FIRST ANNUAL

2005

NEW ZEALAND
COMPUTER CRIME
AND SECURITY SURVEY

With the cooperation of:

[Logos of various organizations]

Alpha Omega Group
Publications
2005

NEW ZEALAND

COMPUTER CRIME AND SECURITY SURVEY

by KJ Spike Quinn

Introduction

The New Zealand Computer Crime and Security Survey is conducted by the Security Research Group (SRG) of the University of Otago, in partnership with the Computer Security Institute (CSI), New Zealand’s Centre for Critical Infrastructure Protection (CCIP), and the New Zealand Police. This 2005 survey is the inaugural annual survey and is based on the CSI/FBI Computer Crime and Security Survey. The CSI/FBI Survey is 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 2005 survey results are based on the responses of 218 computer security practitioners in New Zealand (NZ) manufacturing, governmental, financial and medical organisations, and tertiary education providers regarding the 2004 calendar year. All monetary figures are in NZ$, roughly equivalent to US$0.5.

Four questions in the 2005 survey address issues considered in a previous 2004 SRG survey, allowing some discussion of trends. Most, however, have not been addressed in New Zealand before so trend analysis awaits subsequent survey results. The trends considered in this survey are:

- Prevalence of security incidents
- Percentage of the Information Technology (IT) department budget spent on security issues
- Use of cyber-security incident insurance
- Use of Intruder Detection Systems (IDS) technology
- Popularity of common workstation operating systems (OS)
Executive Summary

Incidents
The numbers of almost all types of security incidents have grown steadily from 1998 to 2004. Virus numbers in particular have grown almost exponentially. See Figure 16, page 10.

Over 87% of organisations indicated that they had experienced some form of security incident, with Virus Contamination, Laptop/Mobile Hardware Theft, Insider Abuse of Net Access/Email, and Music/Movies/Ripping the most common. The average financial cost of security incidents per organisation in 2004 was over $42,000. See Figures 17 & 18, page 11.

Almost half of respondents did not report intrusions to anyone outside the organisation. Respondents who did not report intrusions to law enforcement rated as important reasons: Competitors would use to their advantage (78%), Civil Remedy seemed the best course (65%), Negative publicity would hurt stock/image (60%), and Unaware of law enforcement interest (58%). See Figure 20, page 12.

A quarter of organisations had experienced unauthorised use of computer systems in the last 12 months, with most experiencing few incidents, but many unable to specify the number of incidents. External incidents are almost as common as internal. See page 10.

In response to incidents/intrusions, 86% did their best to patch security holes in network systems and 46% did not report the intrusion(s) outside the organisation. Only 15% reported intrusions to law enforcement. See Figure 19, page 12.

Budgeting Issues
The NZ figures for percentage of IT budget spent on security are similar to those of Australia and the US for categories below 10%. In the Over 10% category, the NZ figure was 3% of respondents, compared with Australia on 8% and the US on 14%. See Figure 6, page 7.

Average figures for security investment were just under NZ95,000 for Capital Investment and just under $80,000 for Operating Expenditure, with the maximum figures being $3 million and $2 million respectively.

The proportion of respondents with external insurance for cyber-security incidents was 20%, compared with 25% in the US. See Figures 7-9, pages 6 & 7.

More than two thirds of respondents believed that aspects of security were not appropriately funded. See page 18.

Policy & Procedure Issues
Security policy is directed from outside NZ for 1 in 4 non-governmental organisations. See page 6.

Over 65% of respondents indicated that their organisation would not employ reformed hackers. Only 22% would. See page 11.

Training and Qualifications
A total of 63% of respondents indicated that their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness for both General Staff and IT Security Staff and 70% indicated that to also be the case for Management. See Figure 32, page 18.

When considering the Importance of Security Awareness Training, the highest figure was for Network Security, with 80% rating it as important. At the lower end of the importance perceptions was Cryptography on 21%. This low perceived importance rating suggests that it is an under-recognised tool in NZ IT security. See Figure 23, page 14.
Responses indicated that 62% of organisations have no IT staff with any security qualifications, and over 80% of organisations have less than 10% of their IT Staff security qualified. When broken down by organisational activity, Telecommunications had almost double the security-standard qualified staff of most other sectors, which had between 5% and 18% of staff qualified. See Figures 29-31, page 17.

Training/Qualifications of Primary IT Security Staff ranged from 52% holding either Industry Vendor IT Cert. (MCSE, CCNA, etc) or No Formal Qualifications but Over 5 yrs Security Experience, down to just on 12% with Vendor-neutral qualifications. Of 205 responses, only around 8% checked None of the above, with 2% responding that they had Other training/qualifications. See Figure 28, page 16.

Security Standards were adhered to by 38% of respondents. Most popular security standards are AS/NZS ISO/IEC17799:2001 (AS/NZS4444.1), adhered to by 31% of respondents, Other Industry Specific IT Security Standards, adhered to by 25% of respondents, and Vendor-Specific Standards or Guides, adhered to by 15% of respondents. At the lower end of the scale, no respondents adhered to either ISO/IEC 14516 Information Technology or HB 171 2003 IT Evidence Management Guidelines. Adherence to other standards ranged between 2 and 10%. See Figure 27, page 16.

Technologies
The most commonly used Information Security Effectiveness Evaluation Techniques were Email Monitoring Software (79%) and Web Activity Monitoring Software (69%). Only 5% used no effectiveness evaluation techniques. See Figure 24, page 14.

Security audits were conducted by 79% of respondents’ organisations but 20% of those did not report the results to upper management. Internal security audits were conducted by 60% of respondents, and 63% of respondents conducted security audits via an external organisation. Only 5% conducted no security evaluation. See Figure 21, page 13.

Management Issues
Over 81% had an Information Strategic Plan, 75% had a Business Continuity Plan, 50% had an Information Security Strategy, and 49% had a Risk Management Strategy. Adherence to and formal monitoring or regular review of these risk management tools were considerably less common. See Figure 14, page 9.

Respondents indicate that failed convictions total almost half the reported incident figures. See Table 1, page 13.

Concluding Comments
Two thirds of respondents believed aspects of security were inappropriately funded.

The majority of organisations had security technologies in place, but 62% had no IT Staff with security qualifications. One third used security standards, half the Australian figure [2, p.12]. Although the majority of organisations experienced security incidents, most incidents were not reported, yet numbers of security incidents continue to grow and failed convictions total almost half the reported incident figures. Governance and risk management plans exist, yet many are not reviewed.

Author’s note
The inaugural annual survey has taken considerable effort to arrange, manage and compile. With the benefit of this experience, it is intended to synchronise publication of the 2008 and subsequent surveys with the CSI and AusCERT surveys.
DETAILED SURVEY RESULTS

About the Respondents
Respondents were drawn from a total of 550 organisations and two sources, with four additional IT services organisations replying on behalf of some organisations. The two sources were: 1. The top 500 organisations by turnover; 2. national and local government organisations. All 550 were individually contacted by telephone as the person responsible for IT security in their organisation. Of those 550, some were deemed inappropriate due to outsourcing all computing services, and 6 declined to take part. The final list was reduced to 500 by removing the smaller organisations.

Although all 500 agreed to take part in the survey, only 218 actually responded. Figures 1 through 5 summarise information about the organisations that responded to the 2005 survey and the individuals representing those organisations. As with the CSI/FBI survey, the New Zealand survey is 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.

Figure 1 (at left) shows the figures for respondents by industry sector. Manufacturing was the dominant sector at 17% of respondents, with national and local government each representing 12% of respondents.

Interestingly, none of the top 500 organisations by turnover were identified as Legal. This may be due in some measure to the difference between the New Zealand provision of the Accident Compensation Corporation national accident health insurance and the litigious US health insurance system.

Organisational size as measured by number of employees can be seen below in Figure 2. With a total population of just over 4 million, New Zealand may not have been expected to be well represented in the higher employee-number organisations but ‘1000 and Over’ employees accounted for 23% of respondents, with 12% having 500-999 employees. In the lower range, around 20% of respondents employed less than 100 people [1, p.3].
As can be seen above in Figure 3, organisations with revenue generation in excess of $100 million comprised 45% of respondents. Although this figure is somewhat lower than the 57% figure from the 2005 US survey and considerably less than the 66% Australian figure, it may be considered high for a nation with a population of just over 4 million people [1, p.4; 2, p.7].

Areas of Operation results can be seen in Figure 4 (at right). 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 29 organisations that operate only in New Zealand and one other geographical region, it was not surprising that 23 identified Australia as their other area of operation. Interestingly, 19 of those 23 were NZ based, rather than Australian.

Results for Respondents by Job Title can be seen below in Figure 5. Of 218 respondents, over half (56%) were the IT Manager of their organisation, with other titles occurring much less often. Although all respondents were selected as the person responsible for IT Security in their organisation, due to size of organisations, the prevalence of non-security job-titles should not be taken to indicate that the majority of organisations do not have a security focus as “IT Manager” is often used as a cover-all title.
Budgeting Issues

An issue first addressed in the 2004 CSI/FBI survey was the amount of the total IT budget devoted to security issues [1, pp.5-6]. Figure 6 (above) shows percentage of IT Budget Spent on Security, with results being similar to both US and Australian figures [2, p.33]. Slightly over 60% of NZ organisations invest under 5% of their IT budget on security, compared to the Australian 56% and US 59% figures.

A further 17% of NZ respondents indicated they spent between 5 and 10% of their IT budget on security issues, compared with 19% of respondents in the US and 26% in Australia. Around 17% of NZ respondents did not know the percentage of their IT budget allocated to security issues.

When comparing detail, the US figure for 3-5% investment was 24%, but NZ investment was over 29%. This is encouraging in that it suggests that NZ IT security awareness may be higher than might be expected from a nation with a population of around 4 million.

Interestingly, almost a quarter of non-government organisations (24%) indicated that their computer security was dictated from outside New Zealand. Although this might boost IT Security awareness, it also suggests significant international ownership of organisations operating in the country. The NZ Government’s 1980s foray into free-market economic policy was a significant contributor to this phenomenon.

Another question first addressed in the 2004 CSI/FBI survey is that of average reported computer security operating expense and investment per employee [1, pp.6-8].

Figure 7 (below) shows the NZ security expenditure per employee sorted by revenue. The figures for Operational expenditure in the budget categories under $10 million were high, with the Average Reported Total Computer Security Investment Per Employee in the Under $1 million revenue category being $540, and in the $1-10 million revenue category $519.

At this point economies of scale seem to enable drastic savings, such that the $10-100 million revenue category reported total expenditure of only $127 per employee. Beyond here the economies of scale seem less marked and the $100 million - $1 billion revenue category reported a slightly higher...
total spending average per employee. Total expenditure in the Over $1 billion dropped to $109, all of which agrees with the 2005 CSI/FBI survey finding regarding economies of scale levelling-off at some point [1, p.7].

Breaking down the figures by Industry Sector, as seen in Figure 8 (above), Financial was the largest spender with a total of $366, followed by Technology on $312. These two sectors each spent twice that of the next two highest spending sectors: National (Central) Government ($165) and Retail ($145). The remaining sectors’ spending on Operating Expenditure decreased steadily from Transport spending of $46 to Telecommunications on $3.

This last figure was surprising considering the sector’s higher rankings in both Capital Investment and percentage of Security Qualified Primary IT Security Staff and may be a combination of data anomaly due to the dominance of large Telecommunications organisations questioning the sector, plus savings relating to economies of scale in certain industries.

Capital Investment and Operating Expenditure figures were similar in around half the sectors, with the standout differences being Financial and Technology at the top of the spending scale and Educational and Telecommunications lower down. From the medical privacy perspective, some may be concerned that Medical ranked so low in security spending. Once again this may be partly due to having only 8 medical organisations in the 156 responses to the question. Computer security spending per organisation can be seen below in Figure 9.

Spending per organisation ranged from nothing to $3 million for Capital Investment and $120 to $2 million for Operating Expenditure. As the top figures were on a steady curve, they did not artificially inflate the averages.

As pointed out in the 2004 CSI/FBI Survey Report, “Managers are increasingly being asked to justify their budget requests in purely economic terms” [1, p.7]. Respondents were asked to indicate their use of cost/benefit metrics in planning computer security spending. Respondents indicated whether their organisation used Return on Investment (ROI), Net Present Value (NPV) or Internal Rate of Return (IRR). The results can be seen in Figure 10 (next page).

Only one in four respondents conducted any cost-benefit analysis on security expenditure but of the 163 who responded to the question,
many used more than one metric. Note that analysis categories were assessed separately so the figures do not sum to 100.

These results show similarities to those from the 2005 US survey, where the authors suggested the possibility that recent high-profile security breaches may have convinced the industry that managing security is a financially necessary part of operating a business.

The complexity and ever-changing nature of IT means outsourcing is an increasingly attractive option with growing uptake, but security appears not to be part of this trend. As can be seen in Figure 11 (above right), less than one in ten organisations outsourced over 80% of their security function, while almost half outsourced none of it.

Figure 12 (at right) shows outsourcing levels by organisational revenue/budget. Initial outlay on security technology and staff are acknowledged to be high, so it is understandable that organisations with budgets under $1 million are by far the highest outsourcers of the computer security function. US results show a different picture, with the average percentage of outsourcing ranging from 4 to 9% and organisations tending to outsource more security functions the larger their budget i.e. the more they need to spend on security, the more likely they are to outsource. It will be interesting to see if future NZ figures follow this trend.

Despite the best technology, security incidents do still happen and can be very costly, so risk insurance may be considered
just another tool in managing cyber security. Some 20% of 2005 respondents indicated that their organisation had such external cyber-security insurance. As Figure 13 (above) shows, less than half had insurance, with one in three not knowing whether they had it or not.

Comparing this to figures from the 2004 SRG survey of the same 500 organisations, (which had a 32% response rate, as opposed to 44% for this survey) less than one in three had insurance to cover security incidents and almost 40% did not. As the 2004 SRG survey was addressed to ‘the IT Manager’ and the 2005 survey respondents were IT Security staff, some of this perceived decrease may be due to the 2004 respondents being more aware of whether their organisation has cyber-insurance or not. Whether it was an actual reduction will be seen more clearly in the 2006 figures.

As can be seen in Figure 14 (at right), there were 123 responses to the question regarding use of governance and risk management tools.

Of those, 81% had an Information Strategic Plan that three in five regularly reviewed, but only two in five actually adhered to and just under one in four formally monitored it.

Next most common was a Business Continuity Plan, existing in three quarters of organisations but adhered to by two in five, regularly reviewed by just over half and formally monitored by one in three.

Existing in almost equal numbers of around half were Information Security Strategy and Risk Management Strategy.

Information Security Strategy was regularly adhered to and reviewed by under one in three organisations, with formal monitoring performed by under one in five. Risk Management Strategy was adhered to by one in four, regularly reviewed by one in three and formally monitored by around one in five.

Also existing in almost equal response numbers were Use of Information Management Standards and Incident Response Plans. These were also adhered to by less than one in four and regularly reviewed by one in five, with only one in six formally monitoring them.

The take home message seems to be that once plans exist, half of them are never reviewed.
Frequency, Nature and Cost of Cyber Security Breaches

A quarter of respondents’ organisations had experienced unauthorised use of their computer system, with 60% of them experiencing 1-5 incidents, 11% 6-10 incidents, 6% more than 10, and 23% unable to specify the number of incidents. Just on 60% had experienced 1-5 incidents from Outside the organisation, but 70% had experienced 1-5 incidents from Inside the organisation.

The percentage of respondents’ organisations experiencing Unauthorised Computer Use Incidents can be seen in Figure 15 (above). Although 25% of respondents reported incidents, the majority (65%) did not. The high latter figure may be due to little monitoring in NZ. Monitoring will be addressed in future surveys.

Security is holistic by nature so organisations must cover all possibilities in order to be protected. There appears to be little difference in the numbers of incidents originating inside and outside of organisations. As the US report put it, this casts doubt on claims that the vast majority of incidents are caused by insiders.

Figure 16 (below) shows notable numbers and types of detected security incidents. Over 87% of organisations indicated that they had experienced some type of security incident, with the most common incident types being Insider Abuse of Net Access/Email, Laptop/Mobile Hardware Theft, and Music/Movies/Ripping.

Other incident types such as Denial of Service, Unauthorised access/use, Unauthorised Access to Information, Theft (Information), Telecommunication Fraud and Financial Fraud (computer assisted) were also present in notable numbers.

One of the survey questions requested historical data on incident numbers. Figure 17 (next page) shows the growth in incident numbers over the period 1998-2004. NB Virus numbers have grown so spectacularly that it was not possible to include them on this graph, rising as they did from 2,341 in 1998 to 15,940 in 2004.
Most figures show steady, and in some cases accelerating growth in incident numbers, although the definitions of terminology, and therefore responses to some questions in the current survey may not correlate with those in previous SRG surveys. As was commented, does Unauthorised Use include storage of MP3 music files? Does Insider Abuse include private use of organisational web browsing?

To ensure consistency in responses to this survey, each of the technologies and economic crime terms was defined and described in a four-page glossary of terms included in the 2005 and subsequent survey documents.

Figure 18 (below) shows the average cost to the organisation by incident type. Financial Fraud led average costs by a huge margin at just over $358,000, with Telecommunications Fraud coming a very distant second. Incident costs tailed off through Laptop/Hardware Theft (averaging $14,000), Misuse of Public Web Application (12,000) Virus Contamination and Sabotage of Data/Networks and System Penetration by Outsider (each averaging $7-8,000) to Abuse of Wireless Network, the lowest average category cost on $3,000. The total estimated financial cost of all these incidents was almost $6 million for the 139 respondents willing and able to provide figures.

Interestingly, despite 21 organisations identifying Website Defacement as having occurred in their organisation, there were no responses regarding the financial cost to the organisation of these incidents. Is it reasonable to assume that the 40% of respondents with Transactional Websites were adequately protected?

It will be interesting to see whether the 2006 NZ report parallels the reported US growth in Website Defacement incidents or whether Unidentifiable Numbers remains the dominant response.

It seems the notion of set-a-thief-to-catch-a-thief is not supported in NZ IT as over 55% of respondents indicated that their organisation would not employ reformed hackers. Only 22% of respondents indicated that they might do so.

**Incidents and the Law**

The question regarding the actions taken by organisations after incidents/intrusions elicited 166 responses. Results can be seen in Figure 19 (next page). The response given highest priority was Patch Vulnerabilities and/or Change Processes, with 90% of
respondents saying this was their priority after a Computer virus incident, 21% after Denial of Service Attacks, and 16% after either Unauthorised Access/Use or System Penetration/Hacking.

Second equal most common responses to security incidents were Did Not Report and Reported to Law Enforcement. Unsurprisingly Theft Hardware/Assets was the standout figure in incidents reported to law enforcement, with 41% of respondents saying they report incidents of hardware theft.

Also unsurprisingly, the highest Did Not Report figure was for Computer Virus, followed by Insider Abuse, Unauthorised access/use and Denial of Service, although instances of Telecommunication/Toll Fraud, Product Piracy & counterfeiting, Proprietary right infringement (TM etc.), Financial Fraud (computer assisted), and Identity Theft were also not reported.

Although it is not a proportional figure, it is thought provoking that when all the No Action incident-type response percentages were added together, they totalled 46%. The obvious comment is that budgets do not always allow for doing all that should ideally be done.

The perceived importance of the reasons intrusions were not reported to law enforcement can be seen in Figure 20 (below). The reason considered most important was Competitors would use to their Advantage, with 78% rating this an important issue. Other considerations were important to 20% of respondents.

Although many organisations are aware of law enforcement’s function, most do not report computer crime. Overall, this confirms the obvious conclusion that despite the desire to discourage felony, organisations are more interested in pursuing their core business than assisting law enforcement in prosecuting offenders.

Table 1 (next page) shows the incidence and results of prosecutions relating to the reported incidents. It can be seen that the incidence of failed convictions is disconcertingly high; almost half. It is not possible to infer from the data why this should be, but further research might find this a fruitful line of enquiry.

Security Audits and Security Awareness Training

According to this year’s respondents, almost 80% of NZ organisations use security audits
Note that results may be reported to more than one area, so percentages do not sum to 100. Three out of five of those running an audit report the results to the Chief Information Officer and almost half to the Chief Executive Officer. Most interesting is that one in five of those conducting security audits did not report the results to upper management. Results can be seen in Figure 21 (at right).

As Figure 22 (at right) shows, around a quarter of responses indicated that the results were reported to alternative upper management authorities. Among these were: IT Steering Group, IT Security Manager, Internal Audit, External Clients, MIS at Overseas HQ, Regional Head Office, Project Sponsor, Global Leadership Team, Audit & Risk Committee, Senior Management Team, System Owners, Union, Sarbanes Oxley Auditors and Corporate Parent.

Some of these answers clearly indicate overseas parent organisation ownership or control.

Security is widely recognised as requiring management as well as technological solutions. Many NZ organisations have invested in security awareness training for their staff, although reaction to the statement My Organisation Invests Appropriately in Security Awareness Training was notable in that although 24% of respondents agreed, 57% disagreed.

Broken down by sector, New Zealand results show all sectors disagreeing, some more strongly than others. The closest
to a sector agreeing was a 50/50 result in the minimally represented *Telecommunications* sector.

When respondents were asked to consider the relative importance of areas for security awareness training, they predominantly identified the same training areas as very important. As can be seen in Figure 23 (above), the highest rating was for *Network Security*, with four out of five respondents considering it important. Three quarters of respondents perceived *Access Control Systems* as important, with *Security Policy* 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 **Computer Security Economic Considerations** (e.g. Budgeting), Investigations and Legal Issues, and the lowest rating **Cryptography**.

The low (22%) perceived importance rating for cryptography suggests that it is an under-utilised tool in NZ IT security as US importance ratings rose from 28% in 2004 to 51% in 2005 [1, p.17; 3, p.12].

**Security Technologies**

Security technologies that are in use in respondents’ organisations are shown in Figure 24 (below). Due to additional research requirements, categories incorporated, but were not limited to, those used in the CSI/FBI survey.

Network defence technologies consisted of 100% implementation of **Anti-Virus Software**, whilst firewalls had 99% uptake. **Intrusion Detection Systems** (IDS) were installed on 42% of systems (considerably down on the US figure of 72%) but **Intrusion Prevention Systems** were on 46% as compared to 35% in the US [1, p.16]. Organisations not employing **Intrusion Detection Systems** totalled 47%, slightly outnumbering the 42% with IDS, similar to the 2004 SRG Survey figures of 44% without and 43% with. It will be interesting to see if this was a data anomaly or whether future surveys confirm this slight IDS decrease and IPS increase as a trend.

**Server Based Access Management** had been set up by half of respondents. Encryption was considered in separate categories as **Encrypted Data Files**, **Virtual Private Network** and **Public Key Infrastructure** (see Figure 24, below). **Reusable Passwords** was implemented by two out of five respondents and **Smart Cards** by one in four, with **Biometrics** used by only one in ten.
The most commonly used Information Security Technique was Email Monitoring Software with four out of five respondents deploying it. Web Activity Monitoring Software was next most common, with 63% of respondents conducting Security Audits By External Organisation and 60% conducting Security Audits By Internal Staff. Penetration Testing was employed by 46% of respondents and Automated Tools To Check Configuration Of Network Systems by 35%. There were 6% of respondents who used Other techniques. Although a number of respondents were using a minimal set of these easily available techniques, it was pleasing to note that only 5% used no security techniques.

Operating systems (OS) are constantly changing and it is often flaws in operating systems that are exploited to attack systems. For system managers, there is a fine line between leaving older-but-proven operating systems in place and updating to advanced functionality. If the move is too soon, as-yet undiscovered flaws may be exploited and the network compromised. If the move is left too long, the update benefit may be missed.

The SRG survey has been recording numbers of Workstation Operating Systems since 1996 and trends have been similar to Windows (2000/XP) and indeed these accounted for over 81% of respondents’ workstation operating systems. Respondents reported Windows NT a distant second on 11%, with Windows ME on 7% and Other OS on 3% with Linux/Unix not registering.

One point worthy of mention is that between 1996 and 2004, SRG survey figures for Mac usage fluctuated between 1 and 3%, mainly in academia. Figure 25 (above) shows something may now be changing, with 7% of the 2005 survey’s 113,038 PC sample using Mac OS. Next year’s figures may reveal more.

**IT Standards, Policies and Procedures**

Figure 26 (below) shows Use of Computer Security Policies and/or Procedures. It can be expected that as new operating systems have appeared and gradually taken 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 popularity as replacement occurs.
seen that 94% of respondents used Access management (password, privileges, etc) and 93% used Media Back-Up. Dropping down the common-use scale a little, 78% had Documented Standard Operating Procedures, with a similar number having External Network Access Control, Right at the bottom end were 4% with Other forms of policies and/or procedures, and finally 3% with a Forensic Plan. The small size of this last figure suggests that NZ IT management has not yet adopted current research with regards to forensic analysis [4].

One in three organisations (38%) adhere to some form of IT Security-Related Standards but almost twice as many (62%) do not. This compares to 65% adherence in Australia [2, pp.9-11]. Of NZ organisations that did adhere to standards, 95% used more than one (see Figure 27 above).

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 almost a third of respondents. Next most common were Other industry specific IT security standards, adhered to by one in four respondents.

Down the other end of the scale, ACSI 33 – Australian Communications-Electronic Security Instructions 33 and RFC2196 Site Security Handbook both had only 2% adherence, and no respondents adhered to either ISO/IEC 14516 Information Technology - Guidelines on the use and management of trusted third parties’ services or HB 171—2003 Guidelines for the management of IT evidence.

Although it is possible that forensic and other evidence management is an issue yet to gain significance in New Zealand, this last figure tends to reinforce the conclusion that IT management is less than familiar with current forensic data management research [4].

Information Security Training, Qualifications & Certification

The survey question regarding qualifications and/or experience of IT staff primarily responsible for security in their organisation elicited 205 responses and results can be seen in Figure 28 (below). Approximately 52% of these responding organisations had staff with...
Industry Vendor IT Certification (MCSE, CCNA, etc). This figure was almost equalled by the 51% with staff who had No formal qualifications but more than 5 years of security experience.

Around 41% had staff who had been on Ad Hoc IT Security Training Courses, with 38% having staff with Industry Vendor IT Security Certification (Cisco etc). Almost 8% of respondents ticked None of the above.

Following a line of enquiry suggested by the 2005 AusCERT Computer Crime and Security Report, it was found that less than half of NZ IT security staff are security standard qualified. As can be seen in Figure 29 (above), just over 62% of Security Staff have no security standard qualifications.

As can be seen in Figure 30 (above right), when looked at in relation to size of organisational budgets, the percentage of IT security staff that are security standard qualified shows a generally increasing trend. Why there are dips in the $10 to $99 million and Over $1 billion categories is uncertain but the deviations have no statistical significance given the sample size.

When security standards are broken down by industry sector, telecommunications is the clear leader but as discussed earlier, this may be at least partially due to the small number of responses from the sector. Results for IT staff with security standard qualification organised by industry sector can be seen in Figure 31 (below).
Respondents did not appear to be satisfied with the management of IT security, with around two-thirds of respondents considering that their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness in IT staff (63%), management (70%) and general staff (63%). Very few did not express an opinion on this issue. See Figure 32 (at right).

Concluding Comments

As this is the first New Zealand Computer Crime and Security Survey, the data produced some expected results and some surprises. The fact that security policy is directed from for around 1 in 4 non-government organisations suggests substantial overseas ownership of NZ business.

Managing security effectively should be recognised as a financially necessary part of operating a business rather than an option, yet two thirds of respondents believed aspects of security were inappropriately funded.

It was pleasing to note that the majority of organisations had technologies in place to secure their organisations, but 62% had no IT Staff with security qualifications. Around a third used security standards, a figure similar to Australia in 2003, although Australian usage has since grown to two thirds [2, p.12].

Over 87% of organisations indicated that they had experienced some form of security incident but most were not reported, with many stating that competitors would use the information to their advantage. Yet numbers of security incidents continue to grow and failed convictions total almost half the reported incident figures.

The percentages of NZ IT budget spent on security are similar to those of Australia and the US with average Capital Investment and Operating Expenditure figures well in excess of US and Australian figures. Governance and risk management plans exist, yet many are never looked at again.

As expected, the results show a mixed bag of positives and negatives, but on the whole NZ can hold its head up in the IT world.
KEY FINDINGS

Some of the key findings from the 2005 survey are summarised below:

The numbers of almost all types of security incidents have grown steadily from 1998 to 2004. Virus numbers in particular have grown almost exponentially. The 2005 top four incident types in descending order of total cost to respondents were Financial Fraud, Laptop/Mobile Hardware Theft, Telecom Fraud and Insider Abuse of Net Access/Email. The US highest costing incident type (Virus Contamination) came next.

Although it ranked top in the 2004 SRG survey, Virus Contamination ranked a very distant eighth in 2005 average incident-type cost per organisation, after Financial Fraud, Telecom Fraud, Unauthorised Access to Confidential Information, Theft of Proprietary Information Insider Abuse of Net Access/Email, Laptop/Mobile Hardware Theft and Misuse of Public Web Application. This may be due to good management or more likely, Virus Contamination cost figures being unavailable to many 2005 respondents.

Almost half of respondents did not report intrusions to anyone outside the organisation.

Slightly over 60% of NZ organisations invest under 5% of their IT budget on security, but NZ 3-5% investment was higher than in the US, suggesting that NZ IT security awareness may be higher than might be expected from a small nation.

The proportion of respondents with external insurance for cyber-security incidents was 20%, compared with 25% in the US.

Outsourcing of security function was not commonly utilised, with less than one in ten organisations outsourcing over 80% of their security function, and almost half outsourcing none.

More than two thirds of respondents believed that aspects of security were not appropriately funded.

Only one in four respondents conducted any cost-benefit analysis on security expenditure but of the 163 who responded to the question, many used more than one metric, with ROI on 83% usage, slightly ahead of NPV on 80% and IRR on 77%.

Two thirds of respondents indicated that their organisation would not employ reformed hackers. Only one in five would.

Around two thirds of respondents indicated that their organisation needed to do more to ensure an appropriate level of IT security qualification, training, experience or awareness for both General Staff and IT Security Staff and especially Management.

When considering the Importance of Security Awareness Training, the highest figure was for Network Security, with four out of five rating it as important. At the lower end of the importance perceptions was Cryptography on one in five. This low perceived importance rating suggests that it is an under-recognised tool in NZ IT security.

Responses indicated that two thirds of organisations have no IT staff with any security qualifications, and four out of five organisations have less than 10% of their IT Staff security qualified.

Training/Qualifications of Primary IT Security Staff ranged from 52% holding either Industry Vendor IT Cert. (MCSE, CCNA, etc) or No Formal Qualifications but Over 5 yrs Security Experience, down to just 2% responding that they had Other training/qualifications.
Security Standards were adhered to by 38% of respondents.

The most commonly used Information Security Techniques were Email Monitoring Software (79%) and Web Activity Monitoring Software (69%). Only 5% used no security techniques.

Security audits were conducted by four out of five respondents’ organisations but one in five of those did not report the results to upper management. Only 5% conducted no security evaluation.

81% of respondents had an Information Strategic Plan, 75% had a Business Continuity Plan, 50% had an Information Security Strategy and 49% had a Risk Management Strategy. Adherence to and formal monitoring or regular review of these risk management tools were considerably less common.

Respondents indicate that failed convictions total almost half the reported incident figures.

Acknowledgements

Thanks are due to the following people for their contributions to this report: Hank Wolfe, Nigel Stanger, Melanie Middlemiss, Chris Roberts (CCIP), Robert Richardson (CSI) and William Lucyshyn (CSI).

The invaluable support from sponsors, The Computer Security Institute (CSI), The Centre for Critical Infrastructure Protection (CCIP) and the NZ Police is also acknowledged. Particular thanks go to all those respondents who took the time to be involved in the extended 2005 data-gathering exercise. Please join us for the much shorter 2006 survey and the continuing journey.

References


