Published by the:

Alpha-Omega Group, S.A.
P.O. Box 6079
Dunedin 9059
New Zealand
Copyright 2007
ISSN 1177-4207

Acrobat® versions (.PDF) are available free from:

SQuinn@infoscience.otago.ac.nz

Or

hwolfe@infoscience.otago.ac.nz
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 Government Communications Security Bureau’s Centre for Critical Infrastructure Protection (CCIP), New Zealand Police, NZ Internet Task Force, and the Computer Security Institute (CSI). This 2007 survey is the third annual New Zealand (NZ) survey. It is based on the US CSI/FBI 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 2007 survey results are based on the responses of 150 computer security practitioners in NZ manufacturing, governmental, financial and medical organisations, and tertiary education providers regarding the 2005 calendar year. All monetary figures are in NZS, roughly equivalent to US$0.70 at time of publication.

Issues considered in this survey are:

- Types and prevalence of security technologies in use
- Types, cost of, and response to security incidents
- Budgeting issues: percentage of IT budget spent on security, outsourcing of security function, incident insurance, security investment per-employee, cost-benefit metrics in security planning
- Popularity of common workstation operating systems (OS)
- Security audits and security awareness training
- Information security training, qualifications and certification
- IT standards, policies and procedures
- Managing proprietary information on PDAs / Cellphones
- Management of SPAM
- Handling of porn and objectionable material on workplace ICT

NB References to US figures refer to those from CSI surveys, while references to Australian figures refer to those of the 2006 AusCERT survey. In referring to monetary costs, the word ‘thousand’ is substituted by ‘k’ for brevity.
Executive Summary

Key Points
Many IT staff are not aware of their legal obligations on discovery of objectionable (and there-fore illegal) material. On discovery of objectionable material, 95% dealt with it internally.
31% reported Unauthorised Use incidents, up 25% from 2005. See p.9.
Internal unauthorised use was higher in the government sector, although difficult to quantify.
64% invested less than 5% of their IT budget on security. AusCERT calls this insufficient. See p.7.
Average security spending per employee rose noticeably, possibly indicating greater awareness of its importance.
Incident number are down, but were experienced by 87%, and this is expected to rise. See page 10.
Attacks from inside are common. Industry experience suggests background checks lacking.
Few protect information held on Cellphones / PDAs, suggesting exposure risk. See page 21.
One third of respondents were prepared to cooperate with anti-SPAM researchers. See page 22.
73% of respondents reported that their IT staff had no security standard qualification. This Lack of security qualifications should be a bigger issue because of the risk
Infrastructure organisations should be most secure but figures often do not support this

Incidents
83% experienced security incidents and this is expected to rise. See Fig. 13, page 11.
Average cost of incidents per organisation $133k; 78% being Telecommunication Fraud. See p.12.
75% monitored for Unauthorised Use and 31% experienced it. See page 10.

Budgeting Issues
66% spend less than 5% of IT budget on security, now regarded as insufficient. See Fig. 6, page 8.
Average Total Computer Security Investment figures were $311 for Operating Expenditure and $235 for Capital Investment, totalling an investment per employee of $546. See Fig. 7, page 8.
Cyber-security risk insurance use rose slightly in 2007, reversing the downward trend. See pp. 9-10.
Half believed that aspects of security were not appropriately funded, down from 2/3. See page 14.

Policy and Procedure Issues
Security policy is directed from outside NZ for 17% of non-government organisations. See page 8.

Training and Qualifications
Two thirds say they needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness for General Staff, IT Security Staff and Management. See page 20.
73% of IT staff had no security standard qualification See Figure 28, pages 17-18.
9% of Primary IT Security Staff had no qualification. See Fig. 29, page 18.
Around 43% adhere to IT Security Related Standards, 63% of those using more than one. See p.17.

Technologies
Security effectiveness evaluation: Many with minimal use & 4% none. See Fig. 24, p.15.
77% used security audits to assess system management, See Figure 20, page 13.
61% conducted Internal Audits & 56% External Security Audits, down 7% from 2005. 42% used Automated Tools to check Network Systems Configuration. 4% didn’t check. See Fig. 24, page 15.

Management Issues
63% conducted some cost-benefit analysis on security expenditure. See Fig. 9, page 8.
Again, few prosecutions were brought, with even fewer convictions. See Fig.19, page 13.
**DETAILED SURVEY RESULTS**

![Figure 1](https://via.placeholder.com/150)

**Organisational Activity**

<table>
<thead>
<tr>
<th>Organisation</th>
<th>Percentage of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Govt</td>
<td>5</td>
</tr>
<tr>
<td>Manuf./Prod.</td>
<td>5</td>
</tr>
<tr>
<td>Nat. Govt</td>
<td>11</td>
</tr>
<tr>
<td>Financial</td>
<td>12</td>
</tr>
<tr>
<td>Service (comm.,trade)</td>
<td>17</td>
</tr>
<tr>
<td>Utilities (fuel,electr)</td>
<td>5</td>
</tr>
<tr>
<td>Retail</td>
<td>5</td>
</tr>
<tr>
<td>Wholesale</td>
<td>4</td>
</tr>
<tr>
<td>Medical</td>
<td>4</td>
</tr>
<tr>
<td>Transport</td>
<td>3</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
</tr>
<tr>
<td>Education</td>
<td>3</td>
</tr>
<tr>
<td>High Tech</td>
<td>3</td>
</tr>
<tr>
<td>Telecomm.</td>
<td>3</td>
</tr>
<tr>
<td>Construction</td>
<td>3</td>
</tr>
<tr>
<td>Entrance Media</td>
<td>3</td>
</tr>
<tr>
<td>Legal</td>
<td>3</td>
</tr>
</tbody>
</table>

About the Respondents

Respondents were the same set of 500 as used for the previous two surveys, drawn from an original total of 750 organisations and reduced to 500 by removing the smaller ones and those who outsourced all IT. In 2006 four specialist IT services organisations replied on behalf of a number of organisations who now outsource part or all of their IT. The original 750 were drawn from two sources. These were: 1. The 2004 SRG survey respondent list of top 500 organisations by turnover; 2. national and local government organisations.

A few respondent organisations did not respond due to being assimilated in 2007, a few more did not respond due to the contact person leaving. This reduced the previous 500 respondents to 455. Despite this, responses rose from 22% to 33%, well above average in surveys of IT management.

Figures 1 through 5 summarise information about the organisations that responded to the 2007 survey and the individuals representing those organisations. The 2007 survey was no longer anonymous, providing the possibility of direct longitudinal study of data to draw reasonable conclusions as to trends over an extended period.

Figure 1 shows the figures for respondents by industry sector. Local Government was the dominant sector at 17% of respondents, with 14% of responses from the Manufacturing sector. 12% were from National Government, and 11% from the Financial sector.

Organisational size measured by the number of employees can be seen below in Figure 2. There would seem to be a general upward trend in the size or respondent organisations. As in 2005 and 2006, New Zealand’s population of four million was well represented in the higher employee-number organisations with 27% responding that they employed *1000 and Over* people, well up on last year’s 15%, with 11% employing *500-999*, well down on the 2006 figure of 18%, which would seem to be where much of the extra percentage in the higher category came from. At the other end of the scale, 21% of respondents employed fewer than 100 people.

© Security Research Group, University of Otago. All rights reserved.
Figure 3 shows that larger turnover organisations are well represented in the NZ survey, with organisations having revenue generation in excess of $100 million comprising 44% of respondents. The NZ figure was somewhat lower than the 57% in the 2006 & 2007 US surveys.\(^1\), p5; \(^2\), p4. Note that due to rounding, figures in some graphs do not sum to 100%.

Results for Areas of Operation can be seen in Figure 4. Weight of the line indicates the percentage of respondents operating in each region. Figures are very similar to those of 2006, with only minor changes. Australia is our closest business partner with 29% of all respondents also operating there.

The 150 2007 respondents indicated that 13 of their organisations operated only in NZ and one other geographical region. Of these 13, 10 identified Australia as their other region. Interestingly, all of the 10 were NZ based.

Figures for Respondents by Job Title can be seen in Figure 5. Once again, over half respondents to this question (52%) were IT Manager of their organisation, with a huge drop to the next most common title of Systems Administrator at 14% of respondents.

The US survey notes that their respondent pool likely skews toward the more security-conscious due to the preponderance of CSI members and course attendees who become respondents, so because of the nature of the New Zealand respondent pool selection process, this skew does not apply to the NZ survey.\(^1\), p7.
Budgeting Issues

Percentage of IT Budget Spent on Security, may be seen in Figure 6, with the NZ up-to-5% figure once again being slightly higher than that in the US.1, pp.7-8

Once again, around two thirds (66%) of NZ organisations invest up to 5% of their IT budget on security. This is up 2% from 2006, whereas the US 61% figure was up 6%.1, pp.7-8

As mentioned in the previous NZ report, the 2006 Australian report found that 51% of respondents considered under 5% to be inadequate.2, p.13

Around 18% of NZ respondents indicated they spent between 5 and 10% of their IT budget on security issues, the same figure as in the US. Organisations spending more than 10% dropped from 5% to 2% in NZ in 2007, compared with 9% in the US.1, pp.7-8. Around 16% of NZ respondents did not know the percentage of their IT budget allocated to security.

In 2007, 17% of non-governmental respondents indicated that their computer security was dictated from outside NZ, slightly down from 19% in 2006 and 18% in 2005, previously reported, before exclusion of governmental agencies, as 27% and 24% respectively.

Figure 7 shows the Estimated Average Computer Security Expenditure Per Employee by revenue. 2006 figures were considerably lower than 2005, but figures have rebounded with the improved 2007 response rate supporting the conclusion that the low 2006 figures were a data anomaly resulting from a reduced response rate.

Overall, the average Total Computer Security Investment figures were $311 for Operating Expenditure and $235 for Capital Investment, totalling an overall average security investment per employee of $546.

The Under $1m budget category reported average figures of $410 Operating Expenditure and $300 Capital Investment, with the $1-10m category reporting $265 Operating Expenditure and $30 Capital Investment. Figures for the $10-100m category were Operating Expenditure $114 and Capital Investment $77. The $100m-1 billion budget category figures were Operating Expenditure $133 and Capital Investment $58. There was a big jump to the Over 1 billion category, where the figures were Operating Expenditure $631 and Capital Investment $711.

There were similar figures in the mid categories with marked expenditure rises in the lower and upper categories. Given the small 2006 data set, despite the rises between the
2005 and 2007 reports, at this stage it is difficult to reliably forecast on the indicated rising expenditure trend.

Figure 8 shows Estimated Security Related Spending by industry sector. The industry sector investing most in security was National Government at a massive $5,492 per employee, with Financial close behind at $5,450.

The vast majority of all security spending was Operating Expenditure, with National Government spending $5,356 per employee, and Financial spending $4,917. Each of these spent well over double the investments of the next two sectors’, and two thirds of sectors invested only a tenth of National Government or Financial spending.

Regarding Capital Investments, the $1,000 per employee spent by Telecommunications, and the Financial sector’s $533 were both considerably higher than other sectors but most sectors’ capital investment was negligible compared with Operating Expenditure.

Respondents were again asked to state their use of cost-benefit metrics in planning computer security spending. Use of Return on Investment (ROI), Net Present Value (NPV) Internal Rate of Return (IRR) or Other metrics can be seen in Figure 9. Compared to ROI, IRR and NPV dropped this year.

Just under two-thirds (63%) of respondents conducted some cost-benefit analysis on security expenditure, similar to the 2006 figure of 70%. As in previous years, those who use any metrics often use more than one. Note that metrics were assessed separately so figures do not sum to 100.

Outsourcing of IT is a growth area. 2007 figures are similar to 2006, with Figure 10 (page 9) showing 8% of 2007 respondents outsourcing over 80% of their security function, while half outsource none. Figure 10 shows how organisation size affects the percentage of security function outsourced. Both the US and NZ tend toward larger organisations outsourcing more. The US averages range from 22-22%, depending on budget size, with 61% outsourcing no security function. Use of external cyber-security risk insurance as a tool in managing security rose slightly in 2007, reversing the downward trend from 31% in 2004 to 20% in 2005 and 16% in 2006. Just on 46% of 2007 respondents organisations had no cyber-incident insurance, compared with 55% in 2006. In the US, the 29% 2007 figure continued the very slow growth since monitoring began in 2004.
In 2004, 24% of respondents did not know whether they had insurance, but the 34% figure from 2005 was repeated in 2006 and remained steady in 2007 at 33%.

The Frequency, Nature and Cost of Cyber Security Breaches

In 2005, the level of monitoring of unauthorised computer system use was unknown, so this was investigated in the 2006 survey, when 85% of respondent organisations indicated that they did monitor unauthorised use.

The 2007 results can be seen in Figure 11. Almost a third (31%) experienced unauthorised use of their systems.

Once again, incidents originating inside the organisation outnumbered those from outside, supporting the conclusion that insider attacks make up the greatest threat to organisational security.

It is the author’s personal experience, backed up by industry-professional reports that misuse of work- place ICT for pornography, online gaming such as Farmville, social networking, and online trading programs is extremely common, particularly in government organisations where the historical perception of job security still persists. Blocking software is one solution, but in the opinion of this author, better team work, leadership, and clear guidelines and punishment would be more effective.

Almost two thirds (63%) of respondent organisations said they did not experience any Unauthorised Use incidents, but 6% said that they did not know whether they had or not.

Fig 12 shows that despite fluctuating...
responses, the percentages of respondents experiencing Unauthorised Use show minimal proportional change from 2005-2007.

Figure 13 shows the percentages of respondents experiencing various types of security incidents. Around 83% of 2007 respondent organisations had experienced some type of security incident, the most common incident types being Insider Abuse of Net Access/Email, Laptop/Mobile Hardware Theft, Virus, and Music/Movies/Ripping.

Figures, proportions, and category order did not differ significantly from those seen in the 2006 survey.

One of the 2005 survey questions requested historical data on incident numbers, which showed consistent growth from 1998-2004. Large increases in reported incident numbers in the 2007 survey data reversed the dips noted in the 2006 data. These increases are mostly due to the inclusion of data from a few new respondents in the Telecommunications sector, but it is hard to quantify how many of the dips in the 2006 survey data were due to the heavily reduced dataset, and how many resulted from the changes in respondents.

The 2007 survey dataset was improved by the return of a number of organisations that had not re-

sponded the previous year, as well as some previously non-respondent organisations. Every incident category was affected by the inclusion of new data from the previously minimally represented Telecommunications sector.

Figure 14 highlights the difference when data from these organisations is added. As mentioned previously, every one of the categories took a sharp upward turn, but half the category figures were so far off the scale that the graph had to be cropped, with Unauthorised Access/Use averaging 7.75 incidents per organisation, Insider Abuse 14.61, Financial Fraud 21.44, and Telecommunication/Toll Fraud averaging a massive 224 incidents per organisation. These changes were in each case due to the inclusion of either one or only a handful of comparatively huge figures.

It can be seen in Figure 14 that the 2007 incident data far exceeded any trend predictable from the historical 1998-2004 data. It would seem therefore, that the historical data gathered in the inaugural 2005 survey did not adequately represent the Telecommunications sector, but it is pleasing to note that the new respondent input is improving the overall quality of the survey’s data and therefore reliability and usefulness.
Figure 15 shows the average cost of incident types to the respondent organisations. Clearly, the addition of data from the Telecommunications sector had a big influence on incident cost analysis, making Telecommunications Fraud by far the most costly incident type at an average of $104k per respondent, up massively from $0.4k.

This raised the average cost of incidents per organisation to over $133k; 78% being Telecommunication Fraud, whereas the 2006 average was $36k, with Telecommunications Fraud comprising only 1.5% of the total.

At $12k, Financial Fraud retained its second-highest position in the last survey, after leading incident costs in the inaugural 2005 survey. Laptop or Mobile Hardware Theft cost an average of $5k per respondent organisation in 2007, with Misuse of Public Web Application on an average of $4.6k.

Virus (incl. Worms/Spyware) was next on $2.5k, with Music/Movies/Ripping costing an average of $1.4k. Denial of Service cost $1.2k, well down on previous years. Then came System Penetration $0.7k (down from its $12.5k top place) and Unauthorised Access to Information, also at $0.7k. IP Theft average cost was $0.5k, and Abuse of Wireless Network $0.1k, with Website Defacement bringing up the rear on an average of $0.06.

Two 2005 respondents identified Website Defacement as occurring, but supplied no data regarding the financial cost of these incidents. The 2006 survey also had 2 organisations saying that Website Defacement occurred, but data was insufficient to make the average cost calculation worthwhile. The 2007 survey saw 12 organisations reporting Website Defacement.

Employing reform hacks to test security of systems remains unpopular in New Zealand, with the proportions remaining almost static at 64% indicating they would not do so, 22% being unsure, and 15% of the 144 respondents to this question indicating that they might do so.

Incidents and the Law

Responses regarding organisational actions taken after incidents/intrusions can be seen in Figure 16. Respondents checked all relevant categories, so percentages do not total 100.

Figures remained similar to those in previous years, with the most common response being Patched Security Holes (90%). Did Not Report Outside Organisation was the next most common action (56%). Reported to Police was on 13%, with Reported to Legal Counsel...
cused on pursuing their core business than assisting law enforcement in prosecuting offenders, yet crime cannot be reduced without business working with law enforcement.

As with both previous surveys, the highest Did Not Report incident type was Computer Virus, followed this time by Insider abuse, and Telecommunication / Toll Fraud. There were no reported instances of Extortion, Money Laundering, Sabotage, or Theft of Transactional Information.

A surprising number of other illegal incidents were not reported to law enforcement either, including all instances of Financial Fraud, ID Theft, Espionage, Product Piracy, Proprietary Rights Infringement, Theft of Information, or Product Piracy incidents were reported to management, they were seldom reported to Police. See Fig. 17.

Figure 17

![Graph showing external reporting of incidents](image)

Some incident types tend to generate predictable reactions. The main response to Virus, Denial of Service, Unauthorised Use and Insider Abuse incidents was to Patch the System, with only 2 Unauthorised Use and 1 Insider Abuse incidents reported to law enforcement.

At the other end of the scale, all reported cases of Corruption or ID Theft, and most Hardware Theft incidents were reported to both management and Police. Perhaps not surprisingly, only half of Financial Fraud incidents were reported to Police. Although many Telecommunications Fraud, Espionage, Proprietary Rights Infringement, Theft of Information, or Product Piracy incidents were reported to management, they were seldom reported to Police. See Fig. 17.

Figure 18

![Bar chart showing reasons not reported to law enforcement](image)

Theft Hardware/Assets was the incident category most reported to law enforcement at 33%, compared with 37% across all categories. Only around one third of respondents (37%) reported any incidents to law enforcement.

The 2005, 2006, and 2007 surveys indicate that the vast majority of discovered crime goes unreported. It goes without saying that organisations are more fo-
but 2007 showed both Unaware of Law Enforcement Interest and Fear of Negative Publicity as joint leaders, although Unaware of Law Enforcement Interest had fewer considering it unimportant.

Figure 19 shows the number of prosecutions and convictions relating to reported incidents. As found earlier, few prosecutions are brought, with even fewer convictions.

**Security Audits and Security Awareness Training**

Over three quarters (77%) of 2007 respondents used security audits to assess system management. Results may be seen in Figure 20, with two thirds of respondents (66%) reporting audit results to the Chief Information Officer, and 38% to the Chief Executive Officer.

Overall security audit use in 2004 was over 80%, with 20% of those conducting security audits not reporting results to upper management. In 2005 non-reporting dropped to 2%, then 3% in 2006 and 2007.

Once again, round one in five respondents indicated that results were reported to alternative upper management or extra-organisational authorities. Among these were: Audit & Risk Management Committee, Operational Risk, DCE Corporate Technology Committee, Corporate Services Director, HO Security Group, Senior Management, Regional HO, IT Manager, Executive Team, IS Manager, Security Committee, International IT, External Audit, IT Manager, Corporate Security, Technology Managers, Immediate management, External owners, AP A/C team, IT Security Officer, Council as part of external audit, Business Units, Audit /risk Committee, CES, Bank, with one organisation responding significant deficiency reported to senior management.

As with previous surveys, it was inferred that around a quarter of this year’s respondent organisations are in overseas ownership or control.

Of 148 respondents, almost half (49%) believed that aspects of security were not appropriately funded, although this figure was significantly down on both previous survey figures of around two thirds.

Respondents were again asked to rate their level of agreement with the statement *My Organisation Invests Appropriately in Security Awareness Training*. Overall, 28% agreed, with 24% of 2007 respondents undecided. Interestingly, disagreement has reduced 8%
since 2005, suggesting that NZ might be improving accuracy of awareness training investment planning.

When results are viewed by sector however, the majority of sectors still disagree. This year the Services and Utilities sectors joined Telecommunications in agreeing, with High Tech undecided. See Figure 21.

Figure 22 shows that the highest rating was once again for Network Security, with three out of four respondents considering it important. Three quarters of respondents also perceived Access Control Systems and Security Management as important, with Security Policy important to two out of three, down from second position in both previous surveys and the only major change. Security Systems Architecture was important to over half of respondents. In reducing order of importance perceptions were Economic Aspects of Computer Security (e.g. Budgeting), Investigations and Legal Issues, and finally Cryptography, climbing back up 5% to one in four.

Once again, the low perceived importance rating for cryptography suggests that it is an underrated tool in NZ IT security, as US importance ratings rose from 28% in the 2004 survey to 37% in the 2007 survey.1, p.12; 1, Fig.22 p.21

### Security Technologies

Figure 23 (p.15) shows security technologies used in 2007 survey respondents’ organisations. Of the network defence technologies available, 100% of respondents used Anti-Virus Software, 99% had Firewalls in place, and 67% ran Intrusion Detection Systems (IDS) on their networks. This figure has risen slightly from 56% in the last survey but is still below the US figure of 69%.1, p.18

Most respondents (85%) implemented Server Based Access Management, continuing the increase noted in the last survey. Encryption was considered in the same three separate categories as Encrypted Data Files, Virtual Private Network and Public Key Infrastructure. Reusable Passwords use was up to 41% after dropping from 38% in the 2005 survey to 29%. Smart Card use was up slightly on 29%, with Biometrics up to 13% this year, from the last survey’s 1%, and 9% in 2005.

Examining differences in technology usage between the 2005 and 2007 survey data, all usage rose to some degree, despite some apocryphal reductions due to a reduced 2006 survey data set. Looking at changes over a 5% threshold, IDS jumped 25% to 67%, VoIP climbed 8% to 38%, Access Management
2007 NEW ZEALAND COMPUTER CRIME AND SECURITY SURVEY

Figure 23
Technologies in Use

<table>
<thead>
<tr>
<th>Percentage of Responses</th>
<th>2007: 150 Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-virus software</td>
<td>100</td>
</tr>
<tr>
<td>Other</td>
<td>99</td>
</tr>
<tr>
<td>Firewalls</td>
<td>93</td>
</tr>
<tr>
<td>Software upgrades/replacements</td>
<td>89</td>
</tr>
<tr>
<td>Remote access</td>
<td>86</td>
</tr>
<tr>
<td>Mobile Dev. (Laptop, PDA Blackberry etc.)</td>
<td>84</td>
</tr>
<tr>
<td>Hardware upgrades/replacements</td>
<td>84</td>
</tr>
<tr>
<td>Web sites (information)</td>
<td>83</td>
</tr>
<tr>
<td>VPN</td>
<td>82</td>
</tr>
<tr>
<td>Physical security</td>
<td>79</td>
</tr>
<tr>
<td>Access management</td>
<td>73</td>
</tr>
<tr>
<td>Content filtering/monitoring</td>
<td>67</td>
</tr>
<tr>
<td>Anti adware/spyware</td>
<td>61</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>60</td>
</tr>
<tr>
<td>Wireless</td>
<td>59</td>
</tr>
<tr>
<td>Web sites (transactional)</td>
<td>58</td>
</tr>
<tr>
<td>Encrypted login</td>
<td>52</td>
</tr>
<tr>
<td>Reusable passwords</td>
<td>50</td>
</tr>
<tr>
<td>VoIP</td>
<td>49</td>
</tr>
<tr>
<td>Single sign-on provisioning</td>
<td>47</td>
</tr>
<tr>
<td>Smart cards/tokens</td>
<td>45</td>
</tr>
<tr>
<td>PKI</td>
<td>43</td>
</tr>
<tr>
<td>Encrypted data files (data at rest)</td>
<td>41</td>
</tr>
<tr>
<td>Digital IDs</td>
<td>34</td>
</tr>
<tr>
<td>Other Encryption</td>
<td>30</td>
</tr>
<tr>
<td>Biometrics</td>
<td>24</td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
</tr>
</tbody>
</table>

went up 12 to 85%, Content Filtering rose 7 to 84%, and Physical Security also rose 7 to 89%, with VPN up 5 to 90%.

Figure 24 shows popularity of Information Security-Effectiveness Evaluation-Techniques. Web Activity Monitoring Software was most common on 76%, up on the 2005 figure of 70%. Email Monitoring Software took second position with 75% of respondents deploying it, slightly down on the 2005 figure of 79%.

Penetration Testing was employed by 43% of respondents, with this survey returning to the previous single category combining Internal and External Testing. The figure is slightly down on 2005’s 46%.

Internal Audits were conducted by 61% of respondents, 1% up from 2005, with 56% conducting External Security Audits, down 7% from 2005. Automated Tools To Check Configuration Of Network Systems was up 7 to 42%.

Other techniques were used by 8% of respondents. Many respondents used a minimal set of these security effectiveness evaluation tools, with 4% of respondents using none.

In collaboration with Netsafe, a line of questioning was added to this survey to evaluate how organisations handle the necessary updates for operating systems and security software. See Fig. 25.

148 organisations responded regarding how often their organisation applied security patches and updates in four security infrastructure areas; Operating Systems, Firewalls, Anti-Virus, and Anti-Spyware. Only one in four organisations up-
dated all four either daily or automatically. The SRG survey has been recording numbers of NZ Workstation Operating Systems since 1996. As expected, the most common workstation operating system in the 2007 survey was Windows (2000/XP) accounting for over 93% of respondents’ systems. Naturally, as the current Windows version proportion increases, other Windows versions all drop correspondingly. NT barely registered at 0.2%, and Vista was included in the 1% of systems reported as Other, but is expected to feature in subsequent surveys.

Mac once again came a very distant second on 3%, dropping another 2%, with Linux/Unix on 1%. The results can be seen in Figure 26.

**IT Standards, Policies and Procedures**

Policies and procedures are almost essential tools in organisational security. As Centre for Critical Infrastructure Protection Managing Director Richard Byfield said in his introduction to the previous survey, “Technology solutions alone are not enough and organisations need to build a culture of cyber security. People are a key component to raising the security posture of an organisation, but they need to be supported by clear and practical policy and procedures.” 4. p. 1

Figure 27 shows figures for Use of Computer Security Policies and / or Procedures. According to this year’s respondents, no policy or procedure had 100% uptake, but it was interesting to note that the order of popularity remained the same as in the previous survey, with User Access Management (enforcement of password use, user privileges, etc) the most implemented tool, used by 97% of respondents, and Media Back-Up used by 94%.

Next most popular policies/procedures were External Network Access Control on 78%, and Documented Standard Operating Procedures on 77%. Change Control was used by 74%, Controls Against Malicious Software by 72% and Monitoring System Access and Use on 71%.

Responses indicated that 68% relied on User Responsibilities and Incident Management was used by 58%. Segregation of Duties was employed by 46%, and 41% had Management of Removable Computer Media. It was pleasing to note that those with a Forensic Plan rose from 3% to 7% since the last survey. There were no responses of Other.

---

*Figure 26*  
**Operating System Usage**

2007: 140 Responses, comprising 245,606 workstations

- Win 9x/ME 1.3%
- Win NT 0.2%
- Mac OS 3.1%
- Unix/Linux/BSD 0.9%
- Other (incl. Vista) 1.0%

*Figure 27*  
**Security Policies/Procedures**

<table>
<thead>
<tr>
<th>Policy/Media</th>
<th>Percentage of Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access mgmt, (e.g. password, privilege)</td>
<td>97%</td>
</tr>
<tr>
<td>Media backup</td>
<td>94%</td>
</tr>
<tr>
<td>External network access control</td>
<td>79%</td>
</tr>
<tr>
<td>Documented standard operating procedures</td>
<td>77%</td>
</tr>
<tr>
<td>Change control</td>
<td>74%</td>
</tr>
<tr>
<td>Controls against malicious software</td>
<td>72%</td>
</tr>
<tr>
<td>Monitoring system access and use</td>
<td>71%</td>
</tr>
<tr>
<td>User responsibilities</td>
<td>68%</td>
</tr>
<tr>
<td>Incident management</td>
<td>58%</td>
</tr>
<tr>
<td>Segregation of duties</td>
<td>46%</td>
</tr>
<tr>
<td>Management of removable computer media</td>
<td>41%</td>
</tr>
<tr>
<td>Forensic plan</td>
<td>7%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

2007: 150 Responses
The Security Related Standards 2005 list no longer covers all standards used in NZ. It was not possible to update the list this time, but subsequent surveys will use an updated option set. 2007 survey information is included for those monitoring annual trends. See Fig. 28.

The overall figure for respondent organisations’ use of Security Related Standards (SRS) was 43%, down from the previous survey’s figure of 51%, but still up from the 2005 survey’s 38%. It is also encouraging to note that the number of respondent organisations using more than one SRS has risen from a 47% in 2005, through 55% in 2006, to 63% in 2007.

The most commonly used IT Security-Related Standard was AS/NZS ISO/IEC 17799:2001 (previously known as AS/NZS 4444.1:1999): Information Technology - Code of practice for information security management, which was adhered to by 48% of respondents.

Vendor-specific standards or guides were next most commonly used, implemented by 33% of 2007 respondents. Next were Other industry-specific IT security standards, adhered to by 30% of respondents, then Security In the Government Sector (SIGS) on 28%.

ISO/IEC 17799:2005 had 25% of respondents’ adherence, and both AS/NZS 17799.2:2000 (was AS/NZS 4444.2: 2000) and ISO/IEC 13335 IT Guidelines for Mgmt of IT Sec. had 17%, and one point behind was NZSIT 400. Around 8% had No Externally-Produced Standards In Use, but both HB 231: 2000 Info. Sec. Risk Mgmt Guidelines, and ISO/IEC 14516 IT Guidelines on trusted third parties had 3%.

Both ACSI 33 – Australian Communications – Electronic Security Instructions 33, and RFC2196 Site Security Handbook, had 2% of respondents adhering, but none used AS HB 171—2003 Guidelines for the management of IT evidence, although this was not unexpected, being an Australian standard.

### Information Security Training, Qualifications and Certification

The 2007 survey included a new question regarding the percentage of IT staff with Security Standards. See Figure 29. This question received 99 responses. Surprisingly, 73% of these respondents reported that their IT staff had no security standard qualification, with another 20% reporting that less than 10% of their IT staff had any of these qualifications.

Of the remaining 10% of respondents, 1% reported that 11-20% of their IT staff were security standards qualified, another 1% re-
reported 21-30%, another 1% reported 31-40%, and another 1% reported 41-50%.

No respondent had 51-70% of staff qualified, but 2% reported 71-80% of staff as qualified. None had 81-90%, and 1% had 91-100% of their IT staff security standard qualified. Note that due to rounding, percentage figures do not total to 100.

Results for IT Staff Qualifications and / or Training can be seen in Figure 30. The 2007 respondents reported 9% as having no qualification at all, up 5% from 2006, but similar to the more statistically reliable 2005 figure. NB. As most 2007 figures are close to those of 2005 but some differ markedly from 2006, the variance is assumed to result from the reduced 2006 dataset.

Most commonly reported staff qualification was Industry Vendor IT Certification (MCSE, CCNA, etc) at 58%, above the 52% figure from 2005 and well up on the 35% in 2006. Second most common at 43% was Industry Vendor IT Security Certification (Cisco etc), up from 38% in 2005. Ad Hoc IT Security Training Courses came in at 41%, the same figure as in 2005. Respondents reported 39% as having No formal qualifications but more than 5 years of security experience, down from 51% in 2005. Tertiary IT qualifications were held by 36%, and Vendor-neutral IT security certification by 11%, both down 1% on their 2005 figures.

Regarding security standards, almost three quarters of respondent organisations (73%) had no security-standard qualified IT Security staff. Only 7% reported that more than 10% of their IT security staff were security standard qualified.

There is a correlation between higher qualification levels and larger budgets, but in 2005 this seemed to drop off at the upper level. The 2007 figures describe the same correlation but without the top-level tapering-off. See Figure 31. Average percentage of Security-Standard qualified IT staff in the Under 1 Million budget category was at rock bottom on 0%, with 1-10 Million on 0.4%, 10-100 Million on 2.8%, 100 Million–1 Billion on 7%, and Over 1 Billion on 9.8%.

Viewing IT security-standard qualified staff by industry sector, a number of category averages were skewed by single high responses. Conversely, the Telecommunications sector provided 3 responses, removing the previous skew. Until higher response rates can be achieved, this skewing renders more detailed analysis impractical.
Respondents’ level of satisfaction with the management of IT security was again revisited (see Figure 32). Only one respondent did not answer this question. Figures remain similar, with around two-thirds saying their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness in IT Staff (60%), Management (68%) and General Staff (63%). Note that these are separate category figures, so categories do not total to 100.

There were 132 responses to the use of governance and or risk management tools question this time. Results may be seen in Figure 33. All figures are expressed as percentages of the total number of respondents that use governance and/or risk management tools.

NB The original Regularly Reviewed category in the 2005 survey was split into Internally and Externally for 2006. It is not therefore possible to directly compare with the 2005 figures but in general, Review seemed to be up in 2006. The 2007 figures reverse this, throwing doubt on the apparent 2006 rise.

Business Continuity Plans were down 2% from 2006 and up 2 from the 2005 figure, but still the most commonly existing IM tool, with 77% of the question’s respondents having them, although only 38% actually Adhered to, and 16% Formally Monitored them. On the positive side, 58% Internally Reviewed and 23% Externally Reviewed them, and 32% Reported the results to management.

Information Strategic Plans were second most commonly existing on 68%, down 6% from 74% in 2006 and from 81% in 2005. Respondents reported that 42% Adhered to and 17% Formally Monitored them, with 52% Internally Reviewing, 13% Externally Reviewing and 32% Reporting results to management.

Next was Use of Information Management Standards on 51%, up from 26% in 2006 and the 2005 figure of 38%. These were Adhered to by 32%, Formally Monitored by 9%, Internally Reviewed by 33%, Externally Reviewed by 5%, and 13% Reported the results to management.

Following closely, Risk Management Strategy existed in 49% of respondent organisations, with 30% Adhering to it, 14% Formally Monitoring, 35% Internally Reviewing, 14% Externally Reviewing and 22% Reporting the results to management.

An Information Security Strategy Existed in 48% of respondents’ organisations, down 10% from 2006 but only 2% from 2005. This was Adhered to by 32%, Formally Monitored
by 11%, Internally Reviewed by 33%, Externally Reviewed by 14%, and 17% Reported the results to management.

Finally, 40% had an Incident Response Plan, which 26% Adhered to and 8% Formally Monitored. This was Internally Reviewed by 25%, Externally Reviewed by 9%, and 14% Reported the results to management.

The 2005 report commented that once plans exist, half of them are never reviewed, and this still appears to be the case.

**Other Issues**

In collaboration with Netsafe, a number of questions were included in the 2007 survey.

Terms of use agreements are a part of life, especially online. How do organisations manage their employees’ use of ICT. In particular, copyright infringement, the responsibility for which technically devolves upon the ICT owner.

Respondents were asked a number of questions as to whether they employed, and trained users in, ICT use agreements, and how the organisation managed Illegal File Sharing (IFS). Results may be seen in Figure 34.

Respondents indicated that 19% had experienced IFS. Three in four (76%) said their staff signed ICT use agreements. Note that only half of these, (39%) were trained in the application of the agreements regarding everyday use of ICT.

Illegal file sharing was filtered / blocked by 42% of respondent organisations, and 32% monitored for illegal file sharing. Half of those (19%) both blocked/filtered and monitored. These figures suggest that more than 3 in every 5 organisations are oblivious to whether IFS is taking place on their ICT for which the organisation may be accountable.

Personal Digital Assistants (PDA) and cellphones are often used to store proprietary information, including passwords and cryptographic keys. How do organisations manage their use? Results may be seen in Figure 35.

Three quarters of respondents to this question set (76%) had Acceptable Use policies in place for PDA / Cellphone use, but less than half (43%) had Specific Security Policy for PDA / Cellphone use, and only one third (27%) Provide Staff Training on Secure Use of PDAs / Cellphones. Tellingly, 94% did not Require Use of Anti-Malware on PDAs / Cellphones.

Recalling that a chain is only as strong as its weakest link, those with both a Specific Security Policy and who Provided Staff Training...
on Secure Use totalled 14%. Only 2% Require Use of Anti-Malware and Provided Staff Training on Secure Use. Just 1% had Acceptable Use policies, Specific Security Policy, Provided Staff Training on Secure Use and Required Use of Anti-Malware on PDAs / Cellphones. Overall, this suggests that system passwords and other proprietary information held on unprotected Cellphones / PDAs are at significant risk.

Unsolicited email (SPAM) is a growing issue, reducing employee productivity and now making up over 94% of all email traffic. Respondents were asked how they handled SPAM, and whether they would be prepared to work with anti-SPAM researchers. Results may be seen in Figure 36.

Despite no-one ticking the No SPAM filtering / blocking option, analysis indicates that 14% effectively had no controls in place, but there was no discernible correlation to organisation size, budget or industry sector. In absence of evidence to the contrary, it would seem that identification and handling of objectionable material is down to the individual awareness and level of legal understanding of the individual IT staff member.

The vast majority blocked or filtered SPAM at their email server, with a third (37%) blocking at their ISP, and almost all the latter (47 of 55 question responses) did both. Only 1 organisation responded Do not know who provides SPAM Filtering. Only 1% Use email less because of SPAM and other security concerns, which illustrates how necessary email has become to business.

Depending on the readers’ level of cynicism, it might or might not be surprising to read that 13% Complained to the SPAM-mer’s network. Interestingly, half of these were not prepared to cooperate with anti-SPAM researchers. One third of all 2007 respondents were prepared to cooperate with anti-SPAM researchers, which also tends to indicate respondents’ levels of satisfaction with SPAM filtering.

Respondents to the 2007 survey were asked about their understanding of the law regarding objectionable material and also requested to quantify how their organisation handled porn and objectionable material on workplace ICT.

Figure 37 shows results for the question set investigating IT staff awareness of the law regarding objectionable material. Although the percentages were relatively low, some did not recognise sexual exploitation of children, torture or extreme violence, sexual violence or coercion, bestiality, and necrophilia as ob-
jectionable material. Almost half of IT staff questioned were equally unaware of that objectionable (illegal) status applying to both coprophilia and urophilia, and also to representations of a particular class of people as inherently inferior; although this last may be more understandable, as it is a fairly recent innovation to the NZ legal system, and one not without contention.

Results for the question set regarding handling of porn and objectionable material may be seen in Figure 38.

Some 21% did not use any type of blocking / filtering, a third of whom (7%) relied on monitoring and/or logging, and a further 7% relied on trust; i.e. no blocking, filtering, logging or monitoring, but employees signed an objectionable material clause in their ICT use agreement. Of those who had blocking or filtering of some sort, only slightly more than half (57%) were happy with its performance.

It seems that many IT staff are not aware of their legal obligations on discovery of objectionable (and therefore illegal) material on their organisation’s ICT. On discovery of objectionable material, 95% of the 148 respondent organisations dealt with it internally. Less than half (43%) reported to Police, and 7% reported to Internal Affairs.

Only 1% admitted to no further action. Of 17 responses of Other action, 3 would dismiss, 4 said the action taken would depend on the seriousness, including 1 who may report to DIA, 6 said Human Resources investigates and determines whether to report externally, 2 would inform Police if they deemed the activity criminal, 1 may refer after internal investigation and 1 would be handled by internal fraud dept. See Figure 39.

The issue of objectionable material handling raises the question of IT staff policing their organisations’ systems at the juncture with the law of the land. On the one hand, everyone knows that ignorance of the law is no excuse. On the other hand, as cultures merge within national boundaries, statutes often cater for multiple and conflicting cultural sensitivities, and as they attempt to redefine right and wrong, these statutes become increasingly complex.

IT staff are not trained in this area, so it is hardly realistic that they are expected to be aware of, and police, aspects of current statutes pertaining to changing moral issues, which raises the question of what alternatives there are.
Concluding Comments

The author apologises for the delay in publishing this report, which was due to family health. There are a number of issues that require further consideration: The level of investment in IT security, handling of objectionable material, security standard qualification of IT security staff, industry co-operation with anti-SPAM research, infrastructure organisation security levels, prospective staff background checks, and information held on Cellphones / PDAs.

Should you wish to discuss any of these, or to suggest further areas for investigation, please feel free to contact the author.

Acknowledgements

Thanks are due to the following people for their contributions to this report: Paul McKitrick (CCIP), Tony Grasso (Dept of Internal Affairs ANTI-SPAM Unit), John Fenaughty (Netsafe), Jeni Wolfe-Wilson (MoH), Ass Prof Hank Wolfe, and Robert Richardson (CSI).

The invaluable sponsor support from The Centre for Critical Infrastructure Protection (CCIP) and the NZ Internet Task Force, along with support from the Computer Security Institute (CSI), and the NZ Police are also acknowledged. Particular thanks go to all those respondents who took the time to be involved in the 2007 survey.

References
