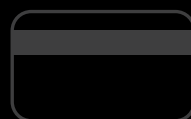


certification »



EDAIR

IT

COMPUTER CRIME & SECURITY

SURVEY





History of Australian Computer Crime and Security Surveys

The current survey partners would like to acknowledge the work of the authors of the three earlier Australian Computer Crime and Security Surveys, whose work helped raise awareness of computer crime and security issues in Australia. The first survey of this type was produced in 1997 by the Office of Strategic Crime Assessments and Victoria Police.¹ In 1999, Deloitte Touche Tohmatsu and Victoria Police² produced the second survey and in 2002, NSW Police, Deloitte Touche Tohmatsu and AusCERT produced the third survey.





The *2003 Australian Computer Crime and Security Survey* has been produced by the Australian Federal Police, Queensland Police, South Australia Police, Western Australia Police and AusCERT, Australia's national computer emergency response team. With the broader involvement of Australian law enforcement agencies in this year's survey, we seek to enhance interest in the survey among Australian public and private sector organisations to better raise awareness of computer crime and security issues.

The 2003 survey has been adapted from the *CSI/FBI Computer Crime and Security Survey* and includes new questions designed to deepen our understanding of the key factors which contribute to computer network attacks. Where appropriate, this survey compares its findings to the *2002 Australian Computer Crime and Security Survey* conducted by AusCERT, Deloitte Touche Tohmatsu and NSW Police in 2002.³

With over 200 responses from Australian public and private sector organisations, this survey provides the most up to date and authoritative analysis of computer network attack, crime and computer misuse trends in Australia over the last 12 months. Above all, the survey aims to raise awareness of the complex nature of computer crime and security issues, identify areas of concern and to promote and motivate the use of effective prevention, detection and response strategies.

EXECUTIVE

SUMMARY

The key findings of the survey are:

- Forty-two percent of respondent organisations experienced one or more computer attacks which harmed the confidentiality, integrity or availability of network data or systems.
- Despite overall lower levels of incidents being reported only 11% of respondents felt they were managing all computer security issues reasonably well. Sixty-seven percent of organisations increased expenditure on network security in the last 12 months as a result of computer security incidents or concerns.
- The trend shows a continuing shift towards a greater occurrence of externally-sourced harmful attacks and fewer internally-sourced harmful attacks. Of those who experienced attacks which harmed data confidentiality, integrity or availability, 91% experienced externally sourced attacks and 36% experienced internally-sourced attacks.
- Total losses for 2003 is more than double the quantified losses for 2002 (about \$12 million, compared to about \$6 million in 2002).
- Financial fraud, laptop theft and virus, worm and trojan infections are the largest source of computer crime losses.
- Despite high use of anti-virus software and policies for developing controls against malicious software, 80% were infected with a virus, worm or trojan and 57% suffered financial loss as a result - more than last year
- Only a minority of respondent organisations hold specialist IT security certifications; with industry vendor IT security certifications at 36% and vendor-neutral IT security certifications at 15%.
- Thirty-eight percent were dissatisfied with the level of IT security qualifications, training or experience within their organisations.



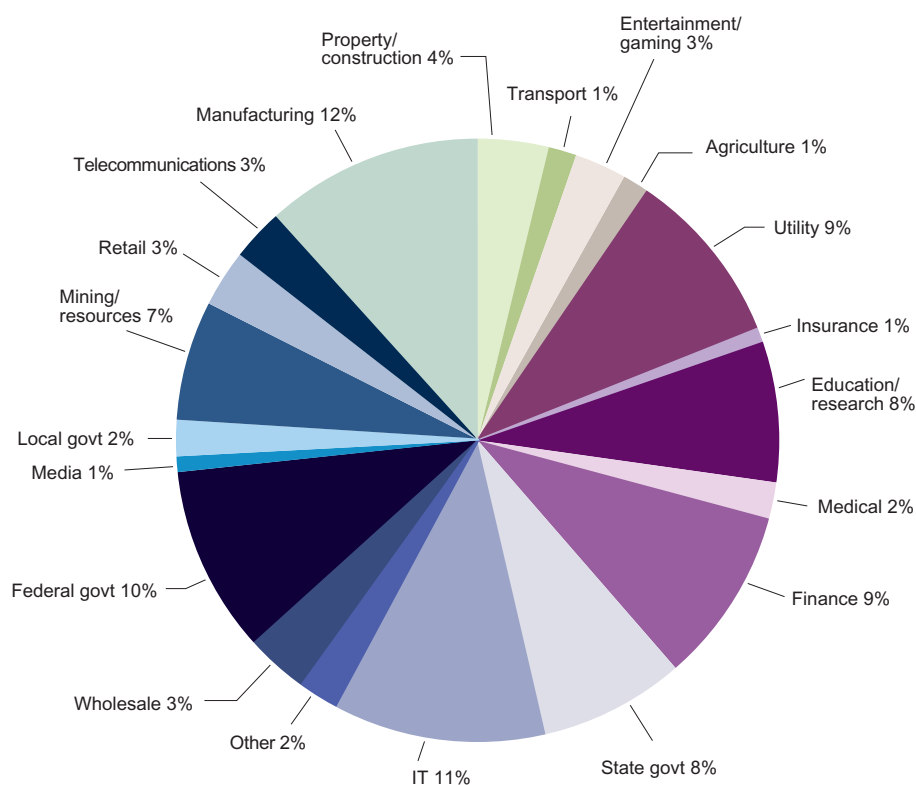
WHO

WE ASKED

With over 200 responses to this year's survey, representation from a broad range of industry groups has increased across most sectors. Manufacturing (12%), information technology (11%), federal government (10%), utilities (9%), finance (9%), education/research (8%) and state government (8%) have the highest levels of representation among sector groups. Also represented are organisations which make up part of the nation's critical information infrastructures - telecommunications, finance, utilities, government, transport and health.



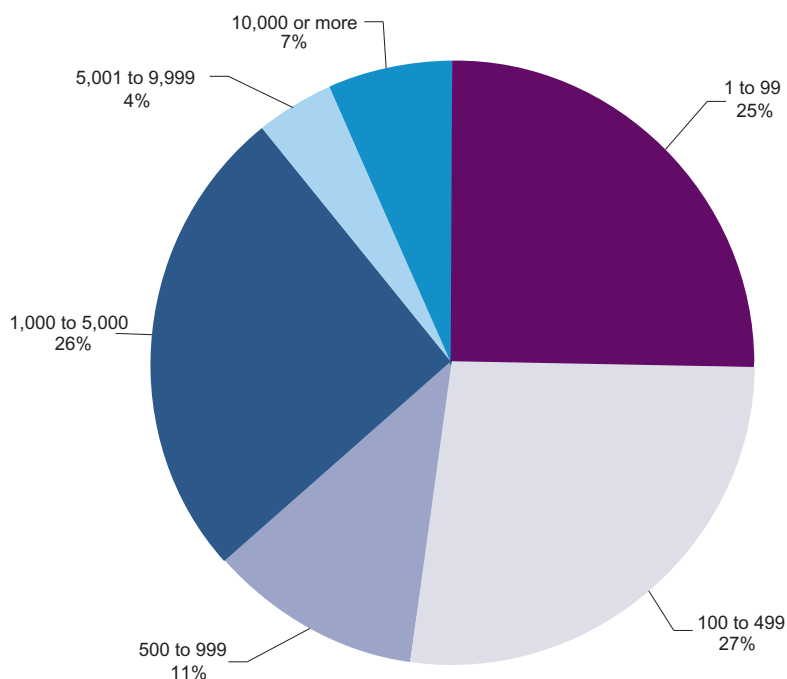
Respondents by industry sector



Source: 2003 Australian Computer Crime and Security Survey
2003: 213 respondents/99%

This year just over half of organisations represented (52%) are small to medium size organisations (up to 499 employees) whilst 37% have 1,000 or more employees. While the majority of organisations may be small to medium enterprises in terms of employee numbers, only 39% have income/expenditure of less than \$100 million. Sixty-one percent have income/expenditure of \$100 million or more and 15% have income/expenditure of over \$1 billion.

Respondents by number of employees

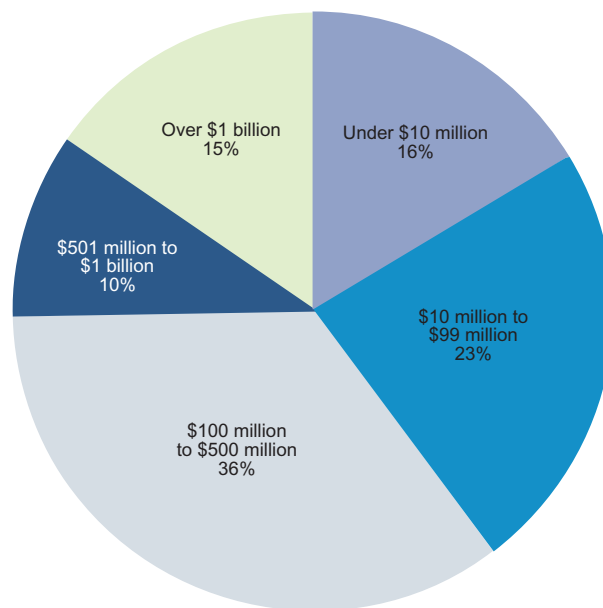


Source: 2003 Australian Computer Crime and Security Survey
2003: 214 respondents/100%

WHAT THEY USE

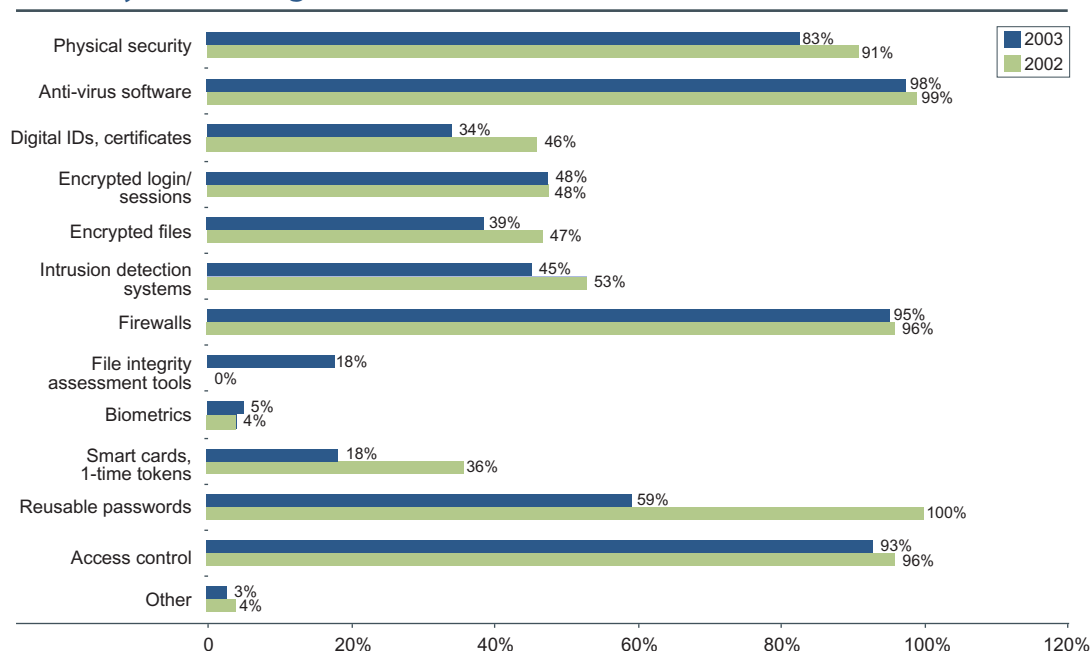
The technologies used by respondent organisations fall into high, medium or low use. Anti-virus software (98%), firewalls (95%), access controls (93%) and physical security (83%) are in common use, whereas file integrity assessment tools (18%) and strong authentication mechanisms, eg, biometrics (5%), smart cards and one-time tokens (18%) are not. The security technologies used in 2003 overall are similar to 2002 results, though usage is consistently lower compared to the previous year.

Respondents by gross income/expenditure



Source: 2003 Australian Computer Crime and Security Survey
2003: 209 respondents/97%

Security technologies used



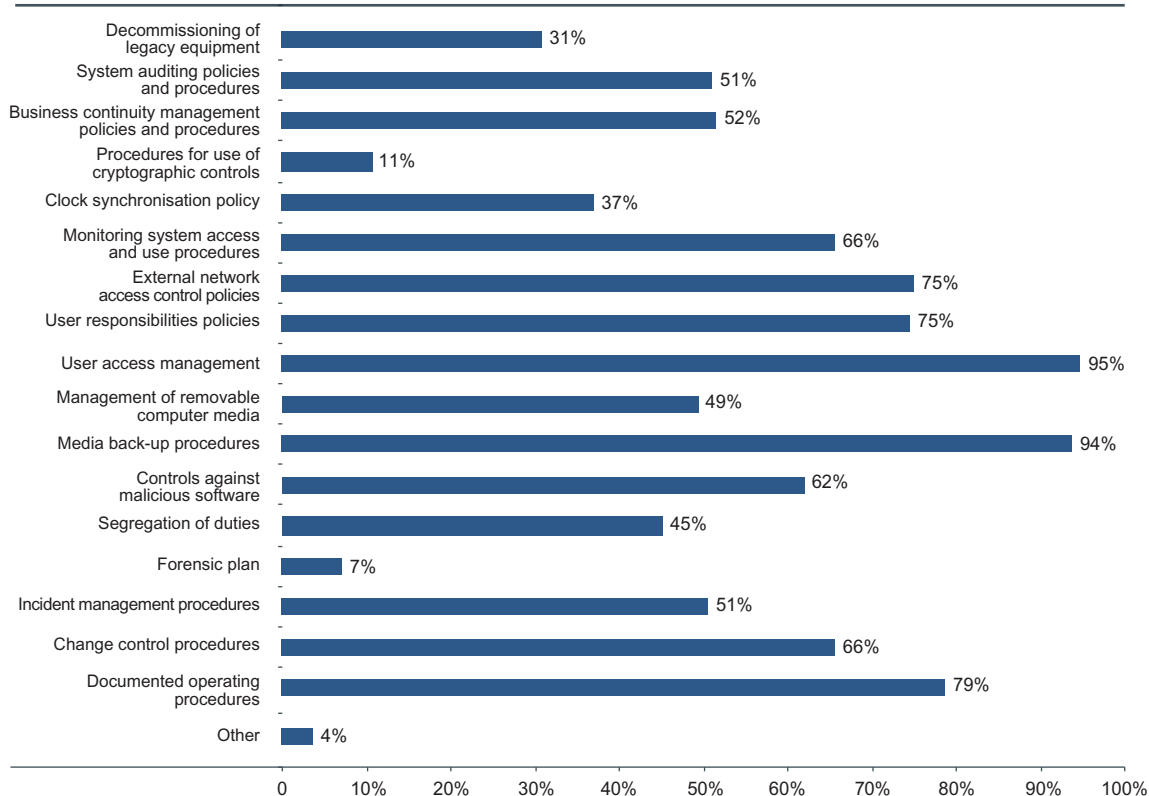
Source: 2003 Australian Computer Crime and Security Survey
2003: 214 respondents/100%, 2002: 92 respondents/97%

Note: In 2002, respondents were not asked if they used file integrity assessment tools.



One of the themes of the 2002 survey was that technology is most effective when it is supported by sound information systems security policies, practices and procedures. Therefore, to better gauge to what extent respondents are applying information systems security policies, practices and procedures, we asked them.

Computer security policies and procedures used



Source: 2003 Australian Computer Crime and Security Survey
2003: 213 respondents/99%

At least half of the respondents are applying most of the listed practices and procedures and in a few areas, the percentage is much higher; primarily for user access management (95%); media back-up (94%); documented operating procedures (79%); external network access control policies (75%) and user responsibilities policies (75%). In some respects, respondents' application of policies and procedures reflected their use of technological counter-measures. For example, 95% of respondents apply user access management procedures and 93% have access controls.

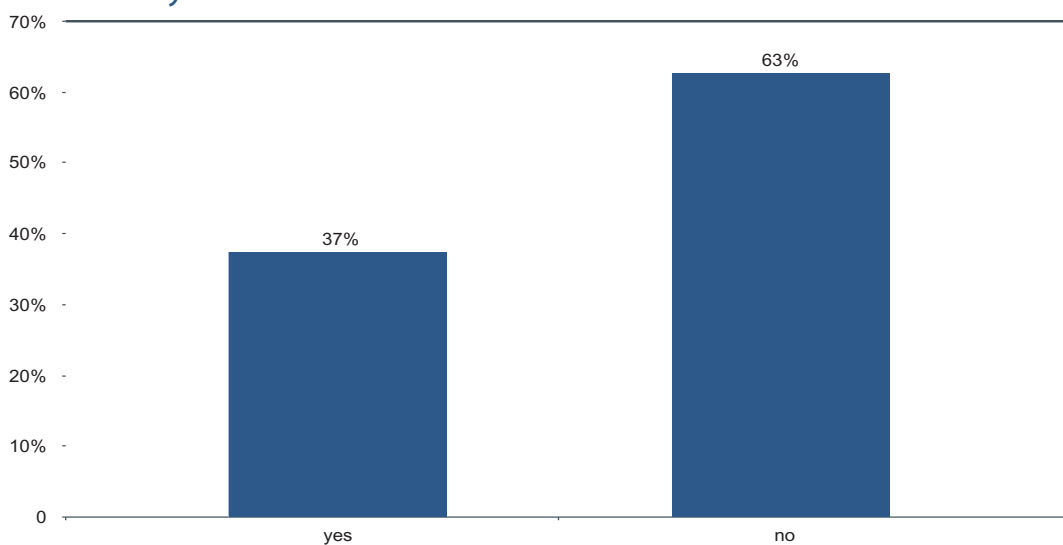
The importance of effective policies and procedures can be demonstrated by way of example. In Western Australia the offence of "unlawful operation of a computer system" refers to a restricted access system where access is obtained "without proper authorization".⁴ Where an organisation experiences an externally-sourced attack, these elements may be readily satisfied. If, however, the incident involves a user or employee of the organisation, establishing what the person is authorised to do and whether they have exceeded their authority is potentially more problematic. Having in place appropriate levels of security, logging and clear and communicated Acceptable Use Policies can have a dramatic effect on the outcome of any legal action, both criminal and civil. Some organisations fall into the trap of having Acceptable Use Policies but because they fail to consistently enforce them, it creates doubt as to what user actions are acceptable in practice.

The evidence must also establish a link between the alleged activity and the person being accused. Collecting evidence usually entails implementing monitoring and logging of system events and usage. Provided employees and users are advised that their on-line activities on the network are being monitored, then a reasonable level of monitoring is fair. A successful investigation and prosecution also depends upon the manner in which the digital evidence is collected and stored.

For organisations that wish to enhance their ability to take legal action against attackers, consideration should be given to developing a forensic plan as an adjunct to incident management procedures, system clock synchronisation policy and

appropriate logging. Sixty-six percent are monitoring system access and use, 51% have incident management procedures, 37% have clock synchronisation policies, but only 7% have a forensic plan. Based on these figures, at least half of the respondents (ie, those who do not have incident management procedures) are less likely to respond well in the event of an incident. Recovery is likely to be an organisation's first priority, but in the medium term, priorities such as seeking justice or legal restitution may weigh more heavily; particularly as organisations begin to appreciate that recovering from computer security attacks may be far more costly and protracted than first thought. However, unless fundamentals such as logging, system clock synchronisation and the manner in which digital evidence is collected and stored are addressed, opportunities for legal action may be reduced from the outset.

Does your organisation follow, or use as a guide, any IT security-related standards?

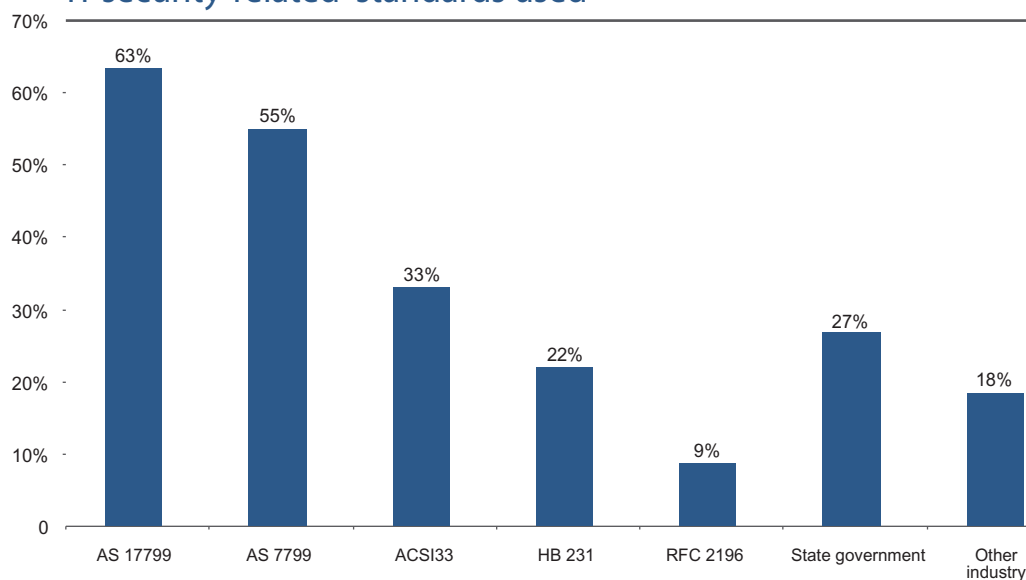


Source: 2003 Australian Computer Crime and Security Survey
2003: 211 respondents/98%

Information security standards

Information security standards provide guidelines for implementing best practice in information security management to help organisations reduce and better manage the risks to their information systems. It is surprising that only 37% of respondents follow or use as a guide an information security standard. Of those few who do use information security standards, as was expected, the Australian standard AS/NZS 17799:2001 (63%) and its counterpart, AS/NZS 7799.2:2003 (55%) were the most commonly used.

IT security-related standards used

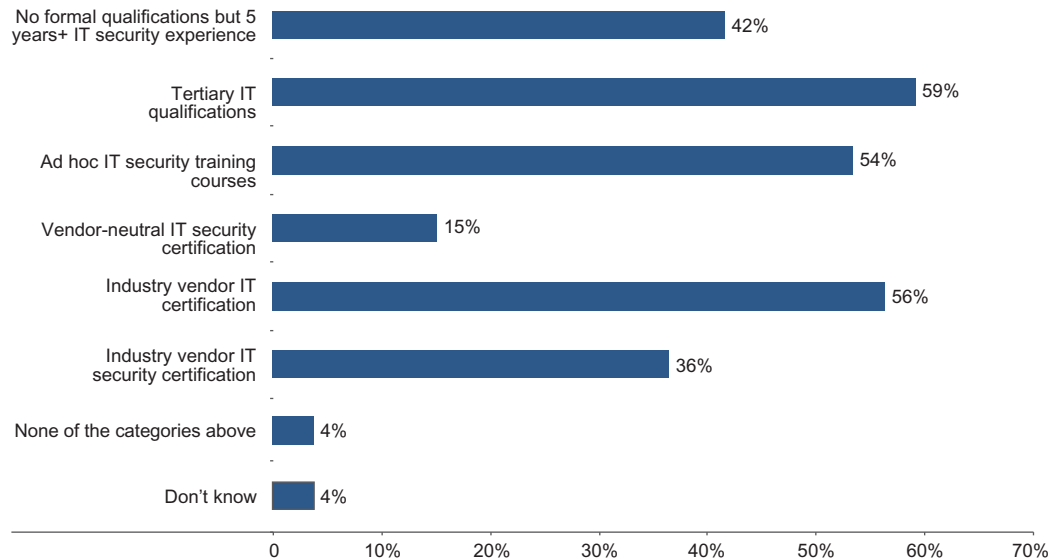


Source: 2003 Australian Computer Crime and Security Survey
2003: 82 respondents/38%

IT security skills, qualifications and experience

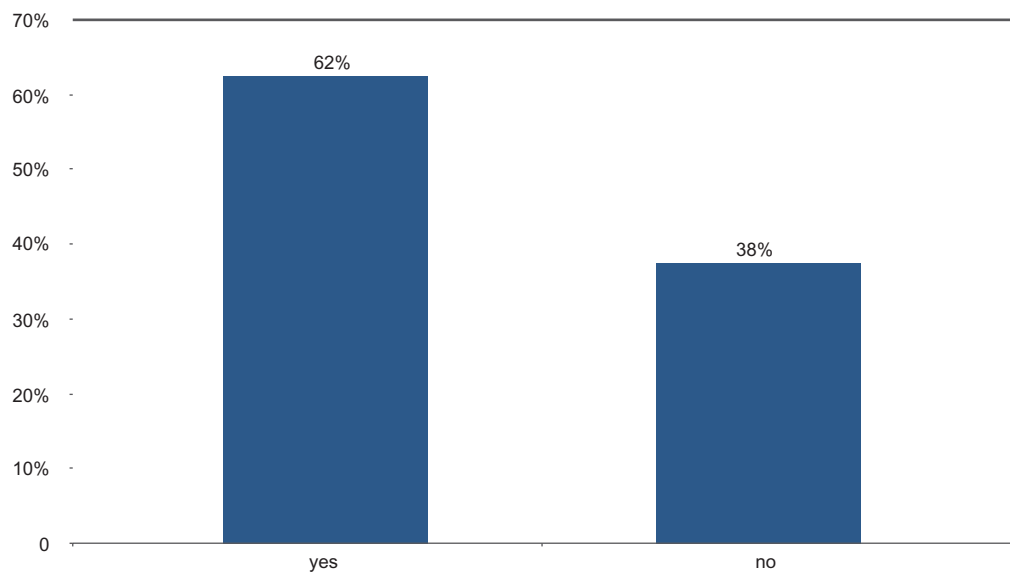
Staff with experience and qualifications in information technology security is as important as adopting sound computer security practices and applying technological counter-measures. The majority of respondent organisations employed staff or contractors with tertiary qualifications in IT (59%) but given the importance of ensuring that personnel employed in these positions are appropriately qualified, the figure was not as high as might be expected. Indeed, the nature of the IT security field is such that tertiary qualifications in IT do not by themselves necessarily equip graduates to fully appreciate and apply computer security principles and counter-measures. Usually some supplementary specialisation is required with the support of an experienced team. Significantly, only a minority of respondent organisations held dedicated IT security certifications, with industry vendor IT security certification at 36% and vendor-neutral IT security certification at 15%. This may be a key factor in assessing why 38% felt dissatisfied with the level of IT security qualifications, training and experience within their organisation.

Nature of IT or IT security qualifications/experience in your organisation



Source: 2003 Australian Computer Crime and Security Survey
2003: 211 respondents/98%

Are you satisfied with the general level of IT security qualifications, training and/or experience within your organisation?



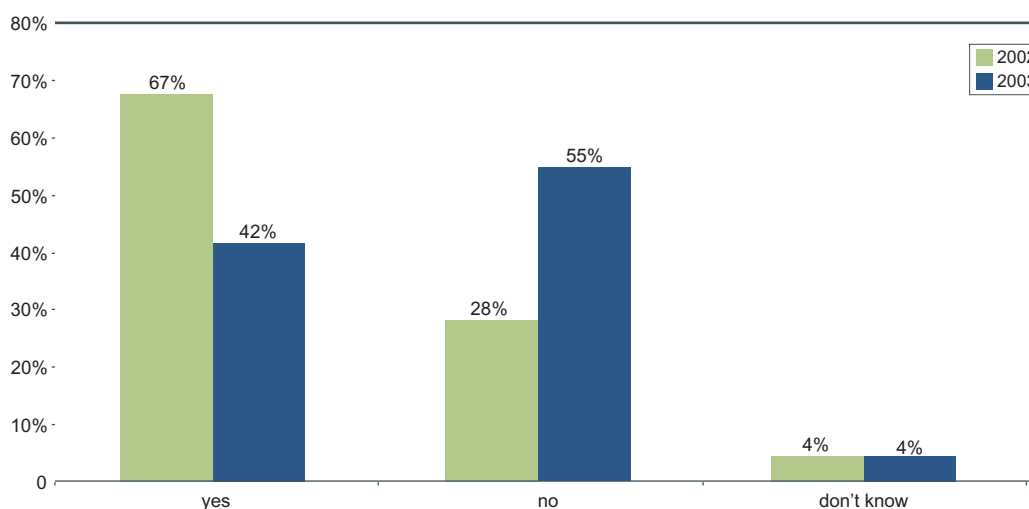
Source: 2003 Australian Computer Crime and Security Survey
2003: 213 respondents/99%



WHAT ARE THE TRENDS?

Forty-two percent of respondent organisations experienced a harmful computer security incident in 2003, considerably fewer than 2002 (67%). For the purposes of this question, a computer security incident was defined as an attack against a computer or network which harmed the confidentiality, integrity or availability of network data or systems. Possible factors which may account for the lower level of reported incidents this year is that, compared to 2002, the definition of a computer security incident is more stringent and the sample size has more than doubled.

Did your organisation experience one or more computer security incidents in the last 12 months?

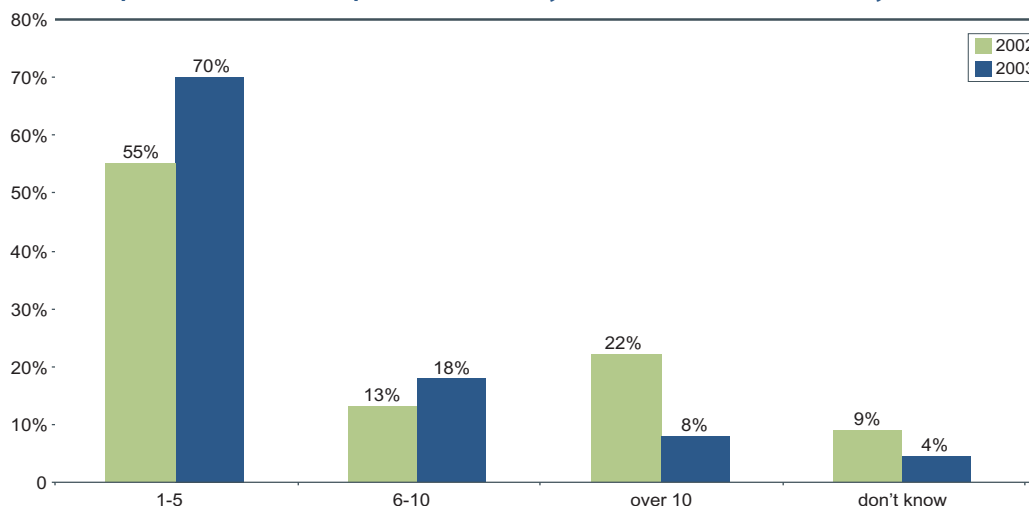


Source: 2003 Australian Computer Crime and Security Survey
2003: 212 respondents/99%, 2002: 92 respondents/97%

Note: In 2003, a computer security incident was defined as an attack against a computer or network which harmed the confidentiality, integrity or availability of network data or systems. In 2002, a computer security incident was defined as an attack against a computer or network, either real or perceived.

Of those which experienced incidents of this type, 70% experienced one to five incidents, an increase of 15% compared to 2002 and 18% experienced six to ten incidents, which is again higher than 2002 (13%).

If experienced computer security incidents, how many?

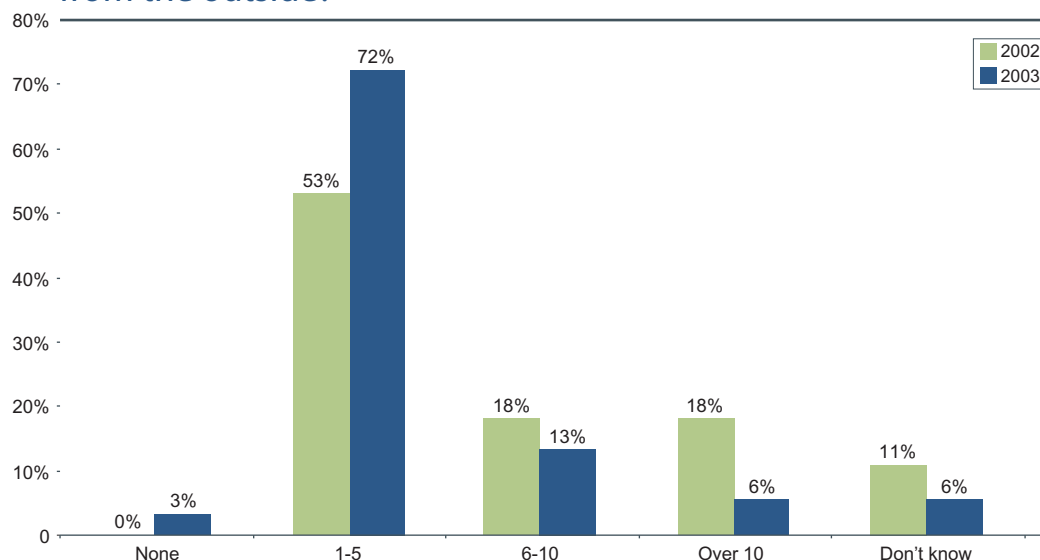


Source: 2003 Australian Computer Crime and Security Survey
2003: 90 respondents/42%, 2002: 67 respondents/71%

For respondents that experienced incidents which harmed data confidentiality, integrity or system availability, 91% experienced externally-sourced incidents; whereas only 36% experienced internally-sourced incidents. Seventy-two percent of respondents experienced between one and five externally-sourced incidents, which is higher than 2002 levels (53%). By comparison, only 29% of respondents experienced between one and five internally-sourced incidents, which was substantially less than 2002 levels (52%). The trend shows a shift towards a greater occurrence of externally sourced harmful attacks and fewer internally sourced attacks. With increasing connectivity to the Internet and to other large networks, this trend is not likely to abate.

The fact that fewer internal attacks are being reported relative to external attacks does not mean the insider threat does not exist - for externally-connected networks, the insider threat is only less likely. The impact of an insider attack, however, can often be more serious and for this reason insider attacks may potentially pose a greater risk to an organisation's operations.

If experienced computer security incidents, how many from the outside?



Source: 2003 Australian Computer Crime and Security Survey
2003: 90 respondents/42%, 2002: 62 respondents/65%

Note: In 2002, respondents were not given the option of selecting "none" in response to this question.

Network intrusion against a major Australian ISP

In December 2001, Optus discovered an intrusion on their production system, which resulted in the unauthorised copying of a database containing usernames and passwords for about 425,000 Optus Internet customers. The discovery was made through an automated process and, on investigation, a rootkit was discovered on a compromised machine. The source of the compromise was in fact a less secure customer's computer in Sydney. An examination of the rootkit showed that its author called himself "SeN". One of the programs in the rootkit was executed in a safe environment, where it connected to an IRC channel, and where one of the participants was also SeN. Further enquiries identified an IP address used by SeN.

The intrusion was reported to the NSW Police Computer Crime Unit and a strike force, with assistance from other law enforcement and government agencies and industry, was established to identify and prosecute the person/s responsible. Investigators conducted covert enquiries and identified the probable location of SeN at an address in Sydney. Covert enquiries and surveillance indicated that the house was occupied by a young man, who had just finished an IT degree at the University of Western Sydney and his parents.



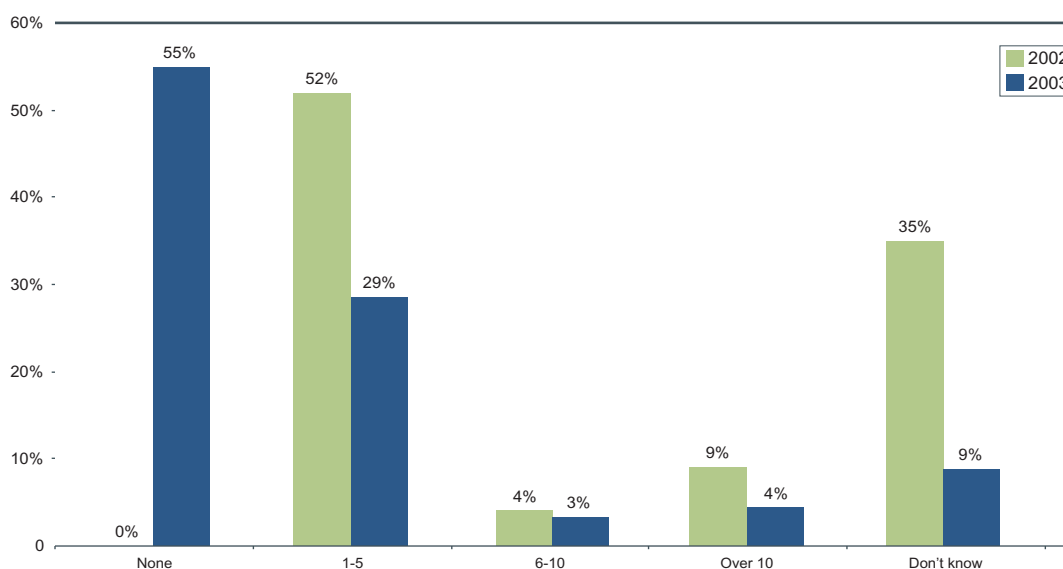


Police used covert law enforcement techniques to monitor the Internet traffic from the suspect's ISP account and address to determine who was using the computers at that address. In July 2002 police executed a search warrant on the suspect's home address. There police found incriminating evidence, including a list of compromised computers maintained by the suspect and a portion of the original compromised usernames and passwords.

Evidence collected from both the covert techniques and the offender's computer provided evidence of the compromise of 119 computers, most of which were located in overseas countries, including China, Russia, Korea, Japan and the USA.

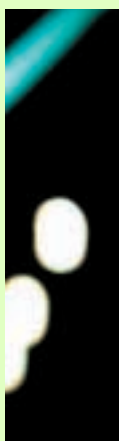
Police investigators were eventually able to collect evidence to prosecute the offender for two "unauthorised modification of data offences" under Section 308D of the *NSW Crimes Act 1900*, including the original hacking of the Optus computers. These offences carry a penalty of 10 years imprisonment. The offender pleaded guilty. He was sentenced on 4 April 2003 at the Downing Centre Local Court where the offence was proved but no conviction was recorded.

If experienced computer security incidents, how many from the inside?



Source: 2003 Australian Computer Crime and Security Survey
2003: 91 respondents/42%, 2002: 46 respondents/48%

Note: In 2002, respondents were not given the option of selecting "none" in response to this question.



Computer fraud attack based on insider knowledge

In January 2003, a former employee of a company used the username and password he held while employed at the company to remotely log into the company's network and accessed the accounts data containing customers' credit card transactions. The offender then changed customers' credit card details and proceeded to make refunds to his credit card through the altered accounts. The company only became aware of an anomaly when it noticed an unusual number of refunds were occurring.

Queensland Police charged the offender under Section 408C fraud under the *Criminal Code (Qld) 1899*. Because the company failed to disable the employee's system account, the attacker could not be charged for computer offences as a case could not be made to show that the access was unauthorised access to a 'restricted' computer.

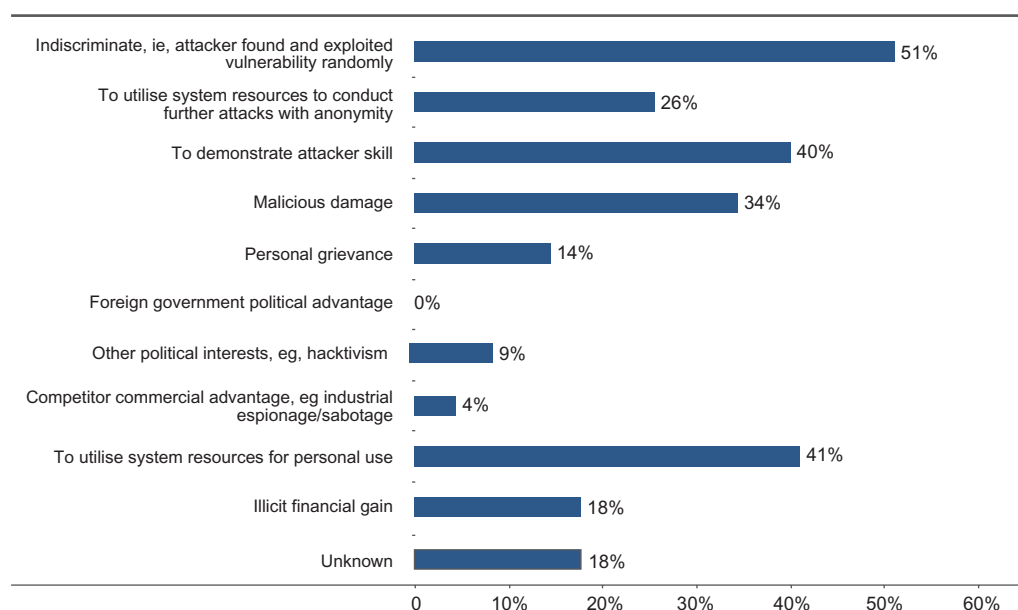
The case highlights the importance of adopting appropriate practices and procedures to ensure that employees or contractors' access to an organisation's networks and premises is withdrawn once their employment has terminated.

Attacker motives

Respondents were asked to give their opinion as to the attacker's likely motive for the attacks which harmed data confidentiality, integrity or system availability. Fifty-one percent thought the attacks were indiscriminate, ie, they occurred as a result of their Internet connectivity. Being reachable meant that any vulnerabilities within their systems could be found from anywhere across the globe and exploited. 'Indiscriminate' also refers the attitude of many hackers towards their acts – if you connect a vulnerable system to the Internet, with automated scanning tools widely accessible, the system will be compromised almost as easily as the vulnerability will be found. It is not uncommon for vulnerable systems to be compromised within minutes of being connected to the Internet. Worms, of course, are the ultimate indiscriminate 'locate and attack' tool on a mass scale. For example, in January 2003, the Slammer worm efficiently exploited a six month old vulnerability in the MS-SQL server enabling it to compromise tens of thousands of unprotected systems in an indiscriminate manner.

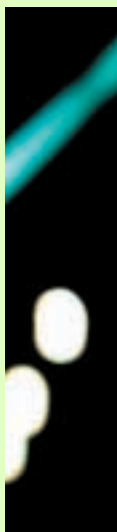
Forty-one per cent of respondents thought the attacks occurred in order to utilise system resources for personal use. In particular, networks with a large bandwidth connection to the Internet are prey to hackers who are looking for both bandwidth and storage capacity to facilitate the transfer and storage of pirated software and music (warez); or for the purposes of establishing Internet Relay Chat (IRC) servers to communicate remotely with other IRC users.

Suspected motive for incidents which harmed confidentiality, integrity or availability in the last 12 months



Source: 2003 Australian Computer Crime and Security Survey
2003: 90 respondents/42%

Twenty-six percent thought their systems were compromised to facilitate attacks against third parties with a degree of anonymity. The installation of attack tools such as log scrubbers, distributed denial of service (DDoS) attack tools, IRC bots and rootkits are indicators of intent to conduct further attacks from the compromised site. In some cases, evidence of outbound DoS traffic will also be present. Forty percent suspected the attacker was merely trying to demonstrate his/her skill and 34% thought the attacker was motivated by the desire to cause malicious damage to the site.

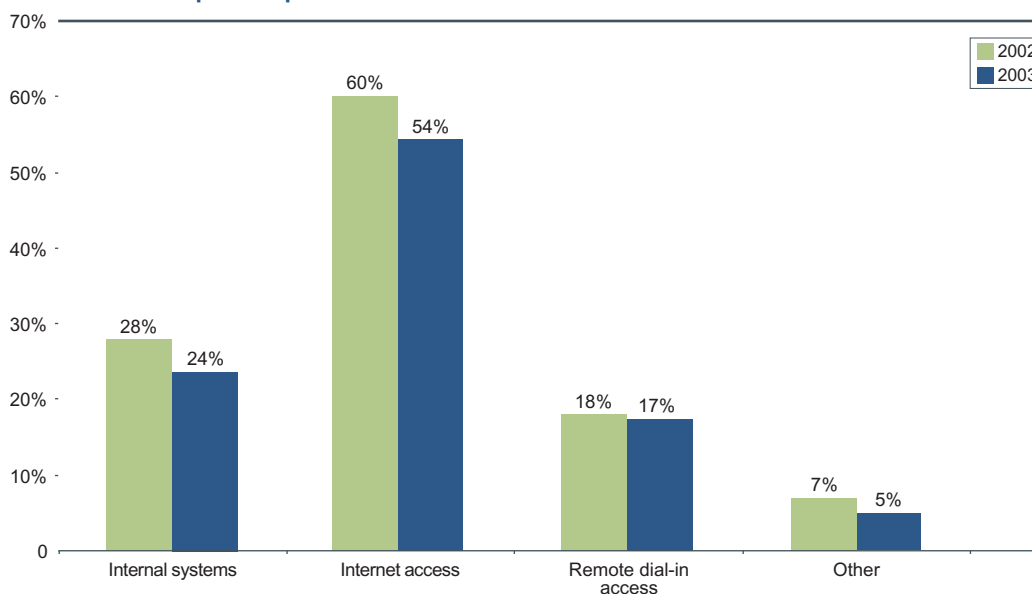


Computer facilitated fraud by former employee

An employee of a telecommunications service in Sydney was dismissed on 23 November 2001. On 16 and 17 January 2002 the employee logged onto a web site which he formerly administered, which allowed corporate customers to procure hardware. Although his access had been cancelled on termination, it was later discovered that the employee had misused his privileges during his term of employment to create additional usernames and passwords. With his newly acquired privileged access, he modified various pricings and availability of the products provided, reducing the price of some to zero dollars and cents. This led to customer service issues and financial losses were incurred to restore the site to its proper condition. Police from the NSW Computer Crime unit were provided with access logs for this event, which readily identified the IP addresses used. From this a residential address was identified; the occupant of which was the former employee. Police executed a search warrant on the premises and found evidence including a handwritten list of the passwords used to commit these crimes. The offender's laptop contained evidence of access to the web pages and the passwords used in these offences. The former employee was arrested and charged with two counts of "unauthorised modification of data" under Section 308D of the NSW *Crimes Act 1900*, offences which carry a maximum penalty of 10 years imprisonment.

The offender pleaded guilty and was given a 12 month suspended sentence. Although not fully compensating for the losses incurred, the offender was also required to pay compensation of \$5,570.

Most frequent points of attack

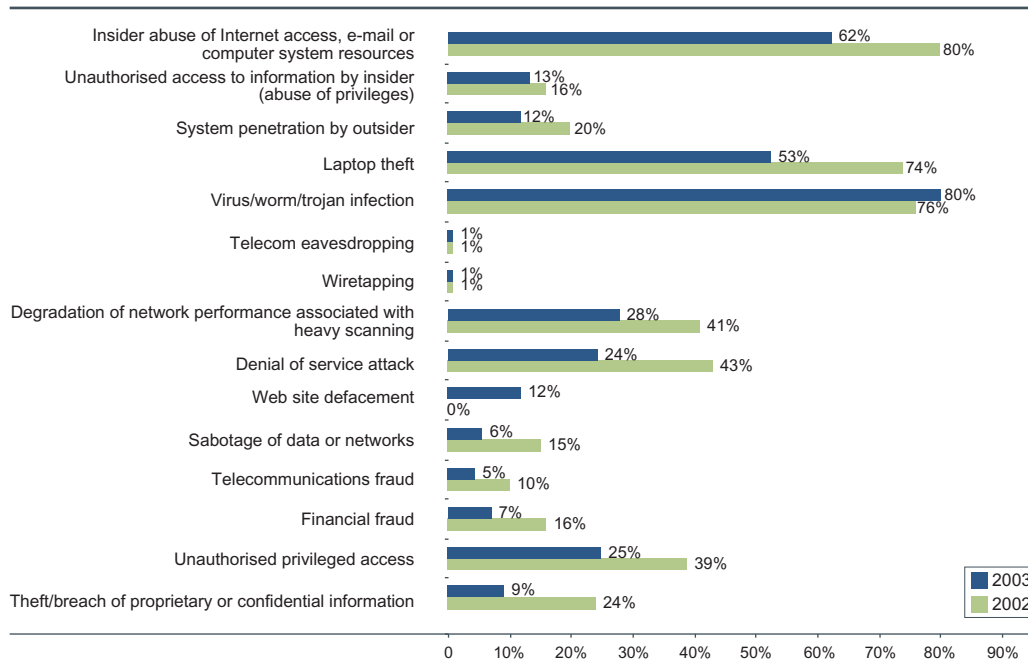


Source: 2003 Australian Computer Crime and Security Survey
2003: 194 respondents/90%, 2002: 75 respondents/79%

Note: Respondents were asked to give a rating of 1 - 5 (1 for least frequent and 5 for most frequent point of attack) for each category.

For the second consecutive year, and consistent with the previous figures, the majority of respondents (54%) reported their externally-exposed systems are subject to greater levels of attack than their internal systems (24%).

Which of the following types of computer attack, crime or misuse did your organisation detect in the last 12 months?



Source: 2003 Australian Computer Crime and Security Survey
2003: 196 respondents/91%, 2002: 93 respondents/98%

Note: In 2002, web site defacement was not a category under this question.

In most categories, the percentage of respondents who detected and suffered losses as a result of certain types of computer crime, attack or abuse has dropped compared to 2002 levels. For the period covered by the 2003 survey, there were fewer serious mass scanning worms in circulation compared to the previous period; naturally fewer respondents (28%) reported experiencing degradation of network performance associated with heavy scanning than 2002 (41%).

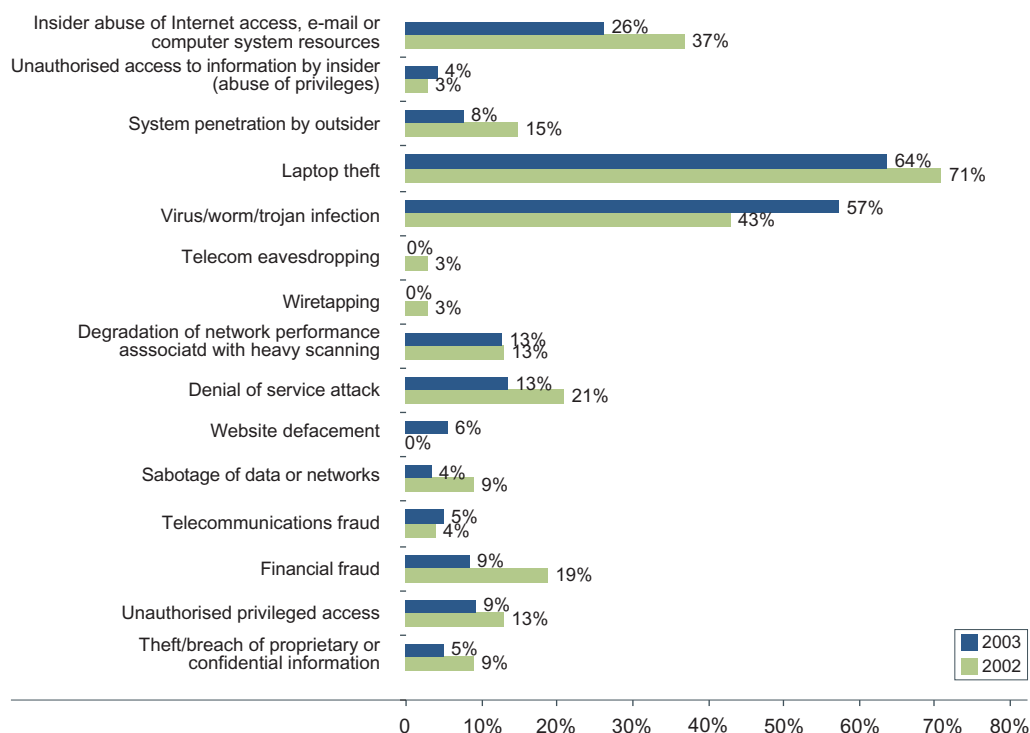
It is not possible to accurately identify other causes for the reduction but it could be due to increased accuracy as a result of the larger survey sample size and improvements in organisations' ability to prevent computer security incidents. The lower levels of reported computer crime and attack are not assessed as being caused by any reduction in malicious activity being directed at organisations' networks.

While overall levels of computer crime, attack and abuse appear to have reduced in the last 12 months, many respondents are still experiencing computer crime and abuse in its various forms. Eighty percent of respondents suffered from worm, virus or trojan infections and compared to 2002 figures (76%) this is one area where the attack level has worsened. Twenty-four percent experienced attacks leading to a denial of service (DoS) and 28% experienced unauthorised privileged access.

In terms of the losses incurred as a result of these incidents, losses are being more commonly experienced as a result of laptop theft (64%); virus, worm or trojan infections (57%) and insider abuse of network systems or resources (26%).



Which of the following types of electronic attack, computer crime or misuse caused your organisation financial loss in the last 12 months?



Source: 2003 Australian Computer Crime and Security Survey
2003: 141 respondents/65%, 2002: 75 respondents/79%

Note: In 2002, web site defacement was not a category under this question.

Measuring the impact of computer attacks and crime

When these losses are quantified, it is possible to gain a better appreciation of what these percentages really mean to those organisations that have been affected. The total quantified losses for 2003 are more than double the total quantified losses for 2002 (about \$12 million, compared to about \$6 million in 2002). Average losses for each category of computer crime or misuse have also increased in most cases.

Although in the majority of cases organisations are recovering quickly from most forms of attack, crime and abuse, quantified losses are still relatively high for those experiencing harmful attacks. In several cases, however, recovery took over a month and in some cases organisations felt they may never fully recover from incidents involving theft/breach of confidential or proprietary information, unauthorised privileged access, financial fraud, network scanning, eavesdropping, virus/worm or trojan infection, laptop theft, unauthorised access to information by an insider and insider abuse of network resources. Of those respondents who estimated the time it took for their organisations to recover from harmful computer security incidents, 12% assessed that their organisations may never fully recover.

Financial fraud

The opportunities for computer facilitated financial fraud are many, particularly for various forms of identity theft. Stealing credit card numbers stored (insecurely) on a web server retained for e-commerce transactions, Automatic Teller Machine skimming or gaining access to customer Internet banking login details are a few examples.

In some cases, for the fraud to succeed, the attacker does not need to attack the information system, but rather only impersonates it. Man-in-the-middle attacks are an older form of impersonation where data transferred between two nodes is intercepted and possibly altered without the knowledge of the communicating parties. These days any reputable organisation which conducts on-line transactions for the public will provide encrypted sessions to avoid confidential data being seen or modified in transit. However, as new technologies are developed to prevent certain types of computer attack, attackers invariably find ways to circumvent them.

Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over the last 12 month period.

| How money was lost | Respondents with quantified losses | | Lowest reported | | Highest reported | | Average loss | | Total annual loss | |
|---|---|------|-----------------|--------|------------------|-----------|--------------|---------|-------------------|------------|
| | 2002 | 2003 | 2002 | 2003 | 2002 | 2003 | 2002 | 2003 | 2002 | 2003 |
| Theft/breach of proprietary or confidential information | 4 | 7 | 10,000 | 3,000 | 150,000 | 150,000 | 72,500 | 36,857 | 290,000 | 258,000 |
| Unauthorised privileged access | 8 | 10 | 1,000 | 1,000 | 50,000 | 200,000 | 13,275 | 32,200 | 106,200 | 322,000 |
| Financial fraud | 7 | 8 | 500 | 10,000 | 600,000 | 1,400,000 | 115,288 | 440,625 | 807,000 | 3,525,000 |
| Telecommunications fraud | 2 | 6 | 1,000 | 200 | 100,000 | 250,000 | 50,500 | 69,200 | 101,000 | 415,200 |
| Sabotage of data or networks | 5 | 3 | 1,000 | 5,000 | 1,000,000 | 100,000 | 204,600 | 41,667 | 1,023,000 | 125,000 |
| Web site defacement | - | 8 | - | 500 | - | 30,000 | - | 7,313 | - | 58,500 |
| Denial of service attack | 8 | 16 | 1,500 | 300 | 100,000 | 200,000 | 22,688 | 24,831 | 181,500 | 397,300 |
| Degradation of network performance associated with heavy scanning | 7 | 14 | 1,500 | 1,000 | 100,000 | 200,000 | 23,071 | 37,729 | 161,500 | 528,200 |
| Wiretapping | 1 | 0 | 1,000 | 0 | 1,000 | 0 | 1,000 | 0 | 1,000 | 0 |
| Telecom eavesdropping | 1 | 1 | 10,000 | 4,000 | 10,000 | 4,000 | 10,000 | 4,000 | 10,000 | 4,000 |
| Virus, worm, trojan infection | 23 | 66 | 100 | 200 | 100,000 | 400,000 | 38,743 | 33,695 | 891,100 | 2,223,900 |
| Laptop theft | 48 | 82 | 2,000 | 1,999 | 100,000 | 350,000 | 26,331 | 27,539 | 1,263,900 | 2,258,183 |
| System penetration by outsider | 7 | 7 | 1,000 | 2,000 | 40,000 | 50,000 | 26,143 | 21,571 | 183,000 | 151,000 |
| Unauthorised access to information by insider | 5 | 3 | 5,000 | 2,000 | 100,000 | 250,000 | 29,000 | 87,333 | 145,000 | 262,000 |
| Insider abuse of internal computer resources, access or e-mail | 17 | 30 | 100 | 500 | 200,000 | 400,000 | 36,300 | 42,417 | 617,100 | 1,272,500 |
| Total annual losses | 2003: 126 respondents/58%; 2002: 75 respondents/80% | | | | | | | | 5,781,300 | 11,800,783 |

Within the last few months in Australia there have been reported several cases of impersonation attacks directed against the users of financial institutions, businesses with facilities for e-commerce transactions and public sector organisations. These types of attacks, because of their simplicity, are seeming to become more common. The attacker - utilising (usually both) email and web site communications - impersonates the electronic communications of a legitimate organisation. Impersonation of electronic communication is easily achieved by copying HTML code so that a fake web site can be established. An email message falsely purporting to be from the organisation is then crafted to trick the recipients into providing their login, password or credit card details. The data entered by the recipient is sent to a web site or anonymous email account established and controlled by the attacker.

Financial institutions and e-commerce businesses risk suffering significant financial losses from this type of activity. In the cases where attackers seek login details to gain access to ordinary system accounts, the attacker could conduct further illegal activities while assuming the on-line identity of the real account owner; this is generally a key motive for seeking access to user accounts.

As no compromise occurs to the confidentiality, integrity or availability of the information system itself, it is difficult to defend against such attacks. The best protection will come from educating on-line customers and system users about the importance of not disclosing login information even to seemingly trusted parties; establishing secure authenticated sessions and checking digital certificates before providing sensitive financial information.



Impersonation attack

In March 2003, Australian law enforcement responded to the unauthorised mirroring of an Australian Internet banking website. The suspects constructed a false web site purporting to be the legitimate Internet banking site of a major Australian bank. Using a spamming technique, a fraudulent email also purporting to be from the bank was sent to Australian recipients. Under a pretext of a "technical update", recipients were urged to "reactivate" their accounts by clicking on the web site link provided and entering their Internet banking login name and password. As a result of believing the request was legitimate, the suspect was able to capture the usernames and passwords of many Internet banking customers. Seventy customer bank accounts were accessed by the suspect and funds from 12 customers transferred to an account belonging to a Sydney based person. This person was subsequently arrested by NSW Police and the AFP in a Sydney bank whilst attempting to withdraw the siphoned monies.

AusCERT, through its global network of computer security incident response team contacts, is aware of an increase in identical fraudulent activity overseas in the last 14 months. In addition to sending emails to direct users to fake web sites, in some countries attackers are attacking information systems themselves by installing trojans to steal usernames and passwords and compromising Domain Name Servers to automatically redirect customers to fake web sites. Usually the IP addresses for these fake web sites are located outside the country where the fraud is being committed, making the closure of the sites more difficult.

Viruses, worms and trojans

Losses arising from malicious code attacks, viruses and worms pose the single worst threat to information systems in Australia in terms of the number of respondent organisations affected. Moreover, this is one of the few areas where attacks have substantially worsened in the last 12 months.

Ninety-six percent of respondents use anti-virus software and 62% have policies and procedures for controls against malicious software. Despite these high figures, 80% were infected with a virus, worm or trojan and 57% suffered financial loss as a result – more than last year. The average cost of virus and worm infections has been approximately \$34,000. About one-third of respondent organisations (33%) recovered quickly – in less than one day; and 30% took between one and seven days to recover. For others recovery was much longer and two respondent organisations felt they may never fully recover.

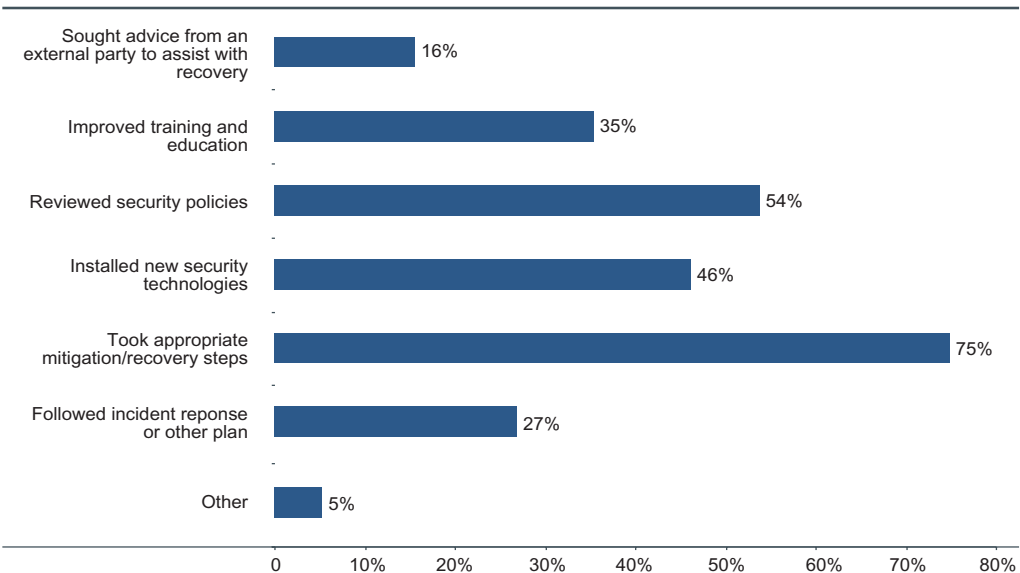
The reason for each of these failures is likely to vary. Some simple reasons are likely to be that anti-virus software was out of date; a user bypassed virus checking mechanisms and introduced an infected disk or file onto the network; or a user opened an attachment with a virus for which the vendor had not yet included the anti-virus signature updates.

Another trend which is likely to worsen is for attackers to release packages of binaries that have the same effect as malicious code but which anti-virus vendors do not include as part of their anti-virus signatures. AusCERT has received reports in Australia where packages of binaries have caused extensive damage in large local area networks (LANs) where

anti-virus software was up to date. An examination of the worm binary in one case revealed a large assortment of vulnerability scanning and system audit tools for a wide range of vulnerabilities. The site's anti-virus vendor advised that such tools had a legitimate function on networks and as such were not included in anti-virus signature files, nor would be in future. In this case, the cause of the infections was a weak password on an account with administrator privileges, which was replicated for all machines with the standard operating environment deployed at the site. Once infection took place the worm spread through file shares to other machines on the LAN.

Anti-virus vendors treat the use of 'legitimate' tools, such as vulnerability scanners, auditing tools and spyware differently; some ignore them completely and others detect them but only provide low level warnings, which could be ignored by uninformed users; or do not quarantine the file. As more worms are created which include otherwise legitimate elements, anti-virus products may become less effective. Anti-spyware may help detect some 'legitimate' tools which can be used to harm systems which anti-virus software may not detect.

If your organisation experienced computer security incidents in the last 12 months, which of the following actions did your organisation take?



Source: 2003 Australian Computer Crime and Security Survey
2003: 167 respondents/78%

Incident detection and response

In 4% of cases, respondent organisations reported that they were unsure whether or not their systems had been compromised. In reality, at least some proportion of those who reported that they had not experienced an incident which harmed confidentiality or integrity, probably had but failed to detect it.

Time lost recovering

For each of the following types of electronic attack, computer crime or misuse which caused harm to your organisation in the last 12 months, how long did it take to recover? Recover means the total time it took to rectify damage, return system to last known good state, complete investigations and no longer lose revenue as a result of the incident.

| | Number of respondent organisations which lost time | | | | | Total respondent organisations which lost time |
|---|--|-------------|-------------------|-------------------|-------------------------|--|
| | Less than 1 day | 1 to 7 days | 8 days to 4 weeks | More than 1 month | May never fully recover | |
| Theft/breach of proprietary or confidential information | 5 | 5 | 1 | 1 | 3 | 15 |
| Unauthorised privileged access | 15 | 10 | 1 | 3 | 2 | 31 |
| Financial fraud | 3 | 2 | - | 4 | 2 | 11 |
| Telecommunications fraud | 4 | 2 | 1 | 2 | - | 9 |
| Sabotage of data or networks | 2 | 3 | 1 | - | - | 6 |
| Web site defacement | 9 | 11 | - | - | - | 20 |
| Denial of service attack | 25 | 15 | 2 | 1 | - | 43 |
| Degradation of network performance associated with heavy scanning | 13 | 11 | 2 | 4 | 1 | 31 |
| Wiretapping | 1 | 1 | - | - | - | 2 |
| Telecom eavesdropping | 1 | 1 | - | - | 1 | 3 |
| Virus, worm, trojan infection | 59 | 54 | 9 | 2 | 2 | 126 |
| Laptop theft | 17 | 40 | 26 | 6 | 6 | 95 |
| System penetration by outsider | 2 | 15 | 4 | 1 | - | 22 |
| Unauthorised access to information by insider | 4 | 7 | - | 2 | 2 | 15 |
| Insider abuse of internal computer resources, access or e-mail | 44 | 18 | 6 | 5 | 2 | 75 |
| 2003: 175 respondents/81% | | | | | | |

Detecting covert forms of attack with any degree of confidence, particularly in networks which do not restrict or monitor inbound and outbound connections to essential services is not an easy task. These difficulties are compounded by hacker techniques which seek to evade detection, obfuscate and conceal evidence of intrusion. Relying too heavily on intrusion detection system (IDS) technologies to the exclusion of other counter-measures can also compound the difficulties of detecting an intrusion. IDSs tend to exhibit a certain proportion of false positives and false negatives. Evaluating whether an intrusion alarm is a false positive or a real event can be a resource intensive task, especially in an environment where network attacks occur on an almost continuous basis. Failure to follow up means that a real attack could be easily hidden amongst the noise of the false positives. Conversely, a low false positive rate increases the risk that a real intrusion will not be detected. Finally, gaining the expertise and skill to interpret anomalous log records and apply forensic computing techniques is a specialist field generally beyond the scope of most individuals without IT security qualifications.

Given some of these challenges, it is not surprising that 16% of respondent organisations sought outside assistance to help with incident recovery and response. The following is one such case.

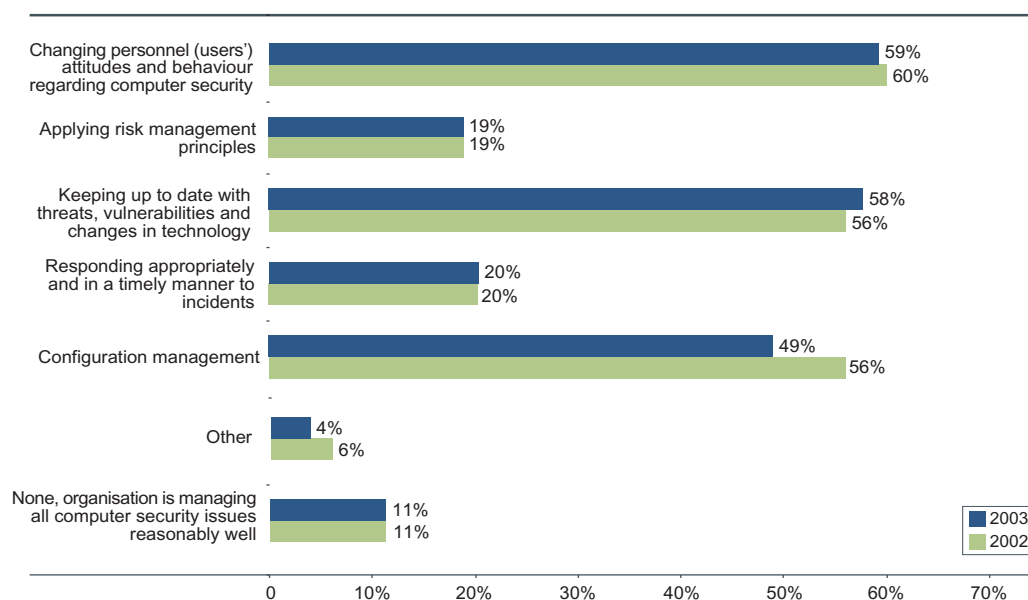
Difficulties detecting, investigating and responding to computer security incidents - Stephen Ford, Deloitte Touche Tohmatsu

Deloitte Touche Tohmatsu provided assistance to an Australian SME (the client) who discovered anomalies in their information systems which led them to believe their system may have been compromised. Upon being locked out of critical servers, the client discovered that timestamps and some administrator passwords had changed. Using forensic analysis techniques, Deloitte examined intrusion detection logs, firewall logs and system audit trails. Further vulnerability analysis was performed against various servers and network devices and hacking techniques were used to extract information about the nature and causes of the anomalous events.

The likely causes of the anomalies were assessed to be some procedural errors coupled with system internal errors triggered by a denial of service (DoS) attack. Evidence of regular malicious activity directed at the client's systems from a wide range of IP addresses was also present. This activity comprised a wide range of Microsoft IIS attacks, server-specific denial of service attacks and port scanning. SYN flood DoS attacks appeared to have triggered the timestamp anomalies. By reviewing the types of attacks occurring and examining the log and target files on the target systems, it was shown the attacks had not succeeded in reaching their intended destinations. By providing an understanding of how the suspicious events occurred, the client was given assurance that, although malicious activity had been occurring, no compromise had taken place. A number of recommendations were made to increase the security of the client's systems through network redesign, device configuration and procedural modifications.

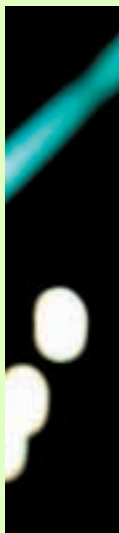
The challenges associated with managing IT security issues, particularly in the area of incident detection and response, can be compounded for organisations with a small IT team. The breadth of expertise and skill which is needed is not necessarily less than for a larger organisation, yet fewer people are available to acquire what are essentially specialist skills.

What aspects of computer security management does your organisation find most challenging or problematic?



Source: 2003 Australian Computer Crime and Security Survey
2003: 206 respondents/96%, 2002: 88 respondents/93%

For a second year, the three areas which respondent organisations consider to be the most problematic or challenging is changing users' attitudes and behaviours regarding their computer security practices (59%), keeping up to date with threats, vulnerabilities and changes in technology (58%) and configuration management (49%). The following case highlights the consequences of not keeping up to date with threat information.



Domain name hijacking and compromise and sabotage of system files

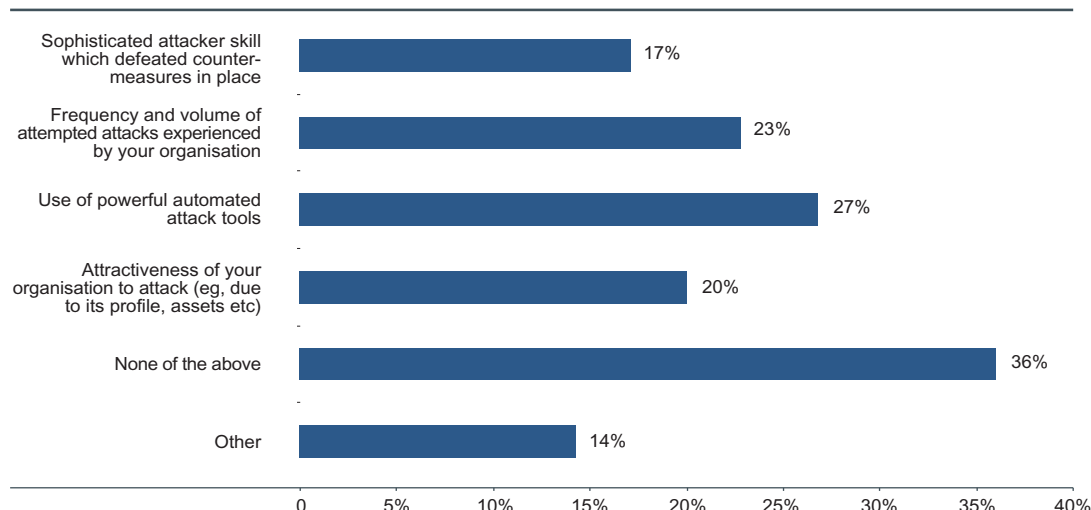
The following case study outlines events which commenced in 2000 and which took many months to investigate before the case was closed in 2002. In 2000, a web hosting company's server was attacked using a known vulnerability in Apache web server, enabling the attacker to obtain root privileges. The attacker deleted all files on the hard drive including backups made to a second hard drive connected to the same computer.

The computer was re-built and was subsequently attacked, exploiting the same vulnerability again. On the second occasion, the attacker took control of the company's email system and sent defamatory emails to numerous people. Using the compromised email system, the attacker sent an email to .au Domain Administration Ltd (auDA) claiming the company had forgotten its password to its auDA account. This account enables organisations to modify their domain name details for inclusion in the top level domain name servers. auDA reset the company password and sent the password back to the company via email which the attacker intercepted. With access to the company's account at auDA, the attacker transferred the ownership of the company's domain name to another party. This had the affect of denying or redirecting inbound Internet access to the company.

Initial investigations and identification of the source of the attack was impeded because the web hosting company did not have logging in place. Subsequent investigations showed malicious activity directed from the IP address of a competitor Internet service provider/web hosting company and the IP address of a home computer used by the two owners of the same ISP. Because both individuals had access to the computers at both premises it was not possible to mount a case 'beyond reasonable doubt' against either suspect so the case was dropped. A personal grievance between the parties who were personally known to each other was the primary motive suspected.

The case demonstrates the ease with which network systems connected to the Internet can be compromised at a privileged level by failing to patch known vulnerabilities. As well as stealing and destroying important system data, attackers can damage a company's reputation and sabotage its operations by hijacking its company's on-line identity, either by launching attacks from the compromised site or, in this case, sending defamatory emails from the company and hijacking its domain name. The case also demonstrates the importance of ensuring that back up systems and log files are stored separately and securely to aid with recovery and investigation in the event of a system compromise. The most worrying aspect of this case is that the web hosting company failed to protect its systems properly after the first compromise occurred via a known vulnerability. As the task of applying a single patch is a relatively trivial exercise, it is more likely the company failed to keep abreast of all known vulnerabilities for the systems it was running.

In terms of the threat faced by your organisation, what factors may have contributed to those attacks which harmed your organisation in the last 12 months?



Source: 2003 Australian Computer Crime and Security Survey
2003: 175 respondents/81%

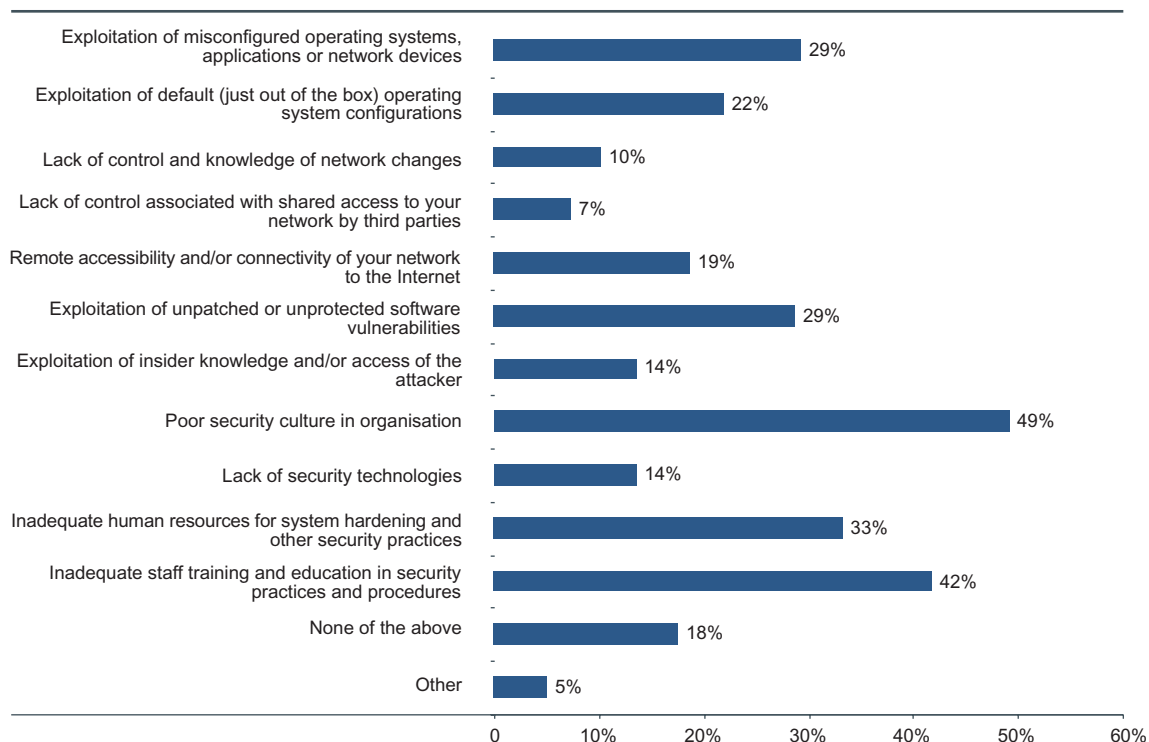
Computer network threats and vulnerabilities

The precursor to a harmful and deliberate attack on an organisation's information system requires the existence of a person with both the capability and intent to harm that information system. Even indiscriminate damage caused by self-propagating malicious code is the result actions of the person who authored and/or released the code. Persons with the desire to harm but who otherwise would have little capability, can now do so utilising readily accessible, powerful and easy to use attack tools. Similarly, persons who have the capability to conduct attacks may not be inclined to do so unless they perceive some value or reward for doing so. What motivates an individual to attack one organisation over another will always vary but reasons are likely to fall into one or more of the broad categories mentioned earlier. However, the mere existence of a threat is not sufficient for an attack to occur. The attacker must find a vulnerability to exploit, or a way to defeat counter-measures in place. Sometimes a single vulnerability can contribute to an attack but often it is the accumulation of multiple vulnerabilities which combine to allow attackers to succeed.

Generally, the actions that can be taken to minimise the threats is limited; however much more can be done to minimise vulnerabilities. To this end, organisations appear to be applying a broad range of technology counter-measures and a range of security policies and procedures to complement and provide a layered or in-depth approach to security. Despite the use of counter-measures (technical and procedural), in many cases respondents have vulnerabilities which they assess may have contributed to the occurrence of successful attacks on their systems. Twenty-nine percent thought attackers may have exploited misconfigured operating systems, applications or network devices; 22% thought attackers may have exploited 'just out of the box' operating system configurations; and 29% thought attackers may have exploited unpatched or unprotected software vulnerabilities. The failure to patch vulnerable systems is probably the single most important factor which contributes to remote privileged access attacks primarily because attackers use powerful scanning tools to find vulnerable machines wherever they are accessible through the Internet.



In terms of the nature of your organisation's vulnerabilities, what factors may have contributed to those attacks which harmed your organisation in the last 12 months?



Source: 2003 Australian Computer Crime and Security Survey
2003: 177 respondents/82%

Challenges and conflicting priorities with systems management - Gary Gaskell, System Administrators Guild of Australia (SAGE-AU)

SAGE-AU security specialist, Gary Gaskell believes that challenges faced by system and network administrators seem to be ever increasing. "Increasing network interconnection, security vulnerability announcements, uptime requirements, business dependence on information technology and technology proliferation all contribute to these challenges. System administrators are also expected to administer more systems with fewer staff."

But not all changes are bad. According to Gaskell, many of the new technologies and integrated services offer greater convenience. Most vendors now provide detailed guidance on secure configuration and operation. Previously, the secure configuration and operation of their systems was more "black art" and, in this area, the life of a system administrator has become a bit easier. The change to a disclosure policy by vendors is also applauded. Previously vendors kept the existence of known security vulnerabilities from their customers, which meant that often hackers/crackers knew about the weaknesses before system administrators.

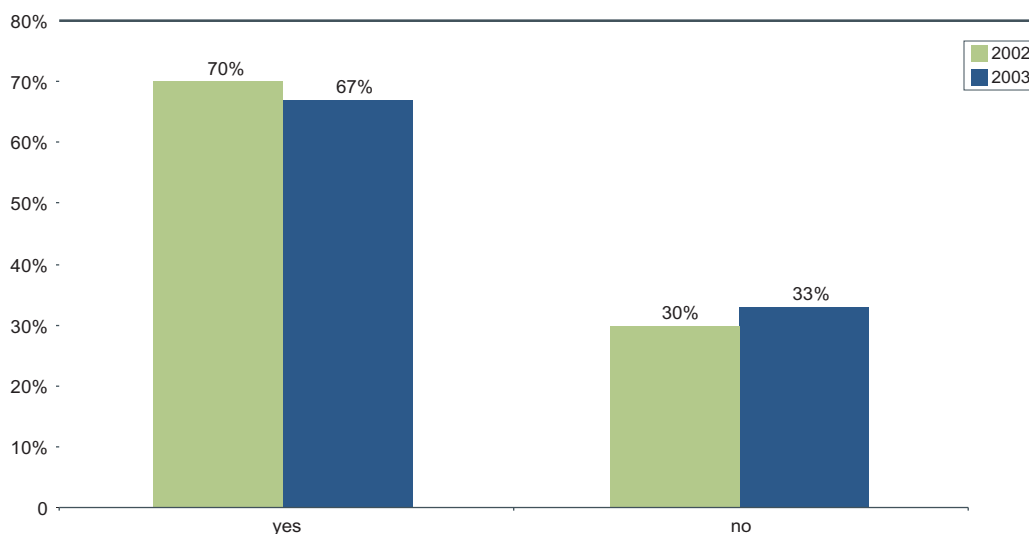
The changing operational environment also amplifies the conflict between the traditional change control process and the need to quickly repair a system with a known security vulnerability. This is especially true when an exploit tool has been publicly released. According to Gaskell, "too many organisations are slow to realise that their change control processes are not keeping up with the rate at which information about vulnerabilities is publicly disclosed and automated exploitation worms are released into the wild. Organisations must seriously consider whether the risk of system compromise is higher than the risk of downtime due to a flawed patch. The speed at which vulnerabilities are being exploited is such that the risk of compromise is often becoming the higher risk."

Systemic vulnerabilities are harder to address

As was the case involving the web hosting company, sometimes only a single vulnerability needs to exist for an attack to occur. Often, a series of vulnerabilities combine to make attempts by attackers to harm an organisation's network possible. In many cases, respondents acknowledged the presence of systemic vulnerabilities as a potential contributing factor to incidents which harmed their systems: lack of control and knowledge over network changes was cited by 10% of respondents; and poor security culture in their organisations was cited by 49%. Attempts to address these vulnerabilities are likely to require a multi-faceted approach and an organisational wide commitment, particularly from senior management. Information security standards can provide a useful guide for organisations that want to initiate, implement or maintain information security in their organisation,⁵ and can help address systemic vulnerabilities.

Nineteen percent of respondents thought the external connectivity of their organisation's network to the Internet may have contributed to those attacks which harmed their systems; 7% thought their connectivity to other external parties' networks over which they had no control may have been a contributing factor. Organisations which connect to the Internet or other people's networks should conduct an assessment of the risks involved, and if accepted, have a plan to manage those risks.

As a result of computer security concerns or incidents, has your organisation increased computer security-related expenditure in the last 12 months?



Source: 2003 Australian Computer Crime and Security Survey
2003: 130 respondents/60%, 2002: 90 respondents/95%

Threats to data confidentiality when extending the corporate network boundaries - Rowan Price, Information Systems Audit and Control Association (ISACA)

Nine percent experienced the theft or breach of confidential information electronically and 5% suffered a financial loss from this type of incident. For a few organisations, the loss of confidentiality was such that they felt they may not ever fully recover. Theft or breach of proprietary or confidential organisation information can occur in numerous ways.

ISACA information security specialist, Rowan Price, believes that common work practices may be contributing to breaches in data confidentiality. According to Price, the almost universal use of the Internet and email has extended the definition of our networks into locations previously unconsidered. In an effort to accommodate flexibility in working hours and reduce operational costs many workers and companies are resorting to a defacto conversion of the home to a work environment. While the concept of working from home is not new, what is new is that many companies expect workers to provide their own equipment so they can work from home.

According to Price, "sending electronic business documentation home by email or other means may appear expedient

and support the requirements of the accounting department, but this exposes the organisation's information to significantly greater risk from breaches to data confidentiality." Implementing complicated and expensive controls on the corporate/business network will be undermined if the same information is transferred insecurely and kept in an inherently insecure and untrusted environment - ie, the home PC.

The transfer of information to the home environment may breach confidentiality by shared access to confidential information by other household occupants. Where Internet connectivity to the home PC is present, the PC is likely to be vulnerable to a broad range of remote forms of attack that could compromise data confidentiality. Moreover, it is unlikely that home users will have the skill to secure and maintain these systems to the level required of the corporate network. Where the business information includes 'personal' information, compliance with the *Privacy Act 1988* may be breached if the home PC is not properly secured.

Often the most overlooked aspect of a working from home arrangement is the issue of gaining legal access to information created or stored on equipment not owned by the organisation. In the event of a security incident occurring, the organisation needs to be able to investigate potential sources of compromise. The refusal of an employee to grant access to private computing equipment exacerbates the risk, particularly if the owner is not the employee. The right of an employee or rightful owner to expect that information of a personal nature stored on the computer remain private is likely to pose a serious impediment to any investigation where the organisation seeks to access or attempt to access the computer.

Price said if the risk of allowing the removal of organisational information to home PCs is accepted, it can be better managed by adopting appropriate policies, procedures and controls. Some of these include:

- encrypting organisational information during transmission and subsequent storage on private computers;
- automatically updating anti-virus and firewall software (approved by the organisation) via trusted connections to service providers each time the home PC connects to the Internet;
- requiring that confidential information may only be sent to email accounts which are not shared with other household or family members; and
- providing comprehensive and regular awareness programs to all staff working from home.

Reporting computer security attacks

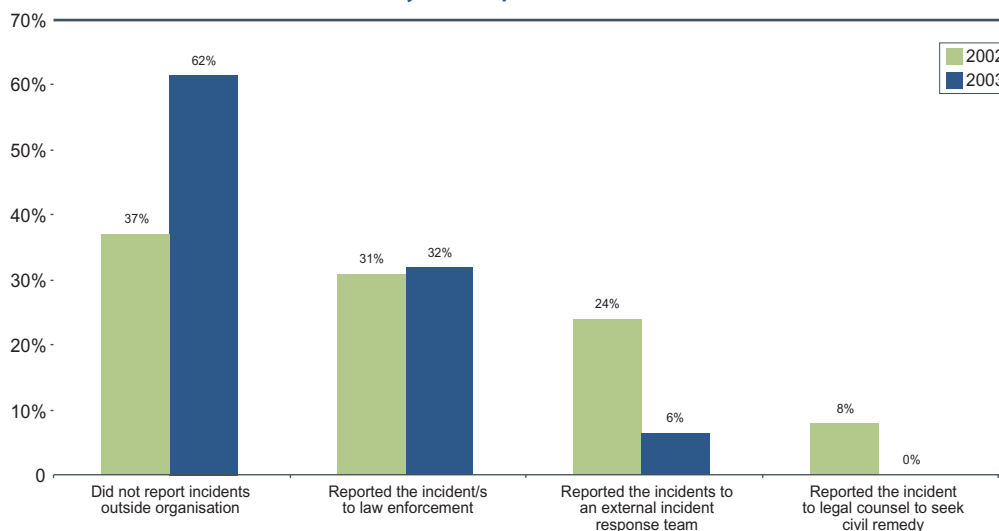
For 2003, while the percentage of those reporting to law enforcement agencies has remained constant, no respondents reported pursuing civil legal remedies. The potential for attacks to be routed through third parties is apparent from the 26% who thought their systems were compromised in order to attack other parties with a degree of anonymity. Given some of the difficulties in pursuing criminal action – such as jurisdiction, positively identifying the person using the IP address, or even being able to find the correct source IP address when the attack is routed through a variety of networks around the globe – we are likely to see greater interest in pursuing civil legal action against softer third party targets – targets in their own right or unwitting participants.

Civil liability for e-security breaches - Phillip Hourigan, Deacons

Phillip Hourigan, a partner at Deacons law firm believes that "legal risks associated with ineffective security is becoming a primary driver of e-security strategies. The touchstone for determining legal liability is generally whether an organisation can show that it took reasonable steps to maintain e-security. Heightened awareness of the range of attacks and what could be done to prevent them has the unfortunate side effect in that it has raised the bar in relation to what will be regarded as 'reasonable steps'. For those that suffer an electronic attack the legal questions tend to focus on 'who can be sued'. However, another important line of enquiry following an attack now is 'who can sue you.'"

Relevant legal considerations for breaches of e-security include analysis of contractual relationships and contract terms, expressed or implied warranties, trade practices implications, liability of directors or other officers, trespass or other similar remedies in tort, vicarious liability for the acts of employees, the impact of continuous disclosure requirements for listed entities and privacy. The list is not exhaustive but provides an indication of the complex legal issues that arise as a consequence of an attack.⁶ According to Hourigan, regardless of an organisation's profile or size, failure to comprehensively understand and then address civil liability risks borders on recklessness.

If your organisation experienced harmful computer security incidents, to whom did you report the incidents?



Source: 2003 Australian Computer Crime and Security Survey
 2003: 94 respondents/43%, 2002: 59 respondents/62%

Civil remedies - Ajoy Ghosh

Ajoy Ghosh, lecturer and consultant in cybercrime and forensics, believes that tort law (specifically the tort of negligence) may provide a more viable legal solution to prevent cyber crime than is possible under the criminal justice system. The threat of being sued for negligence is likely to pressure large market actors (eg, ISPs) to adopt socially valuable security measures that prevent cyber-criminals from plying their trade and more readily identifies them if they do. Proponents of a tort law framework cite the inadequacies of enforcement agencies to identify, locate and prosecute cyber-criminals coupled with the rapidly developing infrastructure and judicial conundrums of cyberspace.

From a victim's perspective, Ghosh believes the rationale for pursuing civil rather than criminal remedies offers a number of advantages which include:

- **Confidentiality** — the option of settlement means that corporations can guarantee that their involvement in the matter remains confidential, thus negating any bad publicity resulting from the publication of court proceedings.
- **Corporate liability** — the victim need not identify a particular individual as the computer hacker, since a corporation can be liable for damages either vicariously or through contributory negligence. This also provides the claimant with the ability to access significant damages.
- **Standard of proof** — is on the balance of probability and does not require evidence to be presented that is beyond reasonable doubt.
- **Timeliness** — if a settlement is negotiated, the victim can be compensated in a timely fashion, rather than having to wait for the completion of criminal actions.
- **Control and flexibility** — victims feel in control of the incident, with their own legal teams making key decisions, such as engaging expert resources. This also gives them the flexibility to agree to settlement conditions, including stopping the pursuit.

"The following case study is typical of the dozen or so instances where I have advised either the litigant or respondent in a civil action. Whilst the events and settlement are factual, the names and dates have been changed to obfuscate the involved parties," said Ghosh.

Case study - civil suit for alleged hacking by corporate competitor

On 19 February 2002, the CEO of a regional ISP (let's call it "SmallISP.com.au") received a telephone call from an unknown person who introduced himself as a salesman from a national ISP (let's call it "BigISP.com.au").

The caller stated that he had a listing of about 1,200 clients of SmallISP and would start calling them unless he was paid a sizeable amount. When questioned about the origin of the list, the caller stated that a colleague had hacked into SmallISP and retrieved the monthly billings file. The CEO and a system administrator immediately queried their firewall and other Internet connected computers but were unable to find any evidence of an intrusion.

On 21 February, SmallISP performed scheduled upgrades of several computers, including the firewall and primary web-server. Over the following week, about 50 of SmallISP's customers rang to say that they were contacted by BigISP who knew exactly what they were paying each month and were offered a cheaper deal to move their business.

SmallISP's legal team were brought in and engaged Ghosh as an expert. After their system upgrade, SmallISP had disposed of some equipment, so not all the necessary evidence could be reconstructed. Ghosh, however, was able to reconstruct certain log files that showed evidence that on Valentine's Day an intruder had downloaded the monthly billings file. Further, there were several prior intrusions and they all either originated from, or passed through, BigISP's network. The prior intrusions corresponded to times that SmallISP's services were mysteriously interrupted, causing SmallISP to schedule the upgrade of 21 February.

The actual cost of the intrusions, including customer refunds for outages, the unnecessary system upgrade, salaries, technical and legal fees were estimated at about \$150,000. A forensic accountant estimated the cost of lost opportunity at \$20million. This included one significant contract that was lost after a Fortune100 customer trialled SmallISP's services, only to experience service interruptions – that corresponded to the system intrusions – and subsequently decided to award the contract to BigISP.

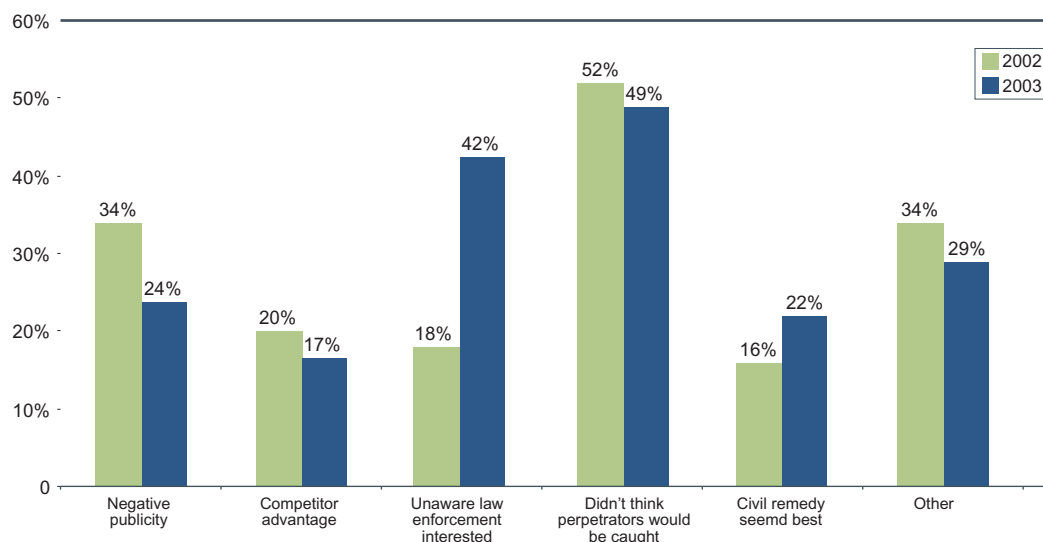
The police were called but they advised that:

- (i) the evidence was incomplete and an expert witness could create reasonable doubt over the authenticity of the available evidence; and
- (ii) without evidence identifying an individual employee of BigISP, they were powerless to act; and
- (iii) even if they could, there was no hope of recovering substantial costs from a hacker with few means.

SmallISP's legal team was convinced that, on the balance of probability, the evidence showed that either an employee of BigISP hacked into SmallISP or BigISP had negligently allowed someone to use their computer network to hack into SmallISP. They met with senior executives at BigISP and put forward the evidence and a claim for damages based on BigISP's contributory negligence for allowing the hacker to use their network. They also put forward further evidence that would allow BigISP to identify the computer hacker if it was an employee.

Within a month of the original telephone call, BigISP settled the claim for \$5 million, stipulating two conditions: confidentiality and that SmallISP stop further attempts to identify the individual computer hacker. SmallISP agreed since the sum covered the actual losses and provided significant capital to pursue new opportunities.

Most important reasons organisations did not report computer security incidents to law enforcement



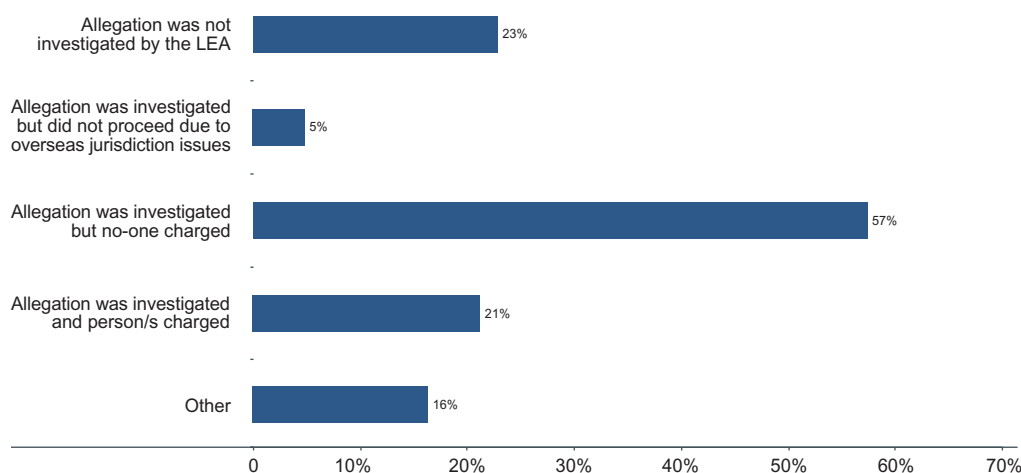
Source: 2003 Australian Computer Crime and Security Survey
2003: 107 respondents/50%, 2002: 27 respondents/28%

Note: Respondents were asked to give a ranking of 1 - 5 (1 for least important and 5 for most important) for each category.

Reporting to law enforcement agencies

For a second year in a row, the prime reason organisations failed to report computer security incidents is the perception that it will be difficult to catch the perpetrators. Of those computer security incidents reported to law enforcement agencies, in 23% of cases the computer security incident was not investigated by police and in 57% of cases the allegations were investigated but no persons were charged.

Outcome of incident allegations reported to law enforcement agencies



Source: 2003 Australian Computer Crime and Security Survey
2003: 61 respondents/28%



Decisions by police not to investigate a reported computer security incident and police investigations which result in no persons being charged usually occur for any of the following reasons: whether the incident falls under relevant legislation; the quality, or the expected quality, of the forensic evidence and the likelihood of achieving a successful prosecution on that evidence. Lack of evidence may be due to inadequate logging by the complainant or the ISP whose connection that attacker used to launch the attack. The use of methods by attackers to conceal their identity such as - proxies, Internet cafes, anonymisers and free web based email accounts also limit the ability of law enforcement to trace attacks to their source. Overseas companies, including ISPs, require court orders to provide basic information to identify suspects who hold system accounts with the company; and a high level of criminal burden of proof (beyond reasonable doubt) is required to prove the identity of a person who actually committed the offence, when numerous persons may have had access to a computer.

Legislative interpretations applied to the actual facts of an incident may be required to determine whether or not a criminal offence has even been committed. In Western Australia, the definition provided for "things capable of being stolen", under Section 370 of the *WA Criminal Code*, does not include "information". Hence a situation where a person copied a client database from his former place of employment may in fact not be a criminal offence. Employers, involved in such a situation, may either have to consider civil avenues of redress; or alternatively consider whether offences other than stealing could have application to the facts of the case (for example Unlawful Operation of a Computer System, Section 440A of the *Criminal Code*).

Strategies for fighting e-crime

Where Internet connectivity exists, electronic attacks may be sourced from, and routed through, almost any country in the world, and often quite deliberately in an attempt to obfuscate the true source of the attack and make investigation difficult. Law enforcement agencies in Australia and internationally have many established ways for cooperating when investigating matters that expand beyond national borders. These methods encompass both informal and formal processes. In addition, there are two specific computer crime related protocols which can be used to quickly pursue computer crime and electronic evidence matters offshore through Interpol and the G8 Hi-Tech crime points of contact. In addition, the AFP maintains an extensive international liaison officer network to provide a direct point of contact with overseas police forces, which covers most countries of the world.

In November 2002, Australian Police Ministers endorsed the need for an Australian Hi-Tech Crime Centre. This Centre, which is expected to be operational in the second half of 2003, will be hosted by the AFP and staffed by representatives from all police jurisdictions. The Centre's role will be to:

- provide a coordinated national approach to combating hi-tech crimes of a serious, complex and/or multi-jurisdictional nature generally beyond the capability of one jurisdiction;
- assist in improving the capacity of all participating jurisdictions to deal with e-crime matters; and
- support efforts to protect the National Information Infrastructure.



METHODOLOGY

AusCERT would like to thank the Computer Security Institute for permission to use questions from its annual *CSI/FBI Computer Crime and Security Survey* in this survey. Unfortunately, a copy of the 2003 *CSI/FBI Computer Crime and Security Survey* was not available for comparison of USA and Australian trends at the time of writing.

Survey questionnaires with business reply envelopes were sent to chief information security officers or their equivalents of the top 350 Australian public companies. These companies were invited to complete the survey on-line via a secure web site or return the questionnaire via a reply-paid envelope. Responses were also sought from a number of industry groups whose members were invited to complete the survey via the secure web site. Each industry group was allocated a generic access code to help ensure the integrity of anonymous survey data submitted electronically. Responses to the survey totalled 214, which included 88 hard copy submissions and 126 on-line submissions. All responses are anonymous.

Being both a voluntary and anonymous survey, there are limitations as to the level of rigour which can be applied to ensure the results are scientifically valid. We do not claim that this survey meets such a standard. For example, there are likely to be discrepancies associated with respondents' interpretation of questions, errors in respondents' recollections of events or difficulties in determining which of the answer options listed were actually applicable to the respondent's organisation. One senior public sector official commented that they would like to know the answers to the survey questions themselves but simply did not have a full appreciation of the extent of their exposure or the number of computer security incidents because they outsourced their information services.

The value of this survey is that it depicts the best effort responses from a broad range of respondent organisations in a given period of time. The results provide a useful benchmark for various forms of computer crime and abuse, which with the exception of a survey by the Australian Bureau of Statistics,⁷ would not otherwise be available.

SURVEY

PARTNERS

Federal Agent Alastair MacGibbon

Coordinator
High Tech Crime
Australian Federal Police
GPO Box 401
CANBERRA ACT 2601

Detective Superintendent Tony Rankine

OIC
Commercial and Electronic Crime Branch
South Australia Police
Box 1539, GPO
ADELAIDE SA 5001

Detective Sergeant Ted Wisniewski

OIC
Computer Crime Investigation
Commercial Crime Division
Western Australia Police
Level 7, 233 Adelaide Terrace
PERTH WA 6000

Detective Inspector Ken Webster

Major Fraud Investigation Group
Crime Operations Branch
Queensland Police Service
GPO Box 1440
BRISBANE QLD 4001

AusCERT

The University of Queensland QLD 4072
www.auscert.org.au
Tel 07 3365 4417

Michael Rothery

Senior Adviser
National Information Infrastructure
Attorney-General's Department (Sponsor)
Robert Garran Offices
National Circuit
BARTON ACT 2600



SURVEY

CONTRIBUTORS

Ajoy Ghosh, Lecturer and Consultant in Cybercrime and Forensics

ajoy@law.uts.edu.au

Tel (02) 9908 3812

Phillip Hourigan, Partner, Deacons

phillip.hourigan@deacons.com.au

Tel (07) 3309 0865

Rowan Price, Information Security Specialist, Information Systems Audit and Control Association

debrowan@bigpond.net.au

Tel 0407 015 527

Stephen Ford, Account Director, Enterprise Risk Services, Deloitte Touche Tohmatsu

stephford@deloitte.com.au

Tel (02) 9322 7476

Gary Gaskell, System Administrators Guild of Australia

gary.gaskell@member.sage-au.org.au

Tel 0438 603 307

NSW Police, Computer Crime Investigation Unit, Fraud Squad

Tel (02) 9269 9776

-
- ¹ Office of Strategic Crime Assessments & Victoria Police, *1997 Computer Crime and Security Survey*
- ² Deloitte Touche Tohmatsu & Victoria Police, *Computer Crime and Security Survey 1999*
- ³ AusCERT, NSW Police, Deloitte Touche Tohmatsu, *2002 Australian Computer Crime and Security Survey*
- ⁴ Section 440A, "Unlawful Operation of a Computer System", *Western Australia Criminal Code*
- ⁵ Standards Australia, AS/NZS ISO/IEC 17799:2001 *Information technology – Code of practice for information security management*, page 1
- ⁶ For a comprehensive overview of the legal consideration in e-security refer to Gamertsfelder, McMillan, Handelsmann and Hourigan "E-security" *Report 4 in the series "E-commerce: The Implications for the Law*, Lawbook Co 2002.
- ⁷ Australian Bureau of Statistics (2003) *Business Use of Information Technology*, 2001-02, 8129.0