5. Which operating system does your computer use?
6. Does your computer automatically update the operating system(also known as patching)?
7. Do your installed applications, for example, Microsoft Office, Adobe Reader/ Acrobat/Flash, Firefox etc, get updated automatically (also known as patching)?
8. Do you control access to your computer? E.g. have different users set up on your computer and / or require passwords?
9. If you have different user logons configured on your computer what privileges/ rights/ user levels do the user logons your computer have?
10. Please describe and give an example of a strong password.
11. From the following options please select all the options that best describe your understanding of anti-virus software:
12. Do you think that Microsoft or Apple would telephone to advise you that they have detected an issue or virus on your computer?
13. If you received a call from someone saying they were from Microsoft or Apple and that a problem or virus was detected on your computer would you follow the steps they ask you to?
14. If you did follow the steps the person from Microsoft or Apple gave you and then they asked you for money to fix the problem, would you pay them (please assume that you have the money to spare)?
15. Which of the following options describe social engineering?
16. Who do you think is responsible for teaching the public about technology security practices?
17. If you were told that there were four things, that didn't cost anything and

could be done in less than ten simple steps, that would reduce the chances of you getting hacked by 70% would you make those changes?

18. Which of the following options would be the best way to provide security awareness training to you?

Appendix B – Acronyms and Abreviations

AV	Anti-Virus
CFH	Cown Fibre Holdings
DoS	Denial of Service
DSD	Defense Signals Directorate
FTC	Federal Trade Council
GCSB	Government Communications Security Bureau
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IPS	Intrusion Detection & Prevention Systems
ISP	Internet Service Provider
IFT	Informal Formal Technical
IT	Information Technology
NBR	National Business Review
NCSC	National Cyber Security Centre
NZCSS	New Zealand Cyber Security Strategy
NZDIA	New Zealand Department of Internal Affairs
NZISM	New Zealand Information Security Manual
NZMED	New Zealand Ministry of Economic Development
NZSIT	New Zealand Security of Information Technology
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
TAM	Technology Acceptance Model
TJX	TJX Companies Incorporated