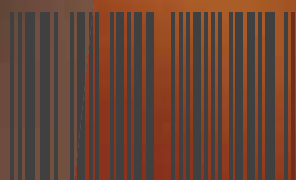
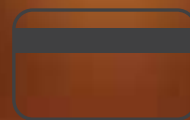


certification »



CRIME

COMPUTER CRIME & SECURITY

SURVEY

ISBN 1-864-99773-7

Foreward

The *Australian Computer Crime and Security Survey* provides a unique insight into the computer security operations of Australia's private and public sector organisations, ranging from large corporations to single person enterprises, spanning a range of industries and businesses. The results show that many of the problems faced are common amongst respondents.

We believe that the analysis provided is useful to a broad audience: IT security professionals who play such a vital role in modern commerce; managers wishing to benchmark their organisations; companies offering technical solutions to problems highlighted; and the community more generally who rely on secure functioning businesses.

Police find the survey useful because it highlights vulnerabilities (and therefore potential vectors for victimisation); because it goes some way to quantifying the victim base; and because it gives us some indication of what businesses think and how they respond to incidents. Australian policing is committed to pursuing crimes of this nature and the formation of the Australian High Tech Crime Centre in July 2003 is just one illustration of that desire. The fact that all Australian police services banded together to support AusCERT's efforts in this survey is another.

We hope the survey will be used, where appropriate, as a catalyst to support the positive changes needed to eliminate some of the more easily preventable security incidents within networked organisations.

Finally, we would like to thank respondent organisations that took the time to answer the survey and for their honesty in providing responses to a range of questions about their organisation's information security situation and arrangements. Without their support and cooperation this survey would not be possible.

Alastair MacGibbon

Director
Australian High Tech Crime Centre





Introduction

The Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP), New South Wales Police, Northern Territory Police, Queensland Police, South Australia Police, Tasmania Police, Victoria Police, Western Australia Police and AusCERT have partnered to produce the *2004 Australian Computer Crime and Security Survey*. AusCERT is the national computer emergency response team for Australia based at the University of Queensland, and a leading CERT in the Asia-Pacific region. Now, with every Australian police law enforcement agency involved 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 2004 survey has been adapted from the *CSI/FBI Computer Crime and Security Survey*¹ and includes several new questions designed to deepen our understanding of the key factors which contribute to electronic attacks and other forms of computer crime. Where relevant, this survey compares its findings to the *2002 Australian Computer Crime and Security Survey* conducted by AusCERT, Deloitte Touche Tohmatsu and NSW Police in 2002² and the *2003 Australian Computer Crime and Security Survey*.³

With representation from a broad cross section of Australian industry, including public and private sector organisations, this survey provides the most up to date and authoritative analysis of computer network attack, crime and computer access 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.

AusCERT would like to thank the AFP, the Australian government's Attorney-General's Department and the Department of Communications, Information Technology and the Arts for supporting the production of this survey.



EXECUTIVE

SUMMARY

The key findings for 2004 are:

Electronic attack, computer crime, computer access misuse and abuse trends

- More respondent organisations experienced electronic attacks that harmed the confidentiality, integrity or availability of network data or systems (49% in 2004 compared to 42% in 2003).
- Most of these attacks were again sourced externally (88%) compared to internally (only 36%), but fewer respondents experienced external attacks compared to 2003 (91%).
- Infections from viruses, worms or trojans were the most common form of electronic attack reported by respondents for the third consecutive year. They were the greatest cause of financial losses and accounted for 45% of total losses for 2004.
- The next most common causes of financial loss are laptop theft and abuse and misuse of computer network access or resources.
- Average annual losses for electronic attack, computer crime, or computer access misuse or abuse increased by 20% to \$116,212 per organisation compared to 2003.
- As a percentage, more critical national information infrastructure (CNII) organisations reported experiencing harmful electronic attacks (50%) compared to non-CNII organisations (42%).
- On average, losses reported by CNII organisations (\$98,685), were almost double average losses for non-CNII organisations (\$56,531).

Readiness to protect and manage the security of IT systems

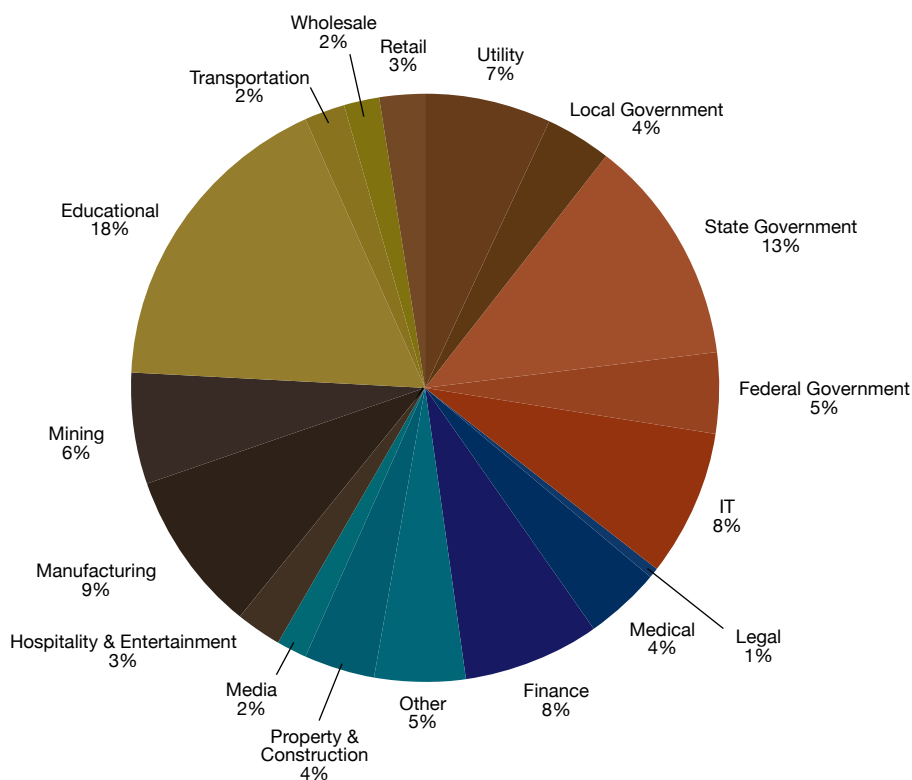
- The readiness of organisations to protect their IT systems has improved in three key areas: the use of information security policies, practices and procedures; the use of information security standards or guides; and the number of organisations with experienced, trained, qualified or certified staff.
- Despite these improvements, fewer respondent organisations reported they were managing all computer security issues reasonably well (only 5% in 2004 compared to 11% in 2002 and 2003);
- The need for greater understanding of, or support for, IT security issues from senior management was important to 45% of respondents.
- Unpatched or unprotected software vulnerabilities (reported by 60% of respondents) and inadequate staff training and education in security practices (reported by 49% of respondents) were identified as the two most common factors which contributed to harmful electronic attacks.
- The most common challenges and difficulties respondent organisations faced were changing user attitudes and behaviour (reported by 65% of respondents) and keeping up to date with information about the latest computer threats and vulnerabilities (reported by 61% of respondents).
- Thus, the efforts being made by respondent organisations to improve their readiness to protect their systems appear to be insufficient to cope with the changing nature of the threats and vulnerabilities they are exposed to—most specifically this includes the increased number and severity of system vulnerabilities; and the number, and rapid propagation, of Internet worms and viruses.

WHO WE ASKED

THEIR PROFILE

Survey respondents again represent a broad range of industry sectors, including from the public and private sectors. Over 17 different private industry sectors, plus local, state and federal government sectors are represented. This year, the industries with the greatest representation are the education sector (18%), the State government sector (13%) and manufacturing sector (9%).

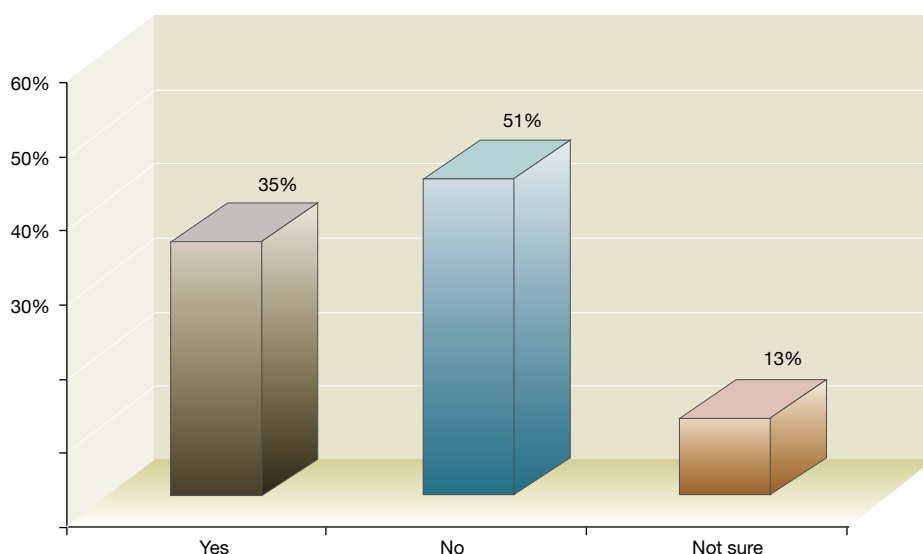
Respondents by industry sector



Source: 2004 Australian Computer Crime and Security Survey
2004: 199 respondents/83%

Thirty-five percent of respondents consider their organisation to be part of the critical national information infrastructure (CNII). These organisations, by definition, are those which provide essential telecommunications, banking, power and water services (to name a few) and have information systems that are critical to the supply and distribution of these services, which "if destroyed, degraded or rendered unavailable for an extended period, [would] impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defence and ensure national security."⁴ (See "How did critical national information infrastructure organisations fare compared to others?" page 33).

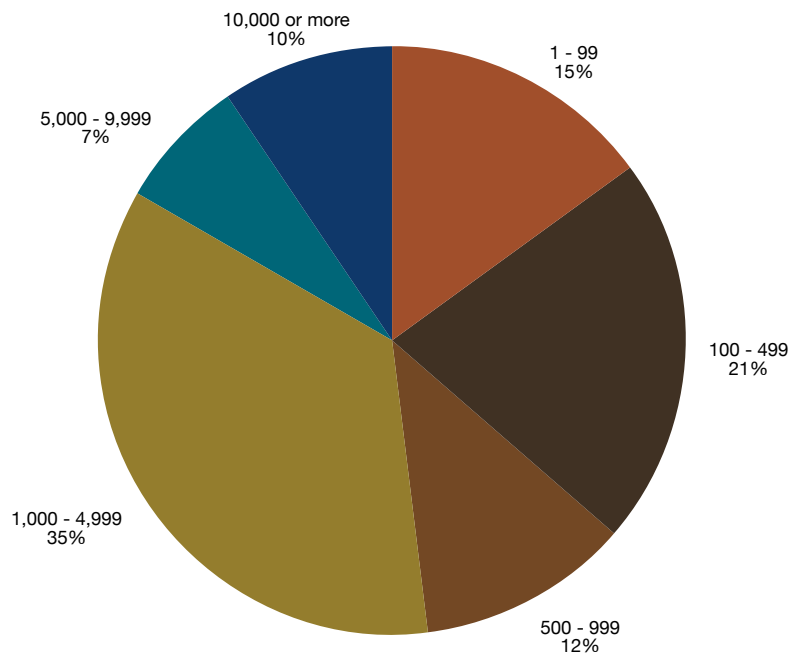
Do you consider your organisation to be part of the critical national information infrastructure?



Source: 2004 Australian Computer Crime and Security Survey
2004: 239 respondents/99.6%

Most respondent organisations were large organisations in terms of employee numbers and/or in terms of annual income or expenditure. Fifty-two percent of respondents come from organisations with 1,000 or more employees and 17% have 5,000 or more employees. Small to medium organisations are also well represented; 15% belong to organisations with one to 99 employees; and 33% belong to organisations with 100 to 999 employees.

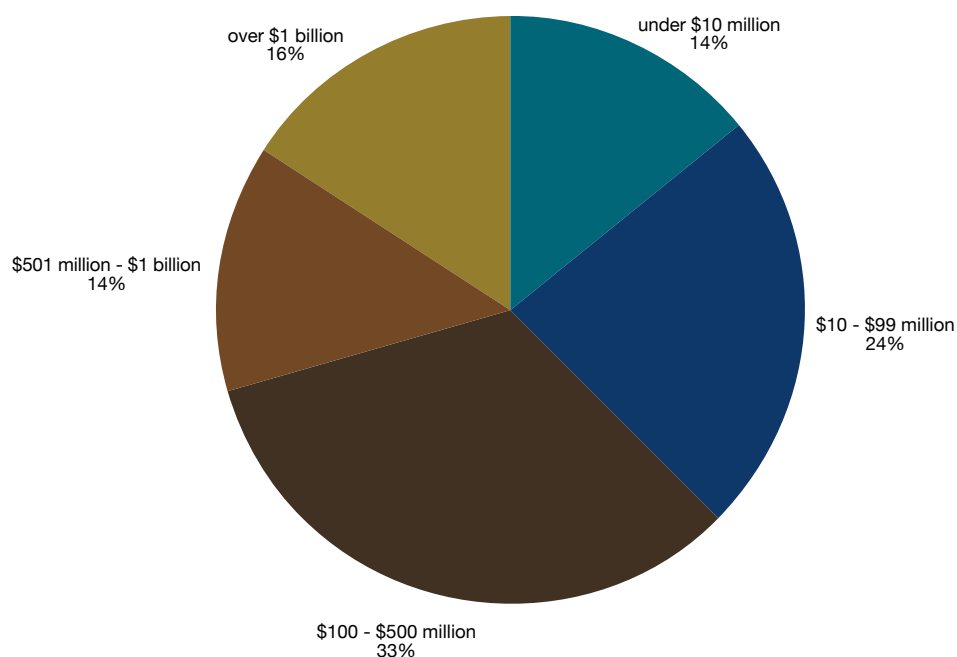
Respondents by number of employees



Source: 2004 Australian Computer Crime and Security Survey
2004: 240 respondents/100%

Thirty percent of respondent organisations have income or expenditure of \$501 million or more; 16% have income/expenditure of over \$1 billion. Fifty-seven percent have income or expenditure of between \$10 million to \$500 million annually. With such wide representation, the *2004 Australian Computer Crime and Security Survey* is proving to be a benchmark survey for the Australian business sector in its field.

Respondents by gross annual income/expenditure



Source: 2004 Australian Computer Crime and Security Survey
2004: 234 respondents/98%



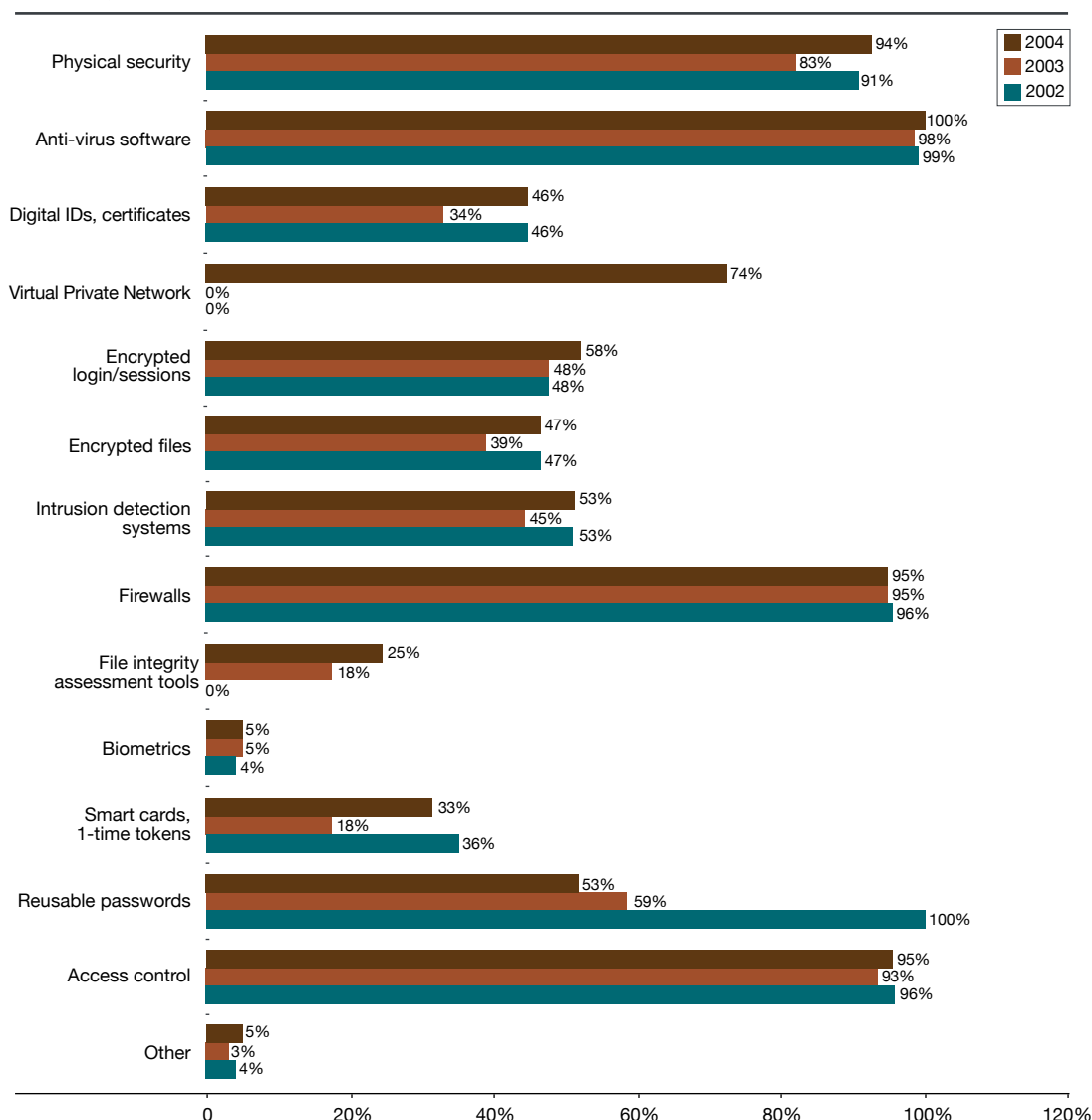
READINESS

TO PROTECT IT SYSTEMS

The percentage of respondents that use various types of security technologies is mostly consistent with previous years. However, the mere use or presence of such technologies is not a reliable indicator of the effectiveness of respondent organisations' information security. The firewall may be poorly configured, or the reusable passwords may be weak and easily cracked, or worse-may be kept on a sticky note beside the workstation. We know that anti-virus software, even if it is up to date, is not always capable of stopping a new fast spreading virus or worm infection; and the security of Virtual Private Networks is generally only as good as the security of the systems that facilitate the VPN connection.

Effective information security comes from applying security strategies "in-depth". Using a range of information security technologies, security policies and procedures can provide a high level of assurance in the confidentiality, integrity and availability of information systems.

Security technologies used

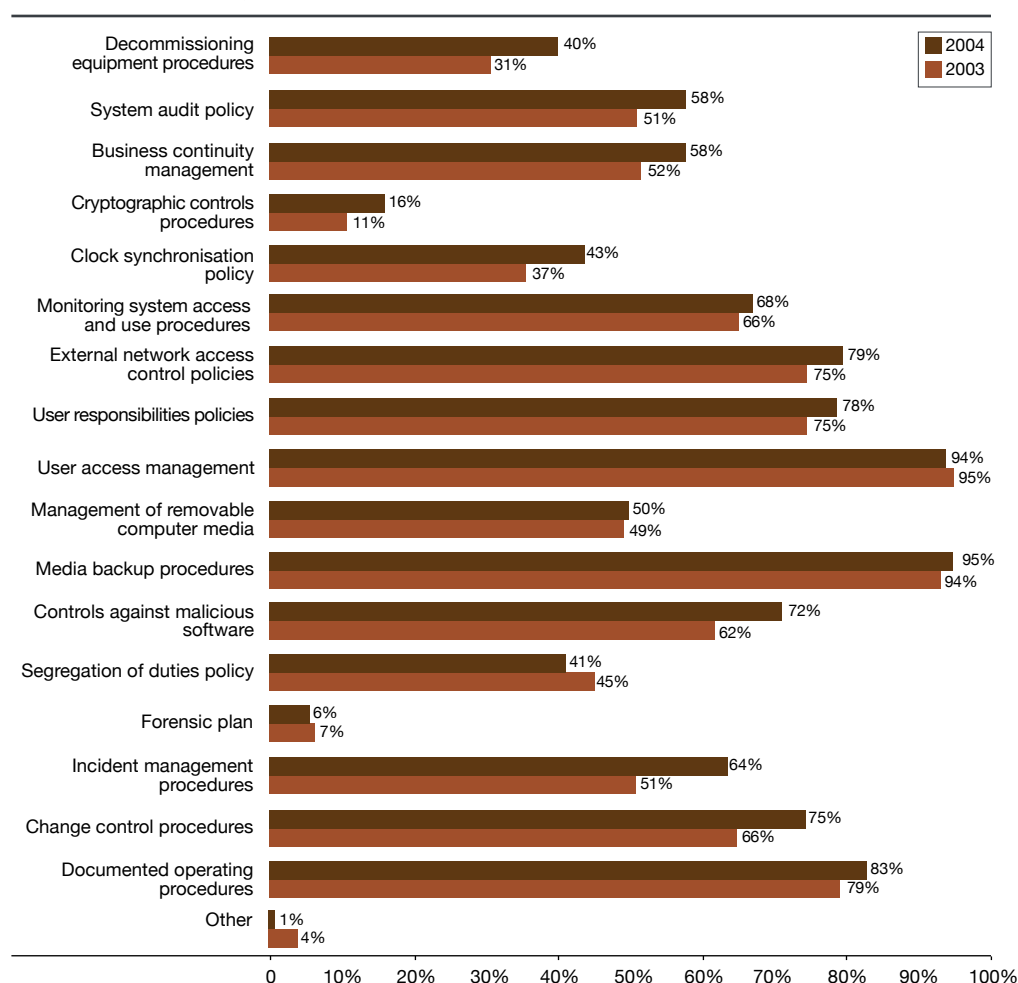


Source: 2004 Australian Computer Crime and Security Survey
2004: 182 respondents/76%, 2003: 214 respondents/100%,
2002: 92 respondents/97%

Note: In 2002, respondents were not asked if they used 'file integrity assessment tools' and in 2002 and 2003, respondents were not asked if they used 'Virtual Private Networks'.

Since 2003, there has been a small but consistent increase in the use of computer security policies and procedures across most categories. This is positive indication that there is greater recognition of the importance of having appropriate information security policies and procedures in place to more effectively manage network security. The biggest increases were in the use of incident management procedures (from 51% in 2003 to 64% in 2004); and procedures for controls against malicious software (from 62% in 2003 to 72% in 2004). While it is speculation, these increases may well be a reaction to poorly-handled security incidents or failing to prevent malicious code attacks in the first place.

Computer security policies and procedures used



Source: 2004 Australian Computer Crime and Security Survey
2004: 173 respondents/72%, 2003: 213 respondents/99%

Note: This question was not asked in the 2002 Australian Computer Crime and Security Survey.

For a second year, very few organisations reported having a forensic plan (6%) but the majority have incident management procedures (64%). Incident management procedures that help an organisation detect security breaches, investigate their cause and recover quickly can help reduce the impact of an incident. However, sometimes the cause of an incident may not always be clear, or, as the case below demonstrates, may not be as it first seems. A forensic plan can help investigators identify and confirm the real cause of an incident, particularly for cases where the attacker has concealed their tracks or used obfuscation techniques to fool investigators. Having a forensic plan that draws upon appropriate guidelines, such as Standards Australia's *HB171 - Guidelines for the Management of IT Evidence*,⁵ can help ensure an organisation's forensic investigations are conducted professionally and with integrity; and will help increase the chances of a successful criminal prosecution or civil litigation, should either of these options be chosen as an appropriate course of action. Moreover, a forensic plan that has been developed and implemented prior to an incident will enable a choice to be made and will be more effective than one developed "on the fly" during an incident.

The importance of sound evaluation of forensic evidence when litigating computer crime, Ajoy Ghosh, University of Technology Sydney

When litigating computer-related crimes, whether in the criminal or civil arena, solicitors face a major problem with evidence. The problem is that there is very little Australian case law to provide an interpretation of the existing legislation for determining if computer-based evidence is admissible. The situation is worse in the civil context, where litigation is being settled prior to the recording and subsequent publicity of a court hearing.

In our adversarial legal system, the onus is on either party to produce to the court, any evidence they feel is relevant and lawyers are increasingly using computer forensic examiners in the hope of finding a “smoking gun” or to challenge the evidence of the accuser.

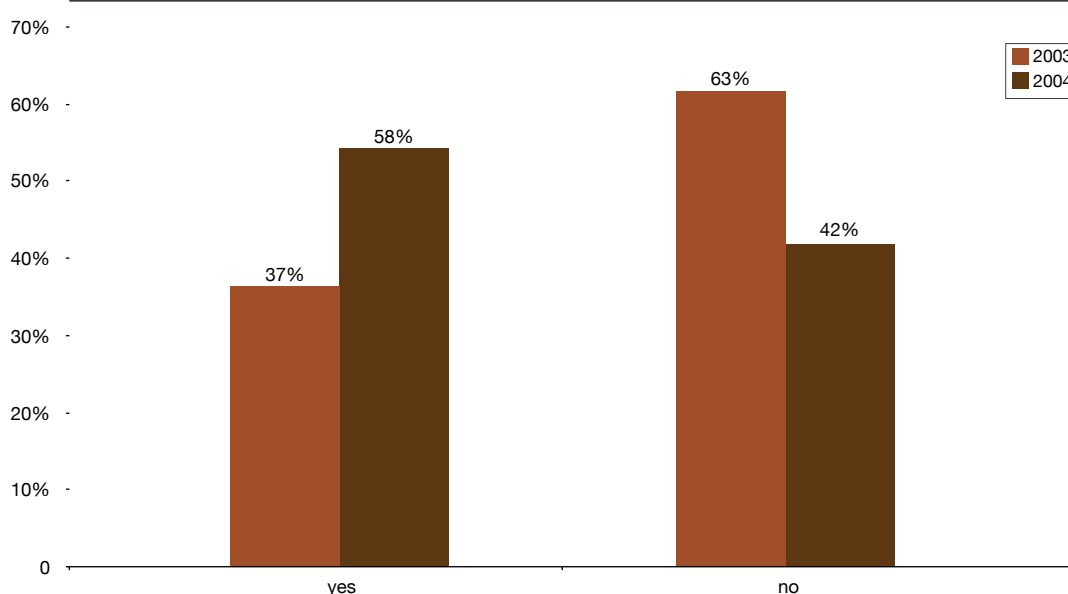
As the following case demonstrates, if you fail to correctly examine electronic evidence, the other side will probably use an expert examination against you:

Citing evidence of transactions made using a junior clerk’s userid, an auditor claimed the clerk was fraudulently diverting funds from the company payroll. The clerk was summarily terminated and asked to repay the funds or face criminal charges. The company’s lawyer engaged a computer forensic consultant who examined various company computers. The clerk’s union-provided solicitor requested an independent examination of the evidence, which revealed the suspect transactions were in fact made by a company director pretending to be the clerk. Examination of company emails also revealed that the company requested its forensic consultant to make certain omissions in his report.

The clerk no longer wished to work at that company and agreed to a substantial termination payment along with signing a deed of confidentiality. The company director had already returned the money and resigned and the alleged fraud was never reported to police.

This case demonstrates that not only is it important to examine the allegedly incriminating evidence but also to examine all contextual evidence, such as email. The Expert Witness Code of Conduct states: “an expert witness has an overriding duty to assist the Court impartially on all matters relevant to the expert’s area of expertise”. In other words, an expert is duty bound to report both incriminating and exculpatory (ie, proving innocence) evidence. This duty is especially important when dealing with computer-based evidence that is relatively easily misinterpreted (at best) or tampered with.

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



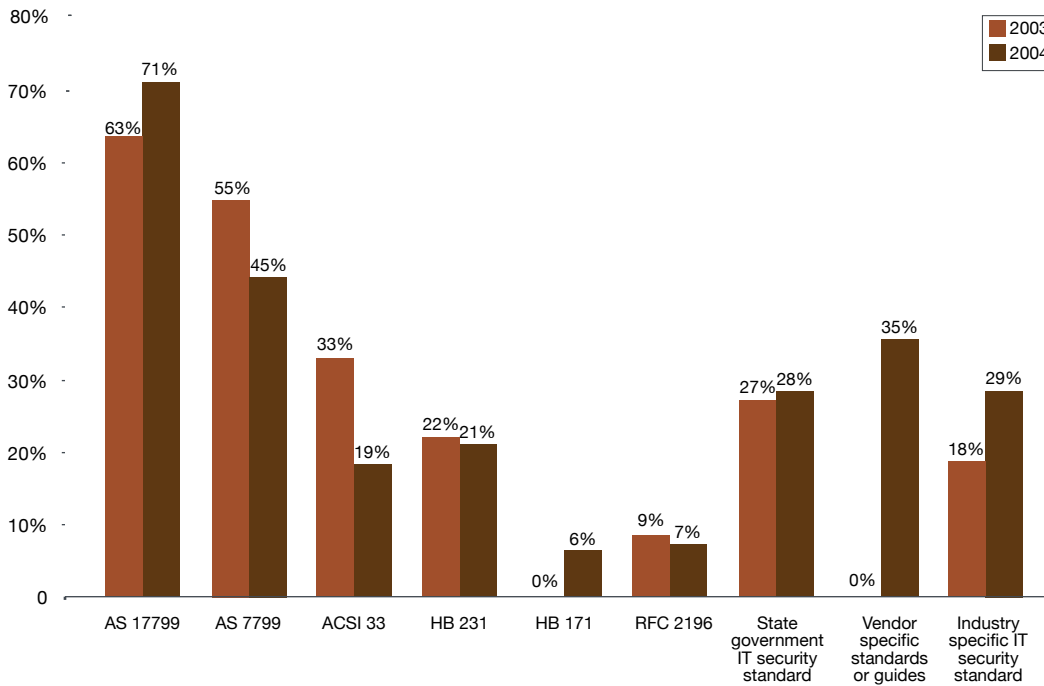
Source: 2004 Australian Computer Crime and Security Survey
2004: 236 respondents/98%, 2003: 211 respondents/98%

Note: This question was not asked in the 2002 Australian Computer Crime and Security Survey.

Information security standards

Another positive development in this year's survey is the marked increase in respondents that report that their organisations follow, or use as guides, IT security related standards; from only 37% in 2003 to 58% in 2004. Information security standards provide a framework from which to develop information security policies, practices and procedures tailored to an organisation's risk requirements.

IT security-related standards used

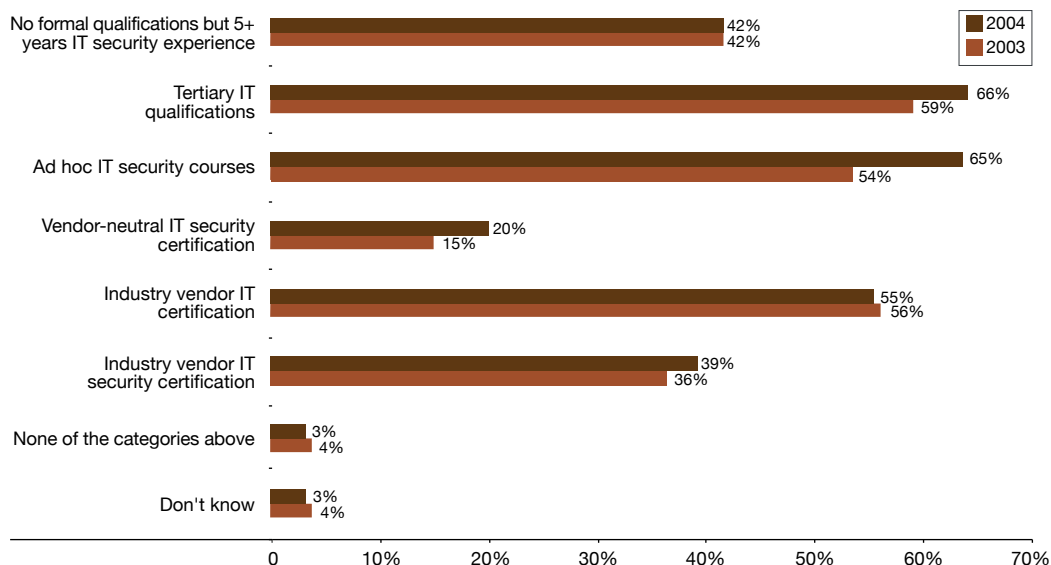


Source: 2004 Australian Computer Crime and Security Survey
2004: 141 respondents/59%, 2003: 82 respondents/38%

Note: In 2003, respondents were not asked if they used HB 171 or vendor specific standards or guides. HB 171 Guidelines for the Management of IT Evidence is a new standard published in late 2003.

Information security training, qualifications and certification

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

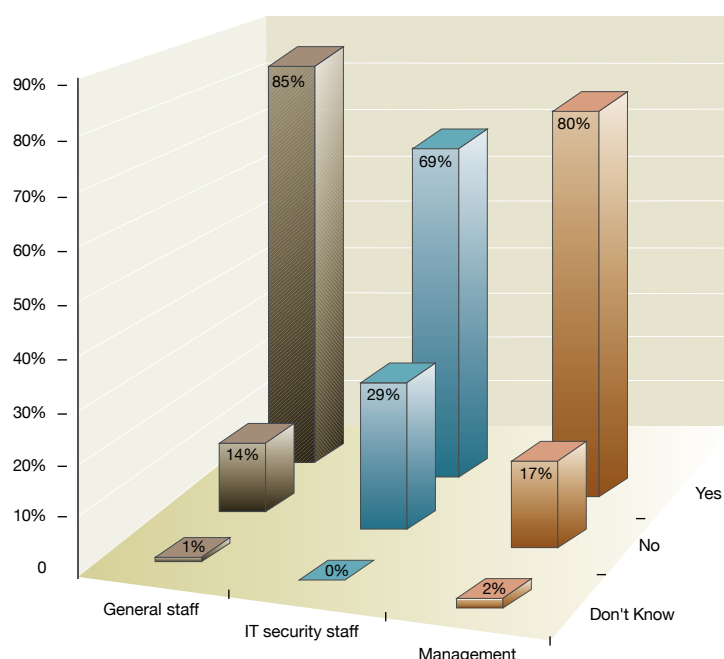


Source: 2004 Australian Computer Crime and Security Survey
2004: 238 respondents/99%, 2003: 211 respondents/98%

Note: This question was not asked in the 2002 Australian Computer Crime and Security Survey.

For 2004, the number of respondent organisations that reported employing experienced, qualified, trained and certified staff has increased across most categories. Despite this increase, a sizeable majority of respondent organisations (69%) reported that their IT security staff did not have sufficient experience and skill to meet their organisations' needs and believed that their organisations needed to do more to address this. Respondents also expressed significant concern about the adequacy of awareness training for general staff and management; 85% and 80% respectively. This level of dissatisfaction seems appropriate given the level of attacks and other forms of computer crime which organisations are still grappling with and the level of vulnerabilities reported by respondent organisations.

Do you think your organisation needs to do more to ensure an appropriate level of IT security qualification, training, experience or awareness for general staff, IT security staff and management?



Source: 2004 Australian Computer Crime and Security Survey
2004: 238 respondents/99%

Note: This question was not asked in previous Australian Computer Crime and Security Surveys.

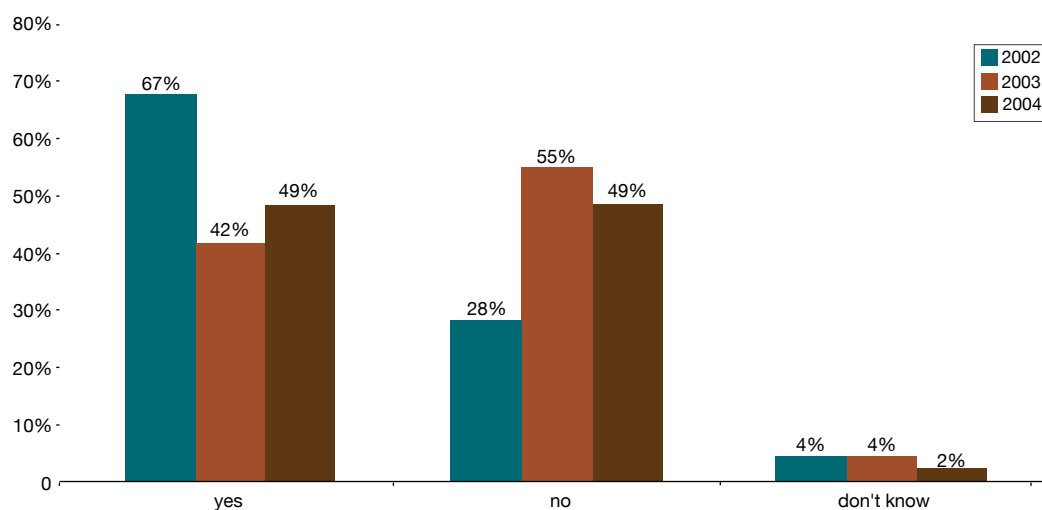
Based on the responses, the readiness of organisations to protect their IT systems appears to have substantially improved in three key areas: the use of information security policies, practices and procedures; the use of information security standards or guides; and the number of organisations with experienced, trained, qualified or certified staff.

In the pages ahead we look at what impact these improvements have had on the level of reported vulnerabilities, electronic attacks, computer crime, or computer access misuse and abuse.

WHAT ARE THE TRENDS?

Electronic attacks which harmed the confidentiality, integrity or availability of network data or systems

Did your organisation experience one or more electronic attacks in the last 12 months?



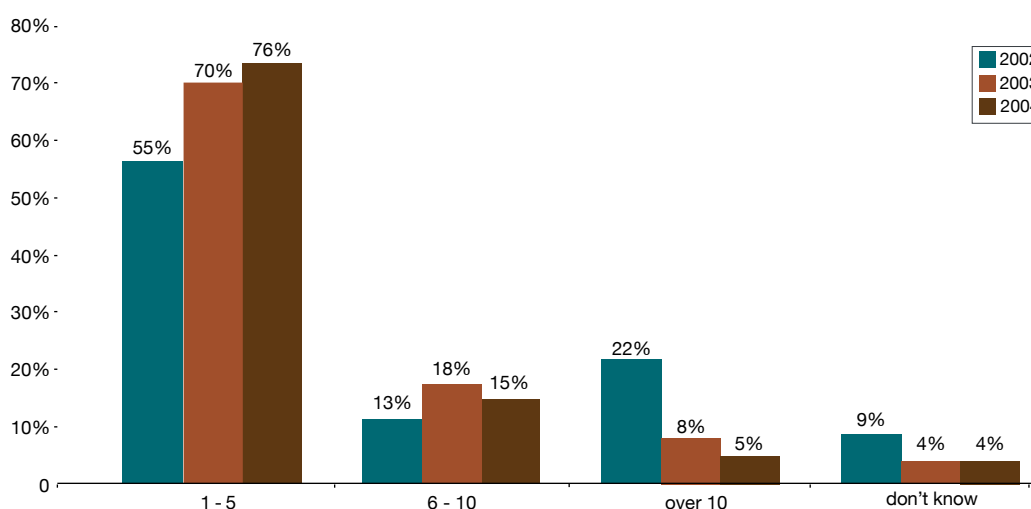
Source: 2004 Australian Computer Crime and Security Survey
2004: 238 respondents/99%, 2003: 212 respondents/99%,
2002: 92 respondents/97%

Note: In 2004, an electronic attack was defined an attack which harmed the confidentiality, integrity or availability of network data or systems. In 2003, the term 'computer security incidents' was used instead of 'electronic attacks' and 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.

Any form of computer attack that occurs electronically, often remotely, and which has the ability to harm data confidentiality and integrity or system availability, represents one of the greatest threats that has emerged in parallel with our increasing levels of Internet connectivity and dependency on publicly-connected networks. One of the most important indicators in this survey of how we as a nation are managing network security threats, is the question whether an organisation experienced electronic attacks.* It is concerning, therefore, that the number of respondents that experienced electronic attacks that harmed data confidentiality, integrity or system availability in some way, increased to 49% in the last 12 months (compared to 42% for 2003).

While this may only be a small increase, the importance of this measure in its own right, and the fact that many more respondents have adopted strategies to improve the readiness of their organisations to protect their IT systems, suggests that their efforts to “catch up” have, so far, been insufficient to cope with the changing nature of the threats they face.

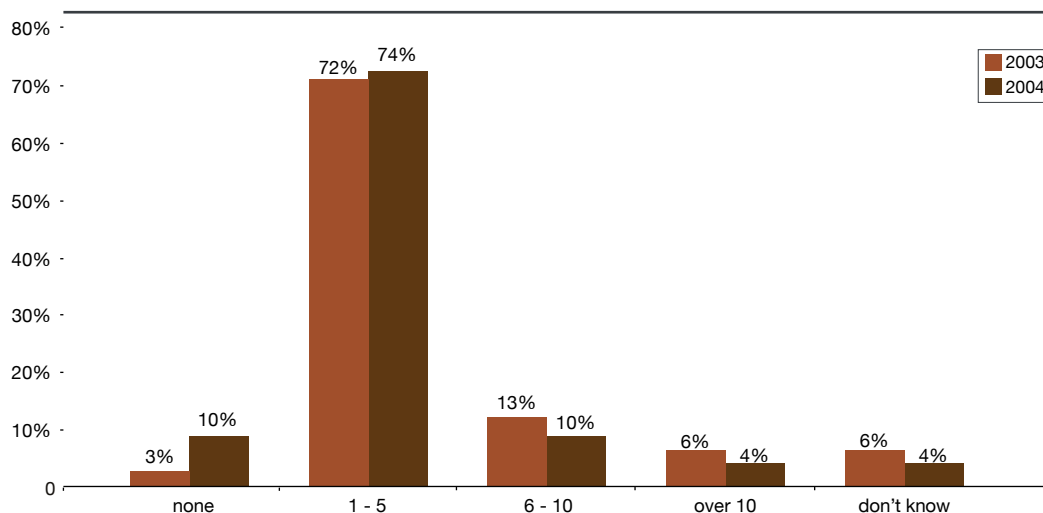
If experienced electronic attacks, how many?



Source: 2004 Australian Computer Crime and Security Survey
 2004: 85 respondents/35.4%, 2003: 90 respondents/42%,
 2002: 67 respondents/71%

* For the purposes of this question, an electronic attack was defined as one which harmed the confidentiality, integrity or availability of network data or systems.

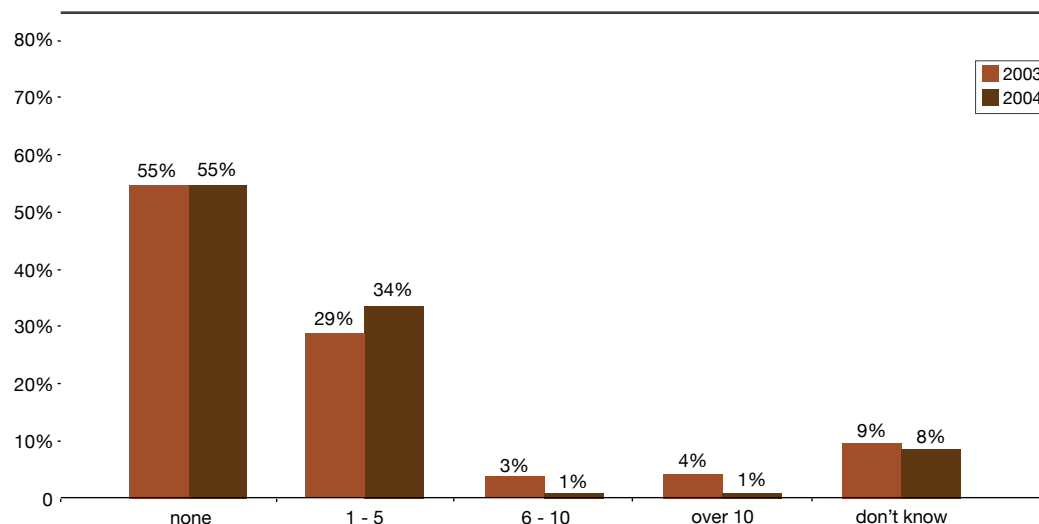
If experienced electronic attacks, how many from the outside?



Source: 2004 Australian Computer Crime and Security Survey
2004: 84 respondents/35%, 2003: 90 respondents/42%

As with the 2003 survey, a substantially higher proportion of respondents experienced harmful externally sourced attacks (88%) than harmful internally sourced attacks (36%). Compared to 2003, there was a slight drop in the percentage that reported harmful externally sourced attacks (91% in 2003) and no change to the percentage that reported internally sourced attacks. This trend continues to demonstrate that organisation that connect to the Internet face a higher level of threats than those that don't; and that organisations seem to be finding it more difficult to prevent externally sourced attacks. The figures also show that organisations cannot afford to ignore the internal threats, which still harmed 36% of the respondent organisations that reported electronic attacks.

If experienced electronic attacks, how many from the inside?



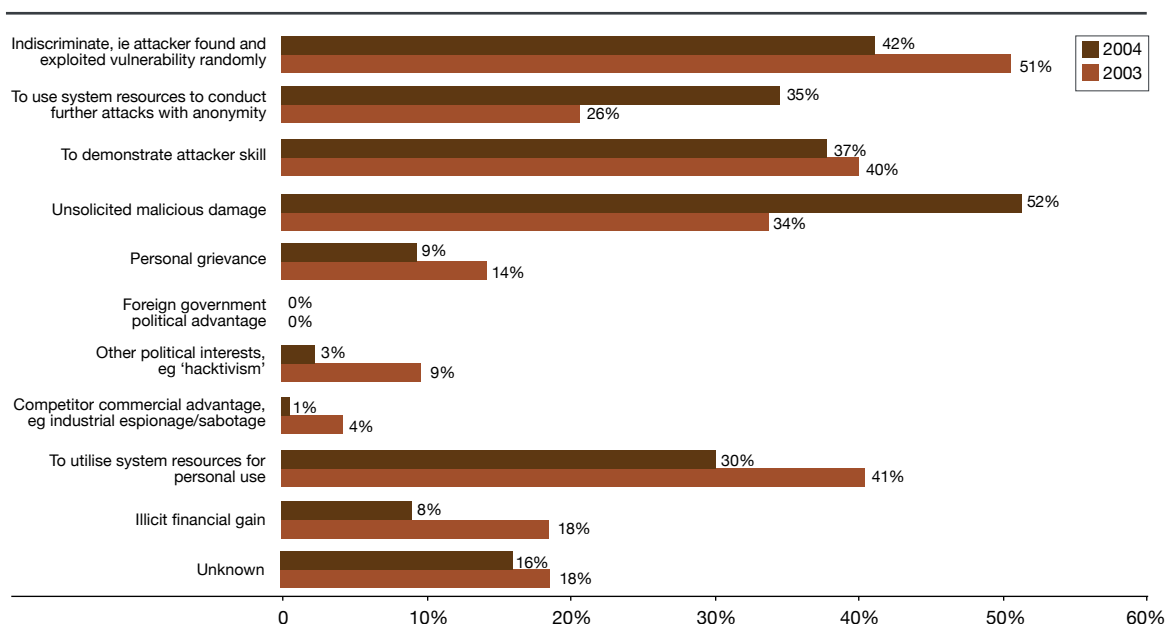
Source: 2004 Australian Computer Crime and Security Survey
2004: 83 respondents/34.6%, 2003: 91 respondents/42%

Attacker motives for electronic attacks

Most respondents identified "unsolicited malicious damage" (52%) as the primary motive for the harmful electronic attacks against their organisations. This figure is consistent with the high number of respondents (88%) who reported their organisations had experienced one or more virus, worm or trojan infections in the last 12 months. However, not all virus, worm and trojan attacks are motivated by a desire to cause (unsolicited) malicious damage. Sometimes

malicious code writers are motivated by the possibility of illicit financial gain or commercially motivated sabotage. (See “Commercially-motivated cyber attacks” page 25).

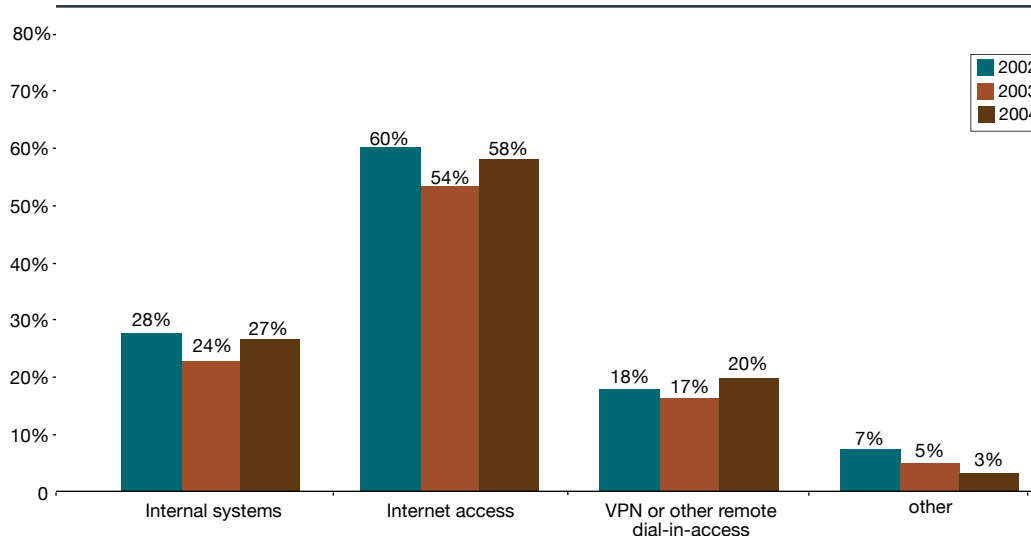
Suspected motive for electronic attacks which harmed confidentiality, integrity or availability in the last 12 months



Source: 2004 Australian Computer Crime and Security Survey
2004: 118 respondents/49%, 2003: 90 respondents/42%

Note: This question was not asked in the 2002 Australian Computer Crime and Security Survey.

Most frequent points of attack or attempted attack



Source: 2004 Australian Computer Crime and Security Survey
2004: 163 respondents/68%, 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.

The background is a gradient of warm colors, from dark red at the bottom to bright yellow at the top. There are several large, dark grey, stylized star or asterisk shapes scattered across the upper half. In the lower half, there are large, overlapping, semi-transparent geometric shapes in shades of grey and red, creating a layered effect.

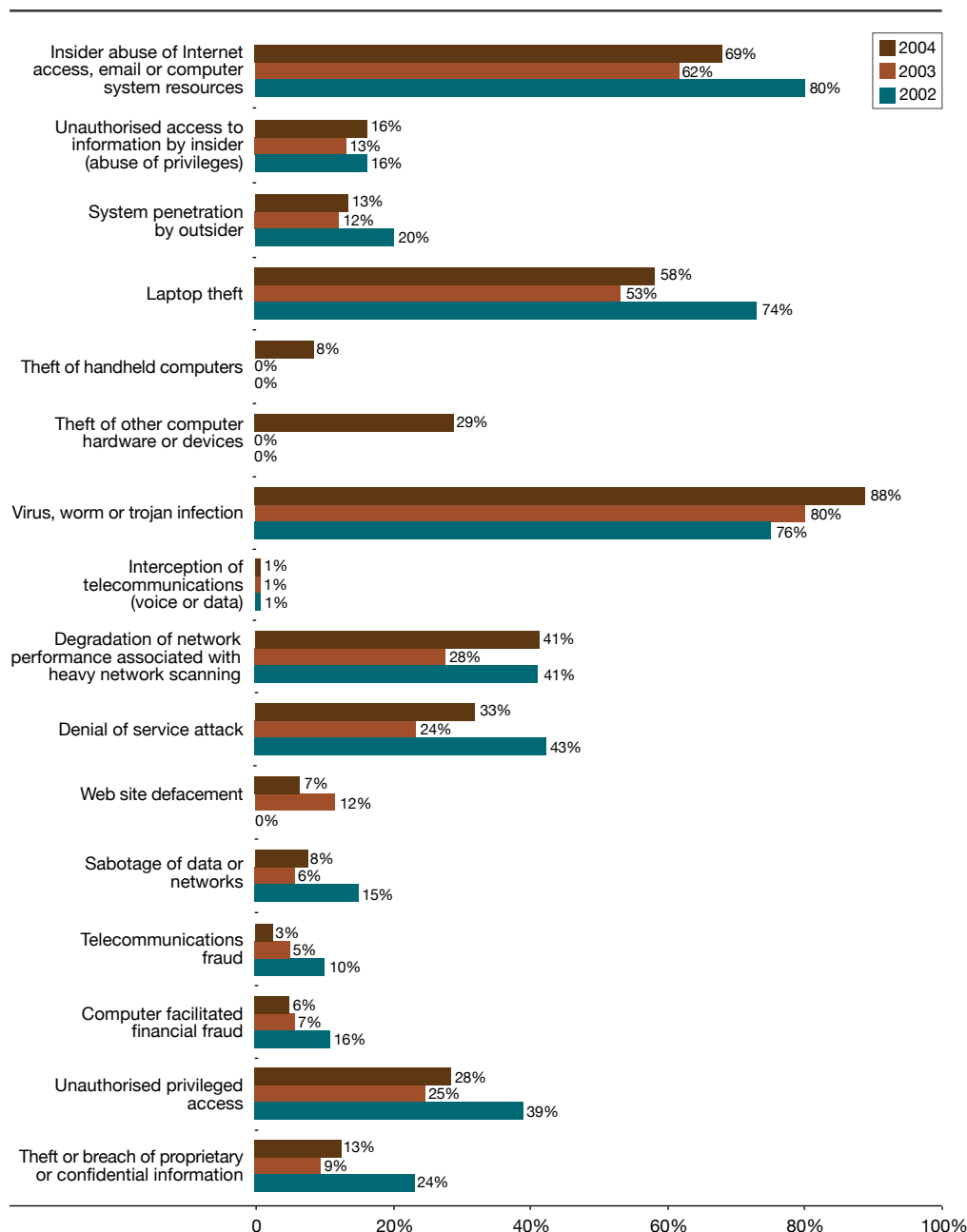
NATURE AND

OF ELECTRONIC ATTACKS, COMPUTER CRIME
AND COMPUTER ACCESS MISUSE AND ABUSE

IMPACT

Ninety-five percent of respondents reported experiencing one or more incidents of electronic attack, computer crime, computer access misuse or abuse in the last 12 months, across 16 categories. The most common incidents were virus, worm and trojan infections (reported by 88% in 2004, compared to 80% in 2003 and 76% in 2002); insider abuse of Internet access, email or computer system resources (reported by 69% in 2004, compared to 62% in 2003 and 80% in 2002); and laptop theft (reported by 58% in 2004, compared to 53% in 2003 and 74% in 2002).

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



Source: 2004 Australian Computer Crime and Security Survey
2004: 227 respondents/95%, 2003: 196 respondents/91%,
2002: 93 respondents/98%

Note: In 2002 and 2003, respondents were asked if they had experienced 'telecommunications eavesdropping' or 'wiretapping' instead of 'interception of telecommunications (voice or data)'. Also, in 2002 and 2003, 'theft of handheld computers' and 'theft of other computer hardware devices' were not included under this question. In 2002, web site defacement was not a category under this question.

Virus, worm and trojan infections - a growing concern

In the case of respondent organisation that suffered virus, worm or trojan infections, 71% reported these infections caused them financial loss and virus, worm and trojan infections accounted for 45% of all quantified losses in this survey, the single greatest cause of financial loss reported. This represents an increase from 2003 when losses from virus, worm or trojan infections accounted for 19% of total losses. For one organisation, its reported losses due to worm, virus or trojan infections for the last 12 months was \$2 million. Of those respondents that quantified the time it took to recover from these infections, 26% said they recovered in less than one day; 40% said it took between one and seven days to recover; 11% said it took between eight days and four weeks to recover; and 5% said it took more than one month to fully recover.

Consistent with these trends, the most common threats reported by respondents which they believed contributed to harmful electronic attacks was the use of powerful automated attack tools (47%); which by definition, includes worms and viruses. Conversely, the type of vulnerability that respondents reported had been exploited most often was unpatched or unprotected software vulnerabilities (60%).

Based on AusCERT information, there were about twice as many serious worm and virus hybrids in circulation between January 2003 and February 2004 (the period during which survey respondents were asked to report on their experiences), than for the previous survey period. A feature of many of these worms/viruses was that they exploited unprotected software vulnerabilities; and/or used social engineering ploys with executable attachments. Many spread widely and rapidly before anti-virus vendors were able to update, and organisations were able to apply, their anti-virus signatures.

The combination of fast-spreading, self-propagating worms in circulation across the Internet, users opening malicious code email attachments and the presence of vulnerable and inadequately protected software is, as the survey shows, a dangerous combination. But causes of virus/worm infections are not always due to just these factors alone; and effective solutions can be equally as complex.

Computer worms and viruses: fact or fad? Danny Smith, Sun Microsystems

Computer worms and viruses have been around for more than 20 years, yet many organisations continue to suffer serious compromise and disruption due to virus and worm infections. Organisations can best protect against virus infection by adopting both technical and non-technical approaches. Recent viruses, such as SoBig, MyDoom, Bagle and Netsky, spread successfully due to the actions of users and the nature of the technology being used.

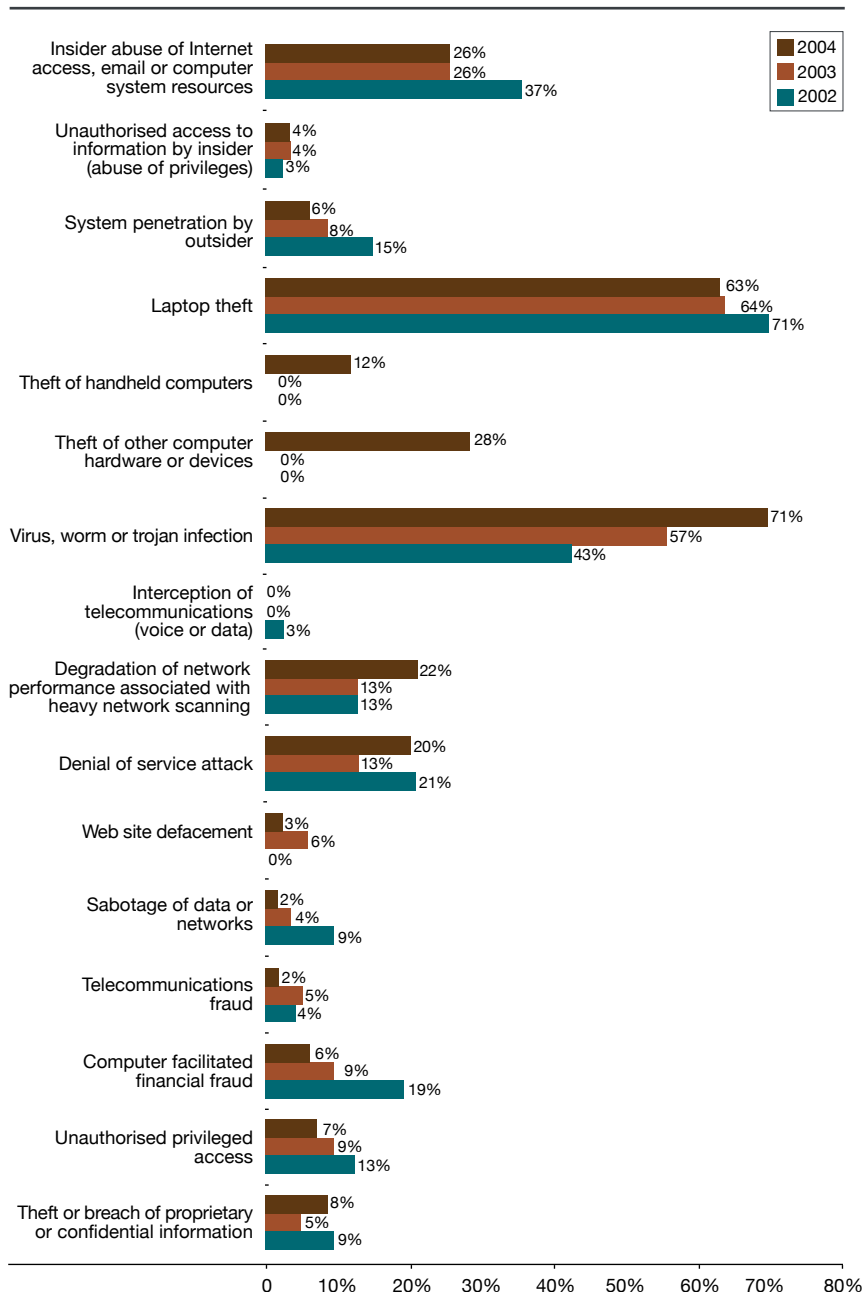
Users continue to ask for increased functionality, often at the expense of security, and computer systems continue to confuse "program" and "data" in the race to provide that functionality. From a user perspective it can be very difficult to tell the difference between viewing content and executing code. This is especially true when "data" actually hides "a program" within it in order to be displayed correctly such as via the web or email.

By choosing to use operating systems and applications that are configured to restrict executables from running automatically, including within email attachments, organisations will help avoid user mistakes and limit the spread of infections within their network.

Thin client technology can also enhance protection against malicious code that propagates with or without user intervention. Instead of thousands of fat clients sitting idle on desks waiting to be patched and configured, it can all be done in a single server. Centralised policy enforcement gives the IT department the possibility to help users protect themselves against a variety of malicious attacks.

With the rapid and widespread propagation of today's worms and viruses, technology solutions are, by themselves, inadequate. Organisations need to assess the vulnerability of their system software, features and configurations and increase user awareness and education. With these techniques, it should be possible to finally call the computer worm and virus a passing fad-at least, in your corner of the Internet world.

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



Source: 2004 Australian Computer Crime and Security Survey
2004: 172 respondents/72%, 2003: 141 respondents/65%,
2002: 75 respondents/79%

Note: In 2002 and 2003, respondents were asked if they had experienced 'telecommunications eavesdropping' or 'wiretapping' instead of 'interception of telecommunications (voice or data)'. Also, in 2002 and 2003, 'theft of handheld computers' and 'theft of other computer hardware or devices' were not categories under this question. In 2002, web site defacement was not a category under this question.

Computer access misuse and abuse

Insider abuse of their work Internet access, email and network resources typically includes downloading, storage or distribution of pornography, pirated software, music or movie files but may also include sending offensive email, distributing spam, use of peer-to-peer software or on-line gambling. Of the 16 types of electronic attack, computer crime and computer access misuse surveyed, insider abuse of Internet access, email or computer system resources has, for the last two years, been the second most common incident reported overall with 69% of respondents reporting it occurred; and 26% reporting financial losses as a result of this activity.

Insider computer access misuse and abuse, Kim Valois, Computer Sciences Corporation

Unfettered and easily available Internet access throughout a workday has spawned a workplace subculture that can be involved in the illicit downloading of music or movie files, web surfing on company time, and storage or distribution of offensive materials such as pornographic images on an employer's computer systems.

Despite the growth in this computer crime, misuse and abuse activity, it is often difficult to detect. Controls and auditing take resources and money to deploy. Many organisations only learn they have a problem by accident, maybe when stumbling across inappropriate materials or behaviors carried out on their systems; or widespread or extensive use peer-to-peer applications (eg, Kazaa, eDonkey, etc) on the company's systems chews up so many resources it takes down a network, the true cause of the problem gets discovered.

However, on discovery of a problem, further investigation often reveals prolonged and widespread misuse activity. Often, the issue may be followed up in human resources or management channels with technical collection or forensics style investigative techniques being considered late in the inquiry. But waiting too long can compromise the ability to gather evidence necessary to prove that misuse has occurred, or by whom it has been committed.

Organisations bear significant cost and impact from these incidents and depending on the activity may increase an organisation's legal risks. Many are contemplating deployment of tools to prevent abuses, especially those that block peer-to-peer protocols and applications. Other mitigating controls include actively monitoring the activity in the environment, such as with logging, intrusion detection monitoring, and host-based security controls. It is prudent to refresh security and "appropriate use" policies to address prevalent and new forms of misuse. Of course, employees need to be advised of their obligation to use computer systems and resources appropriately. It is also helpful to educate management and human resources on when and how to use technical methods or computer forensics in their inquiries, particularly early on in an investigation when better evidence and results can be obtained.

Measuring the impact of electronic attacks, computer crime and computer access misuse

Impact can be measured in direct and indirect costs; time to recover; and intangible impacts such as damage to an organisation's credibility, trustworthiness or reputation. The impact of electronic attacks, computer crime and computer access misuse ranges from negligible to grave, in both cost and time. Overall, the losses incurred by respondent organisations as a whole have worsened (20% higher than in 2003) with average losses of \$116,212 for each organisation that quantified their losses. By comparison, in 2003 the average loss was \$93,657 and in 2002 it was \$77,084.

Total losses reported by respondents for 2004 were close to \$16 million. However, this figure is not representative of the total losses due to computer crime, electronic attack and computer access misuse and abuse in Australia during the survey period. Rather, it represents the total losses reported by a portion (57%) of respondent organisations. If these results are typical of other Australian public and private sector organisations, the figure represents only a small fraction of total losses due to computer crime, electronic attack and computer access misuse and abuse in Australia during the survey period.



The cost of computer crime

Indicate the approximate dollar value that your organisation lost in total due to the following types of electronic attack, computer crime, computer access misuse, or abuse within the last 12 months. When estimating losses consider costs associated with recovery and investigation, lost revenue earnings and cost of damage to reputation etc, if applicable.

How losses were incurred	Number of respondents with quantified losses			Lowest reported			Highest reported			Average loss			Total annual loss		
	2002	2003	2004	2002	2003	2004	2002	2003	2004	2002	2003	2004	2002	2003	2004
Theft/breach of proprietary or confidential information	4	7	8	10,000	3,000	10,000	150,000	150,000	500,000	72,500	36,857	167,500	290,000	258,000	1,340,000
Unauthorised privileged access	8	10	7	1,000	1,000	1,000	50,000	200,000	50,000	13,275	32,200	9,714	106,200	322,000	68,000
Computer facilitated financial fraud	7	8	8	500	10,000	2,000	600,000	1,400,000	1,500,000	115,288	440,625	307,125	807,000	3,525,000	2,457,000
Telecommunications fraud	2	6	6	1,000	200	1,000	100,000	250,000	130,000	50,500	69,200	36,370	101,000	415,200	218,220
Sabotage of data or networks	5	3	3	1,000	5,000	4,000	1,000,000	100,000	80,000	204,600	41,667	44,667	1,023,000	125,000	134,000
Web site defacement	-	8	2	-	500	1,000	-	30,000	2,000	-	7,313	1,500	-	58,500	3,000
Denial of service attack	8	16	15	1,500	300	1,000	100,000	200,000	100,000	22,688	24,831	25,200	181,500	397,300	378,000
Degradation of network performance associated with heavy scanning	7	14	24	1,500	1,000	500	100,000	200,000	700,000	23,071	37,729	71,208	161,500	528,200	1,709,000
Interception of telecommunications (voice or data)	2	1	1	1,000	4,000	5,000	10,000	4,000	5,000	5,500	4,000	5,000	11,000	4,000	5,000
Virus, worm, trojan infection	23	66	93	100	200	100	100,000	400,000	2,000,000	38,743	33,695	76,313	891,100	2,223,900	7,097,100
Laptop theft	48	82	84	2,000	1,999	1,000	100,000	350,000	200,000	26,331	27,539	17,670	1,263,900	2,258,183	1,484,244
Theft of handheld computers	-	-	12	-	-	1,000	-	-	10,000	-	-	4,708	-	-	56,500
Theft of other computer hardware or devices	-	-	30	-	-	1,000	-	-	60,000	-	-	14,333	-	-	430,000
System penetration by outsider	7	7	6	1,000	2,000	1,000	40,000	50,000	250,000	26,143	21,571	51,833	183,000	151,000	311,000
Unauthorised access to information by insider	5	3	3	5,000	2,000	5,000	100,000	250,000	200,000	29,000	87,333	70,000	145,000	262,000	210,000
Insider abuse of Internet access, email or internal computer resources	17	30	1	100	500	20,000	200,000	400,000	20,000	36,300	42,417	20,000	617,100	1,272,500	20,000
TOTAL ANNUAL LOSSES													5,781,300	11,800,783	15,921,064
2004: 137 respondents/57%, 2003: 126 respondents/58%, 2002: 75 respondents/80%															

As was the case in 2003, for the vast majority of electronic attacks, computer crime and computer access misuse incidents, recovery time was between one and seven days or less than a day. For respondents that estimated the time it took to recover from the most serious incident they had in each of the 16 listed categories, 60% estimated they recovered in less than a day; 74% estimated that recovery took between one and seven days; 28% estimated that recovery took between eight days and four weeks; 13% estimated that recovery took more than one month; and 5% experienced incidents which they assessed they may never recover from.

Unauthorised privileged access

In 2003, an Australian ISP reported intrusions into a significant number of their servers. During the investigation it was revealed that the offender may have also broken into a number of overseas educational institutions and other organisations using a particular exploit. Following the chain of computers compromised with this particular exploit, a suspect was identified and a search warrant was executed at the suspect's premises. Analysis of the exploit code and seized hard drives was conducted by police. A male person is currently facing several charges in relation to this matter.

The incidents which resulted in the largest overall losses - after virus, worm and trojan infections - were: computer facilitated financial fraud, which accounted for 15% of total losses; degradation of network performance associated with network scanning, which accounted for 11% of total losses; laptop theft, which accounted for 9% of total losses; and theft of confidential and proprietary information, which accounted for 8% of total losses (an increase from only 2% of total losses in 2003). Although these types of incidents were less common than virus, worm and trojan infections, combined they accounted for 43% of total losses for 2004.

Time lost recovering

For the most serious incident that occurred for each of the following types of electronic attack, computer crime or computer access misuse or abuse 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											
	Less than 1 day		1 to 7 days		8 days to 4 weeks		More than 1 month		May never fully recover		Total respondent organisations which lost time	
	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004	2003	2004
Theft/breach of proprietary or confidential information	5	4	5	9	1	1	1	2	3	2	15	18
Unauthorised privileged access	15	14	10	13	1	1	3	1	2	-	31	29
Computer facilitated financial fraud	3	2	2	-	-	1	4	3	2	2	11	8
Telecommunications fraud	4	2	2	2	1	-	2	2	-	-	9	6
Sabotage of data or networks	2	3	3	6	1	-	-	-	-	-	6	9
Web site defacement	9	7	11	6	-	-	-	-	-	-	20	13
Denial of service attack	25	29	15	22	2	5	1	-	-	-	43	56
Degradation of network performance associated with heavy scanning	13	29	11	28	2	4	4	1	1	1	31	63
Interception of telecommunications (voice or data)	2	1	2	2	-	-	-	-	1	-	5	3
Virus, worm, trojan infection	59	54	54	83	9	22	2	10	2	0	126	169
Laptop theft	17	17	40	52	26	26	6	1	6	1	95	97
Theft of handheld computers	-	1	-	5	-	11	-	1	-	1	-	19
Theft of other computer hardware or devices	-	9	-	17	-	13	-	-	-	2	-	41
System penetration by outsider	2	7	15	10	4	5	1	-	-	-	22	22
Unauthorised access to information by insider	4	6	7	8	-	1	2	-	2	2	15	17
Insider abuse of Internet access, email or internal computer resources	44	31	18	27	6	9	5	6	2	5	75	78
	2004: 206 respondents/86%, 2003: 175 respondents/81%											

Note: In 2003, respondents were asked "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' was defined as above.

On-line banking and e-commerce fraud

Since the last *Australian Computer Crime and Security Survey*, AusCERT has seen a steady increase in the number, and sophistication, of scamming techniques directed against users of online banking and electronic payment sites.⁶

In early 2003, scamming techniques were fairly rudimentary but sufficiently effective that they continued to flourish. At best, using spamming techniques scammers sent HTML formatted emails with embedded URL links to large numbers of potential victims and tricked them into submitting their account access details and passwords to fake banking or electronic payments web sites. Scammers simply created hyperlinks which on casual scrutiny appeared to be links to legitimate sites, but in effect, were hyperlinks to scammer sites.

During the latter part of 2003, scammers made use of hexadecimal URL encoding so hyperlink embedded URLs appeared more genuine. For example, by crafting URLs with hexadecimal encoding, typically “%20”, which the browser renders into a string of spaces, scammers were able to cause the scammer’s web site address to be “pushed off screen” or not be displayed when the cursor is placed over the hyperlink, or in the address and/or status bars of the browser window when the link is accessed. Instead, the legitimate web site address will be displayed while still allowing a connection to be made to the fraudulent web site address.

When used in conjunction with the “@” symbol in the hyperlink embedded URL, browsers interpret the part of the URL that precedes the “@” character as a username/password to access the web site. If there is no need for authentication everything before the “@” will be ignored. An example of a hyperlink crafted with these techniques would look like:

www.yourrealbank.com.au.

By 2004, scammers had also tried to capture Internet banking customer account access details through more subtle means. By using social engineering in conjunction with other URL obfuscation techniques such as hexadecimal/octal encoding, scammers have sought to lure users to click on hyperlinks to trojaned web sites under a pretext which may have nothing to do with Internet banking.⁷ Once the trojaned web site is accessed, and if the client machine is not appropriately secured, it could result in malicious code, such as a keylogger, being installed on the client machine. The effect is the same whether the unsuspecting users submits their account details to a fraudulent web site, or whether the account details are captured from user keystrokes and surreptitiously forwarded to an attacker.

Since early 2004, scammers also commenced exploiting a number of (then) relatively new vulnerabilities³ in the Microsoft Internet Explorer browser and Outlook and Outlook Express clients in combination with previous techniques. Microsoft has released patches for some of these vulnerabilities.⁹

One of these vulnerabilities¹⁰ allowed a URL pointing to executable code to be retrieved and executed without the victim clicking on it or otherwise opening it; nor was it reliant on scripting being enabled in the web browser settings. The malicious code would either be in the HTML of the scam email or in a web page the email induced the victim to visit. The malicious code could potentially perform any range of functions on the user's system, but in this context, scammers had exploited the vulnerability to install a keylogger[†] designed to capture banking details sometimes specifically targeting Australian banks on the victim's machine. The Bagle.Q worm utilised the same vulnerability.¹¹ This development meant now the scam had the potential to affect vastly more victims - not just those who were fooled into believing the scam email was sent from a legitimate source.

Identity theft to facilitate fraud in the on-line environment is by no means new – rather, it is the evolving, more sophisticated and more “believable” nature of the techniques and the increasing rate of attacks which is most concerning. Much of the success of these scams depends on their believability – the scammer creates a pretext, supported by the technology, to persuade the potential victim to take certain actions necessary for the fraud to occur. The ability to impersonate an on-line identity is a feature of many types of electronic attack and computer facilitated fraud; attackers can also easily “spoof” a user’s email address, a hostname or hijack a user account identity. For many of the scams identified above, there are a variety of cryptographic solutions that can provide integrity and assurance to enable users to accurately verify on-line identity be it for a person or machine. Unfortunately, average users don’t appear to have sufficient awareness, or competency, in the use of these technologies, for example, how to verify digital certificates (or digital signatures) and the technology is not being used to its full advantage.

For some of the other scams described, attackers are taking advantage of vulnerabilities inherent in the software itself, which without adequate alternate counter-measures in place, such as up to date anti-virus software, personal firewalls etc, can mean that malicious code is automatically installed, becomes active and remains resident on the victim's machine without the user's knowledge.

† Keylogger programs record user keystrokes and surreptitiously transmit this data to a remote location in the control of an attacker.



As long as there remains even a small proportion of users that fall victim to these types of scams they will continue to proliferate. In some countries the problem is more serious and the techniques fraudsters are using are more aggressive. The potential exists for Australia to follow a similar trend. The problem is complex and necessitates a range of prevention strategies. More secure software; user education;¹² improved authentication; ensuring network hosts (who ever owns them) are not able to be compromised and used by attackers to host fraudulent web sites; and closing the open mail relays which allow the attackers to send the fraudulent spam bait would all help. Users of Internet banking and e-commerce services should ensure that the machine, through which they access the web, can be trusted and is well secured.

It is not uncommon for home users or small businesses with ADSL, cable broadband or ISDN connections to be used as open proxies to disseminate bulk fraudulent email, or as a point for the illicit transfer of funds. Typically such machines are attractive because they are easily located within specific netblock ranges, “always on”, often insecure and have the bandwidth necessary to support the activities of attackers.

Unprotected home computer with broadband access

In 2003, an Australian bank alerted the AHTCC that a computer in Perth had been involved in the unauthorised access and removal of money from the Internet banking accounts of seven of the bank’s customers. On the basis of this information, a computer at a residential address was examined. It was identified that the owners of the computer had broadband Internet access attached to this computer, but that this computer was not protected by a firewall or anti-virus software. After a forensic examination of the machine, it was established that criminals from overseas had used a computer virus to gain remote access and control this computer to undertake the Internet banking thefts. Inquiries are continuing with the assistance of overseas law enforcement agencies.

Once a fraudulent web site is established, speedy and effective response strategies are required. The computer emergency response team (CERT) community, of which AusCERT is part, can help locate and close down fraudulent web sites and open mail relays. Prosecution of fraudsters, both locally and overseas is also vital.

Commercially-motivated cyber attacks

Spammers are no longer content to limit their activities to disseminating spam - some appear to be engaging in active electronic attacks that help them to continue their trade. In the same way that web proxies (see “Computer security management, vulnerabilities, threats and challenges” see page 29) may be configured to permit use by untrusted parties, spammers and scammers take advantage of poorly-configured mail relays that allow them to send anonymous unsolicited bulk email via third parties, at someone else’s expense and blame.

For example, spammers appear to be behind the creation of the SoBig worm variants that, by creating back doors, facilitate the creation of the open mail relays that are used by them to send spam.¹³ As anti-spam groups identify open relays that generate spam, and organisations use this information to block email from these addresses, this has contributed to an increase in demand for new open mail relays. Releasing worms that have the capacity to compromise and create open mail relays in thousands of machines helps achieve this goal very quickly.

Computer enhanced fraud

In March 2003, a Tasmanian organisation reported to police that they suspected one of their employees to be misappropriating funds. From checks of their accounting system and paper records it was suspected that the employee was producing forged invoices for payment, which he would then bring to work. These invoices would purport to be from a regular supplier to the organisation and the employee would enter them into the accounting system as such.

The organisation performed a cheque run once a week to pay all outstanding invoices. Immediately before this run was performed the employee used a supervisory access account to alter records in the accounting system and change the payee for the invoices he had entered to the name of a business he had registered. Once the cheque had printed he would take it and then alter the details in the accounting system back to being those on the forged invoice. Between April 2001 and March 2003 the employee fraudulently appropriated over \$370,000.

In response to this complaint, police executed a warrant on the employee’s residence where a computer was seized. Examination of the employee’s computer revealed copies of the forged invoices which had been created by scanning legitimate invoices he had taken from his work place and then altering them.

In October 2003, the employee was convicted of 16 counts of forgery, 16 counts of uttering, 16 counts of inserting false information as data, 15 counts of altering computer data with intent to defraud, and one count of computer related fraud. He received a penalty of three and a half years imprisonment for these offences.

Denial of service attacks – a weapon of extortionists and saboteurs

A third of respondents experienced denial of service attacks and 22% reported financial losses as a result of this activity. Often victims of DoS attacks appear to have been targeted indiscriminately—more because they are reachable, rather than because of any specific motive of the attacker. But sometimes, DoS attacks have also been launched against particular organisations for quite specific reasons, as the following case studies illustrate.

Denial of service attack

In late 2002, an Australian company reported an ongoing denial of service (DoS) attack on the company web server allegedly being conducted by an ex-employee. The type of DoS experienced was a SYN packet flood which was sufficiently large to deny legitimate customers access to the web server, causing a loss of productivity for the company. The company's email server was also targeted. The attacks continued into early 2003.

Packet header information was obtained from the victim's service provider, which led to a search warrant being executed at the suspect's premises. Forensic examination of the computer owned by the suspect yielded a computer program that may have been used to launch the attacks.

The matter is currently before the court.

Deriving income from denial of service attacks, Oliver Binz, b-sec

One reason why many poorly protected computer systems operate for years seemingly untroubled by computer crime is the relative difficulty in making money from an attack. Real criminals want money. Though rudimentary, the distributed denial of service (DDoS) attack has proven to be an effective extortion tool.

b-sec recently received a call from a customer who trades over \$500M a year through its e-commerce web site. No online presence equals no income. The customer also has strong competition and somewhat fickle customer loyalty, making any downtime even more damaging in the long term. One night the site went unexpectedly off the air. Initial investigation showed enormous traffic volumes flooding the customer's multiple 10Mbps Internet links. A closer look showed over 7,000 devices from around the world involved in a highly organised DDoS attack. The attackers had the ability to control thousands of "zombie" servers to effectively stop the online site from trading with its genuine customers. This alone does not generate income for an attacker; however coupled with good old fashioned "stand over" tactics it can be quite lucrative. Instead of threatening violence, the threat now is to an organisation's income and possibly even its existence and paying money for "protection" appears to be an option some companies have chosen.

Within 12 hours of the first "show of strength attack", the first email arrived demanding \$USD25,000 be transferred to a particular bank account so that further planned attacks would not occur. As a value added service the extortionists also promised to protect the customer from attack from other people using the same technique (which of course is impossible).

b-sec strongly advised the customer against payment and recommended involving the Australian High Tech Crime Centre and AusCERT. b-sec's immediate concern was to get the organisation back online and generating revenue.

The options for defending against this type of attack are limited. Due to the (ever increasing) ability for an attacker to flood even the largest of pipes, the trick is to get your Internet service provider (ISP) involved. In this case, through close collaboration between the customer, b-sec (using in-house developed analysis tools) and Optus - the ISP - we were able to provide an almost immediate workaround solution to get the service back on its feet.

The moral of the story is simple. Attacks (such as DoS), which until now have been uninteresting to criminals are becoming more popular, and no business which conducts significant business online can afford to ignore the risks. Attention to effective defence in depth, secure applications, appropriate patching and change control techniques, will ensure resilient defence for your online business against the expected next round of attacks.

It is an accepted axiom that the security of an organisation's network is affected by the security of every other network to which it is connected. If you are connected to the Internet then this provides an almost limitless range of opportunities to be attacked. The ability of attackers to compromise and coordinate the activities of thousands of insecure hosts on disparate networks in a DDoS attack demonstrates the potential harm which may arise due to the insecure state of other connected networks. But it also demonstrates the power of taking a distributed coordinated approach to a task. If telecommunications providers and ISPs adopted a similar distributed coordinated approach to DDoS mitigation, then DDoS attacks would be fewer, less effective and less attractive for attackers.

Proactive protection by ISPs against DDoS attacks, Cisco Systems

Defending against distributed denial of service (DDoS) attacks is difficult. The large number of machines that can be used to participate in such attacks makes the task of blocking the attack at the victim's router or firewall time-consuming, or if the attackers are using spoofed IP addresses, impossible. Even with effective blocking, the volume of traffic generated by such attacks can completely consume an organisation's Internet link (or links). DDoS attacks can only be effectively mitigated in conjunction with the organisation's Internet service provider (ISP), and mitigated in general by greater cooperation between all ISPs.

Preparation – the widespread deployment of basic ingress and egress filtering makes the use of spoofed IP address much more difficult for attackers. Training in, and deployment of, mitigation tools and techniques by ISPs needs to be done before an attack takes place - not during an attack.

Detection – anomaly-detection systems using router traffic flow data can detect and characterise undesirable traffic, such as DDoS attacks and can also indicate where filters should be applied to limit attacks and assist in traceback.

Traceback – to be able to block or drop DDoS traffic, it is necessary to traceback a DDoS attack to its sources. To do this efficiently, and to reliably traceback an attack using spoofed IP addresses, backscatter traceback is required. Backscatter takes advantage of Border Gateway Protocol (BGP), the routing protocol pervasively deployed in ISP networks, to drop traffic originally destined for the victim and enables the creation of unreachable Internet Control Message Protocol (ICMP) messages to identify routers that are transmitting data intended for the target of the DDoS attack. Once ingress routers have been identified, upstream ISPs can be contacted to continue traceback on their networks.

Reaction/Containment – when an ISP knows where an attack is coming from it can apply containment mechanisms such as ACLs and/or rate limiting. Many ISPs also use BGP to propagate remote triggered drop instructions to many routers quickly and efficiently so that traffic destined to the attack target is dropped on ingress into the ISP network. In many cases this is an effective reaction to a large attack but ISPs can also limit the rate at which administratively identified traffic is allowed into the network or to an organisation. For instance, a provider can, upon detecting a high rate of ICMP traffic, rate-limit that traffic to alleviate the effects of the attack. As with traffic filtering, a provider can use Quality of Service Policy Propagation via BGP to remotely trigger rate-limiting configurations.

Postmortem – finally, ISPs should review what was most effective during an attack and what could be improved. Postmortems should be conducted not only internally, but with other providers.

For more information see: <http://www.nanog.org/ispsecurity.html>

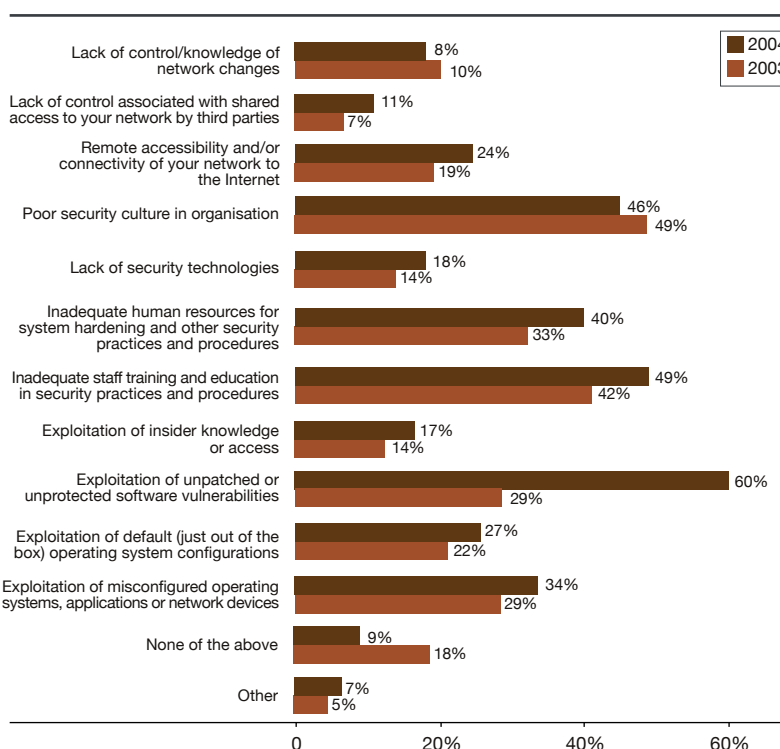
COMPUTER SECURITY MANAGEMENT



VULNERABILITIES, THREATS AND CHALLENGES

Responses to this year's survey indicate that in a number of key areas, perceptions about the level of organisational, network and system vulnerabilities; threats and performance in managing computer security have worsened. These results are disconcerting given that more respondent organisations have skilled and trained staff; more are using a variety of security policies and procedures and information security standards (See "Readiness to protect IT systems", page 7) and the majority have increased spending on computer security in the last 12 months.

In terms of the nature of your organisation's potential vulnerabilities, what factors may have contributed to those electronic attacks which harmed the confidentiality, integrity or availability of your network data or systems in the last 12 months?



Source: 2004 Australian Computer Crime and Security Survey
2004: 168 respondents/70%, 2003: 177 respondents/82%

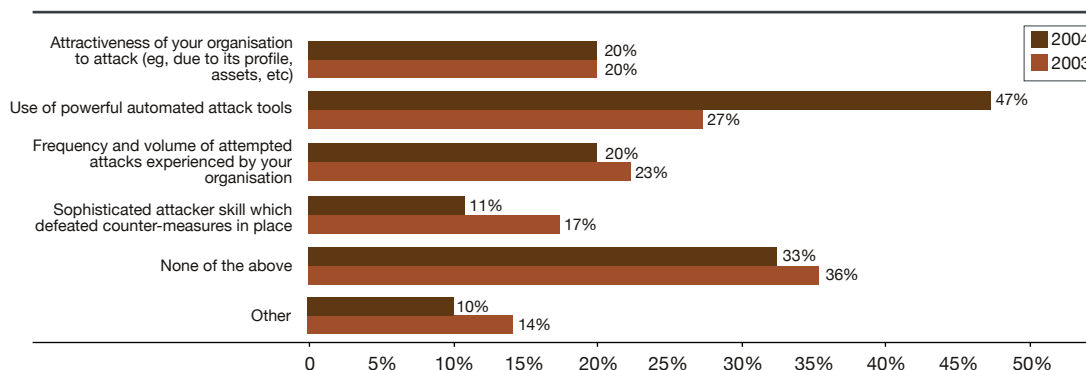
Sixty percent of respondents reported that exploitation of unpatched or unprotected software vulnerabilities probably contributed to the success of harmful electronic attacks directed against their organisations, compared to 2003, when only 29% of respondents made this claim. The significant jump in this figure suggests that organisations are finding it increasingly difficult to apply all critical patches on their systems in a timely manner. Indeed, 61%, (most of whom were the same respondents) reported that keeping up to date with computer threats and vulnerabilities, was one of the most challenging or problematic aspects of computer security management they faced. These figures are not that surprising, given the corresponding increase in the number of serious vulnerabilities that have been reported in 2003. Therefore, as the discovery and reporting of software vulnerabilities has increased, the capacity to mitigate these vulnerabilities appears to have declined for most respondent organisations.

Respondents also cited inadequate human resources for system hardening and performing other security practices and procedures (49%); and poor security culture in organisation (46%) as factors which probably contributed to the harmful electronic attacks experienced in the last 12 months. Thirty-four percent of respondents identified misconfigured operating systems, applications or network devices as a probable cause of electronic attacks against their network. The following is an example of what can occur in such a situation.

Open proxy

A small organisation recently noted increasingly large bandwidth bills from their Internet service provider and reported the matter to police. Analysis of their network established that they had inadvertently configured their web proxy server in such a manner whereby it could be accessed and used as a relay by people on the Internet when accessing other sites. As knowledge of this spread on the Internet, more and more users began accessing it. This is a common technique utilised by unscrupulous persons wishing to make their traffic difficult to trace or for launching attacks against other systems.

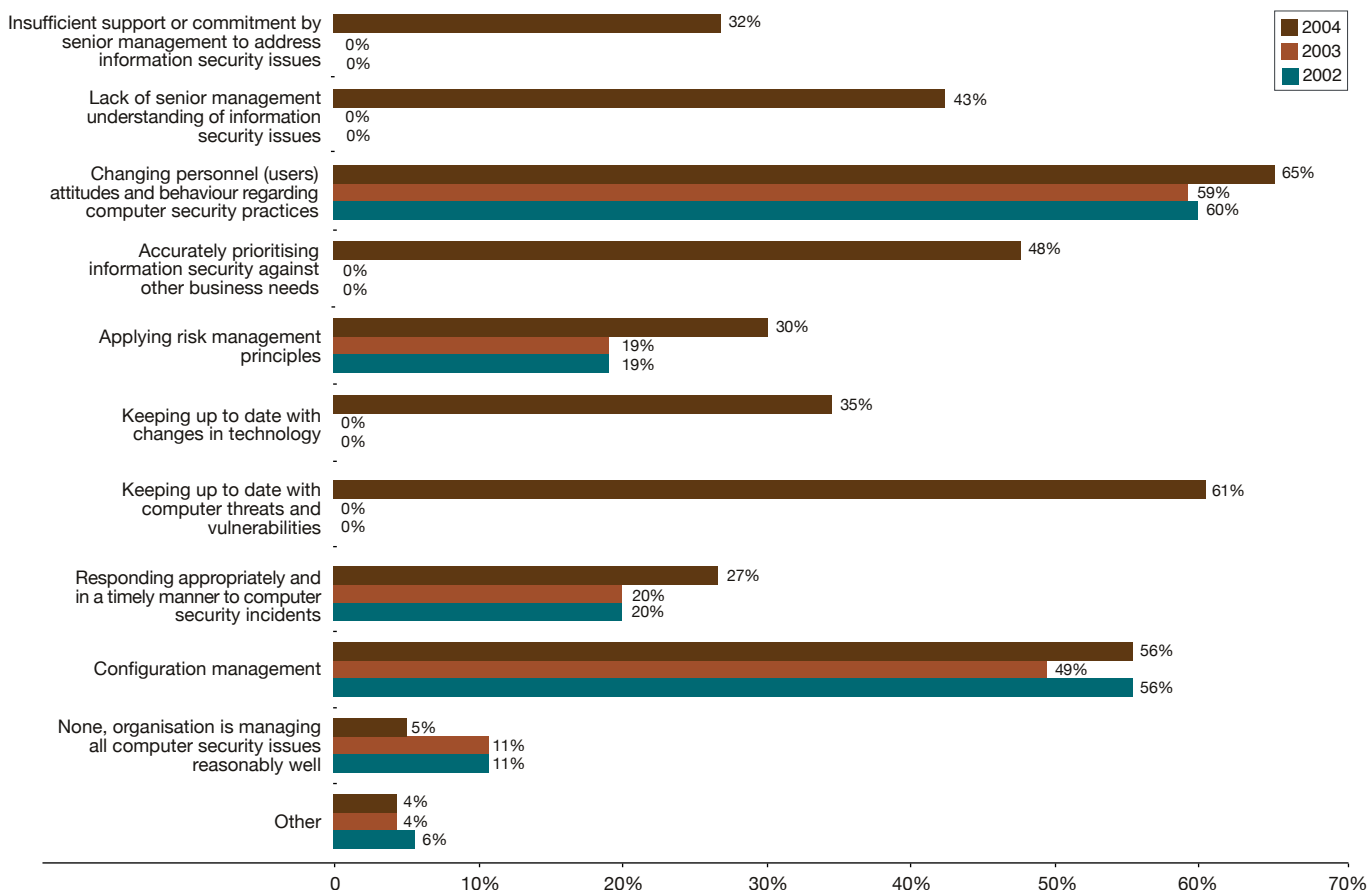
In terms of the threat faced by your organisation, what factors may have contributed to those electronic attacks which harmed the confidentiality, integrity or availability of your network data or systems in the last 12 months?



Source: 2004 Australian Computer Crime and Security Survey
2004: 167 respondents/70%, 2003: 175 respondents/81%

Respondents were asked to identify those aspects of computer security management which they found most problematic or challenging. Changing user attitudes and behaviour regarding computer security practices was the most challenging problem for the majority of organisations (65% in 2004 compared to 59% in 2003). Configuration management (56% in 2004, compared to 49% in 2003); accurately prioritising information security against other business needs (48%); lack of senior management understanding of information security issues (43%); and insufficient support or commitment by senior management to address information security issues (32%) were considered to be among the most challenging or difficult aspects of computer security to manage.

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



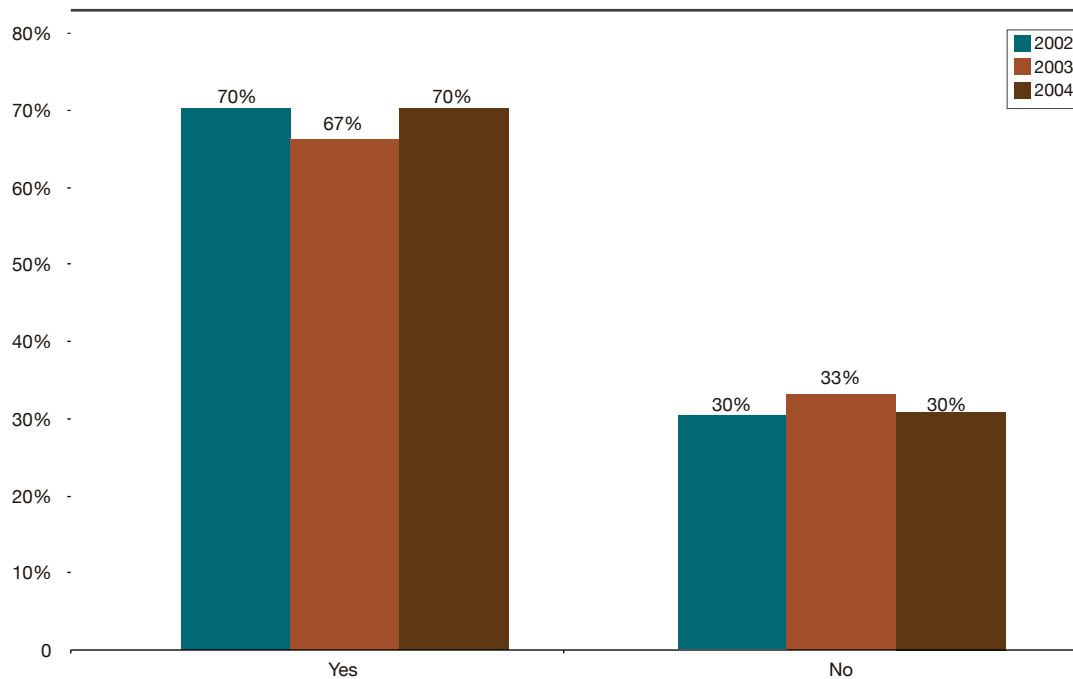
Source: 2004 Australian Computer Crime and Security Survey
2004: 179 respondents/75%, 2003: 206 respondents/96%,
2002: 88 respondents/93%

Note: In 2002 and 2003, 'insufficient support or commitment by senior management', 'lack of senior management understanding of information security issues' and 'accurately prioritising information security against other business needs' were not categories under this question. Also, in 2002 and 2003, 'keeping up to date with changes in technology and computer threats and vulnerabilities' was one category not two separate categories.

Most concerning of all is that only 5% believed they were managing *all* computer security management issues reasonably well. This shows a further deterioration in an already low level of confidence in organisational performance compared to 2002 and 2003 when 11% of respondents felt they were managing all computer security issues reasonably well.

Another reflection of the level of concern that exists about respondent organisations' performance in managing the security of their information systems is that 70% reported they had increased spending on some aspect of computer security during the last 12 months due to concerns about the adequacy of computer security within their organisations.

Has your organisation increased expenditure on computer security, including physical or personnel security, in the last 12 months due to concerns about the adequacy of computer security within your organisation?



Source: 2004 Australian Computer Crime and Security Survey
2004: 233 respondents/97%, 2003: 130 respondents/60%
2002: 90 respondents/95%

How did critical national information infrastructure organisations fare compared to others?‡

Thirty-five percent of respondents (ie, 84 respondents) consider their organisation to be part of the critical national information infrastructure (CNII); 51% (123 respondents) do not; and the rest were not sure of their status.

Total losses for CNII organisations was over \$8 million (or 52% of total losses for 2004) compared to under \$7 million (or 44% of total losses for 2004) for non-CNII organisations.[§] A comparison of the average annual losses for CNII organisations (\$98,685) versus non-CNII organisations (\$56,531) shows a greater disparity (almost double) between the financial impact of incidents between the groups. Also significant is that a greater percentage of CNII organisations (50%) reported experiencing one or more harmful electronic attacks than non-CNII organisations (42%) did. Therefore, although CNII organisations respondents are fewer in number, as a percentage they reported more harmful electronic attacks and their losses overall were substantially higher.

Harmful electronic attacks – including those which provide an attacker with administrator level privileges – commonly occur due to the presence of unpatched or unprotected software vulnerabilities or misconfigured^{**} operating systems, applications or network devices. Indeed, malicious scanning for software and system vulnerabilities occurs globally 24 x 7 in mammoth proportions. With the nature of scanning and exploit tools available to attackers, vulnerable systems are thus easily found and compromised. Forty-nine percent of CNII organisations (or 41 respondents) reported that it was the presence of unpatched software vulnerabilities and/or misconfigured operating systems and the like that contributed to the harmful electronic attacks directed against their systems. This figure compares to 48% (or 59 respondents) of non-CNII organisation respondents who made the same claim. Therefore, CNII organisations appear to share the same difficulties with patch management and system hardening that non-CNII organisations do. Given the criticality of CNII organisation networks and the seriousness of these types of vulnerabilities, this is concerning.

Notwithstanding the small sample size being analysed, there could be a variety of possible explanations for these results, however, which of these are valid and which are not is speculation. For example, CNII organisations may be better able to detect, investigate and cost successful attacks, thus making their reporting more accurate and under-reported for non-CNII organisations; or perhaps, CNII organisations, because of their profile, are more attractive targets for attackers and are attacked more often, resulting in a higher number of incidents and losses. We should also note that losses associated with computer security breaches are relative – a high dollar loss for one organisations might for them be an acceptable risk; whereas for a smaller organisation, it could mean financial ruin. So while, CNII organisations may appear to be bearing greater losses (impacts) than their non-CNII counterparts, these losses (impacts) may still be within an acceptable range if CNII organisations have sufficient resources to absorb such losses.

Whatever the actual explanation, these figures are still surprising as it would be expected that CNII organisations would fare better than other organisations because they should, arguably, be doing more to manage their higher risk. A risk assessment of any CNII organisation would recommend that organisations that supply essential services for the well-being of the community and economy, need to minimise their risks to protect not only their own information security interests (and if applicable, the interests of their shareholders) but the services they deliver to the community and on which the community and other industry depend. CNII organisations generally face similar threats and are susceptible to the same vulnerabilities and economic constraints as other organisations. But because the potential impact of breaches may be more serious for CNII organisations, the risk – if it is not properly mitigated and managed – will be higher. As such there is generally a more stringent requirement for security counter-measures in CNII organisations; and if this requirement is being met it should translate into fewer harmful incidents with lower impacts and fewer vulnerabilities. The figures in this survey show the contrary.

‡ This is the first year we have analysed how different organisation types perform in relation to each other; albeit we have limited this comparison to CNII versus non-CNII organisations. The problem with such comparisons is that the data sets being compared become even smaller and the validity of the results may be questioned. Notwithstanding this, critical information infrastructure protection is an important issue for most technologically dependent societies and we thought the results would be of interest.

§ Please note these quantified losses include all forms of computer crime and computer access misuse and abuse - not just harmful electronic attack incidents.

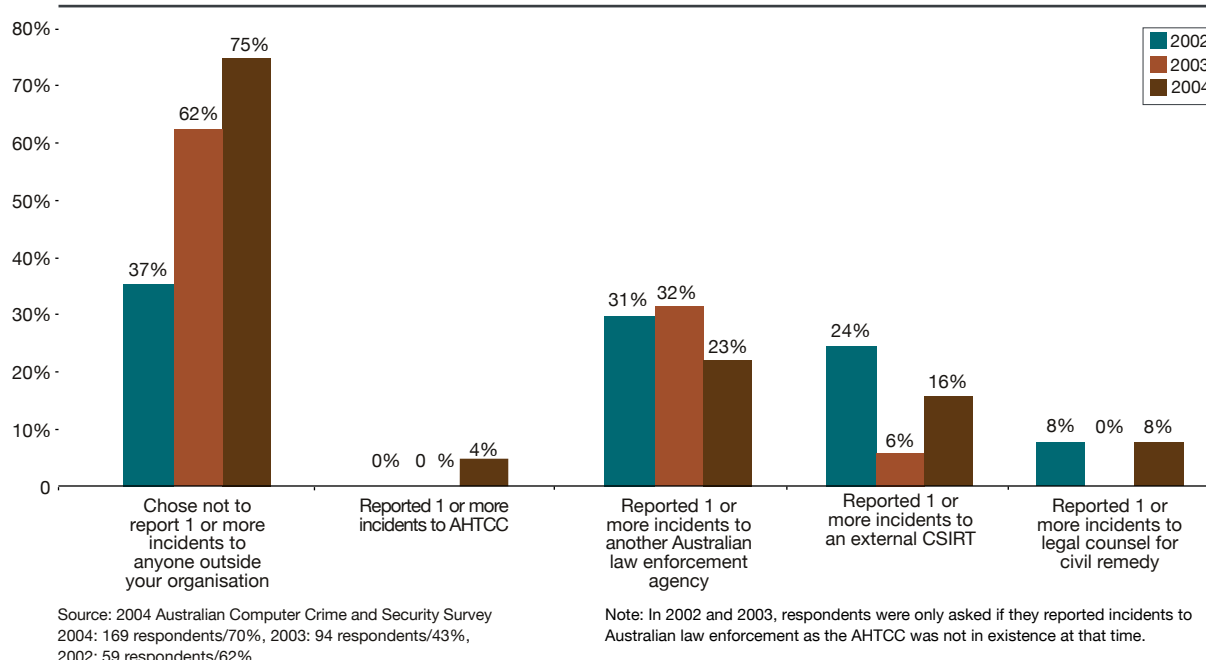
** Such misconfigurations may be caused unwittingly by administrators; or because administrators have not changed default low-security configurations of installed operating systems; or may be due to system changes that were made during a previous compromise.



REPORTING

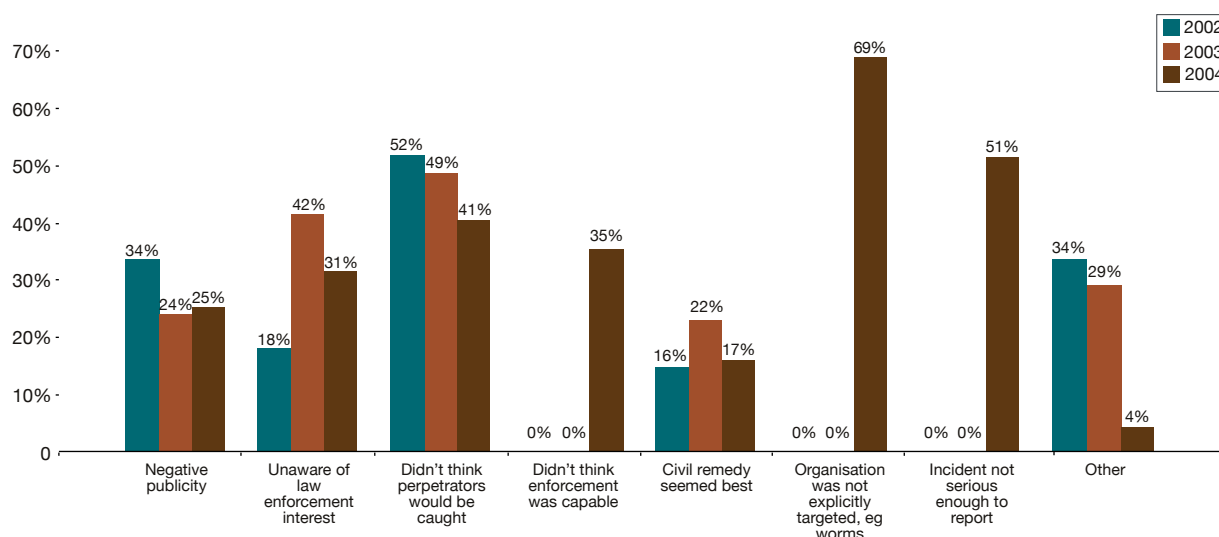
BEHAVIOURS AND ATTITUDES

If your organisation experienced electronic attacks which harmed the confidentiality, integrity or availability of computer network data or systems or other forms of computer crime within the last 12 months, to whom did you report the incidents?



This year, substantially more respondents (70%, compared to 62% in 2003) are reporting that they chose not to report harmful electronic attacks or other forms of computer crime to any outside party, including law enforcement. Based on feedback from previous surveys, we included new categories for reasons why organisations chose not to report what were otherwise harmful incidents of electronic attack or other forms of computer crime to law enforcement agencies.

If your organisation did not report electronic attacks which harmed the confidentiality, integrity or availability of computer network data or systems or other forms of computer crime to a law enforcement agency, what were the most important reasons?

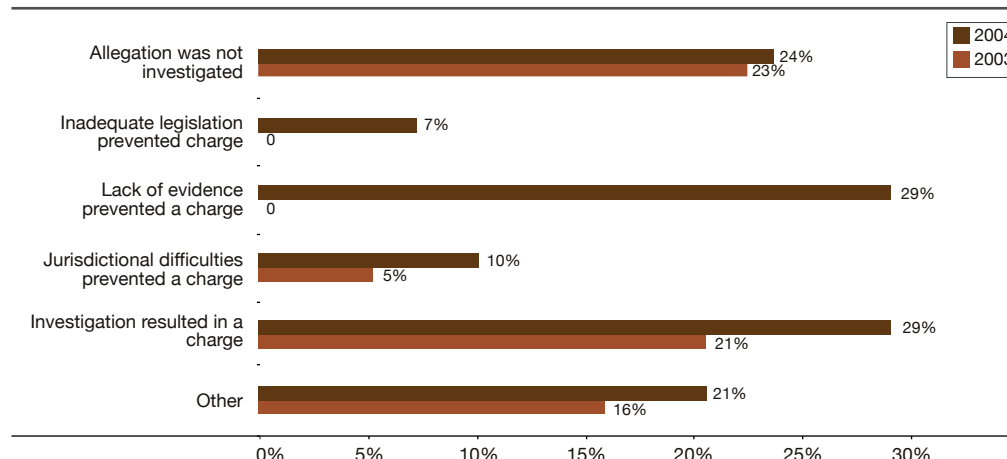


Source: 2004 Australian Computer Crime and Security Survey
2004: 107 respondents/45%, 2003: 107 respondents/50%,
2002: 27 respondents/28%

Note: In 2002 and 2003, 'didn't think law enforcement was capable', 'organisation was not explicitly targeted' and 'incident not serious enough to report' were not categories in this question.

The two most common reasons incidents of this type were not reported were that, although harmful, they were not considered serious enough (according to 51% of respondents) or, as is the case with virus or worm infections, the organisation had not been explicitly targeted (in the case of 69% of respondents).

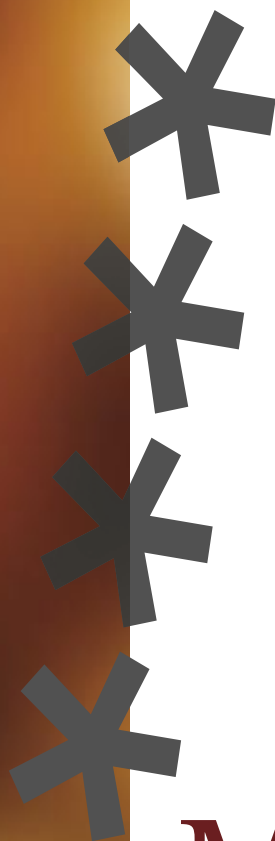
Outcome of incident allegations reported to law enforcement agencies



Source: 2004 Australian Computer Crime and Security Survey
2004: 42 respondents/18%, 2003: 61 respondents/28%

Note: In 2003, 'lack of evidence prevented a charge' and 'inadequate legislation prevented a charge' were not categories in this question.

For incidents that were reported to police, lack of evidence prevented a charge in 29% of cases; the incident was not investigated in 24% of cases; and the incident resulted in an investigation in 29% of cases, compared to only 21% of cases for 2003. Please note these figures are based on respondent reports only.



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 *2004 CSI/FBI Computer Crime and Security Survey* was not available for comparison of USA and Australian trends at the time of writing. However, readers may obtain a PDF copy from the CSI web site: www.gocsi.com.

The survey partners would also like to acknowledge the work of the authors of the four previous Australian Computer Crime and Security Surveys published in 1997,¹⁴ 1999,¹⁵ 2002¹⁶ and 2003.¹⁷ As a 2002 survey partner, we would like to thank Deloitte Touche Tohmatsu for permission to include results of the *2002 Australian Computer Crime and Security Survey* for comparison in this survey.

Survey questionnaires with business reply envelopes were sent to chief information security officers or their equivalents at 350 of Australia's largest enterprises. Most of these were private sector enterprises but also included large government departments. These enterprises 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 private and public sector 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 240, which included 75 hard copy submissions and 165 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 this standard. Also, in revising the survey each year, small changes to some questions have been made which makes absolute comparisons impossible. However, where questions have remained largely similar we have included previous years' responses as a guide to indicate general, rather than absolute, trends as they have been reported to us.

The value of this survey is that it depicts the best effort responses of IT professionals from a broad range of Australian organisations in the 12 month period prior to January 2004 when the survey collection phase commenced. It also provides a useful benchmark for various forms of computer crime and abuse. For readers interested in further information on this topic, the Australian Bureau of Statistics' *Business Use of Information Technology* survey¹⁸ also provides some data on the use of security technologies and the exposure to security incidents/breaches by Australian business.

SURVEY

PARTNERS, SPONSORS AND CONTRIBUTORS





Survey partners

Kathryn Kerr
AusCERT
The University of Queensland QLD 4072
www.auscert.org.au
Ph: 07 3365 4417
auscert@auscert.org.au

Australian Federal Police
(see AHTCC)

Alastair MacGibbon
Director
Australian High Tech Crime Centre
PO Box 401
Canberra ACT 2602
www.ahtcc.gov.au
Ph: 02 6246 2101
enquiries@ahtcc.gov.au

Detective Inspector Bruce van der Graaf
Computer Crime Team
New South Wales Police
PO Box Q566 Post Office
Sydney NSW 1230
Ph: 02 9269 3719
Fax: 02 9269 9797

Detective Superintendent Bert Hofer
Major & Organised Crime Division
Northern Territory Police Force
PO Box 39764
Winnellie NT 0830
Ph: 08 892 2344

Detective Inspector Brian J Hay
Major Fraud Investigation Group
State Crime Operations Comman
Queensland Police Service
GPO Box 1440
Brisbane Qld 4001
Ph: 07 3364 6464
Hay.BrianJ@police.qld.gov.au

Detective Senior Sergeant John Schrader
Officer in Charge
Electronic Crime Section
South Australia Police
GPO Box 1539
Adelaide SA 5001
Ph: 08 8463 7450

Detective Inspector Michael Grant
Officer in Charge
Fraud Investigation Services
Tasmania Police
GPO Box 308
Hobart TAS 7001
Ph: 03 6230 2956
michael.grant@police.tas.gov.au

Detective Acting Inspector Peter Wheeler
Major Fraud Investigation Division
Criminal Proceeds Squad & Computer Crime Squad
Victoria Police
Level 2, 549 St. Kilda Road
Melbourne VIC 3004
Ph: 03 9526 6622

Senior Detective Tim Thomas
Computer Crime Investigation
Western Australia Police Service
Level 7, 233 Adelaide Terrace
Perth WA 6000
Ph: 08 9220 0700
Fax: 08 9225 4489

Sponsors

Australian Federal Police

Attorney-General's Department

Department of Communications, Information Technology
and the Arts

Survey contributors

Oliver Binz
General Manager
b-sec Consulting Pty Ltd
Ph: 03 9682 5700
obinz@b-sec.com

Peter Elford
Consulting Engineer
Cisco Systems
Ph: 02 6243 0620
pelford@cisco.com

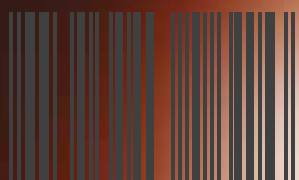
Ajoy Ghosh
Lecturer and Consultant in Cybercrime and Forensics
University of Technology Sydney
Ph: 02 9908 3812
ajoy@law.uts.edu.au

Danny Smith
Security Specialist, IT Security Office
Sun Microsystems
Ph: 07 3238 8321

Kim Valois
Director, Global Security Solutions, International and
Australia Region
Computer Sciences Corporation
Ph: 02 9034 3168
kvalois@csc.com.au

REFERENCES

- ¹ Computer Security Institute (2003), 2003 CSI/FBI Computer Crime and Security Survey, <http://www.gocsi.com/awareness/fbi.jhtml;jsessionid=JRSJPV0AGXCROQSNDDBCSKHY>
- ² AusCERT, NSW Police, Deloitte Touche Tohmatsu, 2002 Australian Computer Crime and Security Survey
- ³ AusCERT, AFP, Queensland Police, South Australia Police, Western Australia Police, 2003 Australian Computer Crime and Security Survey, <http://www.auscert.org.au/crimesurvey>
- ⁴ Attorney-General's Department (2003), Trusted Information Sharing Network for Critical Infrastructure, <http://www.cript.gov.au/www/CriptHome.nsf/HeadingPagesDisplay/What+is+Critical+Infrastructure?OpenDocument>
- ⁵ Standards Australia (2003), HB 171-2003 : Guidelines for the management of IT evidence, <http://www.standards.com.au>
- ⁶ AusCERT (28 March 2003), AL-2003.04 - Increase in fraudulent activity targeting users of online banking and electronic payment sites, <http://www.auscert.org.au/2909>
- ⁷ McNamara, Daniel, (15 February 2004) Police Investigation Trojan, <http://www.codephish.info/modules.php?op=modload&name=News&file=article&sid=55>
- ⁸ AusCERT (26 August 2003), AA-2003.03 - Recent Microsoft Vulnerabilities and Patches, <http://www.auscert.org.au/3379>
- AusCERT (10 December 2003), AA-2003.04 - Microsoft Internet Explorer incorrectly displays URLs, <http://www.auscert.org.au/3680>
- AusCERT (4 April 2004), AL-2004.10 - AUSCERT ALERT - Bogus Banking Email Allows Trojan Infection for Outlook Users, <http://www.auscert.org.au/3981>
- AusCERT (5 April 2004), AU-2004.007 - AusCERT Update - Vulnerability in Internet Explorer Allows Program Execution, <http://www.auscert.org.au/render.html?it=3990> (at the time of writing, no patches were available for this vulnerability).
- McNamara, Daniel (4 April 2004), The "Bank Withdrawal" trojan, <http://www.codephish.info/modules.php?op=modload&name=News&file=article&sid=96>
- ⁹ AusCERT (21 August 2003), ESB-2003.0588 - Microsoft Security Bulletin MS03-032 - Cumulative Patch for Internet Explorer (Q822925), <http://www.auscert.org.au/3371>
- AusCERT (26 August 2003), AA-2003.03 - Recent Microsoft Vulnerabilities and Patches, <http://www.auscert.org.au/3379>
- ¹⁰ AusCERT (26 August 2003), AA-2003.03 - Recent Microsoft Vulnerabilities and Patches, <http://www.auscert.org.au/3379>
- ¹¹ AusCERT (18 March 2004), AL-2004.07 - New Bagle.Q Worm Spreading Rapidly, <http://www.auscert.org.au/3957>
- ¹² Microsoft (February 2004), Microsoft Knowledge Base Article - 833786, Steps that you can take to help identify and to help protect yourself from deceptive (spoofed) Web sites and malicious hyperlinks, <http://support.microsoft.com/?id=833786>
- ¹³ LURHQ Threat Intelligence Group (2004), Sobig.a and the Spam You Received Today, <http://www.lurhq.com/sobig.html>; LURHQ Threat Intelligence Group (2004), Sobig.f Examined, <http://www.lurhq.com/sobig-f.html>
- ¹⁴ Office of Strategic Crime Assessments & Victoria Police, 1997 Computer Crime and Security Survey
- ¹⁵ Deloitte Touche Tohmatsu & Victoria Police, Computer Crime and Security Survey 1999
- ¹⁶ *ibid.*
- ¹⁷ *ibid.*
- ¹⁸ Australian Bureau of Statistics (2004), Business Use of Information Technology, 2002-03, 8129.0



.04