2010 NEW ZEALAND COMPUTER CRIME AND SECURITY SURVEY

by KJ Spike Quinn

Introduction

The New Zealand Computer Crime and Security Survey is conducted by the Security Research Group (SRG) of the University of Otago, in partnership with the NZ Internet Task Force (NZITF), New Zealand Police, and the Computer Security Institute (CSI). This 2010 survey is the fourth annual New Zealand (NZ) survey. It is based on the US CSI Computer Crime and Security Survey, the longest running continuous survey in the information security field and commonly known as a leading source of statistics related to computer crime and security.

The 2010 survey results are based on the responses of 176 computer security practitioners in NZ utility, manufacturing / production, financial, telecommunications, transport, high technology, medical, wholesale, retail, tertiary education, legal, national and local government agencies, entertainment/media, construction, commercial/trade services providers regarding the 2009 calendar year. All monetary figures are in NZ$, roughly equivalent to US$0.75 at time of publication.

Considerations in this survey are:

- Budgeting: percentage of IT budget spent on security, outsourcing of security function, incident insurance, security investment, cost-benefit metrics in security planning
- Frequency, Nature and Cost of Cyber Security Breaches
- Incidents and the Law
- Security Audits and Security Awareness
- Security Technologies
- IT Standards, Policies and Procedures
- Information Security Training, Qualifications and Certification
- Perceived Importance of Threats
- Mobile device deployment prevalence, security incident incidence and protection measures
- Conficker incidence, handling and cost
- USB Protection

NB References to US figures refer to those from CSI surveys. In referring to monetary costs, ‘k’ is substituted for ‘thousand’ for brevity.
Executive Summary

Key Points
There was a marked reduction in incident numbers and costs per organisation since 2007. Over 60% of NZ respondents still use less than 5% of their IT budget on security, and investment continues to drop in all budget categories. NZ organisations are tending to outsource more security function, whereas those in the US are outsourcing less. Industry Vendor IT Certification dropped 12% since 2007, Tertiary IT Qualifications rose 5%, and No formal qualifications but > 5 years security experience, dropped from 51% in 2005 to 37% in 2010 suggesting the trend is toward tertiary qualifications to prepare people for ICT employment. Almost half of the respondents thought their organisation needed to do more to ensure 3rd party contractors’ level of IT security qualification, training, experience or awareness. At 46%, Generic External Threat (Virus/malware) was by far the greatest perceived issue. 1 in 4 Mobile Device Security Measures respondents had No security tools or procedures. By far the main vector was USB. Over half respondents had no USB incident protection in place.

Incidents
24% were infected with Conficker, with ¾ having up to 10% of machines infected. The level of those monitoring unauthorised use remained essentially unchanged. There was a marked reduction in incident numbers and costs per organisation. Incident type overall costs for all 176 respondents had the same 3 top categories with Financial Fraud costing over $1m, and Virus and Laptop/mobile hardware theft each costing 2010 respondents a quarter of a million.

Budgeting Issues
Over 60% of NZ respondents still use less than 5% of their IT budget on security, and investment continues to drop in all budget categories. NZ organisations are tending to outsource more security function, whereas those in the US are outsourcing less. Cyber-security risk insurance use continued to drop, from 31% in 2004 to 15% in 2010, but also continued to climb in the US at 32%.

Policy and Procedure Issues
Computer security policies, user access management, and media back-up continue to be highly important within most organizations. Over half respondents now have Cellphone & PDA policies. Almost all respondents have Leaving staff policy, and most enforce it, but over half fail to change shared passwords or preserve logs.

Training / Qualifications / Certification
82% of the respondents said their staff had no specific qualifications or certification. 47% thought their organisation needed to do more to ensure 3rd party contractors’ level of IT security qualification, training, experience or awareness.

Security Technologies
Respondents continue to use Email Monitoring Software, with 73% using Web Activity Monitoring Software. Only 1 in 3 organisations update software either daily or automatically. Windows of various flavours continue to dominate operating systems accounting for more than 90% of all respondent systems in place.
About the Respondents

Respondents came from the same set of 500 as the previous three surveys. These were from two sources: 1. The 2004 SRG survey respondent list of top 500 organisations by turnover; 2. National and local government organisations. As some organisations have been assimilated or no longer exist, a few new respondent organisations were added.

As with earlier surveys, respondents were contacted by telephone to request their input, and the response form then emailed to them. Unfortunately, a number of organisations were simply unable to be contacted. Quite a few more were unable to respond this time due to workload and time constraints. This further reduced the previous pool of 455 possible respondents to 398. Despite this, responses (176) rose from 33% to 44%, back to the original 2005 survey response rate and well above average in surveys of IT management.

Figures 1-5 summarise information about the organisations that responded to the 2010 survey and individuals representing those organisations.

Figure 1 shows proportions of respondents by industry sector. Local Government was again the dominant sector at 17% of respondents, with 16% of responses from the Manufacturing sector. 11% were from National Government, and 6% from the Financial sector.

Figure 2 shows organisational size measured by the number of employees. As with earlier surveys, the higher employee-number organisations were well represented, with 25% employing 1000 and Over people, 14% employing 500-999, 20% employing 200-499, 10% with 50-99 employees, and 21% of respondents employing Fewer than 100 people.

Figure 3 shows Gross Revenue. Once again, larger turnover organisations are well represented, with organisations generating revenue
in excess of $100 million comprising 46% of respondents, up 2%, and closer to the 2009 US figure of 50%, but well down from 57% in 2007.\(^1,\)\(^p4\)\(^,\)\(^2,\)\(^p4\)

Figure 4 shows Areas of Operation. Weight of the line indicates the percentage of respondents operating in each region. Percentages in 2007 were almost identical to 2006, but this year they appear to have halved. As one would expect, as our closest geographical neighbour, Australia is still also our closest business partner with 25% of all respondents also operating there.

Figure 5 shows Respondents by Rôle. Almost half of respondents to this question (48%) held the title of IT Manager, with the next most common title being Chief Information Officer at 21% of respondents. Other responses included Loss Prevention Manager, various Directors and Managers, Accountants, Chief Financial Officer, Business Analyst, Co- and Deputy-CEOs.

**Budget**

Figure 6 shows IT Budget Security Investment Level, with the NZ 5% or less figure remaining somewhat higher at 60.3% than the US 51.8%.\(^1,\)\(^p23\)

Since recording of this began in 2005, around two thirds of NZ organisations have invested under 5% of their IT budget on security. This level of investment is down 6% from 2007, and the US figure was also down 1%.\(^2,\)\(^p8\)

NZ respondents spending between 5 and 10% of their IT budget on security dropped from 18% to 15.5%, whereas the US figure rose from 19% to 22.1%. NZ organisations spending more than 10% continued to drop from 5% in 2007 to just 1.1%, while the US figure
continues to rise at 12.8%.\textsuperscript{1, p23} 23% of NZ respondents did not know the level. 56% thought spending adequate; 15% didn’t know.

Computer security was dictated from outside NZ for 21% of non-governmental respondents, up from 17% in 2007.\textsuperscript{2}

Too few respondents provided figures for computer security related activities, some providing only Operating Expenditure or Capital Investment. Average organisational investment was $52k Capital Investment and $112k Operating Expenditure, although high end figures meant that figures for average security related spending per employee were too skewed to use.

Cost-Benefit metric use results for Return on Investment (ROI), Net Present Value (NPV) Internal Rate of Return (IRR) are shown in Figure 7. Other responses were: compliance costs, metrics not used but costs need to be justified, reputation & downtime, risk assessment, and post-incident audit.

NB: As organisations may use more than 1 metric, percentages do not sum to 100.

Although outsourcing IT is growing, the 2009 US survey indicated that this did not apply to security function.\textsuperscript{1p,23} Interestingly, Figure 8 shows that NZ security outsourcing has increased since 2006, with those outsourcing over 80% of their security function doubling from 8% in 2006 to 15% in 2009, while those outsourcing none dropped from 50% to 42% in the same period.

Analysis showed that medium to large organisations tend to outsource more but very large organisations tend to outsource none. In the US, 71% outsourced no security function, with another 21% outsourcing up to 20%. The remaining 8% of US respondents covered all outsourcing from 21% to 80%, showing that organisations are tending to either one extreme or the other.\textsuperscript{1, p24}

Cyber-security risk insurance use continued its downward trend from 31% in 2004 to 15% in 2010, with 42% having none. In the US, cyber insurance continued its slow 6 year climb to now sit on 32%.\textsuperscript{1, p33} Interestingly, the percentage of respondents who did not know whether their organisation had such insurance continues to increase, from 24% in 2004, to 34% in 2005 and 2006, 33% in 2007, to now reach 43%.\textsuperscript{5,4,2}

Frequency, Nature and Cost of Cyber Security Breaches

The level of monitoring of unauthorised computer system use was again explored and 73% of 2010 respondent organisations indicated that they did monitor unauthorised use. This is unchanged from 2007, and
consistent with the 75% who indicated similarly in 2006.\textsuperscript{4,2}

Figure 9 shows the sources of unauthorised incidents. Some 28% experienced unauthorised use of their systems, down from 31% in the 2007 report.\textsuperscript{2}

As in previous years, internal threat exceeded that of external sources, but not by a great deal, and mainly by those unable to specify numbers. It should be noted that the number of responses (37) is not sufficient to draw any significant conclusions that would challenge the status quo on this threat.

Yet again, two thirds (66.7%) of respondent organisations said they did not experience any \textit{Unauthorised Use} incidents, and 3% said that they did not know.

Figure 10 shows the proportions of respondents experiencing \textit{Unauthorised Use} in percentages from 2006 to 2010.

The percentages of respondents experiencing various types of security incidents may be seen in Figure 11. Just over 70% of respondent organisations experienced some type of security incident in the 2009 calendar year. The most common incident types were \textit{Laptop/Mobile Hardware Theft}, \textit{Virus Contamination}, \textit{Malware Infection}, \textit{Insider Abuse of Net Access/Email}, \textit{Theft of Hardware or assets}, and \textit{Music/Movies/Ripping}.

Incidence overall seem to have reduced since 2007, with \textit{Laptop/Mobile Hardware Theft} dropping 8% since 2007, yet still moving up a place to become most widely experienced incident, affecting 44% of respondents. \textit{Virus Contamination} was next most common on 37%, down 12% from 2007, with new category \textit{Malware Infection} third, affecting 22%. 

© Security Research Group, University of Otago. All rights reserved.  Page 7
Figure 12 shows Average Incidents per Organization for the 2009 calendar year data. The initial (2005) report used historical data to graph average incident numbers that showed consistent growth from 1998-2004.

In order to keep pace with ever changing exploit types the 2010 survey added some new categories. For example Laptop and Mobil Hardware Theft has been added and shows a significant number of incidents.

Bear in mind that the 1998-2004 data was gathered as historic data during the 2005 survey, so because of the small NZ dataset compared to the US survey, the variation in continuity before and after 2004 shows up the difference in respondents between the 2005 and later surveys.

From 1998-2004, the data showed a low-level increase in incident numbers in almost all categories. The low response rate to the 2006 survey lowered the figures in some categories but others saw continued increase.

The 2007 survey saw figures increase in every category, in some cases massively, due to the addition of some previously non-responsive telecoms organisations.

The 2009 dataset saw some marked reductions, so it will be interesting to see if this continues. Highlighting the improvement, the overall average cost of reported incidents per organisation in 2009 was $15k, well down from $133k in 2007 and $36k in 2006.

Figure 13 shows the Average Cost of Incident Types to the Respondent Organisations. With the reduction in telecoms respondents, Financial Fraud was back to being the most costly incident type, at an average cost of $8k per respondent, down from $11.5k.

Virus contamination went up 3 places since the last survey, but dropped in cost from $2.5k to $1.9k. Laptop or mobile hardware theft was next most costly at $1.8k, followed by a new category, Malware, on $1k. Theft of Hardware / Assets cost an average per organisation of $0.5k.

Insider Abuse of Net Access cost an average of $286 per organisation, with Telecommunications Fraud well down at an average cost of $242. The new category of Unauthorised Access/ Privilege Escalation by Insider cost $223, with Phishing, another new category at $210 and ID Theft $161. Misuse of Public Web Application cost was $121, with Bots/Zombies $117.

Social networking is increasing, so it was interesting to see that Exploit of Users Social Network Profile was shown to have a cost to employers. The total cost of the 3 incidents was $3k. Note that Extortion/Blackmail Regarding Threat of System Attack or for
Release of Stolen Data has now arisen in NZ, costing $2k.

Three respondents reported Website Defacement, with the total cost of these incidents being $400.

Figure 14 shows the total costs of 2009 incidents by incident type. With the reduction in Telecommunications figures this time, Financial Fraud was very close to the 2007 figure at just over $1M, double the 2006 figure but half that of 2005. Virus costs parallel this rise & fall. Laptop Theft has seen steady reduction since the $1.1M 2005 figure.2,5

Incidents and the Law

Figure 15 shows responses regarding Organisational Actions Taken After Incidents/Intrusions. Note that percentages do not total 100 as respondents checked all relevant categories.

At the suggestion of NZITF members, new response categories were added to the question this year, but Patched Security Holes remained the most common action for 80% of respondents.

55% Patched Hardware or Infrastructure, 32.5% Changed Software Systems, 30% Provided Additional Security Awareness Training, and 27.5% Did Not Report Outside Organisation, well down from 56% in 2007.

Reported to Police had halved since 2007 at 7.5%, the same figure as Reported to Legal Counsel. Other actions taken were Manual clean-up, Program of improvement, and Hardened configuration of vulnerable device.

Figure 16 (next page) shows respondents’ perceived importance of reasons why intrusions were not reported to law enforcement.

NB: Categories were considered separately so percentages do not add to 100.

Half the respondents (49%) thought their incidents Too Small to Report, and 44% thought Law Enforcement Would Not be Able to Help. 31% were Unaware of Law Enforcement Interest, with 36% ticking Negative Publicity Might Damage the Organisation’s Reputation, and 18% concerned that Competitors Would Use it to Advantage.

Civil Remedy was preferred by 20.5% of respondents. Other responses were: Internal employment issue that needed to follow employment policy/agreement, and policy not to report unless legally required.
Security Audits and Security Awareness Training

Over two thirds (68%) of 2010 respondents conducted internal security audits, down from 77% in 2007. Figure 17 shows 70% reporting results to the Chief Information Officer, 44% to the Chief Financial Officer, 40% to the Board, and 38% to the Chief Executive Officer.

In 2004 20% of those conducting security audits did not report results to upper management. Non-reporting dropped to 2% in 2005, 3% in 2006 and 2007 and rose again to 6% in 2009.

One third of respondents (35%) reported results to other authorities, including Patient Information Manager, Auditors, Shareholder, and Managers of Departments with issues.

It was once again possible to infer overseas ownership of respondent organisations and the 2010 figure is 21%.

Overall, only 25% of respondents agree with the statement My Organisation Invests Appropriately in Security Awareness Training, with 22% of respondents undecided. In 2007, it was noted that those who disagreed with this statement had reduced 8% since 2005, but in 2010 those who disagreed rose by 4% to 53%.

As may be seen in Figure 18, broken down by sector, a large majority disagree. This year the Services and Financial sectors were the only sectors to agree, with Telecommunications now disagreeing, although as stated earlier, Telecommunications responses were very limited. No sector was undecided.

Broken down by employee numbers or revenue, only the smallest organisations of 1-49 Employees, or turning over Less than $1 million thought that their organisation invested appropriately in security awareness training.
Small organisations would logically be least likely to invest in security awareness training.

Respondents were asked to arrange Security Awareness Training in Order of Perceived Importance. Results may be seen in Figure 19, indicating that the highest rating was Access Control Systems on 76.2%, edging out 2006 & 2007 leader Network Security.

Almost three quarters of respondents still perceived Network Security as important. Security Management and Security Policy were again considered important to two out of three. Security Systems Architecture was important to 55.1%.

Investigations and Legal Issues was rated important by 46% and finally Cryptography on 19.7%, dropping the 5% regained in 2007.

Security Technologies

Figure 20 shows order of popularity of information security effectiveness evaluation tool use. Most common was Email Monitoring Software, with 75% of respondents using this tool, unchanged from 2007. Web Activity Monitoring Software was second on 73%, down 3% from 2007.

External Security Audits regained 5% of use lost since 2005 at 61%, whereas Internal Audits was on 56%, down 4%.

External Penetration Testing was done for 44% of respondents.

Automated Tools To Check Configuration Of Network Systems was back down from 42% in 2007 to 36%.

Internal Penetration Testing was done by 18%, with 8% using no evaluation and 5% Other. These were: Packet inspection tools, vulnerability assessment, WebMarshal, host based intrusion prevention system, IDS, IPS, Endpoint control, peer review, incident review, a lot of network monitoring.

In 2007, collaboration with Netsafe created a new question recording how organisations handle updates for operating systems and security software. 2010 results are in Figure 21 (next page).

Organisations were again asked how often they applied security patches and updates to Operating Systems, Firewalls, Anti-Virus, Anti-Spyware and Applications.

One in three organisations updated all five either daily or automatically.

The question regarding prevalence of operating systems continues the SRG survey of NZ Workstation Operating Systems, which has been running since 1996.

This time the most popular workstation operating system was Windows XP at over 63% of
systems. Windows 95/ME and NT were just visible on the graph, with Unix/Linux on 2%. Win2k and Mac were both on 5%.

Windows 7 debuted on 5%, and Vista managed 15%. This time only 2% of systems were Other, comprised of: Thin Clients, Win2003 Server Terminal, Server 2008 R2 Terminal Services, Windows CE, WYSE Terminal, Citrix, AIX, Windows Embedded, and DOS. Results may be seen in Figure 22.

**IT Standards, Policies and Procedures**

Workplace policies and procedures provide guidelines that build a culture of security.

Figure 23 shows figures for Use of Computer Security Policies and/or Procedures. Popularity retained the top 2 order of previous surveys, with User Access Management (enforcement of password use, user privileges, etc) used by 96% of respondents, and Media Back-Up by 95%.

Change Control moved up 5% to 81%. Documented Standard Operating Procedures was also up 3% to 80%. Next was Controls Against Malicious Software, also up at 80%, followed by External Network Access Control steady on 78%.

Respondents trusting User Responsibilities rose 6% to 74%, and Incident Management was on 69%, well up from 54% in 2007. Monitoring System Access and Use dropped 6% to 65%. Segregation of Duties was up 11% to 57%, Cell phone & PDA Policies made its debut also at 57%, and 49% used Management of Removable Computer Media, up 8%. In 2007 those with a Forensic Plan rose from 3% to 7%, and in 2010, to 8%.

Responses of Other were: Accepted use policy, identity & management of devices on
Figure 24 shows Policies for Leaving Staff. All but 1 respondent completed this question and it is clear that the vast majority of respondent organisations have some form of leaving policy in place, and for the most part enforce it. Over three quarters revoke access and recover keys, cards and ICT; but less than half change shared passwords or preserve logs.

Other responses were reported as: Certificates revoked, isolated privileges revoked, code of conduct policy, IT use policy, VPN revoked, and all files & profiles reserved and reviewed.

Figure 25 displays Security Related Standards (SRS) used in NZ. There were 158 responses to this question, of which 40.5% had No external standards, however, 33% had Internally Produced Standards in use, making the figure for respondent organisations’ using some form of SRS 47.5%, up from 43% in 2007, and 38% in 2005.

Many respondent organisations use more than one SRS, and the level rose from 47% in 2005, through 55% in 2006, to 63% in 2007. This year the level dropped to 35%, although this may be due to a change in question structure and wording.

The structure and content of the question changed for the 2010 survey, so it is impractical to compare earlier results without considering this. Internally Produced Standards topped the 2010 list, but the most commonly used IT Security-Related Standard was ISO/IEC 27002 (previously known as ISO 17799) - Information Technology - Information Security Management Standard, which was used by around 20%.

Probably due to the high response rate from both national and local government sectors, NZ Government – Security in the Government Sector (SIGS) was next most common on 17.1%, followed by ISO/IEC 27001 – Information Technology – Information Security Management System and AS/NZS ISO/IEC 17799 (previously known as AS/NZS 4444) Information Technology - Code of Practice For Information Security Management both on 16%. Vendor-Specific Standards or Guides were used by 14%.

The NZ Government NZSIT 400 series had 12% use, with around 10% using Other NZ or International Industry Specific IT Security Standards. Other responses were reported as: ISACA, CISM, COBIT, GSO IBM Protocol, Info Security Policy Made Easy (C. Cresson Woods), advice from GCSB & other govt depts., BS5999, Audit NZ recommendations, and Sarbanes Oxley.
Information Security Training, Qualifications and Certification

The question regarding the **Percentage of IT Staff With Security Qualifications** received 160 responses. Around 83% of these respondents said that their IT staff had **No Security Standard Qualification**, with another 15% reporting that **Less Than 10%** of their IT staff had any security qualification.

The remaining 2% of respondents said between 41 and 60% of their IT staff were security qualified.

Results for **Levels of Qualification and Training of IT Staff and Contractors** can be seen in Figure 26. Staff with **No Qualification** remained at the 2007 level of 9%, similar to that of 2005.

As in 2007, the most commonly held category of staff qualification was **Industry Vendor IT Certification** (MCSE, CCNA, etc) at 46%, well down on 58% in 2007 and the 52% 2005 figure. Second most held at 41% were **Tertiary IT Qualifications**.

39% held **Industry Vendor IT Security Certification** (Cisco etc), holding steady from 38% in 2005. **Tertiary IT Qualifications** came in at 41%, up from 36% in 2007 and 37% in 2005. Around 37% were reported as having **No formal qualifications** but more than 5 years of security experience, this category dropping steadily from 51% in 2005 and 39% in 2007. **Vendor-Neutral IT Security Certification** was held by 11%, up 7% from 2007. The only response of **Other** was military.

Respondents’ level of satisfaction with the management of IT security may be seen in Figure 27. Around two-thirds still say their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness in **IT Staff** (62%), **Management** (65%) and **General Staff** (69%).

This year the additional category regarding **Contractors** threw up the interesting result that 47% of respondents considered their organisation also needed to do more to ensure 3rd party contractors’ level of IT security qualification, training, experience or awareness. Note that these are separate category figures, so percentages do not sum to 100.

**Other Issues**

In collaboration with NZITF, a number of questions were added to the 2010 survey.

The first was of organisations having a designated first responder; someone trained in areas outside standard IT support, such as where the need arises to preserve forensic or dynamic evidence undamaged and untainted.六
Of 176 respondent 2010 organisations, 11% had a designated first responder, with 5% of respondents not knowing if the organisation had one or not, leaving 84% of respondent organisations without first responder capability. This may change as ISO/IEC 27037 comes into use.

Another question dealt with comparative importance perception of various security issues. Respondents ranked 7 issues in order of perceived importance. Results may be seen in Figure 28, where it is clear that Generic External Threat (e.g. Virus/malware) (46%) was the greatest perceived issue by a wide margin.

That Security Policy Compliance and Protection from Internal Users were the second and third largest perceived issues backs up the 2007 report finding that insider threat poses the greater risk to organisational security.

Unsurprisingly, 94% of the 172 respondents to the question on mobile device use deployed them. Perhaps less obvious, that 63 mobile devices being lost or stolen in 1 year from the 162 Mobile Device Security Incident question respondents challenges the 5% perceived importance rating for mobile device security.

Related to this was the 11-14% range of respondent organisations unaware if their mobile devices suffered any security incidents.

Instances of virus or malware infection, phishing, and unauthorised network access were reported on mobile devices, so it seems organisations are seeing them more as extensions of the network that optional extras. Other responses were: Device loss only; data encrypted, unauthorized toll calls. See Figure 29.

Along this line of enquiry, Mobile Device Security Measures were also investigated and results may be seen in Figure 30 (next page). Immediately noticeable are the 1 in 4 respondents with No Security Tools or Procedures.

Despite cryptography having a low rating in security awareness training, it made a showing in Mobile Security, with respondents deploying it on around a quarter of PDAs, Smartphones, and Other Devices, although few employed it on Old Cell Phones.

There were quite a number of Other responses: Enforce Use Policy, lock down policy, remote wipe, remote killing, traffic encrypted, locking policy PIN, password use & lockout, Good technology mail client, all devices replaced with Blackberry, cached domain credentials for laptops, policy enforcement through ActiveSync – MS Exchange, rely on network software, all phone use through proxy, 2-tier password protection, security certificates, VPN tunnel network connection
Malware infections are becoming more common and more difficult to detect and remove, as the creators make use of many sophisticated techniques and as ‘improved’ variations appear.

Conficker had nothing new but was difficult to find and erase because it combined so many advanced malware techniques. Estimates differ widely, but variations of the worm infected millions of machines around the world and experts are still discussing the ramifications.

The questions regarding Conficker gained 175 responses, with 24% of respondent organisations saying they had been infected, and 2% unsure.

As may be seen in Figure 31, the scale of infection varied from Up to 1% of machines for half the organisations infected, to 98% for 1 organisation, with 3 out of 4 affected organisations having less than 10% of their machines infected.

The time taken to remove Conficker completely from respondents’ networks also varied widely, with some managing to remove it to their satisfaction within an hour, but more than one still being uncertain of complete removal after a month. See Figure 32.

Some respondents set the cost of removal at $0, yet one spent over a month and $200k to clear it off all their machines. Many were simply unable to put a cost on removal. See Figure 33 (next page).

Respondents were asked whether they were able to trace the source of the infection, and among the vectors were: USB via 3rd party network segment, USB via antivirus laptop, USB PowerPoint by overseas visitor, USB by security guard, remote laptop connecting to web outside secure VPN, Win2k patch pushed but not applied, Active Directory Accounts being locked out, unpatched site server mistakenly

---

**Figure 30** Mobile Device Security Measures

<table>
<thead>
<tr>
<th>Device</th>
<th>Response Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDA</td>
<td>24</td>
</tr>
<tr>
<td>Smart Phone</td>
<td>25</td>
</tr>
<tr>
<td>Other Mobile Device</td>
<td>20</td>
</tr>
<tr>
<td>Old Cellphone</td>
<td>24</td>
</tr>
</tbody>
</table>

---

**Figure 31** Percentage of Respondents’ Networks Infected

<table>
<thead>
<tr>
<th>Percentage of Infection</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 1%</td>
<td>50</td>
</tr>
<tr>
<td>2-10%</td>
<td>23.8</td>
</tr>
<tr>
<td>11-20%</td>
<td>7.2</td>
</tr>
<tr>
<td>21-30%</td>
<td>2.4</td>
</tr>
<tr>
<td>31-40%</td>
<td>0</td>
</tr>
<tr>
<td>41-50%</td>
<td>0</td>
</tr>
<tr>
<td>51-60%</td>
<td>2.4</td>
</tr>
<tr>
<td>61-70%</td>
<td>0</td>
</tr>
<tr>
<td>71-80%</td>
<td>0</td>
</tr>
<tr>
<td>81-90%</td>
<td>11.9</td>
</tr>
<tr>
<td>91-100%</td>
<td>2.4</td>
</tr>
</tbody>
</table>

---

**Figure 32** Time to Fully Remove Conficker

<table>
<thead>
<tr>
<th>Time Period</th>
<th>Percentage of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 hr</td>
<td>9.5</td>
</tr>
<tr>
<td>3 hr</td>
<td>9.5</td>
</tr>
<tr>
<td>6 hr</td>
<td>9.5</td>
</tr>
<tr>
<td>12 hr</td>
<td>11.9</td>
</tr>
<tr>
<td>24 hr</td>
<td>4.8</td>
</tr>
<tr>
<td>2 days</td>
<td>11.9</td>
</tr>
<tr>
<td>1 week</td>
<td>16.7</td>
</tr>
<tr>
<td>Up to 1 month</td>
<td>9.5</td>
</tr>
<tr>
<td>Over 1 month</td>
<td>7.1</td>
</tr>
<tr>
<td>Not certain of removal</td>
<td>9.5</td>
</tr>
</tbody>
</table>
installed, laptop used on home network, machine brought onto network without antivirus, overseas operating company attack, and through use of antivirus software. One respondent traced source through system logs & user activity. One respondent reported Conficker prevented by antivirus, so patched proactively. By far the main vector was USB.

Besides being one of the main vectors for virus and malware infection, USB has also been one of the main vectors for data loss incidents. Respondents were asked what forms of protection their organisation had in place to defend against USB incidents and 174 responded to this question.

As may be seen in Figure 34, over half of respondent organisations had No Protection In Place. Around 17% avoided the problem by having Removed USB Capability or having None. One organisation in ten had USB Copy Protection, and 6% had File Copy Protection. Note that these were multi-choice options so percentages do not total 100.

Responses of Other were reported as: Autorun/Autoplay Disabled, Ironkey Only, Network Access Control; Auto Virus/Spy/Malware Scan on Insert, Encryption, Authorized USB Access Control, End Point Control, USB File Transfer Scanning, Approved Users Only, Internal Policy, and Only Encrypted Drives Allowed.

Finally, some respondent observations: One respondent commented that they had “visual biometric” because they could visually identify anyone unauthorised for access.

Another reported an attack where someone hacked into a DDI that wasn't protected by a password. That got them into the PBX, where they used the voicemail dial-in facilities to program that DDI to divert calls to Slovenia. The DDI then received 4-5,000 calls within a few hours, but having very recently installed locally built PBX firewall software, (Callista) it blocked the call diversions and saved the organisation a $4k+ phone bill.

One wit commented, “We know we have a worm when the firewall gets busy.”
Concluding Comments

There are some issues raised here that require further investigation: In an environment of ever-increasing risk, that investment of IT budget on security continues to drop might be cause for concern. The trend toward trusting tertiary qualifications to prepare people for ICT employment might also need further thought. Something is not right when almost half of respondents are dissatisfied with 3rd party contractor management. USB devices are clearly a major risk factor, so management of USB is an issue for further work. Should you wish to discuss any of the findings contained in this report or suggest areas for further investigation, please feel free to contact the author.

Acknowledgements

For the funding which made this survey possible, InternetNZ; for their support, the New Zealand Internet Task Force and New Zealand Police. For their contributions to this initiative, Paul McKittrick of the Domain Name Commission, Tony Grasso of the Department of Internal Affairs Anti-Spam Unit, Associate Professor Hank Wolfe and Dax Roberts of the Otago University Security Research Group, Adam Fier of Victoria University of Wellington IT Services Security, Dr Russell Smith and Dr Raymond Choo of the Australian Institute of Criminology, and Robert Richardson of the Computer Security Institute.

Particular thanks to all those respondents who took the time to participate in the 2010 survey.

References

NEW ZEALAND

COMPUTER CRIME
AND SECURITY SURVEY

2010