Author’s note
Now that the first two annual surveys have been published, analysis has begun on the 2007 data. Starting in 2008, NZ surveys and publication will be synchronised with the US and Australian Computer Crime and Security surveys.
Foreword

Today, Information and Communication Technology plays a vital role in all sectors of our modern society. The interconnected and interdependent nature of the Internet forces everyone to trust each other implicitly or explicitly, at least in cyberspace. A cyber security risk accepted by an individual or organisation therefore potentially becomes imposed on all.

Information today is the lifeblood of all our organisations and protecting this information now requires far more attention than in the past. With the increasing availability of on-line services, the reputation of an organisation is reliant upon safeguarding citizens’ personal data and corporately sensitive information, as well as, maintaining business continuity.

Security threats and risks continue to increase and evolve to defeat our best defences. Key cyber threats today include those from foreign intelligence services, organised crime syndicates, political activists, individuals acting alone, botnets and spam. As the tools and techniques of the adversaries improve, so must our ability to detect and deter these threats.

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. On-going cyber security education and awareness initiatives are essential to ensuring that people are sensitised to the threats.

The greatest impediment to effective cyber security is indifference.

Richard Byfield
Managing Director
Centre for Critical Infrastructure Protection
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, Centre for Critical Infrastructure Protection (CCIP), New Zealand Police, and the Computer Security Institute (CSI). This 2006 survey is the second 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 2006 survey results are based on the responses of 113 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 NZ$, roughly equivalent to US$0.70 at time of publication.

It is probable that the lowered response rate to the 2006 survey was due to conducting it in parallel with the 2007 survey in one twelve-month period. This was necessary to bring publication dates in line with those of the US (CSI/FBI) and Australian Computer Crime and Security surveys with work on the 2007 New Zealand survey report already underway.

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

NB References to US figures refer to those from CSI/FBI surveys, while references to Australian figures refer to those of the 2005-2006 AusCERT surveys. In referring to monetary costs, for brevity the word ‘thousand’ is substituted by ‘k’.
Executive Summary

Key Points
IT management practices are found to be inadequate to preserve forensic evidence for successful use in court. See page 17.

Only 22% of NZ respondents reported Unauthorised Use, but the US figure was 52%. See page 9.

Two-thirds of NZ organisations invest less than 5% of their IT budget on security issues. Australian research has found that this is considered insufficient. See page 7.

Although incident number reports appear to be down, this is no reason for complacency. This apparent reduction may be anomalous and unsupported by the 2007 survey findings. Security incidents were experienced by 87% of respondents, and both incident numbers and costs are still concerningly high. These are all clear indicators of the need for vigilance. See page 10.

It is also of concern to note that IT enrolments are down, indicating future shortages of qualified staff, with the consequent increasing impact of cyber attacks, cyber crime and related losses.

Incidents
The prevalence of almost all types of security incidents grew steadily from 1998 to 2005, then appeared to drop in 2006, although this may be due to different respondents than those providing the 1998-2005 historical data gathered in the 2005 survey. See Fig. 14, page 10.

Over 87% of respondents had experienced security incidents in the 2005 calendar year, the most common again being Virus, Laptop/Mobile Hardware Theft, Insider Abuse of Net Access/Email and Music/Movies/Ripping. See Fig. 13, page 10.

The average financial cost of security incidents per organisation in 2006 was around $13k, well down on 2005’s $42k figure, although the change in figures may be due to respondent changes and is no reason to sit back. See Fig. 15, page 11. NB Figures such as incident costs are calculated as averages of respondents’ best guess reported figures.

Most respondents (85%) monitored for Unauthorised Use. Almost a quarter (22%) experienced unauthorised use. Half experienced 1-5 incidents from Outside, with slightly more from Inside, but larger numbers of incidents all came from outside. See page 9.

Respondents who did not report intrusions to law enforcement stated as important reasons: Unaware of law enforcement interest (32%), Negative publicity would hurt stock/image (24%), Civil Remedy seemed the best course (20%) and Competitors would use to their advantage (8%). See Fig. 17, page 12.

In response to incidents/intrusions, 40% reported the incident to management, 30% did their best to patch security holes in network systems. Only 16% reported intrusions to law enforcement. See Fig. 16, pages 11-12.

Budgeting Issues
Regarding percentage of IT budget spent on security, 66% spend up to 5%, now regarded as insufficient, with the NZ figure for organisations spending Over 10% around 5%, compared with the Australian and US figures of 14% and 13% respectively. See Fig. 6, page 7.

Average reported Total Computer Security Investment figures were $155 for Operating Expenditure and $48 for Capital Investment, totalling $203 security investment per employee. See Fig. 7, page 7.

The NZ decline in use of cyber-incident insurance continued in 2006, with use sliding from 31% in 2004 through 20% in 2005 to 16% in 2006, but 29% in 2006 in the US. See Fig. 11, pages 8-9.

More than two thirds of respondents again believed that aspects of security were not appropriately funded. See Fig. 20, page 13.
Policy and Procedure Issues
Security policy is directed from outside NZ for 27% of non-government organisations. See page 7. 63% of respondent organisations indicated they would not employ reformed hackers. See page 11.

Training and Qualifications
Two thirds of respondents again indicated that their organisation 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 Fig. 31, page 19.

The highest rating in Importance of Security Awareness Training was Network Security, with 80% considering it important. The lowest rated was Cryptography on 18%, suggesting that it is still under-recognised in NZ IT security. See Fig. 21, page 14.

Responses indicated that 53% of organisations have no IT staff with any security qualifications, down on 2005’s figure of 62%, and the graph shows that over 76% of organisations have less than 10% of their IT Staff security standard qualified. Larger budget organisations tend to outsource security so there was a marked qualifications drop in the $Over 1 billion category. See Figures 27 and 28, pages 17-18.

Respondents indicated that 4% of Primary IT Security Staff had no qualification of any sort, down 4% from 2005 but having no statistical significance, with 35% having Industry Vendor IT Certification (MCSE, CCNA, etc) and 30% having No formal qualifications but more than 5 years of security experience, well down on the previously reported figure of 51%. Figures ranged down to 8% with Vendor-neutral IT Security Qualifications. See Fig. 27, page 17.

Around 51% of organisations adhere to some form of IT Security Related Standards, two thirds of those using more than one. The most common was AS/NZS ISO/IEC 17799:2001, adhered to by 40%. Other industry-specific IT security standards came next, adhered to by one in three, then Vendor-specific standards or guides, adhered to by one in four. Significant to the forensic readiness issue, no organisation adhered to Australian standard HB 171—2003 Guidelines for the management of IT evidence (available from Standards NZ). See Fig. 26, page 16.

Technologies
The most common security effectiveness evaluation technique was again Email Monitoring Software on 84%, slightly up on the 2005 figure of 79%. Web Activity Monitoring Software was next on 79%, well up on the 2005 figure of 60%. Penetration Testing was employed by 72%. See Fig. 23, page 15.

Over 60% of this year’s respondents use security audits for assessment of system management. In 2005 20% did not report the results to upper management but 2006 respondents indicate this has dropped to 2%. See page 15.

Internal Audits were reported as being conducted by 64% of respondents, up 4% from 2005, with 53% conducting External Security Audits, down 10% from 2005. Automated Tools To Check Configuration Of Network Systems was up 11% to 46%. Only 3% used no security techniques. See Fig. 23, page 15.

Management Issues
Over two thirds of respondents conducted some cost-benefit analysis on security expenditure, a huge increase on the 2005 figure of one quarter. See Fig. 8, page 8.

79% had a Business Continuity Plan, up 4% from 2005. Information Strategic Plans were on 74%, down from 81%, and an Information Security Strategy on 58%, up from 50%. Risk Management Strategy was less popular on 43%, with both Incident Response Plan and Use of Information Management Standards on 42%. See Fig. 32, page 19.

Few prosecutions are brought, with even fewer convictions. See page 12.
DETAILED SURVEY RESULTS

About the Respondents

Respondents were the same set of 500 as used for the 2005 survey, 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.

Unfortunately, due to time and budget constraints this year, very few respondents were contacted by telephone and as a result, responses dropped to 22%, although this is still considerably above average in surveys of IT management.

Figures 1 through 5 summarise information about the organisations that responded to the 2006 survey and the individuals representing those organisations. As with the US (CSI/FBI) survey, the 2006 survey was anonymous, removing the possibility of direct longitudinal study of data. However, with subsequent surveys it should be possible to draw reasonable conclusions as to trends over three years.

Figure 1 shows the figures for respondents by industry sector. Manufacturing was the dominant sector at 17% of respondents, with National and Local Government representing 15% and 13% of respondents respectively.

Once again, none of the top 500 organisations by turnover were identified as Legal, maybe in part due to the difference between the NZ provision of the Accident Compensation Corporation national accident health insurance, and the US health insurance system.

Organisational size as measured by number of employees can be seen below in Figure 2. Once again, with a total population of just over four million, NZ may not have been expected to be well represented in the higher employee-number organisations but 1000 and Over employees accounted for 15% of respondents, with 18% having 500-999 employees. In the lower range, around 22% of respondents employed fewer than 100 people.
As can be seen above in Figure 3, organisations with revenue generation in excess of $100 million comprised 38% of respondents. This is lower than the 57% 2006 US survey figure but similar to the 36% Australian figure, which was well down on their 2005 figure of 66%.

Note that due to rounding, figures in some graph do not sum to 100%.

On the surface, NZ’s 38% may be considered high for a nation of somewhat over four million, but the growing proportion of organisations in overseas ownership through the process of internationalisation may be responsible for this.

Areas of Operation results can be seen in Figure 4. Each percentage indicates the fraction of respondents that operate in that particular region, so a figure of 100% indicates that all respondents operate in that region.

Of the nine organisations that operate only in NZ and one other geographical region, it was not surprising that five identified Australia as their other area of operation. As with 2005 proportions, four of the five were NZ rather than Australian based.

Results for Respondents by Job Title can be seen in Figure 5. Of 110 respondents to this question, over half (60%) were the IT Manager of their organisation, with other titles occurring much less often.

As in 2005, respondents were selected specifically as the person responsible for IT Security in their organisation, so the prevalence of non-security-related job-titles should not be taken to indicate that the majority of organisa-
Budgeting Issues

Figure 6 shows Percentage of IT Budget Spent on Security, with the NZ up-to-5% figure being higher than those in both the US and Australia.\(^1\), pp.5-7, 2, p.13

Around 66% of NZ organisations invest up to 5% of their IT budget on security, compared to the Australian 43% and US 55% figures. On the surface this sounds encouraging, but this category includes those with zero or minimal investment, and as found in the 2006 Australian report, 51% of respondents considered under 5% to be inadequate.\(^1\), pp.5-7, 2, p.13

A further 16% of NZ respondents indicated they spent between 5 and 10% of their IT budget on security issues, not comparing well with 21% of respondents in the US and 23% in Australia. Only 5% of NZ organisations spent more than 10% on security, compared with 13% in the US and 14% in Australia.\(^1\), pp.5-7, 2, p.13

Around 14% of NZ respondents did not know the percentage of their IT budget allocated to security.

Excluding governmental responses, this year slightly more than one-in-four organisations (27%) indicated that their computer security was dictated from outside NZ. Overseas ownership is a mixed blessing, with the advantage of access to technology and markets offset by the disadvantage of profits leaving the local organisation, not to mention the NZ economy.

Figure 7 shows the Estimated Average Total Computer Security Investment Per Employee sorted by revenue. All figures were considerably lower than in 2005, but these differences are not statistically significant and are probably due to a drop in responses from running the 2006 and 2007 surveys in a single calendar year to bring NZ publication dates in line with the US and Australian surveys.

The reported security expenditure per employee shows very similar averages across most budget categories, between $116 and $141. Two statistical anomalies showed up due to low 2006 responses, with the Under $1 million revenue category not reporting any Capital Investment and one respondent reporting very high Operating Expenditure in the Over $1 billion budget category, pushing the category average to $485. Overall, the average Total Computer Security Investment figures were $155 for Operating Expenditure and $48 for Capital Investment, totalling an overall average security investment per employee of $203.
Organisations were again asked to indicate their use of cost/benefit metrics in planning computer security spending. Respondents’ use of Return on Investment (ROI), Net Present Value (NPV) Internal Rate of Return (IRR) or Other metrics can be seen in Figure 8. Use of IRR and NPV dropped this year in comparison to ROI.

Over two-thirds (70%) of respondents conducted some cost-benefit analysis on security expenditure, a huge increase on 2005’s figure of one quarter. Once again, many of this question’s 79 respondents used more than one metric. Note that metrics were assessed separately so the figures do not sum to 100.

Outsourcing of IT is a growing phenomenon, yet when uncritically viewed, the security function appears to buck the trend. Proportions in 2006 are similar to 2005, with Figure 9 showing less than 10% of the 2006 respondents outsourcing over 80% of their security function, while half outsource none.

Figure 10 reveals the relationship between organisation size and the percentage of security function they outsource. The NZ trend is for larger organisations to outsource more. US results show the same picture, with the average ranging from 8-15%, depending on budget size.1, p.9

External cyber-security risk insurance is another tool in managing security, with the number of 2006 NZ respondents having such insurance down from the 2005 figure, which was also down on 2004. The 2006 US figure was 29%, where the trend is uncertain, although use may be on the rise.1, pp.9-11
As Figure 11 shows, the NZ decline in use of cyber-incident insurance continued in 2006, with use sliding from 31% in 2004 through 20% in 2005 to 16% in 2006. Just on 55% of 2006 respondent organisations had no cyber-incident insurance, compared to 43% in 2005 and 40% in 2004.

In 2004, 24% responded that they did not know whether they had insurance, whereas the 34% figure from 2005 was repeated in 2006. As IT managers are more likely to deal with cyber-incident insurance than security technicians, it is worth reiterating here that the 2004 SRG survey was impersonally addressed to The IT Manager of each organisation, whereas in subsequent surveys the person specifically responsible for IT security in their organisation was identified and contacted personally to request their involvement with the project.

**Frequency, Nature and Cost of Cyber Security Breaches**

In 2005, the level of monitoring of unauthorised computer system use was unknown, so the 2006 survey explored this, with 85% of this year’s respondents indicating that their organisation did monitor unauthorised use.

As in 2005, around a quarter (22%) experienced unauthorised use of their systems, with 70% of these experiencing 1-5 incidents, 4% 6-10 incidents, 9% more than 10, and 17% unable to specify numbers.

Incidents originating inside the organisation outnumbered those from outside, with around 45% experiencing 1-5 incidents from Outside, and 63% experiencing 1-5 incidents from Inside. Although there were no reports of More than 5 incidents from inside, 5% of respondents reported More than 5 incidents from outside, and 5% reported More than 10.

The percentage of respondents’ organisations experiencing Unauthorised Computer Use can be seen in Figure 12. Levels were lower than in the US but ratios remained consistent.

It is interesting that the 22% 2006 NZ figure is considerably lower than the 52% 2006 US figure. This may be attributable to monitoring and management, but is more likely to be simply a reflection of the high NZ incidence of computers and Internet access per head of population outside the work environment. People are less likely to risk being caught misusing computer systems at work when they have risk-free home access to computers and the Internet.
On the other hand, the 2006 percentage of NZ organisations experiencing *No Unauthorised Use* was 68%, compared with 38% in the US.\(^1\)\(^{11}\) The 9% 2006 NZ figure for *Unknown* was similar to 2005’s 10%, and the same as the US figure.\(^1\)\(^{12-13}\)

Figure 13 shows percentages of respondents experiencing security incidents. Over 87% of organisations indicated that they had experienced some type of security incident, with the most common incident types being the same as in 2005. It can be seen that the leading incident types were once again *Virus, Laptop/Mobile Hardware Theft, Insider Abuse of Net Access/Email* and *Music/Movies/Ripping*.

One of the 2005 survey questions requested historical data on incident numbers. The 2005 calendar year data show a reversal in the previous upward trend in incident numbers in half the categories. Figure 14 shows steady, and in some cases accelerating growth from 1998-2004, then some marked reductions in the 2005 calendar year. This may be a data anomaly from a few high figures in the historical 1998-2004 data, with the 2005 data showing evidence of coming from different respondents. The 2007 survey will soon reveal how much of this apparent reversal in trend is actual and how much is due to respondent variations.

On a similar theme, *Virus* numbers grew from 2,341 in 1998 to 15,940 in 2004, but plummeted to 115 in 2005. This may to some extent be due to possibly anomalous high figures provided by one 2005 respondent, which strongly influenced the historical 1998-2004 data. Once again, the 2007 data will reveal more.

Figure 15 shows the average cost to the organisation by incident type. To ensure consistency in responses, category terms were defined and described in a four-page glossary of terms attached to the survey form.

*System Penetration* led average costs by a considerable margin at $12.5k, with *Financial Fraud* second at $9k. *Music/Movies/Ripping* was third on $6.7k. *Denial of Service* was next on $5.4k, slightly up on 2005. Then came *Misuse of Public Web Application* on an average of $2.5k, *IP Theft* (averaging around $2.2k) and *Abuse of Wireless Network* (1.6k).

Figures decreased steadily from *Insider Abuse of Net Access or Email* ($600), through *Telecommunications Fraud* ($400), *Laptop or Mobile Hardware Theft* ($300), *Website Defacement* ($300), *Virus* ($200), *Unauthorised Access to Information* ($30) and *Sabotage* (no cost).
The total cost of these incidents to the 63 respondents was over $1.8 million, with *System Penetration* ($12.5k), *Financial Fraud* ($9k), and *Music/Movies/Ripping* ($6.7k) making up over half of that total cost. The average cost per incident was just on $3k, well down on 2005’s $42k figure, but once again this may be due to the difference in respondents. The 2007 survey report due out later this year will reveal more on this issue.

In the 2005 report, despite two organisations identifying *Website Defacement* as having occurred in their organisation, there were no responses regarding the financial cost of these incidents to the organisation.

The 2006 survey saw the same number of affirmative responses to *Website Defacement* as last year and the 2005 data fits with the 1998-2004 data set, suggesting costs were likely to have been similar. 2007 data will show more.

The 2006 respondents indicated the cost per organisation of website defacement to be around $500. Although it is possible that these data come from the same respondents as in 2005, they seem much more likely to come from different organisations. As all of the historical 1998-2004 data set was gathered from only 21 organisations of the 218 responses in 2005, trend analysis will be more robust once the 2007 survey data are added.

It seems that once again two thirds of NZ respondents would not consider employing reformed hackers to test security of their systems, with 63% indicating that they would not do so. 22% were unsure, with only 15% of the 110 respondents indicating that they might do so. The 2006 US figure was also overwhelmingly against at 86%.

### Incidents and the Law

Organisations were questioned regarding actions taken after incidents/intrusions. The results can be seen in Figure 16. Note that respondents checked all relevant categories; therefore percentages do not add to 100.

Overall, the most common response this year was *Patched Security Holes* (88%). *Did Not Report Outside Organisation* was second (52%). *Reported to Police* stood at 12%, with *Reported to Legal Counsel* the lowest on 4%.

As would be expected, certain types of incidents evoke specific reactions, with the main response to *Denial of Service*, *Unauthorised Use* and *Virus* incidents being to *Patch the System*, with only four *Unauthorised Use* and one *Virus* incident reported to law enforcement.
In contrast, almost all reported cases of Financial Fraud, Espionage, Corruption and of course Hardware Theft were reported to both management and Police. Interestingly, although Telecommunications Fraud, ID Theft, Proprietary Rights Infringement, Theft of Information, Product Piracy, Extortion or Sabotage were sometimes reported to management, almost no instances were reported to Police.

2005’s Theft Hardware/Assets was the standout figure in incidents reported to law enforcement, with 41% of respondents doing so, compared with 17% of incidents reported overall. The two extra categories added for 2006 made it unrealistic to directly compare the 2005 and 2006 data, but 32% of all incidents reported by 2006 respondents were reported to Police as opposed to 16% in 2005.

This apparent increase may be partly due to the change in respondents from 2005, so the 2007 and 2008 surveys will reveal more.

In 2005 it was found that despite their desire to discourage felony, organisations are more interested in pursuing their core business than assisting law enforcement in prosecuting offenders. Police, on the other hand, point out that they can do nothing about unreported crimes.

As with 2005, the highest Did Not Report figure was for Computer Virus, followed by Denial of Service, but as noted earlier, some instances of Telecommunication / Toll Fraud and surprisingly quite a number of Hardware Thefts were not reported either.

The importance of reasons why intrusions were not reported to law enforcement can be seen in Figure 17. Categories were considered separately so percentages do not add to 100. Many incidents were not reported to anyone outside the organisation. The reason most often given was Unaware Law Enforcement Interested on 32%. Other considerations were also important to 20% of respondents. Interestingly, category order is reversed from the 2005 report.

Figure 18 shows the number of prosecutions and convictions relating to reported incidents. It can be seen that few prosecutions are brought, with even fewer convictions. Despite the historical lesson that for justice to work in society, it must not only be done but be seen to be done, it may be that organisations found prosecutions not worth the investment and therefore opted not to pursue. Although all figures rose slightly in the 2005 calendar year, this may be due to different respondents.
Security Audits and Security Awareness Training

Over 60% of this year’s respondents use security audits for assessment of system management. Note that audit results may be reported to more than one area, so the percentages do not sum to 100. As shown in Figure 19, 32% of respondents report audit results to the Chief Information Officer, and 28% to the Chief Executive Officer.

In 2005 the overall security audit use figure was over 80%, yet 20% of those conducting security audits did not report the results to upper management. This year that 20% dropped to 2%.

Around one in five responses indicated that the results were reported to alternative upper management or extra-organisational authorities. Among these were: Overseas Corporate Parent, Senior Management Group, Auditors, HR Manager, Executive Steering Group for Information Management, COO, Security Committee, External Auditors, General Manager, CTO, Country Coordinating Committee, International Parent Company, Worldwide Corporate Audit (USA), Senior Management and Overseas Parent, Audit NZ, and five responses of IT Committee.

Manager / Staff / Committee.

From these and other data, it is inferred that around a quarter of this year’s respondent organisations are in overseas ownership or control.

Security is holistic, working only as well as the weakest link in the chain. Technological solutions can go only so far without general staff awareness. Some security solutions or components may be funded under other broader groups of funding not identified as separate security funding, but two thirds of 2006 respondents believed that aspects of security were not appropriately funded.

Attitudes to security awareness training for staff also showed it was viewed as worthwhile by NZ organisations. Respondents were asked whether they agreed with the statement My Organisation Invests Appropriately in Security Awareness Training. Overall, 26% agreed, 56% disagreed, down 1% from 57% in 2005, with 18% undecided.

Broken down by sector, 2006 data shows the majority of sectors disagreeing. The only sectors agreeing were again Telecommunications, this year very minimally represented by just one respondent, and Utilities with three respondents agreeing and four disagreeing. See Figure 20.
Respondents predominantly rated the same security awareness training areas as important. Figure 21, shows the figures, which are almost identical to those in the 2005 report. The highest rating was for Network Security, with four out of five respondents considering it important. Three quarters of respondents perceived Security Policy as important, with Access Control Systems and Security Management important to two out of three. Security Systems Architecture was important to three out of five respondents. At the lower end of importance perceptions were Economic Aspects of Computer Security (e.g. Budgeting), Investigations and Legal Issues, and the lowest rating Cryptography, down 3% from 2005 to 18% in 2006.

As pointed out in the 2005 report, 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 2004 to 34% in 2006. Some forms of encryption are reported as being well utilised here, so it may be that some NZ respondents did not link the term cryptography with the forms of encryption they have in use. Subsequent NZ surveys will use both terms to avoid confusion.

Security Technologies

Security technologies used within 2006 respondents’ organisations are shown in Figure 22. As with the 2005 survey, categories incorporated, but were not limited to, those used in the US (CSI/FBI) survey.

With regard to network defence technologies, 99% used Anti-Virus Software, 96% implemented Firewalls and 58% implemented Intrusion Detection Systems (IDS) on their systems (still down on the US figure of 69%).

Server Based Access Management was set up by three quarters of respondents, as opposed to only half of 2005 respondents. Encryption was again considered in three separate categories as Encrypted Data Files, Virtual Private Network and Public Key Infrastructure (see Figure 22). Reusable Passwords were implemented by 29% of respondents and Smart Cards by 24%, with Biometrics used by only 1% this year, the same as 2004, but 9% in 2005.

In terms of changes over a 5% threshold from 2005 to 2006, VoIP dropped 7% to 23%, and PKI returned to the 13% 2004 figure. Reusable Password use also dropped 9%, while VPN dropped 7% to the 2004 figure. Remote Access also went down 7% to 88%.
Encrypted Data Files plummeted 19% to 8%, and Intrusion Detection rose back to 58%. Some of this variation is undoubtedly due to differing sources, so addition of the 2007 data will enable a somewhat clearer analysis.

Popularity of Information Security-Effectiveness Evaluation-Techniques can be seen in Figure 23. Overall proportions and positions remained similar to 2005. The most commonly used technique was again Email Monitoring Software with 84% of respondents deploying it, slightly up on the 2005 figure of 79%. Web Activity Monitoring Software was next most common on 79%, up on the 2005 figure of 70%.

Penetration Testing was employed by 72% of respondents, although this year the previous single category was split into Internal Testing (28%) and External Testing (44%). The combined figure is well up on 2005’s 46%.

Internal Audits were conducted by 64% of respondents, up 4% from 2005, with 53% conducting External Security Audits, down 10% from 2005. Automated Tools To Check Configuration Of Network Systems was up 11 to 46%.

Other techniques were used by 4% of respondents. Once again, some used a minimal set of these techniques, but 3% of respondents reported that they employed none.

Attackers constantly seek flaws in operating systems (OS) to enable their attacks, so operating systems are constantly in need of updating. System managers must choose the best time for their organisation to perform the next upgrade or even make the expensive and labour-intensive move to a new operating system.

The SRG survey has been recording numbers of Workstation Operating Systems for over a decade, watching new operating systems gradually take up the majority of the market once past the ‘beta’ teething stage. As they approach the replacement stage of the operating system lifecycle, they decrease in number as replacement occurs.

Timing an upgrade is crucial. In considering both risk and investment value, a balance must be struck between danger from as yet undiscovered O/S flaws that allow compromise of networks, and getting the best investment return for the organisation. The intention is for these figures to afford respondents improved information for that timing.

The 2006 results can be seen in Figure 24. Unsurprisingly, the most common workstation operating system category was Windows (2000/XP) accounting for over 86% of
all respondents’ systems, with other Windows versions all dropping correspondingly. Mac came a distant second on 5%, dropping back down 2%, with Linux/Unix on 2%, and Other operating systems not even registering. It is expected that Windows Vista will begin to erode 2000/XP’s dominance in 2008, but the cost of hardware upgrades needed to run the new OS may slow its uptake.

### IT Standards, Policies and Procedures

To quote security consultant Charles Cresson Wood, “Just as it is unthinkable that millions of automobile drivers would be on the road without laws about the right of way, it is also unthinkable that millions of business people would operate systems without information security policies.”

Figure 25 shows Use of Computer Security Policies and/or Procedures. Both User Access Management (enforcement of password use, user privileges, etc) and Media Back-Up were implemented Following were External Network Access Control on 80%, and Documented Standard Operating Procedures on 76%. Other forms of policies and/or procedures accounted for 2% of respondents, with only 3% having a Forensic Plan. The relevance of this last figure can be seen when examining this year’s results regarding Forensic Readiness.

Three questions were asked to investigate forensic readiness. Note that a graph was not included on this subject. Despite 5% of respondents employing staff with forensic experience and/or training, and 24% of respondents contracting in a forensics professional, current levels of internal policy and procedures, management planning for forensic investigation, and management of forensic training were found to be woefully short of ensuring admissibility of forensic evidence in court. Only one in five 2006 respondents had prepared forensic evidence for court.

Only 7% of 2006 respondents had a forensically trained first responder. It has been well stated that this person is the key IT staff member who enhances the likelihood of successful prosecution.

These figures, coupled with the forensic readiness finding, predict a rise in failed prosecutions.

Slightly over half of respondent organisations (51%) adhere to some form of IT Security Related Standards, two thirds of those using more than one. See Figure 26.
The adherence figure is up from the 38% reported in 2005, and closer to the 47% figure in Australia. Interestingly, while NZ adherence has risen, in Australia it declined.

The most common IT Security-Related Standard in use 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 40% of respondents.

Next most common were Other industry-specific IT security standards, adhered to by one in three respondents. Vendor-specific standards or guides were next most popular, adhered to by one in four 2006 respondents.

At the lower end of the usage scale, both ACSI 33 – Australian Communications – Electronic Security Instructions 33 and ISO/IEC 14516 Information Technology - Guidelines on the use and management of trusted third parties’ services had only 4% adherence, and no respondents adhered to RFC2196 Site Security Handbook.

Although an Australian standard, it is significant to the forensic readiness issue discussed earlier, that neither did any organisation adhere to AS HB 171—2003 Guidelines for the management of IT evidence.

Information Security Training, Qualifications and Certification

The 2006 survey received 108 responses regarding IT Staff Security Qualifications and / or Training. Results can be seen in Figure 27. Respondents this year indicated that only 4% had no qualification of any sort, down 4% from 2005, which, although without statistical significance, is encouraging.

Looking at the detail, 35% responded as having Industry Vendor IT Certification (MCSE, CCNA, etc), also down from the 52% 2005 figure. Second most common was No formal qualifications but more than 5 years of security experience on 30%, well down on the previous report’s figure of 51%. Will the 2007 figures see this confirmed as a trend?

Just over 27% employed staff with Tertiary IT Qualifications, down from 37% in 2005, and 24% had staff who had been on Ad Hoc IT Security Training Courses, well down from 41% in 2005. Next came the 19% of respondents having staff with Industry Vendor IT Security Certification (Cisco etc), down from 38% in 2005, then Vendor-neutral IT security certification on 8%, also down from 12%.
The 2006 survey continued following a line of enquiry suggested by the Australian Computer Crime and Security Survey regarding security standards qualifications of IT security staff. Once again, less than half of NZ IT security staff are security standard qualified.

It can be seen in Figure 28 (p17), that just over 53% of NZ IT security staff have no security standard qualifications, but this tally is down on 2005’s figure of 62%. 2007 survey results will clarify whether this apparent drop is actual or a statistical data anomaly.

Another quarter of organisations had under 10% of IT security staff with security standard qualifications, leaving less than a quarter of organisations with more than 10% of their IT security staff security standard qualified.

In 2005, greater qualification levels seemed to be associated with larger budgets, but this seemed to drop off at a certain point. With response levels down this year, the figures are uncertain, but in general the same is true.

Figure 29 shows this general increasing trend dropping off in the upper mid range of organisational budgets. Dips were noted in 2005 in the $10 to $99 million and Over $1 billion categories but the deviations had no statistical significance given the sample size.

Due to the reduced response rate to the 2006 survey, the statistical significance problem remains this year, but the larger budget organisations tend to outsource their security function and to consequently employ fewer security staff. Hence, the conclusion that budget is linked with the level of IT security staff qualification is bolstered by noting that larger budgets tend to outsource more security function.

Results for IT staff with security standard qualifications organised by industry sector can be seen in Figure 30. When IT staff by security standard figures are broken down by industry sector, there is no discernable pattern, apart from the obvious conclusion that telecommunications is the clear leader on 33% of IT staff with security standard qualifications, the same figure as in 2005, but this may be at least partially due to the temporarily reduced response rate, comprised of only a single organisation in this category.

The National Government category is in second place on 19% after a marked jump from 7% in 2005. How much of this reported figure is an actual increase and how much is due to the change in respondents from IT managers to security staff remains to be seen, with the 2007 data expected to make this clearer.
The 2006 respondents did not appear to be any more satisfied with the management of IT security than did the 2005 respondents (see Figure 31). Only five respondents did not express an opinion on this. Two-thirds believed that their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness in IT Staff (64%), Management (66%) and General Staff (59%). Note that numbers do not total to 100 due to rounding.

The use of governance and or risk management tools was again looked at and results can be seen in Figure 32. All figures are expressed as percentages of the total number of respondents using governance and/or risk management tools.

Despite two new categories being added in 2006, comparisons with 2005 are generally possible. Business Continuity Plans were most common, rising 4% from 2005 to 79%. Information Strategic Plans were almost as popular on 74%, down 7%, with an Information Security Strategy held by 58% of respondents, up 28% from 50%. Risk Management Strategy was less common on 43%, with existence of both Incident Response Plan and Use of Information Management Standards least common, each having 42% of respondents using them.

Adherence to these existing governance and risk management strategies and methods was less common however, with only 46% of respondents actually adhering to their Business Continuity Plan, up 6% from 2005, with Information Strategic Plans faring slightly better on 49% adherence. Information Security Strategy was up 10% with adherence at 39% and Use of Information Management Standards was down 1% on 26%, with Risk Management Strategy (up 3%) and Incident Response Plan (up 5%) both on 28%.

The 2005 Regularly Reviewed category was split into Internally and Externally for 2006. It was not therefore possible to directly compare the 2005 Review category but in general, Regularly Reviewed was up, as with all other figures. It remains to be seen whether the 2007 report figures will show this apparent rise in usage of these tools as continuing.

Formal monitoring of governance / risk management tools was a mixed bag, with figures similar to 2005, but generally up slightly.

The new Reported to Senior Management category results were similar to those for monitoring, as seen in Figure 32.
Concluding Comments

With fewer and differing respondents from the first Computer Crime and Security Survey in 2005, the 2006 data produced some surprises along with the expected results.

The majority of organisations had technologies in place to secure their organisations, but 53% had no IT Staff with security qualifications, and less than a quarter of respondent organisations had more than 10% of their IT security staff security standard qualified.

Despite security being an integral part of operating a business, as in the 2005 report, two thirds of respondents believed aspects of security were inappropriately funded.

Once again, over 87% of organisations indicated that they had experienced some form of security incident but most were not reported. Many stated that they were not aware of police interest.

The percentages of NZ IT budget spent on security are similar to those of Australia and the US up to the Over 10% range, at which point the NZ figure drops dramatically. It is possible that larger multinational organisations’ outsourced IT security is part of centralised operational funding; hence costs would not appear in the NZ budget figures.

As is currently the case in NZ, the 2006 Australian survey found that substantial drops in University IT enrolments threaten to exacerbate the shortage of qualified IT staff, and especially security practitioners. This in turn will increase the impact of cyber attacks, cyber crime and related losses.

KEY FINDINGS

Some of the key findings from the 2006 survey are summarised below:

Forensic Readiness appears poised to become an issue, with the vast majority of organisations unprepared for preservation of forensic evidence for admission in court.

Only 22% of NZ respondents reported Unauthorised Use, with the US figure being 52%.

Two-thirds of NZ organisations invest less than 5% of their IT budget on security issues. Australian research has found that this is considered insufficient.

Although incident number reports appear to be down, this may be a statistical anomaly. Over 87% experienced security incidents, with incident numbers and costs both still concerningly high.

Few report intrusions outside the organisation. The most common reported reason was Unaware Law Enforcement Interested. Of incidents reported to Police, 24% resulted in prosecutions and 18% in convictions.

Respondents with external insurance for cyber-security incidents dropped to 16%, compared with 29% in the US, where use may be rising.

2006 once again saw half of organisations outsourcing none of the security function. Larger budget organisations appear to outsource more.

Over two thirds conducted some cost-benefit analysis on security expenditure, a huge increase on 2005. Many used more than one metric, with ROI used by 33%, well ahead of NPV and IRR.

Two thirds of respondents again indicated that their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness.

Average Security Expenditure figures were $155 for Operating Expenditure and $48 for Capital Investment, totalling $203 per employee.

Security Awareness Training was considered important in Network Security by 80% of respondents. Three quarters thought it was important in Security Policy, and two-thirds in both Access Control Systems and Security Management. Cryptography was down 3% from 2005 to 18% in 2006, while ratings rose in the US, suggesting that it is an under-recognised tool in New Zealand.
Anti-virus was implemented by 99% of respondents, 96% had firewalls, and 58% had Intrusion Detection.

Training/Qualifications of Primary IT Security Staff ranged from 35% with Industry Vendor IT Certifications and 30% with No Formal Qualifications but Over 5 yrs Security Experience, down to 8% holding Vendor-neutral IT security certifications, with 3% having Other qualifications.

Security Standards were adhered to by 51% of organisations, up from 38% in 2005. Over half of organisations had no security qualified IT staff, and three quarters had less than 10% of their IT Staff security qualified.

Win2k/XP accounted for 86% of workstation O/S, with Mac on 5% and Linux on 2%.

Security audits were conducted by 62% with only 2% not reporting the results to upper management. 34% conducted no security audit.

It is of concern to note that IT enrolments are down, indicating future shortages of qualified staff, with the consequent increasing impact of cyber attacks, cyber crime and related losses.

Acknowledgements

Thanks are due to the following people for their contributions to this report: Hank Wolfe, Nigel Stanger, Melanie Middlemiss, Jeni Wolfe-Wilson and Craig Hallam (MoH), Nick Lavery (NZCERT), Chris Roberts (SSC), and Robert Richardson (CSI).

The invaluable sponsor support from The Centre for Critical Infrastructure Protection (CCIP), the Computer Security Institute (CSI), and the NZ Police is also acknowledged. Particular thanks go to all those respondents who took the time to be involved in the 2006 data-gathering exercise. Please join us for the next survey and the continuing journey.

References
