AUSCERT

NEW SOUTH WALES POLICE

Deloitte Touche Tohmatsu

2002 Australian Computer Crime and Security Survey

Contents

1. Executive Summary

This 2002 Australian Computer Crime and Security Survey has been produced jointly by AusCERT, Deloitte Touche Tohmatsu and the NSW Police.

As the only survey of its type in Australia focusing on the actual extent and nature of security incidents in this country, this year's survey builds on the two earlier surveys conducted in 1997[1] and 1999[2]. The survey has also been adapted this year to facilitate comparison with the pre-eminent equivalent USA survey, the 2002 CSI/FBI Computer Crime and Security Survey[3].

The survey presents a snapshot of Australian computer crime and security trends now and in the future. In particular, the survey objectives are to heighten awareness of the broad and complex nature of computer crime and security issues and trends; to seek to understand why such trends are occurring; and to promote the use of effective prevention, detection and response strategies.

Key Findings

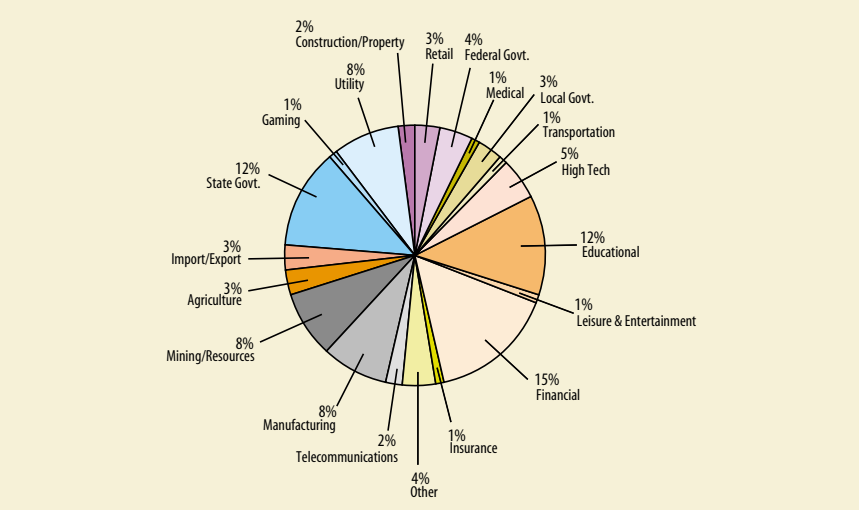
Based on survey responses from a wide cross section of Australian organisations in respect of the past 12 months, our key findings are as follows :

- Consistent with global trends, the volume of computer crime and security incidents in Australia is growing rapidly. 67% of respondents suffered a computer security incident in 2002, twice the level of 1999 (and higher than the USA), and 35% of these experienced six or more incidents.
- For the first time in Australia, the growing threat of external attack has now surpassed the threat of internal attack. 89% of Australian organisations suffering a computer security incident were attacked externally, while less than 65% were attacked internally.
- Although Australian organisations have invested heavily in security technologies, a significant level of computer crime and abuse continues to occur.
- 98% of respondents experienced some form of broader computer crime or abuse. The areas of greatest financial impact were laptop theft, data or network sabotage, virus and trojan infection, and computer fraud.
- Other frequently experienced incidents of computer crime or abuse which proved more difficult to quantify included denial of service attacks, and excessive network resource consumption through external scanning.
- The number of organisations reporting security incidents to law enforcement authorities has more than doubled to 31%, but most attacks are still going unreported to law enforcement. Pessimism regarding the apprehension of attackers is the primary inhibitor to greater reporting.
- Australian organisations are four times more likely to respond to security incidents with criminal action rather than civil lawsuits, the reverse of the trend in the USA.
- 43% of Australian organisations are willing to knowingly hire ex-hackers, three times more than in the USA.
- 60% of respondents recognised changing user attitudes as the most significant barrier to improved security. Other significant barriers included managing software upgrades and bug patches in a complex IT infrastructure, and keeping up to date with fast changing security threats.
- 70% of Australian organisations have increased their expenditure on information security over the past 12 months in response to security concerns or incidents.

2. Profile of Respondents

Our respondents come from public and private sector organisations and in terms of size and revenue (or budget expenditure) represent some of the largest organisations in Australia and – in the case of private sector organisations – they are also some of the most commercially successful. The most common sector groups to respond were the financial sector (15%), government sector (19% including local, state and federal) and the education sector (12%). At least 15% of organisations, excluding government agencies, (utilities, telecommunications, agriculture, transportation and medical) provide vital basic services to the community.

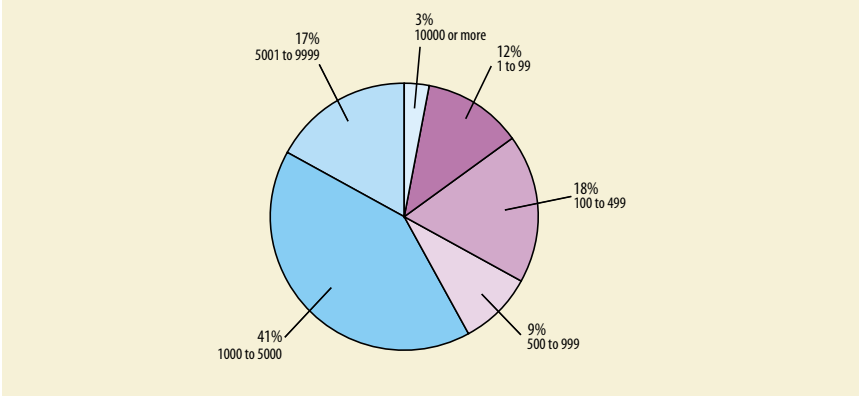
Respondents by Industry Sector



Source: Australian Computer Crime and Security Survey 2002
2002: 91 respondents/96%

The responses came mostly from large organisations in terms of both employees and annual gross income (or expenditure in the case of public sector organisations). The majority (61%) came from organisations which have 1,000 or more employees and 39% from small to medium size organisations up to 999 employees. Twenty percent of respondent organisations had over 5,000 employees.

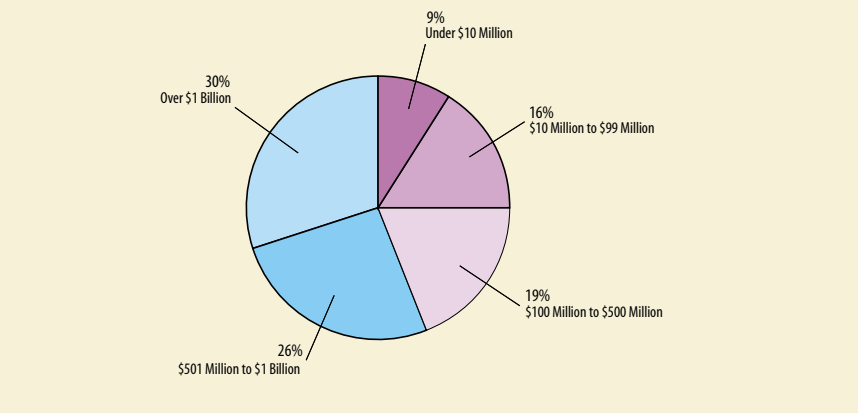
Respondents by Number of Employees



Source: Australian Computer Crime and Security Survey 2002
2002: 93 respondents/98%

Fifty-six percent of respondents have a gross income or expenditure in excess of $500 million. Thirty percent have a gross income or expenditure of over $1 billion annually. The profile of respondents overall is significant in terms of their importance to the economy. If these organisations also have information systems which are vital to the provision of critical services and/or their ability to earn revenue, then attacks against their networks may not only prove costly but may also have serious and widespread economic and social ramifications.

Respondents by Gross Income/Expenditure



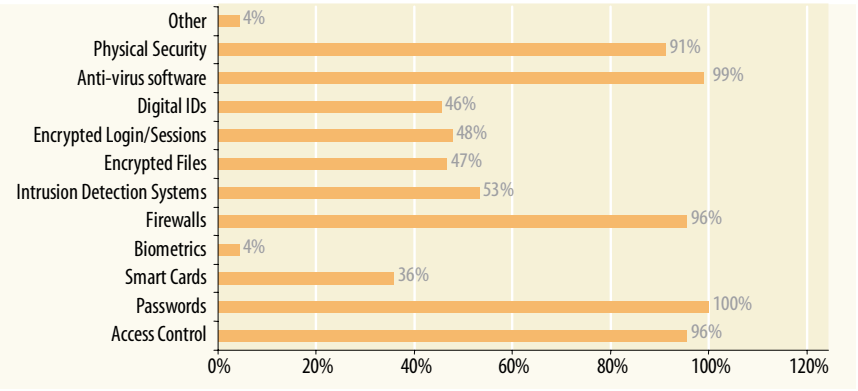
Source: Australian Computer Crime and Security Survey 2002
2002: 93 respondents/98%

What they use

The majority of respondents have physical security (91%), password protection (100%), access controls (96%), firewalls (96%) and use anti-virus software (99%). A smaller proportion uses encryption technologies (encrypted login/sessions 48% and encrypted files 47%) and stronger authentication technologies (biometrics 4%, digital IDs 46% and smart cards 36%).

The majority of respondents have a high uptake of basic computer security technologies. The lower uptake of stronger authentication and encryption technologies should not necessarily be interpreted as a deficiency in security. Such technologies are only useful if there is a recognised need to provide strong protection (confidentiality and integrity) to network data and services, and if they are implemented as part of an overall security policy framework which makes provision for monitoring and maintenance of this technology and the information systems they seek to protect.

Security Technologies Used



Source: Australian Computer Crime and Security Survey
2002: 92 respondents/97%

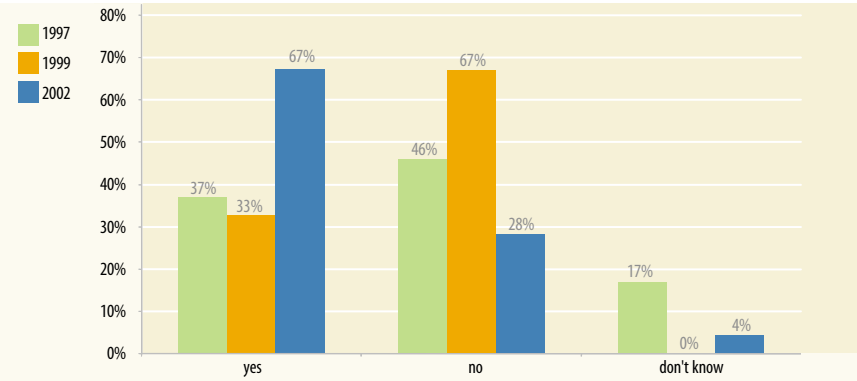
More respondents reported use of firewalls in Australia than intrusion detection systems (IDS) which is to be expected given that firewalls perform a more fundamental role in network security. However, as IDSs can be a valuable adjunct to a network security framework by assisting with the detection of computer attacks within a network perimeter, particularly when some attacks are capable of bypassing firewalls, it is surprising that the use of IDSs in Australia was not higher. Only 53% of respondents used IDSs in Australia compared to 60% in the USA, but in most other categories, the percentage usage of these technologies is very similar[4].

Of course the mere presence of computer network security technologies will not, by themselves, prevent or detect computer attacks. These technologies can only be effective if they, and the information systems they protect, are well supported and maintained and if their limitations are well understood. For example, a firewall which permits valid web traffic will not protect against web based attacks. Technology will not prevent all attacks but it can aid risk mitigation.

3. Security Incident Trends

The percentage of respondents who indicated that their organisation experienced computer security incidents or attacks in the last 12 months has approximately doubled compared to 1999 figures. Sixty-seven percent of respondents reported they had experienced a computer security incident or attack[i] in the last 12 months which is higher than the USA where 60% of respondents reported that they had experienced such incidents[5].

Did your organisation experience computer security incidents or attacks against its computer systems in the last 12 months?



**Note in 1999, respondents were not asked if they 'didn't know'*
Source: Australian Computer Crime and Security Survey
2002: 92 respondents/97%, 1999: 70 respondents/100%, 1997 159 respondents/100%

The figures may also reflect, to a degree, a greater willingness on the part of respondents to admit to experiencing computer attacks than in the past.

While more organisations as a percentage are experiencing attacks, on the positive side fewer organisations are reporting that they don't know if they have been attacked or not. With some forms of computer attacks being surreptitious in nature, detecting them can be difficult if organisations lack the skills, resources and technology necessary to detect such attacks. The task of detecting some attacks is made more difficult by the use of sophisticated hacking tools like root kits, loadable kernel modules and log scrubbers, which enable attackers to cover their tracks once they have gained privileged access.

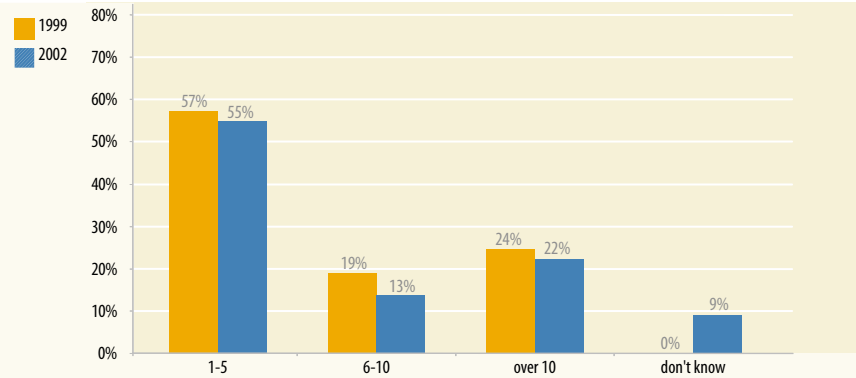
The increase in the number of respondents who have experienced computer security incidents is consistent with a range of other data sources and can be attributed to a variety of factors, including:

- Increased connectivity and use of Internet services which provides increased opportunity for attacks to occur;
- Increasing complexity of computer software which makes them generally more vulnerable to attack;
- The abundance of malicious code and attack tools available to attackers;
- The increasing use of high speed Internet access for home users, eg, cable modem or DSL, which offers attackers bandwidth and availability with generally little or no security;
- The demanding pace of technological change; and
- Users' slow adoption rate of good computer security practices, relative to the rate of uptake of connectivity to the Internet.

i For the purposes of answering this question, respondents were advised that a computer security incident was an attack against a computer or network either real or perceived. In other questions, the term is defined to mean any type of computer network attack, computer related crime, or misuse or abuse of network resources or access.

Despite the high uptake of basic computer security technologies, companies are still vulnerable. Global networks, Internet technologies, and a demanding pace of change are putting companies at risk. Security vulnerabilities in deployed technologies are being discovered and, more importantly, being openly disclosed at an ever increasing rate, with tools to exploit these vulnerabilities being readily available. Vendors attempt to keep pace with these vulnerabilities by issuing advisories and fixes. However, often it is the failure to note such advisories, and apply the recommended fixes, that leave organisations vulnerable to attack.
From time to time, attackers succeed in exploiting vulnerabilities not yet in the public domain and for which vendors have no available fix. Organisations are also more vulnerable to attack between the time when new viruses and worms are released and when anti-virus software vendors develop and make available their new anti-virus signatures. In these cases, sound computer security practices and well developed incident recovery plans will become vital to minimise risk.

If experienced incidents or attacks, how many incidents last year?

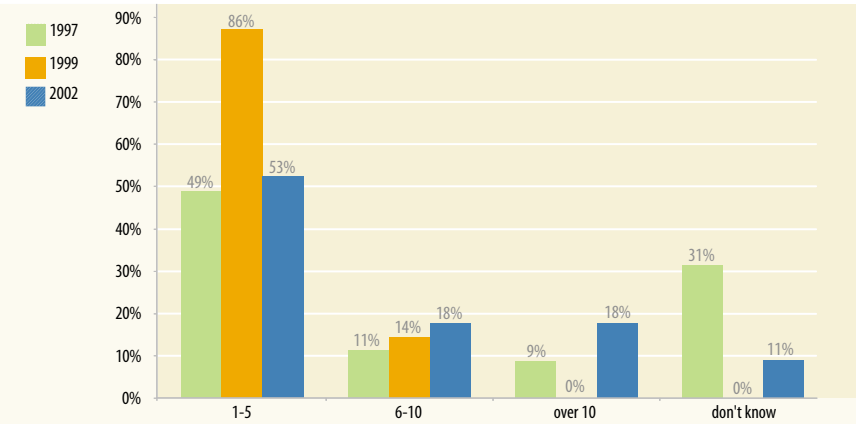


**Note in 1997, respondents were not asked this question. In 1999 respondents were not asked if they did 'not know'.*
Source: Australian Computer Crime and Security Survey 2002
2002: 67 respondents/71%, 1999: 21 respondents/30%

Overall, while more organisations have experienced computer security incidents, the number of incidents experienced by each organisation has declined slightly compared to 1999. However, with more than triple the number of respondents who answered this question compared to 1999, the results continue to be of concern with 13% experiencing between six and 10 computer security incidents and 22% experiencing more than 10 computer security incidents in the last year.

This year more organisations experienced a higher number of external attacks compared to 1999 (18% experienced six to 10 incidents and 18% experienced more than 10 incidents), which suggests that the threat from external attacks is increasing. On the positive side fewer organisations (53%) reported only one to five external attacks. Overall, 89% of Australian organisations suffering a computer security incident were attacked externally.

If experienced incidents or attacks, how many from the outside?

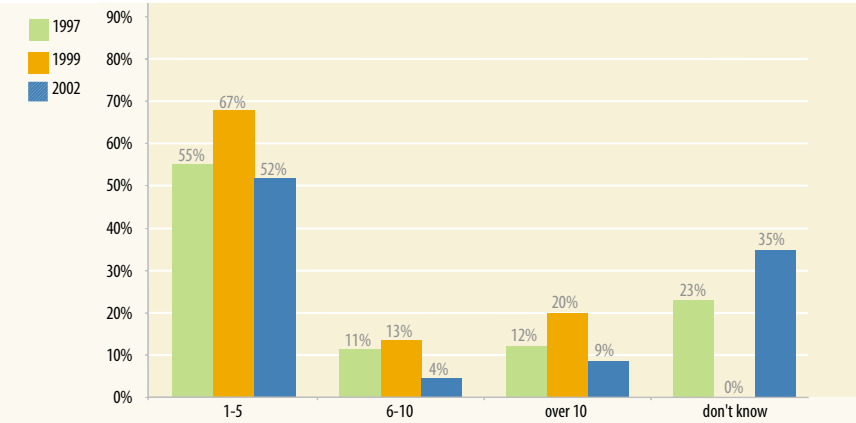


**Note in 1999 respondents were not asked if they did 'not know'.*
Source: Australian Computer Crime and Security Survey 2002
2002: 62 respondents/65%, 1999: 14 respondents/20%, 1997:37 respondents/23%

Fewer respondents experienced internal attacks (65%) compared to external attacks (89%) and compared to previous years. In fact, the gap between the percentage indicating internal and external attacks is possibly even higher, as those respondents who did not answer the question relating to the number of inside attacks, potentially indicate that they experienced no internal attacks at all. A similar trend can be seen from the CSI/FBI survey[6]. This contradicts the popular belief that most attacks originate from the inside and companies should focus more on their employees. It strongly suggests that the threat from insiders is declining relative to external attacks.

This does not mean the threat from insiders should be underestimated – for well-protected systems the opportunity to do the greatest harm will still probably come from insiders. Insiders know their organisation's most valuable assets and greatest vulnerabilities and where a personal grievance is the motivating factor, generally can be more determined to inflict greater harm than an indifferent outsider.

If experienced incidents or attacks, how many from the inside?



**Note in 1999 respondents were not asked if they did 'not know'.*
Source: Australian Computer Crime and Security Survey 2002
2002: 46 respondents/48%, 1999: 15 respondents/21%, 1997: 53 respondents/33%

Case Study

GreenGrocer.com.au

In March 2000, the Computer Crime Investigation Unit of the Commercial Crime Agency, NSW Police, investigated a sabotage attack against the GreenGrocer's network, which made it fail on two occasions. One of the attacks involved remotely deleting operating system files and caused the site to be unavailable for five days while analysis, clean up and recovery occurred. As an e-commerce merchant, GreenGrocer's network was critical to the company's ability to receive orders and earn revenue, which at the time was estimated to be about $22,500 per day.

As a result of a complaint made by GreenGrocer, NSW Police made enquiries with Telstra. An audit trail maintained by Telstra showed a remote connection immediately prior to the two incidents originated from an IP address belonging to a cable modem customer, who was identified as a former computer network engineer who had resigned from GreenGrocer days previously following a dispute with management.

Further forensic analysis showed the perpetrator had on the first occasion telneted into the GreenGrocer's network router and deleted critical router files, rebooted the router and caused GreenGrocer to lose its connection to the Internet. In the second attack, using the pcAnywhere application, the perpetrator remotely accessed a server and deleted critical operating system files causing the server to fail.

The perpetrator launched the attacks by utilising remote access services which were enabled during the period of his employment. The case highlights the importance of adopting sound personnel security practices such as disabling accounts following the departure of employees with privileged levels of access and of the need to monitor and better secure remote access services when they are required. The perpetrator was convicted in February 2002 on two counts of damaging data in a computer, which carries a maximum sentence of 10 years imprisonment under s. 310(a) of the NSW Crimes Act 1900 but received an 18 month suspended sentence.

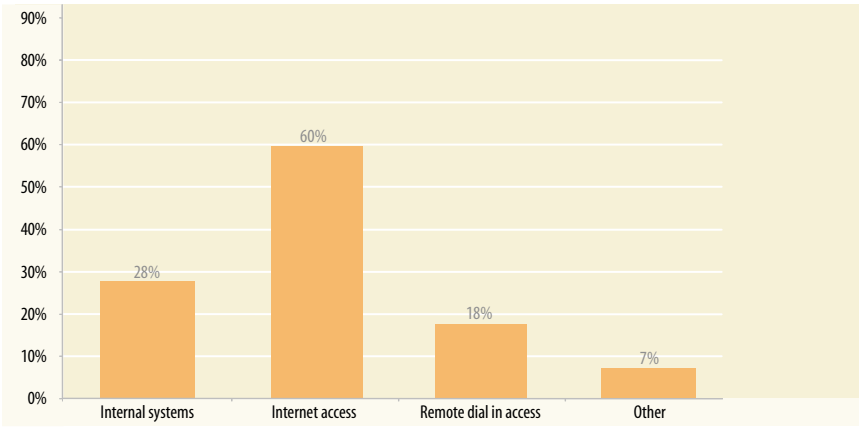
This year respondents were asked whether they knew if an attack came from insiders or outsiders and in the case of insiders, 35% did not know. This uncertainty is probably because insiders have greater legitimate access to an organisation's information systems and, for many organisations, fewer resources are devoted to monitoring or detecting insider use or misuse, or by failing to disable active accounts of former employees/contractors.

With more businesses and organisations moving their operations and data on-line, external attackers will potentially have an increasing number of targets to exploit. Those with the resources, skills and motive to target an organisation represent the most serious external threat.

Many powerful and easy to use attack tools exist in the public domain ready to be used in both a discriminate and indiscriminate manner. Although advanced resources and skills are needed to pose a significant threat to well-protected systems, attackers need only find one vulnerability to exploit (human, procedural or technological) to potentially inflict significant harm.

For 60% of respondents, the Internet was their most frequent point of attack, whereas only 28% cited their internal systems as their most frequent source of attack.

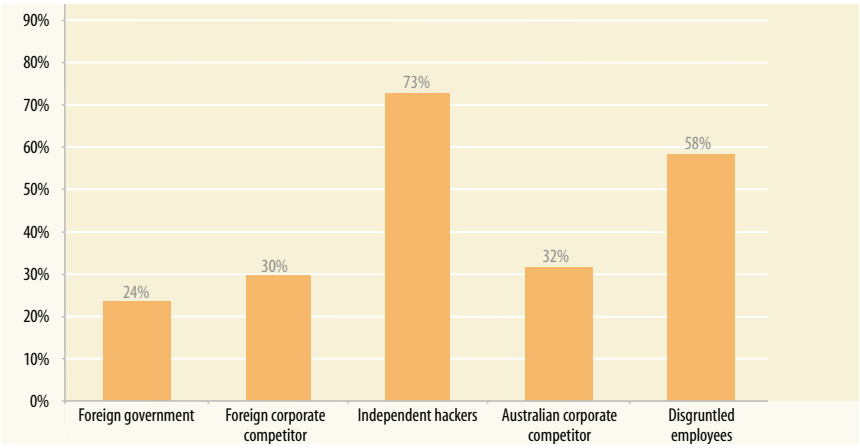
Most Frequent Points of Attack



Note: Respondents were asked to give a rating of 1 - 5 (1 for least and 5 for most frequent point of attack) for each category.
Source: Australian Computer Crime and Security Survey 2002
2002: 75 respondents/79%

The majority of respondents (73%) identified independent hackers as the most likely source of attacks on their network, followed next by disgruntled employees or contractors at 58%. Only 24% thought that foreign governments and 30% thought that foreign corporate competitors were the most likely source of attacks. Certainly, government agencies with national security classified material and companies which have developed or are developing profitable innovations are more likely to be the targets of cyber espionage and/or sabotage.

Most Likely Sources of Attack



Note: Respondents were asked to give a rating of 1 – 5 (1 for very unlikely and 5 for most likely source of attack) for each category.
Source: Australian Computer Crime and Security Survey 2002
2002: 83 respondents/87%

How prevalent is cyber espionage and sabotage?

If foreign governments and corporate competitors choose to direct such activity towards their adversaries or competitors – and many do, they will have at their disposal, more sophisticated computer attack skills and resources than your average script kiddie. In the USA, theft of proprietary information was reported by 13% of respondents as a source of financial loss[7] and was the largest source of financial loss (currently estimated to be over $US170 million) compared to all other categories[8]. Clearly, for those who seek to obtain proprietary information, it can be a lucrative business. But if organisations fully understand and recognise the nature of the threat they face, they will be in a position to more effectively manage it by developing appropriate protection and mitigation strategies to minimise the overall risk to the organisation.

If an attacker is sufficiently skilled and his goal is to steal information rather than destroy data or disrupt services, the attack may never be detected or if an attack is suspected, what is left of the forensic trail is likely to be insufficient to establish or prove a case, let alone identify the true source. With the odds in the skilled attacker's favour, it is likely that more attacks of this nature are occurring than many organisations realise.

It is quite possible, therefore, that of the 20% of respondents that reported system penetration by an outsider, or of the 39% that reported unauthorised privileged access, a proportion of these attacks may have been motivated by the desire to obtain sensitive or proprietary information for personal, political or commercial gain. However, determining the motive of an attack is often difficult to gauge on the basis of the forensic evidence left. For many cases of unauthorised privileged access or system penetration, without a full civil or criminal investigation, determining both the motive and the real impact of the attack may never be known. However, personal or financial gain is likely to be the motive for 24% of respondents who reported they experienced the electronic theft or breach of confidential or proprietary information and for the few who experienced wiretapping (1%) and telecommunications interception (1%).

Case Study

In a recent case, an Australian organisation (the client) discovered that its valuable confidential and strategic information had been leaked to a competitor. The leak was the source of considerable angst and financial loss not only for the client organisation but for the service organisation that was entrusted with the information prior to its leak. In order for the service organisation to preserve its relationship and reputation with its client, it was necessary to conduct a thorough investigation to determine the cause and source of the leak. Law enforcement agencies were also involved in the investigation.

Investigation showed that an employee of the service organisation had used the confidential document as a style template but inadvertently failed to save the changes to the document which would normally have removed the sensitive content. The employee e-mailed the unsaved template to another of its clients. The recipient, or someone within the recipient's organisation, realising the significance of the document, subsequently leaked it to the first client's known competitor.

Improper use of computer technology led to a breach of security and subsequently to a deliberate leak of confidential information. The case also highlights the potential liability issues which can affect organisations if they contribute to someone else's loss, even inadvertently.

Unlike espionage, sabotage can be malicious and indiscriminate, such as occurs when a hacker indiscriminately defaces a web site, launches a denial of service (DoS) attack or releases a virus with a damaging payload. However, like espionage, many forms of sabotage are motivated by personal, financial or commercial gain and for victims often pose a more serious threat. One well-known case of sabotage for personal reasons involved the use of radio-controlled transmissions to attack the Maroochy Shire Council sewerage system in Queensland over a four month period in 1999 and 2000, for which the attacker was convicted in October 2001.

Although the number of respondents who reported financial loss due to sabotage of data or networks was relatively low (9%), in dollar terms the cost of these attacks was high, accounting for 18% of total losses, and the second highest category of loss overall. In reality with 9% reporting financial loss arising from data or network sabotage and only 7% actually quantifying the loss, the costs are likely to be higher. For one organisation that loss was assessed to be $1 million.

Hackers – a problem for every publicly connected network?

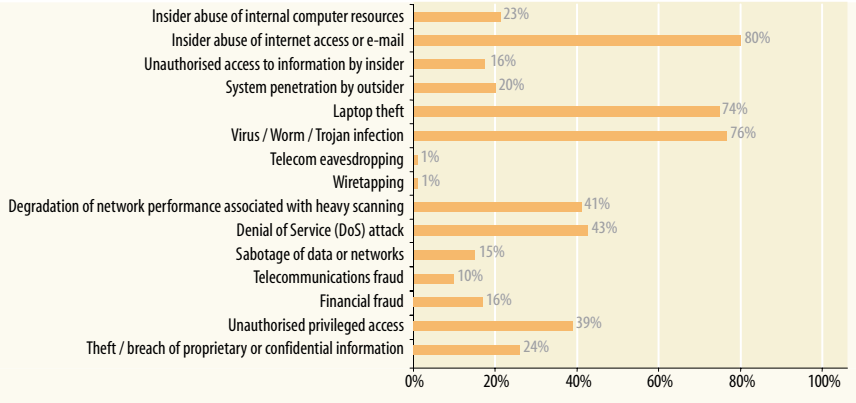
For all organisations with publicly connected networks, independent hackers will always represent a serious threat, regardless of the nature of the organisation's business or its profile. The motive of independent hackers will vary considerably and may include financial gain, malicious damage (eg, web site defacements, DoS attacks, release of viruses and worms) or a common favourite, the theft of network resources (eg, bandwidth usage) for personal use.

The relentless barrage, and global nature, of malicious activity that occurs against networks 24 hours a day, means that network and system administrators have to be constantly up to date with the latest anti-virus signatures, software patches and aware of the nature and impact of ongoing changes to their network architecture and environment. Has a network user, for example, installed an unauthorised modem in order to gain faster access to the Internet and thereby bypassed the firewall, IDS and virus checkers? Did a user introduce an infected floppy disk on the internal network bypassing the gateway virus checking? One small transgression may result in a back door trojan being installed and provide with it, future undetected network access or result in other forms of serious network compromise.

It is not so much that independent hackers are necessarily highly skilled that makes the threat from them so serious – though some are – but rather, it is the combination of the sheer volume of attacks that are attempted on a daily basis; the rapidly changing nature of the attacks and vulnerabilities; and that many attack tools are sophisticated and powerful and provide low-skilled attackers with an easy to use interface.

Network and system administrators have the additional burden of getting network defence right all the time, whereas an attacker needs to find only one point of vulnerability to do damage.

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



Source: Australian Computer Crime and Security Survey 2002
2002: 93 respondents/98%

Viruses, worms and trojans

Although 99% of respondents use anti-virus software, 76% of them reported they had been infected by viruses, worms or trojans and 43% reported financial losses as a result. Clearly, while information and IT security technologies have brought us many benefits, there is still no such thing as "set and forget it" technology. Security will only improve by adopting policies, practices and procedures which allow us to better manage, monitor and interact with the technology deployed on our networks.

In most, but not all cases, infection is usually due to one or two causes – the anti-virus software was not up to date and/or the worm or virus exploited vulnerabilities in unpatched operating systems or applications. Neither solution is in itself difficult to achieve, yet many organisations continue to be attacked. In the case of home users and small businesses, the problem appears primarily to be the need to raise awareness of the importance of patching operating systems and keeping anti-virus software up to date on a daily basis. For larger organisations, which have a better understanding of the threat, the problem emerges from the logistical difficulties when there are hundreds or thousands of machines to be patched on a frequent basis. Evidence that these issues are causing difficulties for organisations, is apparent from the 56% of respondents who acknowledged that configuration management presented challenges or posed difficulties for them, as did the 56% who identified keeping up to date with threat and vulnerability information and changes in technology.

While the deployment of prevention strategies requires a daily commitment of resources, it can pay dividends many times over. Consider the potential impact of recovering from a major worm infection. During 2001, there were several worms and viruses which were particularly insidious. Nimda, Code Red II and Sadmind/IIS are just three examples of worms which caused root (system administrator level) compromise or installed 'backdoors' into infected machines. To avoid the ongoing harm of giving hackers unrestricted access to the network, an infection by any one of these would require the machine to be taken off line, the hard drive formatted and the operating system and local applications reinstalled and re-patched and, where applicable, the files reinstalled from back up copies. If multiple machines on a network are infected, as will occur if the worm exploits network shares, the time for clean up and recovery can potentially stretch to days or weeks, depending on the extent of the infection. It is not surprising that one organisation alone reported the cost of this form of computer attack was $100,000 in the last 12 months.

The media appears less interested in trojans than worms and viruses probably because their impact is often less apparent to victims. Trojans do their greatest harm by working quietly in the background unbeknownst to the user. Trojans commonly are installed unwittingly by users who are duped into opening e-mail attachments containing the executable programs. How many people have sent cute or amusing executable programs as e-mail attachments to their friends? While the program performs one harmless function, in the background it installs a backdoor giving the attacker (either the sender of the e-mail or any other hacker who scans the Internet looking for resident trojans) future undetected access to the network and files.

Case Study

SubSeven trojan

In the following trojan attack, the Australian based hacker chose to advertise his presence, but only after he had covertly observed the victim for a nine month period.

In January 2001, a victim in the United States advised USA law enforcement that a hacker had gained access to his computer via his high-speed cable modem. The victim had installed anti-virus software in late 1999 but had not updated it since that time. The victim alleged the intruder was able to type messages to him on his screen, describe what he was wearing via his web cam and access, delete and modify files on his computer.

Forensic analysis of the victim's computer revealed the presence of the SubSeven trojan. The trojan was placed on the victim's system in May 2000. A personal firewall was installed on the victim's system in October 2000, but the intruder retained access to the victim's computer despite its presence. The trojan was configured to notify the attacker on an IRC chat channel when the victim was online, and with which IP address.

Certain information regarding the source of the intrusion was found through analysis of the victim's computer, including information programmed into the trojan by the attacker. This did not conclusively indicate the source of the attack, but provided avenues of inquiry for investigators. Inquiries with Internet service providers in the United States and subsequently in Australia identified the probable attacker. When interviewed, the offender admitted to his actions and was cautioned but not charged by police.

Network service unavailable or degraded

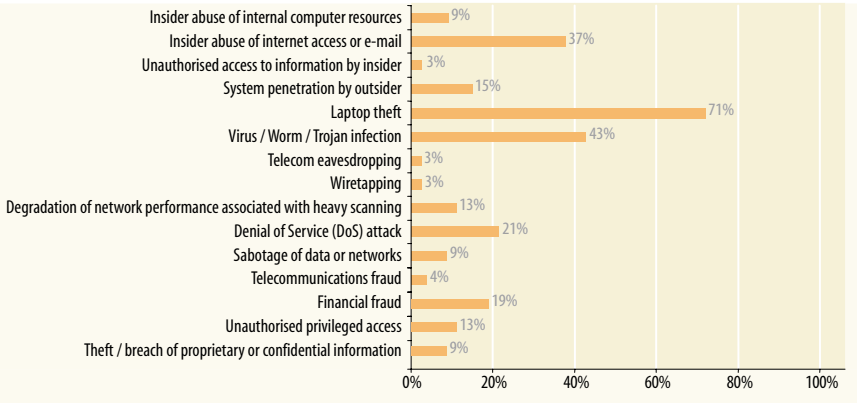
During the latter part of 2001, a spate of worms increased the level of scanning globally, as they looked for new hosts to infect, as well as inflicting other damage. In all likelihood, the degradation of network performance associated with heavy scanning[ii] reported by 41% of respondents, is probably, at least in part, a result of this activity. The degradation reported was of sufficient severity that 13% of organisation experienced financial losses associated with it, and 9% reported losses in the vicinity of over $160,000 overall. Even if organisations have no vulnerabilities to exploit remotely, they may still experience financial losses due to network degradation associated with some forms of propagating malicious code or automated and powerful hacker scanning tools. Where an organisation's Internet bandwidth is saturated by such traffic, legitimate traffic to Internet services, such as e-mail or web etc, will fail. Usually organisations must pay for the extra traffic generated by this activity, further compounding these losses.

While reports of DoS attacks have occasionally featured prominently in the media, few security professionals would classify them as a serious problem for Australian organisations. With 43% of respondents indicating that they experienced DoS attacks and 21% experiencing financial losses associated with such attacks, DoS attacks are probably more serious and more common than many realise.

ii Degradation of network performance associated with heavy scanning is a new category of computer attack/abuse, which does not appear in the CSI/FBI Computer Crime and Security Surveys. It was included to assess the indirect impact of rapidly propagating Internet worms and automated malicious scanning tools.

4. Financial Impact Trends

Which of the following types of computer attack, crime or misuse resulted in financial losses for your organisation in the last 12 months?



Source: Australian Computer Crime and Security Survey 2002
2002: 75 respondents/79%

In the following case, a single report to law enforcement led to the conviction of an Australian hacker and the discovery of a global network of compromised machines, some of which had already been used to launch distributed denial of service (DDoS) attacks. DDoS attacks are more powerful than ordinary DoS attacks as they utilise numerous compromised agents to participate – hence the distributed nature of the attack. Had the attack remained undetected and unreported, given the scale of the compromises and the presence of DDoS tools on some of the compromised machines, a potentially damaging DDoS attack may have resulted.

Case Study

An Australian university reported to law enforcement that a machine within its network had been compromised, allegedly from an Australian ISP. It appeared this machine had been used as a base for the hacking of about 70 other machines over a two week period. The secondary victim sites were predominantly machines owned by academic institutions from around the world.

Utilising AusCERT's contacts, the owners of these machines were notified that they had possibly been compromised and were requested to provide details to law enforcement. A number of secondary victims subsequently confirmed they had been successfully compromised. Law enforcement investigation determined the apparent source of the intrusion into the university was a compromised account with the ISP. Further inquiries identified a telephone number used to dial into the account and a probable attacker.

The attacker installed a trojaned secure shell (ssh) on the primary university system, allowing connection to the machine bypassing other controls. Many of the secondary victim systems were running Red Hat Linux 6.2 'out of the box', with little configuration, no patching and no routine logging or system monitoring. There was evidence the secondary compromised machines had been used to conduct further hacking activity and DDoS attacks. When conducting inquiries with the source ISP and other telecommunication providers, other compromised accounts used by the attacker were identified (in addition to that used to attack the primary university victim).

When interviewed, the offender made a full admission of hacking into the ISP, the university system and then into other systems worldwide. In September 2001, the offender entered a plea of guilty to charges of computer offences. He said he was aware of what he was doing and did it for the 'thrill'.

The 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
Theft/breach of proprietary or confidential information	4	10,000	150,000	72,500	290,000
Unauthorised privileged access	8	1,000	50,000	13,275	106,200
Financial fraud	7	500	600,000	115,288	807,000
Telecommunications fraud	2	1,000	100,000	50,500	101,000
Sabotage of data or networks	5	1,000	1,000,000	204,600	1,023,000
Denial of Service attack	8	1,500	100,000	22,688	181,500
Degradation of network performance associated with heavy scanning	7	1,500	100,000	23,071	161,500
Wiretapping	1	1,000	1,000	1,000	1,000
Telecom eavesdropping	1	10,000	10,000	10,000	10,000
Virus/Worm/Trojan infection	23	100	100,000	38,743	891,100
Laptop theft	48	2,000	100,000	26,331	1,263,900
System penetration by outsider	7	1,000	40,000	26,143	183,000
Unauthorised access to information by insider	5	5,000	100,000	29,000	145,000
Insider abuse of Internet access or e-mail	13	100	200,000	37,162	483,100
Insider abuse of internal computer resources	4	1,000	100,000	33,500	134,000
TOTAL ANNUAL LOSSES					**5,781,300**

Note: 75 survey respondents acknowledged financial losses, but only 60 of these (80%) could quantify the losses.

Calculating the cost of computer crime

Placing a value on intangibles such as lost business opportunities, erosion of consumer confidence or quantifying the cost of misuse or degradation of network performance is difficult. Of those respondents who provided estimates of losses, a few indicated these values reflected the cost of investigation and recovery only. A few others indicated that despite the anonymity of the survey they were not prepared to disclose their losses. While 75 respondents (79% overall) indicated they experienced financial losses arising from various types of computer crime, attack or misuse, only 80% of these were willing or able to quantify those losses. Hence, the estimates of losses provided are undoubtedly conservative.

Where's my laptop?

So while laptop theft resulted in financial losses for 71% of organisations and ranked as the most costly computer crime in Australia, it would also be the easiest for organisations to quantify. But, even though laptop theft is clearly a serious problem experienced by many organisations, we need to be careful how we interpret these figures. It does not necessarily follow that laptop theft poses the single greatest threat to an organisation's computer and network security. Certainly, apart from the loss of the hardware, laptop theft also potentially may be the conduit for theft of confidential or proprietary information or the means by which remote privileged access to a network is achieved. In these cases, the theft of the laptop may exceed the value of the hardware many times over.

Net abuse by employees

Insider abuse of Internet access or e-mail was reported by 80% of the respondents, but only 37% attributed a financial loss arising from this activity. Aside from the difficulties associated with calculating lost worker productivity, organisations may consider this issue more of a personnel policy issue, rather than a direct cost. However, in the USA, abuse of an organisation's Internet access by employees is a growing cost to business that few organisations are tolerating9. It is likely we will see similar trends in Australia. In 2000, Telstra stood down 27 workers for allegedly using company computers to store and distribute pornography. Inappropriate use of e-mail (eg, spam, distribution of pirated software or offensive material) and inappropriate web access or use, (eg, engaging in on-line gambling or visiting pornographic sites) can potentially lead to legal and costly liability issues for organisations, unless appropriate action is taken, or more commonly results in lost productivity and/or the use of valuable network bandwidth. When you consider the amount of some of the losses cited in this category (up to $200,000 in one case), we are likely to see trends similar to the USA in future.

Financial fraud

In the USA, the cost of financial fraud accounts for 25% of electronic crime losses overall – and, after theft of proprietary information, was the second largest loss overall[10]. In Australia, losses arising from financial fraud were reported by 19% of respondents and accounted for 14% of total losses. While electronic fraud does not currently appear to be causing the same sort of losses relative to the USA, Australian law enforcement agencies believe this trend is likely to worsen in future.

Inexperienced on-line merchants

Victoria Police Computer Crime Investigation Squad reports that the use of bogus and/or unauthorised credit card numbers on e-commerce sites is increasing exponentially. And yet in recent times, investigations conducted by the Squad have identified a number of businesses that have entered the on-line trading arena with little or no experience in Internet security, and in doing so, have failed to protect their own interests and the interests of legitimate customers who provide their personal and credit card details. In the majority of cases, the companies involved were of a moderate size and had been trading for a number of years in the retail markets.

In the worst case, one company had no validation processes in place for either the purchaser details or credit card details. Others either failed to capture vital transactional information that would enable an offender to be traced, or had employed insufficiently trained staff to operate their on-line sites, or in some cases, were unable to understand and decipher the information that they were capturing.

In these cases, poor security on the part of the on-line merchant (inadequate customer identification and validation and transaction logging) made it easy for them to be defrauded.

It is therefore little wonder that, when executing a search warrant at a Melbourne address as part of an investigation of obtaining property by deception, police seized over $30,000 worth of goods ranging from computer components and software through to mobile telephones and other electrical equipment, all of which had been purchased from on-line merchants using bogus identities and credit card numbers. In this case the offenders turned out to be two boys, aged 16 and 17 years.

In cases of electronic fraud involving unauthorised credit card transactions, it is the merchant who bears the risk and therefore, it is the merchant, not the financial institution, or the legitimate owner of the credit card who is the victim.

Through the electronic theft of services or products, telecommunications and financial fraud accounted for $908,000 in losses for Australian companies during the last 12 months.

Detective Senior Sergeant Peter Wheeler, Officer in Charge of the Victoria Police Computer Crime Investigation Squad and Detective Senior Constable, Frank Schiliro, of the Computer Crime Investigation Unit, NSW Police, said there has been an increase in the commission of deception related offences against on-line business organisations and a misperception as to who are the real victims of such crimes:

"There has been, for some time, a misperception as to who is the actual victim in circumstances where an individual's credit card number or Internet account is fraudulently used without their authority. From a law enforcement perspective in Victoria, the victim of a fraudulent on-line transaction is the e-commerce merchant, ISP or telecommunications carrier etc that has in fact been deceived in order to provide goods and/or services. The innocent holder of the credit card or Internet account has not been subjected to a deception or suffered any loss and will only ever be a witness in relation to the transaction that has occurred."

"Greater incentive is now created for organisations that conduct on-line business or provide on-line services, to firm up their security, log keeping, screening and validation processes to minimise as far as possible their exposure to being deceived in the manner described. Whilst there is a school of thought that doing so means losing business, the alternative is to risk substantial corporate losses. The traditional processes of verifying identity should not be abandoned in the on-line environment. Companies who find themselves in such circumstances need to decide whether they absorb the loss or report the matter to police for investigation."

Other Australian state and territory jurisdictions have adopted a similar position with regard to the unauthorised use of credit cards over the Internet.

Case Study

On-line banking

In a recent case reported to the Victoria Police Computer Crime Investigation Squad, the client of a financial institution reported that more than $13,000 was missing from their accounts.

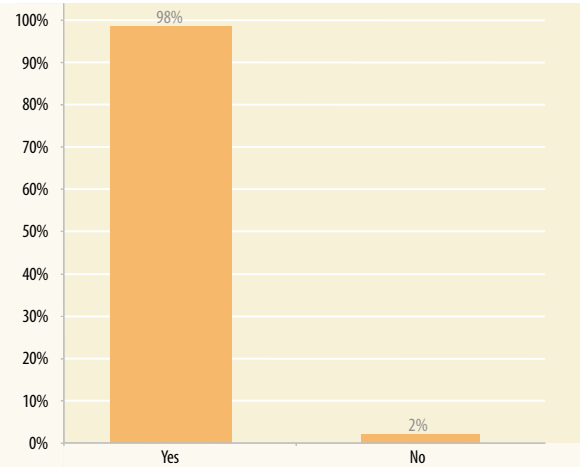
The client contacted the bank who then conducted an internal investigation. The investigation identified that the client's account had been accessed via Internet banking and that funds had been transferred to various overseas accounts. A number of IP addresses relevant to the transfers were captured and logged, as was other relevant information. A trace of the source IP addresses, revealed that the suspect transactions had been made from public Internet cafés. Enquiries at the cafés proved fruitless. As is the case with the majority of Internet cafés, records relating to the identity of users of their service are rarely kept, or at best are extremely poor and unable to be substantiated.

Examination of the client's computer system identified a commonly available trojan program capable of capturing the user's key strokes and therefore the username and password the client typed to access the on-line banking facility.

While only a few cases of this type have been reported to Victoria Police, it is likely that as criminals become more technically competent, there will be an increase in the types of crimes that exploit these security weaknesses. To prevent future occurrences, on-line banking sites may need to make their client identification and authentication processes more secure, for instance, by the use of challenge-response or one-time passwords or security tokens. In the meantime, in the same way that we need to secure our homes to minimise the risk of burglary, Internet banking clients need to implement a basic level of security on their home PCs. This can be achieved by keeping anti-virus software updated daily, ensuring the PC's operating system is patched as soon as notifications of new vulnerabilities emerge and by installing a personal firewall.

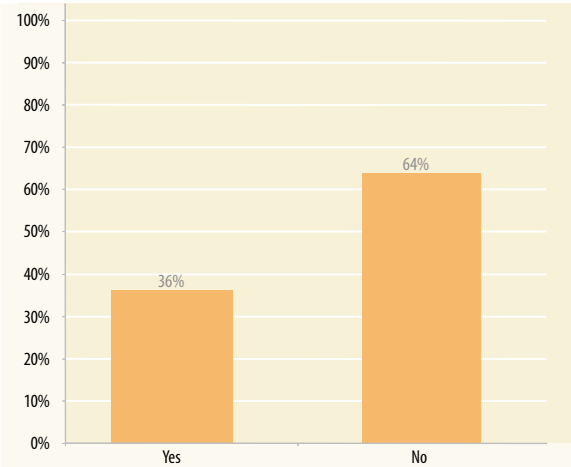
5. Web Incident Trends

Organisations with a Web Site



Source: Australian Computer Crime and Security Survey 2002
2002: 93 respondents/98%

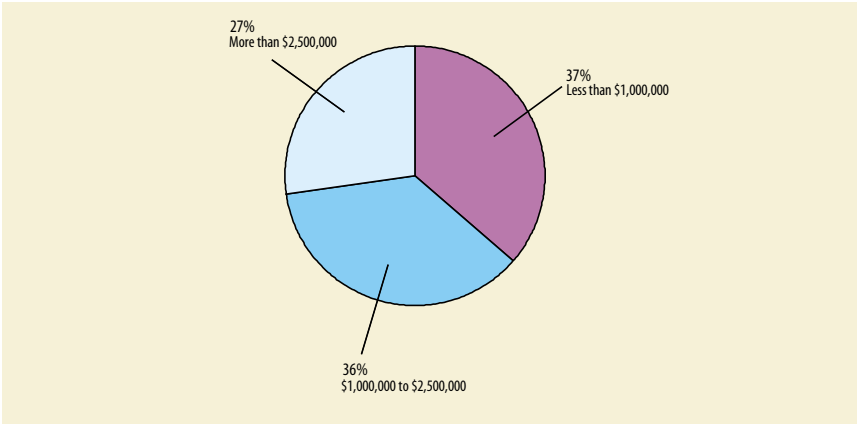
Organisations with Commercial Web Sites



Source: Australian Computer Crime and Security Survey 2002
2002: 92 respondents/97%

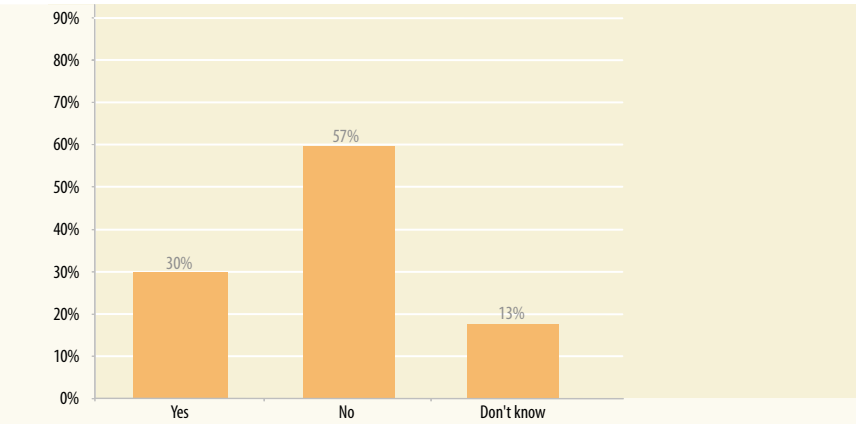
Ninety-eight percent of respondents have web sites, including 36% with commercial web sites. Of the few who quantified the annual revenues from their commercial web sites, 63% generated annual revenues of one million dollars or more.

Annual Revenue from Commercial Web Site



Source: Australian Computer Crime and Security Survey 2002
2002: 11 respondents/12%

Has your web site suffered a computer security incident or misuse within the last 12 months?

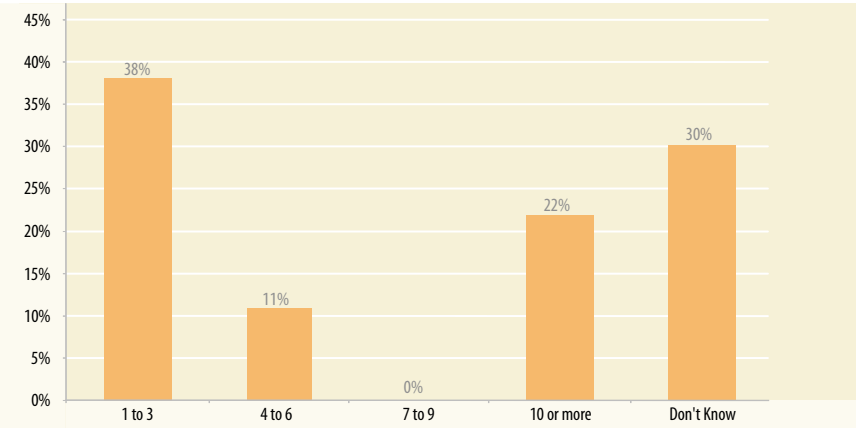


Source: Australian Computer Crime and Security Survey 2002
2002: 91 respondents/96%

Almost a third (30%) of respondents reported security incidents affecting their web sites. Thirteen percent reported lack of knowledge of incidents or misuse on their web sites, which could be due to inadequate collection and monitoring of web server logs.

Depending on the configuration of an organisation's web site, some forms of computer attacks against web servers may allow attackers to gain privileged access to the network and execute arbitrary code. As a general rule no information of value should be stored on the publicly accessible web server. As evident by the number of respondents who were unsure whether their web site had been attacked, or if they had, of the origins of those attacks, it is quite possible for these types of attacks to go unnoticed by under-resourced system administrators. Indeed, for some e-commerce sites or where there may be an opportunity for illicit financial gain, it is more likely an attacker will seek to hide rather than advertise their presence unlike web site defacements.

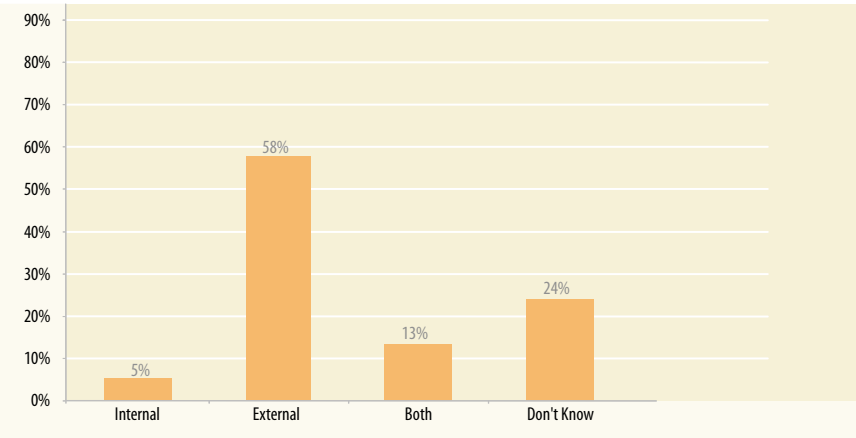
Web Site Incidents: if yes, how many incidents?



Source: Australian Computer Crime and Security Survey 2002
2002: 37 respondents/35%

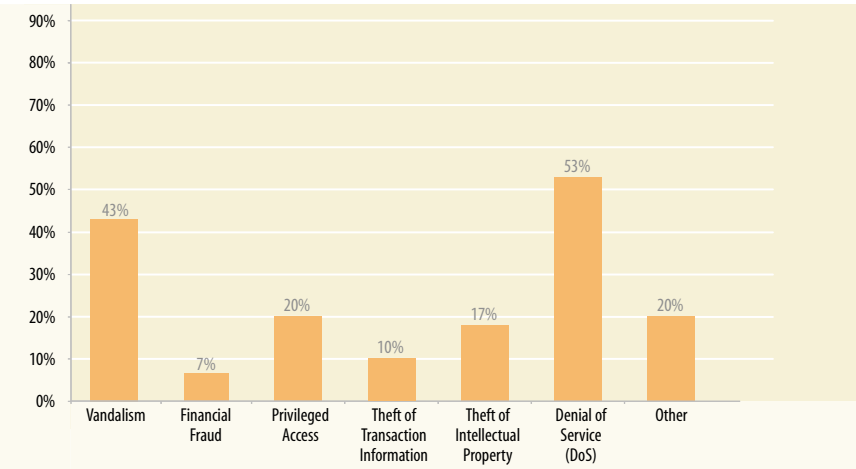
As would be expected, most web site attacks (58%) were externally sourced.

Web Site Incidents: did the attacks come from inside or outside?



Source: Australian Computer Crime and Security Survey 2002
2002: 38 respondents/36%

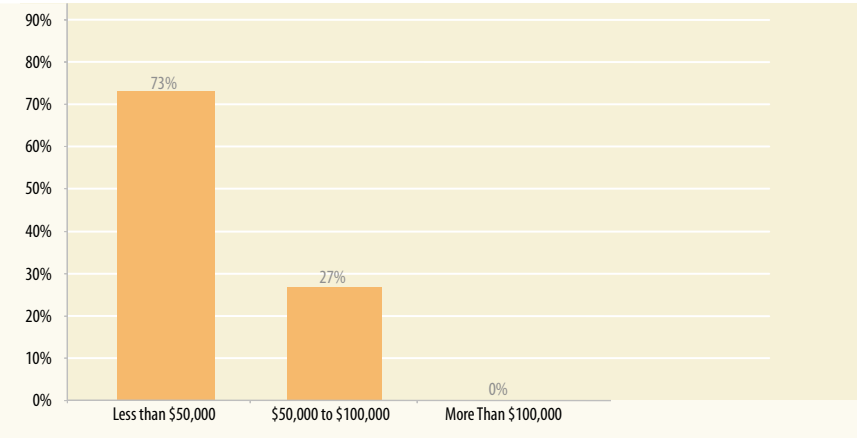
Web Site Incidents: what type of computer security incident or misuse?



Source: Australian Computer Crime and Security Survey 2002
2002: 30 respondents/32%

Of those respondents who reported attacks on their web site, DoS attacks were the most common at 53%, followed closely by web site vandalism (defacements) at 43%. Significantly, other potentially more serious forms of web-related attacks (financial fraud 7%, privileged access 20%, theft of transaction information 10% and theft of intellectual property 17%) were also reported. Within the 'other' category, organisations reported their web sites were used to relay spam, were subject to virus attacks and threats of damage, presumably for the purposes of extortion.

Losses From Web Related Incidents

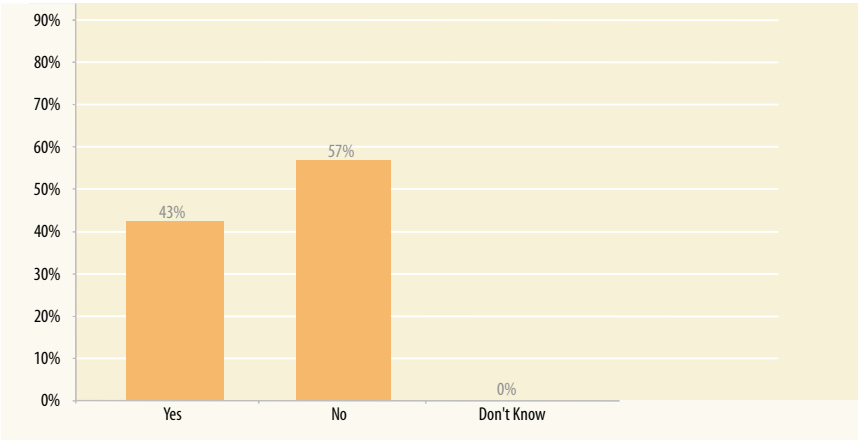


Source: Australian Computer Crime and Security Survey 2002
2002: 11 respondents/12%

From the few responses received, 73% estimated their financial losses from web based attacks were less than $50,000. As organisations build in greater functionality and more services on their web sites and as they become more dependent on the revenue derived from the web site, the potential for more damaging attacks will increase.

6. Security Management Trends

Would your organisation consider hiring reformed hackers?

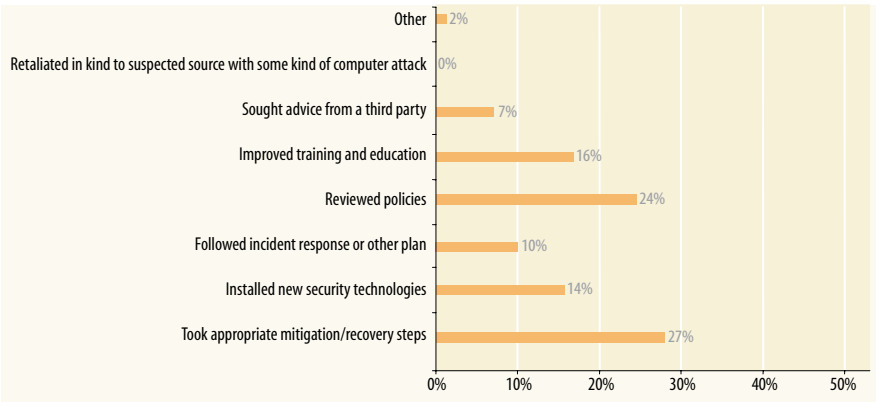


As a hacker you can always change your career and start working for 'the good guys'

Source: Australian Computer Crime and Security Survey 2002
2002: 90 respondents/95%

Respondents were asked if their organisations would consider employing, or hiring as consultants, 'reformed' hackers to perform computer security audits or penetration tests on their networks. Slightly more organisations (57%) reported they would not consider hiring a reformed hacker with the remaining 43% reporting they would. In the USA, few organisations were inclined to hire reformed hackers, with only 14% indicating they would and 69% indicating they would not[11]. Rather than focusing on hackers per se, decisions to employ personnel, be they reformed hackers, convicted criminals or any employee or contractor, in positions of trust, such as those involving privileged levels of access to business critical systems, should be made on an informed basis as far as possible within the limits of existing legislation. Pre-employment screening will not eliminate the insider threat but it may certainly reduce it if considered as part of a risk management and personnel security framework.

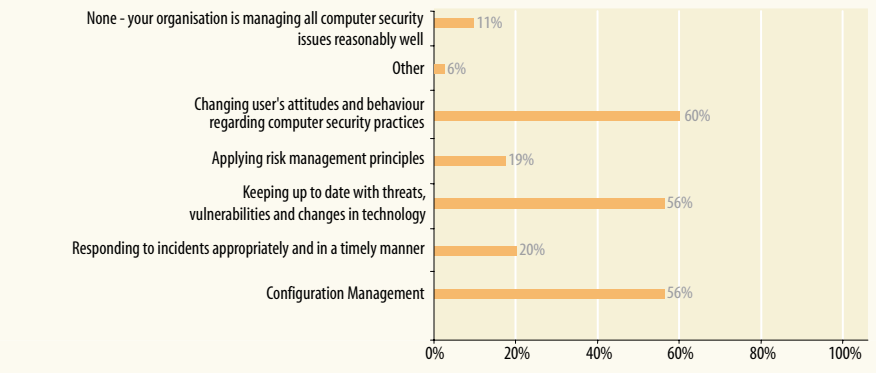
How did your organisation respond to the computer security incidents?



Source: Australian Computer Crime and Security Survey 2002
2002: 75 respondents/79%

Respondents who experienced computer security incidents were asked to report on the type of actions they took. Sixteen percent improved security education and training, which suggests that users may have been inadvertently responsible for contributing to the security breaches. Twenty-four percent reported that they reviewed their computer security policies as a result of computer security incidents. This suggests that, at the very least, these organisations wished to ensure the policies were not deficient, and some possibly were deficient. In practice, reviewing computer security policies following an incident ensures that the policies continue to meet the organisation's needs and are suitable for the changed environment.

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



Source: Australian Computer Crime and Security Survey 2002
2002: 88 respondents/93%

Computer security challenges

It is apparent from this survey that despite a relatively high uptake of fundamental security technologies (passwords, firewalls, anti-virus software), serious computer network attacks continue to occur. Notwithstanding the difficult and challenging threat environment with which organisations must contend, how the security of the network is managed and how users interact with the network, (ie to what extent do users adopt good computer security practices) will also have a bearing on how well organisations minimise their risks.

No organisation can neglect the human and process related network security activities, without experiencing some form of computer attack in the short term. The Honeynet Project studies[12] have consistently shown that default installations of operating systems are insecure. Default installations[iii] of Unix and Windows operating systems have been compromised within minutes of these machines being connected to the Internet. The Honeynet Project also showed that there is a high level of malicious hacker activity which is focused on locating and attacking machines with known and exploitable vulnerabilities connected to the Internet and that, with more efficient automated scanning and exploit tools, the rate of attack has increased.

Many of the most common types of attack – viruses, worms and trojans – could be prevented if organisations kept all their operating system and software application patches and anti-virus software up to date and by users adopting sound computer security practices. However, while this sounds straight forward, for some organisations it is not always easy to achieve.

iii These are operating systems which have been installed as is, 'out of the box'. Default installations have many services enabled that may not be necessary or understood by system administrators resulting in an insecure configuration. A default installation also means an operating system has not been patched to eliminate the various security related vulnerabilities which are discovered after its release on the market. In the case of the Honeynet Project, these machines were not protected by a firewall. Malicious activity was captured by IDSs and because no real network activity was introduced, false positive alerts were eliminated.

Configuration management is the process of managing changes to the network architecture and systems. These relate to changes which are necessary for the network to ensure a basic level of security to counter new and emerging threats and vulnerabilities and which arise from changes that are necessary to accommodate new user requirements. Some user requirements, such as the installation of a new Internet connection, the need for remote access, or maximising web browsing functionality (eg, through enabling Java, ActiveX or downloading other executables) have security implications which must be addressed, as part of a risk management framework and within an organisation's security policy.

While some configuration changes can be automated (eg, updating of anti-virus and IDS signatures), other vital changes – such as the installation of software patches – can be a labour intensive process for many networks. For organisations whose networks perform business critical services, the installation of patches generally occurs first in a test environment. This allows network administrators to identify any potential software conflicts or network failures which might arise from the change before it is implemented in the production environment.

This practice is generally accepted as good for security and business continuity because from a business perspective, a network outage will have the same impact whether it arose from a deliberate attack or incompatible software. One limitation of first applying patches to a test environment is that it increases the period during which an attacker could exploit the vulnerability which the organisation is seeking to eliminate.

How access control lists, systems settings, firewall and IDS rules are configured and maintained can all also potentially affect the network security. System and network administrators must understand the plethora of rules and settings which exist and ensure all are set correctly at all times. An incorrect configuration of the firewall rules, for example, may allow a hacker to transmit data to and from the network with minimal chance of detection.

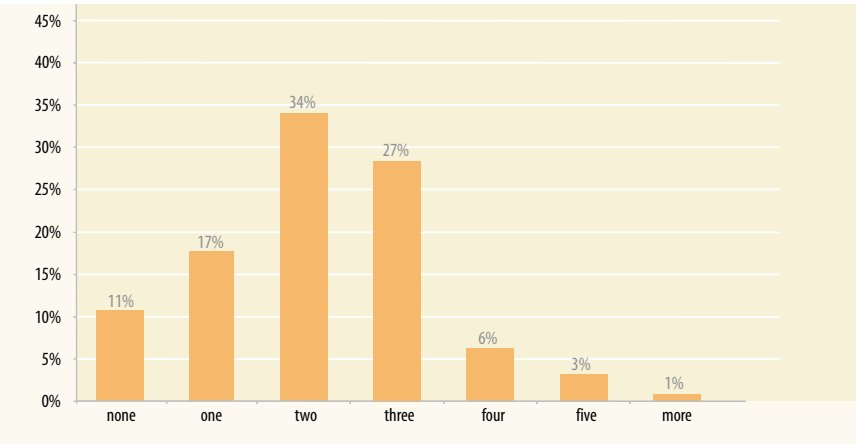
Effectively managing computer and network security is a complex and challenging task, even for organisations which are appropriately equipped, experienced and resourced. IT managers and their staff have to work in an environment in which their organisations are becoming increasingly dependent on the network infrastructure to support critical business services and, therefore, must work under the pressure of higher expectations of uninterrupted availability and increased functionality.

Faced with these kinds of challenges, it is not surprising that the majority of respondents found that there was at least one area of computer security management which posed difficulties or challenges for them. The three areas of human and process related activities which organisations found most challenging or problematic were:

- 60% – changing users' attitudes and behaviour with regard to computer security practices;
- 56% – keeping up to date with threats, vulnerabilities and changes in technology;
- 56% – configuration management.

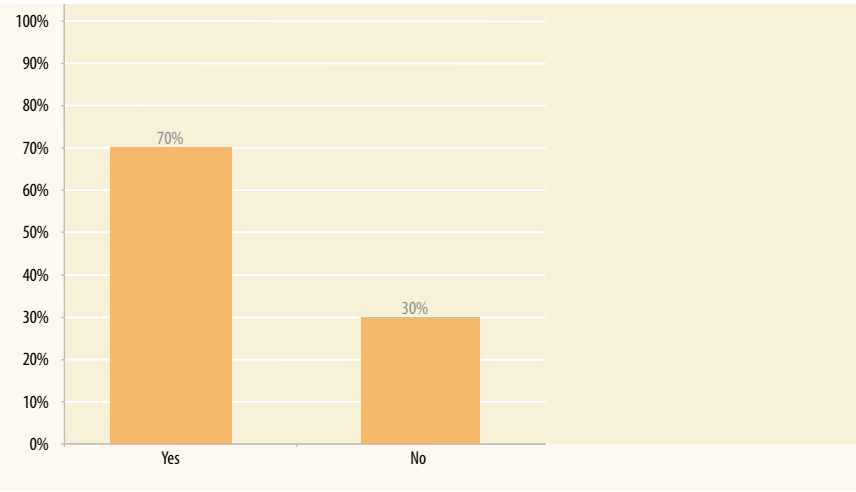
Only 11% of organisations believed they were managing all computer security issues reasonably well. This leaves 89% who felt there were one or more areas of computer security management which posed some difficulties or challenges for them and for 71% of respondents there were at least two areas of concern.

How many areas of computer security management did respondents find problematic or challenging?



Note: This was not a specific question put to respondents, but rather the results are derived from the number of categories which each respondent indicated was/were problematic or challenging based on the results of the previous question.
Source: Australian Computer Crime and Security Survey 2002
2002: 88 respondents/93%

Has your organisation increased computer security-related expenditure in the last year?



Source: Australian Computer Crime and Security Survey 2002
2002: 90 respondents/95%

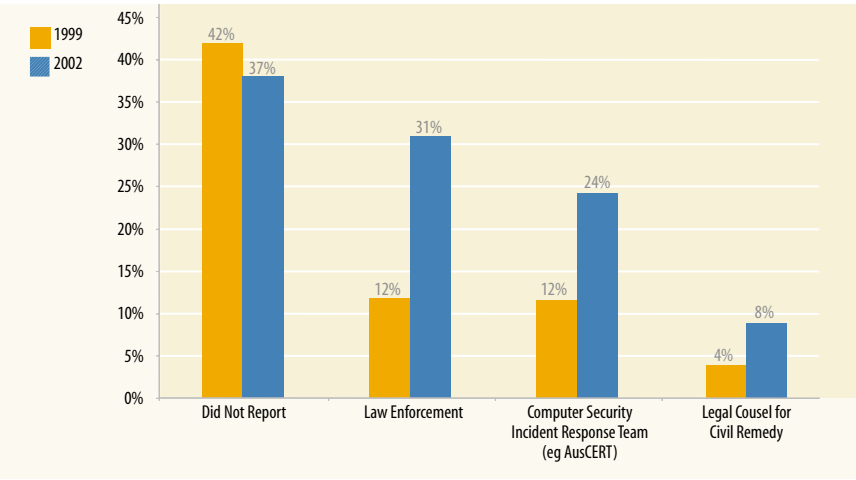
Seventy percent of organisations indicated that they increased computer security related expenditure in the last 12 months as a result of computer security incidents or computer security concerns. Other than being directly related to improving the organisation's network security, respondents were not asked to identify the areas where that expenditure was spent.

This expenditure may have involved purchasing new or upgrading network security technologies, improving personnel or physical security, training, increasing resources for network monitoring and maintenance, or conducting security reviews and audits. How ever that expenditure was incurred, clearly the majority of organisations believed they needed to do more to provide better security for their computer networks. It is therefore encouraging that organisations' concerns about their network security are being translated into positive steps to redress this situation.

7. Incident Reporting Trends

Taking into consideration the statistical differences between the 1999 and 2002 surveys with regard to this question, respondents in general appear more inclined to report computer security incidents to law enforcement or to seek remedy within the civil courts than before, but 61% of respondents reported that they did not take any legal action whatsoever.

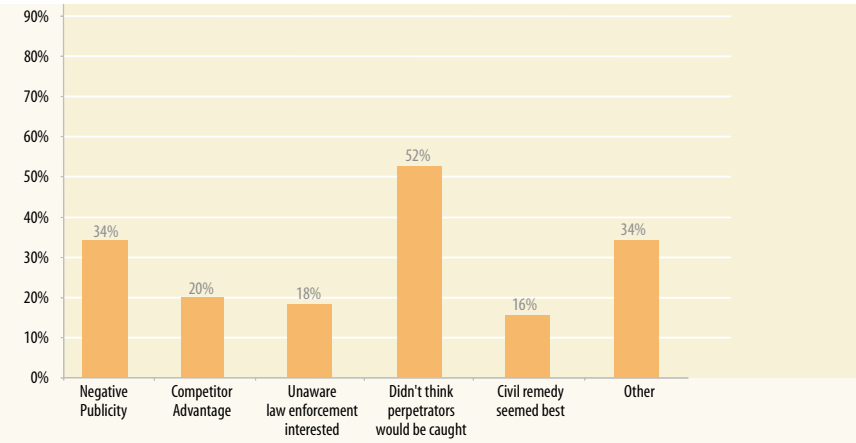
If your organisation experienced successful computer security incidents in the last 12 months, to whom did you report?



** Note in 1999, in addition to the four categories above, respondents were given three other options in how they answered this question. These options were not included in the 2002 survey. The options were – patched holes, ignored event or other. Also in 2002, each of the possible answers to this question was mutually exclusive, whereas in 1999, respondents were able to select one or more options. Therefore, a direct comparison of the results is not possible.*
Source: Australian Computer Crime and Security Survey 2002
2002: 59 respondents/62%, 1999: 37 respondents/52%

Twenty-four percent of respondents reported incidents to a computer security incident response team (CSIRT), such as AusCERT and 8% sought legal counsel for a civil remedy. For organisations that do not wish to pursue legal options, reporting incidents to a CSIRT provides other benefits. The CSIRT, as a trusted third party, can seek redress on behalf of the attacked network by informing the offending network – whether it resides locally or in any one of more than 100 countries world wide – that such actions have been detected, are unwelcome and to suggest that they may wish to conduct their own investigations.

Most Important Reasons Organisations Did Not Report Computer Security Incidents to Law Enforcement



Note: respondents were asked to give a rating of 1-5 (1 for least important and 5 for most important) for each category
Source: Australian Computer Crime and Security Survey 2002
2002: 27 respondents/28%

However, a large proportion of respondents (37%) who experienced some form of computer security incident still did not report outside of their organisation. Negative publicity (34%) and a lack of confidence in law enforcement's ability to catch the perpetrators (52%) were cited as the major reasons for not reporting to law enforcement.

The number of respondents concerned about negative publicity (34%) is very low compared to American organisations where 75% declined to report computer security incidents for this reason. Similarly, only 20% of Australian respondents declined to report because of concerns about competitive disadvantage compared to 72% in the USA[13].

Australian law enforcement agencies recognise genuine difficulties in identifying and tracking perpetrators of computer crime, particularly when the forensic trail crosses international borders and jurisdictions and when various parties – either the victims or others used to facilitate these crimes – have inadequate logging or user identification and authentication in place.

Case Study

In a recent case, an Australian organisation's publicly accessible payroll system was broken into by exploiting a known operating system level vulnerability. The company had not enabled logging at the network, database or operating system levels providing investigators with virtually no forensic trail. Poor security controls and a poor security culture made it easy for the perpetrator to hide his presence. Investigations showed that both the payroll system and its administrator's desktop computer were similarly compromised. This suggests the payroll system was the target of a deliberate, rather than random, attack. It also suggests that the attack was most likely perpetrated by an employee, someone who would have knowledge of the system and who could benefit from modifying the data within it. However, without adequate logging it was difficult to mount a thorough investigation, let alone prove a case. As with any root compromise of a mission critical system, recovery was painful and protracted.

Law enforcement and industry initiatives

In March 2001, the Australian Police Commissioners E-Crime Policing Strategy was launched to address the unique challenges posed by electronic crime. The strategy identified five key focus areas requiring action: prevention, partnerships, education and capability, resources and capacity and regulation and legislation. Work plans have been produced to address each focus area and action taken at both the national and within individual jurisdictions to implement them. Recent developments to assist investigation include increased cooperation between law enforcement and ISPs. Current assistance desired from ISPs includes increasing the length of time data, such as IP address logs, are stored. Furthermore, recent recommendations by the Australian Communications Authority on the Telecommunications Interception Amendment Bill aim to improve interception capabilities at ISPs for law enforcement. However, it is likely investigation techniques will remain slower to progress unless the offences are being reported and organisations are able to supply adequate event logging.

Peter Coroneos, Chief Executive of the Internet Industry Association (IIA), said that *"moves are underway in the industry to lift the success rate of law enforcement and regulatory agencies' investigations by providing more timely access to information and assistance with the identification of on-line criminals. The IIA's Cybercrime Code of Practice is designed to standardise the kind of information that ISPs retain, within the bounds of applicable law, and the circumstances in which the information is disclosed to law enforcement agencies. The IIA's involvement will ensure that these efforts are not at the cost of Internet users' privacy, to which the Association maintains its unequivocal commitment."*

As noted by the Australian Commissioners E-Crime Strategy, it is of mutual benefit for organisations to report serious incidents to law enforcement, thus developing both proactive prevention and effective response strategies to electronic crime.

8. Survey Approach

Around 500 organisations in the public and private sectors were invited to participate in the survey, including the Business Review Weekly's Top 300 Australian companies. Overall, we received responses from 95 public and private sector organisations, which represent an 18% response rate.

The methodology and format of the questions were based closely on the CSI/FBI Computer Crime and Security Survey. We included two additional questions – 'what aspects of computer security management does your organisation find most challenging or problematic?' and 'As a result of computer security concerns and/or incidents, have you increased your expenditure on computer security, including physical or personnel security in the last 12 months?' One existing question was modified to identify what mitigation, preventative or retaliatory actions organisations took in response to a computer security incident.

The following statements by editorial director of the Computer Security Institute, Richard Power, refer to the CSI/FBI Computer Crime and Security Survey, but are equally relevant to this survey. He said that it was "*a non-scientific, informal but narrowly focused poll of information security practioners.* [...] *The survey is at best a series of snapshots that give some sense of the 'facts and grounds' at a particular time.*"[14] Despite the limitations, Power also noted that "*the findings are in large part corroborated by data from other reputable studies, as well as by real-world incidents documented in open source publications.*"

In 2001, Bruce Schneier from Cryptogram commented on the value and limitations of the CSI/FBI survey. "*The results are not statistically meaningful by any stretch of the imagination* [...] *but it is the most interesting data on real world computer and network security that we have. And the numbers tell a coherent story. This data is not statistically rigorous, and should be viewed as suspect for several reasons.* [...] *the data is not necessarily accurate, but only the best recollections of the respondents. And third, most hacks will go unnoticed; the data only represents what the respondents actually noticed. Even so the trends are unnerving. It's clearly a dangerous world and has been for years. It's not getting better, even given the widespread deployment of computer security technologies.*"[15]

Questionnaires with business reply envelopes were sent by post to 307 information security professionals and Chief Information Officers in the public and private sectors. These organisations were invited to complete the survey either on-line via a secure web site or complete the hard copy version. A further 213 organisations were invited to participate via e-mail. Most of these organisations were invited to participate by completing the survey on-line only. Eighty-three completed the survey on-line and 12 sent in hard copy reports.

The responses were anonymous.

Who to call:

Deloitte Touche Tohmatsu
Enterprise Risk Services
For IT security consulting or incident investigation services:
Dean Kingsley, Partner
Ph: (02) 9322 7415
email: dkingsley@deloitte.com.au
website: www.deloitte.com.au

Australian Computer Emergency Response (AusCERT)
The University of Queensland
For computer incident response or membership enquiries:
Ph: (07) 3365 4417
email: auscert@auscert.org.au
website: www.auscert.org.au

The NSW Police
Computer Crime Investigation Unit
Commercial Crime Agency
For referrals on specific criminal investigations:
Ph: (02) 9269 3776
Fax: (02) 9269 3812
website: www.police.nsw.gov.au

Endnotes

[1] Office of Strategic Crime Assessments & Victoria Police, *1997 Computer Crime and Security Survey*

[2] Victoria Police Computer Crime Squad & Deloitte Touche Tohmatsu, *Computer Crime & Security Survey 1999*

[3] Richard Power, *2002 CSI/FBI Computer Crime and Security Survey*, Vol. VIII, No.1, Spring 2002

[4] *ibid.*, 5

[5] *ibid.*, 6

[6] *ibid.*, 7

[7] *ibid.*, 13

[8] *ibid.*, 10 - 11

[9] *ibid.*, 16

[10] *ibid.*, 10 - 11

[11] *ibid.*, 19

[12] *Know Your Enemy*, http://project.honeynet.org/papers/stats, last modified 22 July, 2001

[13] Richard Power, *2002 CSI/FBI Computer Crime and Security Survey*, Vol. VIII, No.1, Spring 2002, 20

[14] *ibid.*, 21

[15] *ibid.*