Trends & issues
in crime and criminal justice

No. 408 February 2011

Australian Government
Australian Institute of Criminology

Cyber threat landscape faced by financial and insurance industry

Kim-Kwang Raymond Choo

Foreword | *Opportunities for criminals to engage in transnational activities have expanded with globalisation and advancements in information and communications technologies. Cyber criminal activities will increasingly affect the financial security of online business. It is widely accepted that the financial and insurance industry is the 'target of choice' for financially motivated cyber criminals. Yet there is a lack of understanding about the true magnitude of cyber crime and its impact on businesses. Drawing on data from a 2008 Australia-wide survey conducted by the Australian Institute of Criminology, this paper contributes to a better understanding of the threat landscape faced by the financial and insurance industry by assessing the top four risk areas reported by the survey respondents. The paper also examines whether the results from the financial and insurance industries differ from other industries and identifies ways in which industries (particularly the financial and insurance industry), can neutralise or reduce cyber crime opportunities.*

Adam Tomison
Director

In 2008, the Australian Institute of Criminology (AIC) commissioned an Australia-wide survey of businesses to identify the prevalence, nature, costs and impacts of computer security incidents against Australian businesses during the 12 month period ending 30 June 2007 (Richards 2009). The Australian Business Assessment of Computer User Security (ABACUS) survey used a random sample of Australian businesses, stratified by industry sector and business size, to enable generalisations to be made about the entire population of Australian businesses—see Challice (2009) for a detailed discussion of the survey methodology. Of the 4,000 survey respondents (a response rate of 29%), 221 respondents were from the financial and insurance industry (FII; see Table 1).

Australia's FII is one of the largest and highest-performing industries in the country, 'generating 8.1 percent or A$81 billion of real gross value added' in the 2008–09 financial year (Austrade 2009: 5). The insurance market is reportedly the twelfth largest in the world and the fourth largest within the Asia–Pacific region (Austrade 2009). The FII is also one of the more sophisticated users of information and communications technologies (ICT), 'with almost 100 per cent of businesses having internet access' (Austrade 2009: 44). The increasing dependence on ICT and the size of the industry, however, expose it to a wide spectrum of financially-motivated cyber criminal activities.

To mitigate cyber criminal risks, it is essential to have a clear understanding of the threat landscape. Yet when asked about the most significant computer security incident that affected their business during the 12 month reporting period, 73 percent (n=161 of 221) of financial and insurance respondents (FIRs) indicated that they had experienced no incidents and 10.4 percent either did not answer the question or indicated that they did not know the answer. It is not clear whether such a high no-incident and no-response rate (approximately 83%) show that the Australian FII is largely free from cyber criminal activities or is due to a reluctance to report victimisation. It could also be possible that some of the respondents were not aware that their businesses had experienced one or more computer security incidents and therefore indicated that they had not experienced any such incidents.

This paper seeks to contribute to a better understanding of the ever-evolving landscape faced by Australian FII and its customers by examining the top four types of computer security incidents reported by the industry during the 12 month survey period (see Table 2). This will enable the industry to incorporate cyber threats into their business decision-making processes, with a view to identifying avenues for risk reduction.

The cyber threat landscape

Although 'the [overall] pattern of victimisation across industry sectors was very similar' (Richards 2009: 62), five industry sectors were substantially less likely than the FII to be

victimised by a computer security incident during the 12 month period:

- health care and social assistance (46% less likely);
- arts and recreation (48% less likely);
- mining (50% less likely);
- construction (52% less likely); and
- other services (69% less likely; Richards & Davis 2010).

Malware (including spyware)

Malicious software (malware) has consistently been ranked as one of the key cyber threats to businesses, governments and individuals. In 2009, for example, the number of new malware signatures (distinctive patterns of malware typically generated by manually analysing the malware) was reported to be just under 2.9 million, a 71 percent increase over 2008 (Symantec 2010). Studies by Microsoft (2010, 2009) also revealed that the threat landscape in Australia was dominated by malware, accounting for 75.1 and 76.2 percent of all threats detected on infected computers in the first and second halves of 2009 respectively. It is, therefore, unsurprising that malware (including spyware) was the computer security incident type experienced by the highest proportion of each industry sector and ranked as the most significant computer security incident experienced by all respondents in the ABACUS survey.

Statistics compiled from the data breach investigations conducted by Verizon Business from 2004 to 2008 indicated that malware (including keyloggers and spyware) is particularly common in the financial services industries (Verizon 2009). Respondents from agriculture, forestry and mining; manufacturing; retail trade; professional, scientific and technical services; educational and training; and health care and social assistance industries reported a substantially lower rate of computer security incident(s) involving malware.

Although the findings of the ABACUS survey appear to support the widespread perception that the FII is the 'target of choice' for financially motivated cyber criminals, the difference in responses could also be due to FIRs having a higher level of security awareness than respondents from the six non-financial and insurance industries who may have been unaware that their machines had been compromised by malware. For example, findings from the ABS (2009) survey on the business use of information technology during the 2007–08 financial year indicated that the financial and insurance sector has the lowest proportion of respondents indicating *don't know* when asked if they had experienced any IT security incident or breach during the 12 month reporting period (5.8% compared with 7 to 12.7% in other industries).

Table 1 Annual turnover of financial and insurance services respondents by business size

	Employees			
	0–19	20–199	200 or more	Total
Did not answer/do not know	23	2	3	28
Less than $100,000	56	0	0	56
$100,000 to $500,000	71	0	0	71
$500,000 to $1m	23	0	0	23
$1m to $10m	27	7	0	34
$10m to $1b	2	4	3	9

Source: AIC, ABACUS 2008 [computer file]

Table 2 Computer security incidents experienced by respondents during the reporting period

	FII	Others
Malware (including spyware)	34 (15.4%)	865 (22.9%)
Phishing	9 (4.1%)	193 (5.1%)
Theft/loss of confidential information/ hardware	9 (4.1%)	142 (3.8%)
Insider abuse of access	9 (4.1%)	96 (2.6%)
Unauthorised network access	7 (3.2%)	71 (1.9%)
Denial of service attack	1 (0.5%)	34 (0.9%)
Incident involving web application	2 (0.9%)	30 (0.8%)
Sabotage of network/data	2 (0.9%)	23 (0.6%)
Other	3 (1.4%)	23 (0.6%)
Total respondents	76 out of 221	1,477 out of 3,779

Note: Due to rounding, percentages may not total 100

Source: AIC, ABACUS 2008 [computer file]

Of the 34 FIRs who provided a substantive answer (either a *yes* or *no*) when asked about experiencing a computer security incident, and described the incident that caused the greatest financial loss to their business during the reporting period, approximately 38 percent indicated the incident involved malware. Respondents were not asked about the types of malware that affected their businesses during the 12 month period, but other studies suggest that there are two common categories—generic malware that targets the general population and customised information-stealing malware targeting specific institutions (Symantec 2010).

The shift in motivation from curiosity and fame-seeking/thrill-seeking to illicit financial gain has been marked by a growing sophistication in the evolution of malware (see malware trends in Microsoft 2010; Symantec 2010, 2009). Bot malware, particularly that designed to steal online banking credentials, will remain a threat to the Australian FII and its customers, further exacerbated by an increase in the availability of easy-to-use toolkits to build malware and botnets (networks of computers infected with bot malware). The Zeus bot malware creator kit, for example, was reportedly sold for around US$400–700 (Symantec 2010). The study by Symantec (2010: 11)

> observed nearly 90,000 unique variants of the basic Zeus toolkit and it was the second most common new malicious code family observed in the [Asia Pacific/ Japan] region [in the 2009 calendar year].

Customised information-stealing malware includes phishing-based keyloggers (programs designed to monitor user activity including keystrokes). APWG (2009) explained that such information-stealing malware had tracking components designed to monitor specific keystroke actions and target specific organisations, particularly financial institutions, online retailers and e-commerce merchants.

Security is only as strong as its weakest link—the FII is often the sector of choice for cyber attacks and suffers financial loss from these attacks, but their customers are typically the real target of the intrusion. Examples include the Bugat Trojan, which has a phishing-based keylogger component designed to facilitate automated clearing

house (ACH) fraud as seen in several cases in the United States (Box 1). Although malware designed to facilitate ACH fraud has yet to become widespread in Australia, customers of the Australian FII are unlikely to be spared from similar targeted attacks.

Phishing

Phishing can be defined as online scams that frequently use unsolicited messages purporting to originate from legitimate organisations, particularly financial and insurance services, to deceive victims into disclosing their financial and/or personal identity information (PII) to commit or facilitate other crimes (eg fraud, identity theft and theft of sensitive information).

Statistics from APWG (2009), Symantec (2010) and Microsoft (2010, 2009) indicated that the financial industry was the most targeted industry sector in phishing attacks in the 2009 calendar year. As expected, a higher proportion of FIRs reported using anti-phishing software than did non-FIRs (40.1% of FIRs compared with 32% of non-FIRs).

What was unexpected, however, was the financial loss due to phishing reported by respondents in the ABACUS survey. The only FIR (and 10 of the 3,779 non-FIRs) that indicated phishing as the most significant incident experienced by their business, estimated that phishing only resulted in financial losses of less than $1,000 during the reporting period. Six of the non-FIRs who indicated phishing as the most significant incident experienced by their business, estimated that phishing resulted in a financial loss of between $10,000 and $99,999.

Respondents in the ABACUS study were not asked to explain how they estimated financial loss to their business due to phishing (and other computer security incidents). It is possible that respondents may not have included the *indirect costs* (eg staff and ICT equipment associated costs and potential non-compliance fines) and *lost opportunity costs* (eg other businesses choosing not to conduct business with partners from jurisdictions deemed to be of high fraud risk) in their estimations. Further research is needed to quantify the direct and indirect losses that businesses suffer as a result of phishing.

Theft or loss of proprietary or confidential information or hardware

Data breaches, particularly those involving PII can receive considerable media attention, which can greatly affect a business's reputation and reduce the public's trust in that business. Data breaches can be broadly categorised into physical breaches (eg due to stolen data storage devices) and non-physical breaches (eg due to computer or network intrusions). The latter category is a cause for concern. Statistics from the data breach investigations conducted by Verizon (2009) from 2004 to 2008, for example, indicated that only nine percent of data breaches are attributable to physical attacks. Hacking was found to be one of the leading causes of data breaches (64% of cases).

A study by Symantec (2010: 28) revealed that the

> financial sector was subject to one of the most notable data breaches reported in 2009…[it] ranked fifth for breaches with 10 percent of the total, but accounted for the largest number of identities exposed with 60 percent.

The ABACUS study reported similar findings—FIRs were more likely to experience incidents involving unauthorised network access than non-FIRs (3.2% of FIRs compared with 1.9% of non-FIRs).

Another 2009 study that examined the actual financial losses incurred by 16 Australian organisations from different industry sectors following a data loss found that

> malicious attacks and botnets are the primary drivers of data breaches and cost substantially more than those caused by human negligence or IT system glitches (Ponemon Institute 2010a: 16).

The study also confirmed what many suspected—the financial sector had one of the highest average costs per compromised record and an abnormally high customer turnover as a result of the data breaches. Similar trends were observed in the financial sector in the United Kingdom during the same reporting period (Ponemon Institute 2010a, 2010b).

Box 1 ACH fraud

In several such incidents in the United States, cybercriminals sent a targeted phishing email aimed at whoever was in charge of an organisation's IT operations. By tricking the victim(s) into opening a harmful attachment or visiting a malicious website, the criminals were able to install malware, including a phishing-based keylogger onto the machine. In addition, the malware could propagate through the organisation's network, enabling cybercriminals to gain access to and/or compromise other workstations and servers. Once the keylogger was installed on the victim's machine, the program then 'faithfully' did what it was designed to do (ie send harvested account numbers, log-in credentials and personal information to cybercriminals). Cybercriminals were then able to initiate funds transfers by masquerading as the legitimate user using the harvested login credentials and personal information. Money could be transferred out of the account using the Automated Clearing House system that banks use to process payments between institutions and/or using traditional wire transfers. Financial losses due to these fraudulent wire transfers averaged US$100,000–200,000 per victim (McGlasson 2010). In addition, malware such as the URLZone Trojan

> can alter the online bank statement to disguise the fact that an illegal transfer has occurred. Victims who check their bank accounts online only, instead of reading paper statements, would not realize their money had been stolen (Cisco 2009: 11).

Insider abuse of access

Insiders (ie employees and individuals who are given authorised insider access) will have access and knowledge of a business's vulnerabilities that may provide them with the ability and opportunity to bypass physical and technical security measures designed to prevent unauthorised access and enable them to carry out malicious activity, if they are motivated to do so. Motivations to offend may include theft or modification of information for financial gain (eg sale of stolen data) and business advantage (eg obtaining information for a new job or starting their own business; Cappelli et al. 2009).

Fifteen percent of FIRs (and 18.6% of non-FIRs) in the ABACUS survey indicated that they did not experience any incidents involving insider abuse of access; 2.7 percent (and 2.5% non-FIRs) indicated that they had experienced incidents involving insider abuse of access; and 82.4 percent (and 80% non-FIRs) were unsure whether they had experienced any such incidents, or they failed to answer the question.

Of the 39 FIRs in the ABACUS survey who provided a substantive answer (either a *yes* or a *no*), three indicated that they had experienced incidents involving insiders abusing their access but not unauthorised network access (7.7%); four indicated that they had experienced incidents involving unauthorised network access (10.3%); and three indicated that they had experienced incidents involving both unauthorised network access and insider abuse of access (7.7%). Data analysis of the 39 responses indicated a significant difference between these two factors (χ^2=4.95; p<0.05). While it is not possible to tell whether the unauthorised network access incidents were due to insiders abusing their privileged access, data analysis of the 39 responses suggested a weak to moderate correlation between these two factors (Cramér's V of 0.36).

A similar finding was observed in the non-FIRs, where 18 of the 797 non-FIRs who provided a substantive answer indicated that they had experienced incidents involving both unauthorised network access and insider abuse of access (2.3%)—a significant difference between these two factors (χ^2=13.03; p<0.001) and Cramér's V of 0.13 indicated that there was a weak correlation between these two factors.

Countermeasures

Cyber crime is becoming increasingly pervasive and sophisticated, and appears to be growing in volume and impact. The 221 FIRs in the ABACUS survey estimated that the total financial losses due to computer security incidents during the 12 month reporting period were approximately $49m. This highlights the impact of cyber criminal activities on valuable business data, processes and assets. It seems inevitable that there will be an increase in the variety and volume of cyber criminal activities targeting Australian businesses and the FII, in particular, is likely to remain the 'target of choice' for financially motivated cyber criminals.

Examples of emerging cyber threats include ATM frauds. In a recent media interview, Australia's Minister for Home Affairs and Justice indicated that 'card skimming may rise to cost the Australian community $100 million' (O'Connor 2010: np). ATM fraud includes card skimming and the installation of ghost ATM and unmanned EFTPOS terminals, with the intention of both surreptitiously recording a card's magnetic stripe and capturing the corresponding personal identification number (PIN). Fraud perpetrated in Australia and overseas on Australian-issued credit/charge and debit cards was estimated to cost the Australian community slightly over $170m in the 2009 calendar year (APCA 2010).

Major industry initiatives such as the introduction of the Europay, MasterCard and VISA (EMV) chip-and-PIN is far from perfect, but statistics have shown that chip-and-PIN implementation in Australia and several European countries has resulted in a decrease in card fraud due to skimming in those countries (APCA 2010; Payments cards and mobile 2009). The statistics also suggested that where chip-and-PIN implementation occurred in European countries, there was increased displacement to neighbouring countries that had yet to implement the chip-and-PIN technology.

Criminals are always on the lookout for new markets for exploitation. For example, security researchers and financial institutions have reported identifying malware designed to record magnetic stripe information and PINs (Kirk 2009). Further, in 2010, a security researcher presented a proof-of-concept malware that exploits vulnerabilities in software used in ATMs at the 2010 Black Hat conference (Jack 2010). Attacks involving the installation of malware, however, are likely to require physical access to the ATM or a port in which the malware could be uploaded (Kirk 2009) as these machines are typically not connected to the internet. This would suggest the need to involve insiders or individuals with physical access to the machines. Because non-bank owners of ATMs are typically not liable for compensating customers who suffer loss as a result of ATM fraud, there is little incentive to develop and install anti-fraud measures at ATMs. Banks, however, continue to deploy security measures as part of their customer service approach. Consideration could be given to requiring non-bank owners of ATMs to ensure that the latest security measures are used on their machines.

The following preventative measures could assist Australian businesses, particularly those outside the FII sector, in mitigating cyber security risks. At present, FII businesses are subject to exacting regulatory requirements that minimise risks of harm from many types of cyber crime.

Technical measures

Although no single technology can completely mitigate cyber security risks, a significant proportion of existing cyber security vulnerabilities can be mitigated using good security practices. The Defence Signals Directorate (DSD), for example, indicated that

> [a]t least 70% of the targeted cyber intrusions that DSD responded to in 2009 could have been prevented if organisations had implemented the first four mitigation strategies recommended by DSD:
>
> - (1 & 2) Patching of the operating system, applications, and third party applications (eg PDF reader and web browser plug-ins);
> - (3) Minimising administrative privileges; and
> - (4) Deploying application whitelisting to help prevent unapproved applications from running (DSD 2010: 2).

In practice, systems are known to have security vulnerabilities, which if left un-patched, can be exploited to compromise systems or to build malware. Businesses, particularly small and medium sized businesses, do not generally patch their systems immediately when security vulnerabilities are reported. Yet the period between patching and exploitation is getting shorter and in recent months, there has been an increase in the number of zero-day exploits (malware that attempts to exploit software/hardware vulnerabilities that are not publicly known or that occur on the same day that the vulnerability becomes publicly known). Recent examples (eg the exploitation of the vulnerability in Microsoft's Internet Explorer 6 to attack Google China and other companies in December 2009—see Symantec 2010) highlighted that cyber attacks are getting more sophisticated and 'going under the radar'. In several of these incidents, victims only realised they were under attack weeks or months after data and corporate secrets were stolen by the intruders.

Although non-FIRs were more likely not to have any manual/automated patch management systems in place than FIRs, it is concerning that 74 percent of the FIRs (80% of non-FIRs) in the ABACUS survey indicated that they did not have any manual/automated patch management systems in place during the reporting period.

Deploying technologies such as patching management systems will help to greatly reduce risks faced by businesses and their customers.

Awareness and education/training

Technical solutions can provide effective protection against security threats, but alone cannot provide a comprehensive solution. Cyber criminal activities such as phishing will continue to evolve into new forms, while continuing to exploit social engineering (human actors are likely to remain one of the weakest links in attempts to secure systems and networks). User awareness and education/training are critical in mitigating cyber threats such as targeted phishing.

In recent years, phishing messages have been increasingly targeting top executives/high net worth individuals—also known as spear phishing—with the aim of gaining access to corporate online banking systems, corporate VPN networks and other online resources. Statistics compiled by APWG (2009: 4), for example, revealed 'a substantial increase in phishing focused on high-value targets such as personnel with treasury authority'. Another study by Verisign (2009: 4; see Box 2) also noted that

> victim counts from these [spear phishing] attacks [are] staggering—over 15,000 corporate users in 15 months. Victims include Fortune 500 companies [and] financial institutions.

Although FIRs were more likely to have some sort of employee education and awareness program in place than non-FIRs, only 20.8 percent of the FIRs (18.1% non-FIRs) in the ABACUS survey indicated they had some sort of employee education and awareness program in place during the reporting period. In addition, only two of the nine FIRs (and 29.5% of the 193 non-FIRs) who reported being victimised by phishing during the reporting period had any employee education initiative in place. This is a rather surprising finding as the FII is often perceived to have a high level of security awareness. One possible explanation is that large businesses, or businesses with high annual turnovers, are more likely to invest in employee education and awareness programs. This is less likely in the case of small businesses, which accounted for approximately 68 percent of the FIRs (their businesses had less than 20 employees and had an annual turnover of less than $500,000; Table 1).

Findings from the ABACUS survey and the escalating complexities of the end-user online environment underscore the need for regular ongoing training programs for basic online security (including new cyber crime trends) and the promotion of a culture of security for information systems and networks among customers and internal staff of Australian businesses. Such initiatives would enable customers and internal staff (including senior management who have privileged access to corporate data and accounts) to maintain current knowledge of the latest cyber crime activities and the best cyber crime prevention measures available, such as the guidelines developed by the Australian Payments Clearing Association to educate merchants about card skimming risks (APCA 2010, Lohman 2010).

There is also a need for coordinated action by government agencies, industry and community organisations to help ensure the most effective cyber crime prevention advice is provided to the community; which was also a recommendation of the House of Representatives Standing Committee on Communications (2010) in its recent report on cyber crime (Recommendation 31).

Insider and vendor management

A 2009 survey of 305 IT security decision makers in North American, European and Australian enterprises highlighted the importance of proprietary knowledge and company secrets. The survey found that proprietary knowledge and company secrets comprised two-thirds of the value of a business's information portfolios and insider theft of sensitive information was 10 times costlier on a per-incident basis than any single incident caused by accidents—hundreds of thousands of dollars versus tens of thousands (Forrester 2010).

However, when asked about staff/user-related policies, an overwhelming proportion of the 221 FIRs (81.9%) and 3,779 non-FIRs (87.4%) in the ABACUS survey indicated that they did not have such policies in place (see Table 3). Since the survey did not ask about vendor management-related policies, it is not clear whether the respondents had any vendor management-related policies in place during the 12 month period.

Third party vendor and trusted business partners who are given authorised insider access are potential sources of data breaches and should be included in the business risk assessment for insider threat. For example, third party vendor and trusted business partners should be required to provide the business with up-to-date lists of all individuals within their organisations who have been given access to the business' confidential information upon engagement. The list should be updated regularly as an up-to-date insider list helps to ensure businesses are able to keep a complete and proper record of all staff with access to confidential information. Such a list also limits the number of staff in possession of that confidential information, helps to promote the 'need-to-know' principle, and acts as a deterrent for those on the list, discouraging careless or inappropriate behaviour. In addition, in the event of a leak an insider list would assist in the investigation (ASIC 2009).

Summary

ICT have advanced, and will continue to advance, rapidly. Legitimate businesses which seek to make best use of technologies must also keep abreast of the latest developments in threat awareness and preventative responses. Cyber threats are increasingly important and strategically relevant to the financial services and insurance sectors and these (and other) sectors need to maintain vigilance with respect to emerging crime threats.

Box 2 Spear phishing

The Hydraq Trojan (also known as Aurora) received considerable media attention between January and April 2010. According to several media articles, media releases (eg Google) and reports such as Symantec (2010: 8)

> dozens of large companies [were reportedly] compromised by attackers using this Trojan…[The] attack begins with some reconnaissance on the part of attackers. This can include researching publicly available information about the company and its employees, such as from social networking sites. This information is then used to create specifically crafted phishing email messages, often referred to as spear phishing, that target the company or even specific staff members. These email messages often contain attachments that exploit vulnerabilities in client-side applications, or links to websites that exploit vulnerabilities in web browsers or browser plug-ins. A successful attack could give the attacker access to the enterprise's network…once they have established access within the enterprise, attackers will use the foothold that they have established to attempt to connect to other computers and servers and compromise them as well. They can do this by stealing credentials on the local computer or capturing data by installing a keystroke logger.

Table 3 Responses about staff/user-related policies

	FIRs	Non-FIRs
No segregation of duties	166 (75.1%)	3,072 (81.3%)
No system content monitoring	172 (77.8%)	3,156 (83.5%)
No wireless technology acceptable use policy	190 (86.0%)	3,311 (87.6%)
No IT acceptable use policy	156 (70.6%)	2,970 (78.6%)
No policies concerning the use of mobile devices	193 (87.3%)	3,390 (89.7%)
No user access management	159 (72.0%)	2,841 (75.2%)
No staff background check policy	184 (83.6%)	3,309 (87.6%)
No mandatory reporting of misuse/abuse of computer equipment	186 (84.2%)	3,318 (87.8%)
No documented standard operation procedures	173 (78.3%)	3,164 (83.7%)
No monitoring of internet connections	167 (75.6%)	3,057 (80.9%)
No account/password management policies	135 (61.1%)	2,604 (68.9%)
No staff/user related policies	181 (81.9%)	3,293 (87.4%)

Note: All percentages have been rounded up to 1 decimal place

Source: AIC, ABACUS 2008 [computer file]

Dr Kim-Kwang Raymond Choo is a Senior Research Analyst at the Australian Institute of Criminology

General editor, *Trends & issues in crime and criminal justice* series: Dr Adam M Tomison, Director, Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Project no. 0133
Ethics approval no. PO114
Dataset no. 0105

The potential for mitigating financially motivated cyber criminal activities lies in an effective partnership between government and business. The role of public policing agencies is only one, albeit important, part of the overall response to cyber crime. The private sector must also play a role in crime prevention. An improved understanding of the cyber crime risk environment will place Australian businesses in a much better position to manage new and emerging cyber threats.

While the responses to some of the questions in the ABACUS survey were very small in number, by comparison to the sector as a whole, the survey provides a good indication of the cyber threat landscape faced by the Australian FII and highlights the need to develop and implement on an ongoing basis preventative measures such as personnel awareness and education/training initiatives, together with insider and vendor management.

Acknowledgements

The ABACUS Survey was conducted by the Social Research Centre, Melbourne. Assistance in preparing this paper was provided by Dr Russell G Smith and Dr Brent Davis of the AIC.

References

URLS correct at December 2010

APWG 2009. *Phishing activity trends report: 4th quarter 2009*. http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

Australian Bureau of Statistics (ABS) 2009. *Business use of it—Summary indicators, 2007–08*. cat. no. 8129.0. Canberra: ABS. http://abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8129.02007-08?OpenDocument

Australian Payments Clearing Association (APCA) 2010. *Payments fraud in Australia: Mixed results*. http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Press_Release_Payments_Fraud_Statistics_8.pdf/$File/Press_Release_Payments_Fraud_Statistics_8.pdf

Australian Trade Commission (Austrade) 2009. *2009 financial services benchmark report*. Canberra: Austrade

Australian Securities and Investments Commission (ASIC) 2009. *Handling confidential information*. Consultation paper 128. http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/cp128.pdf/$file/cp128.pdf

Cappelli D, Moore A, Trzeciak R & Shimeall TJ 2009. *Common sense guide to prevention and detection of insider threats*, 3rd ed—version 3.1. Pittsburgh, PA: Carnegie Mellon University

Challice G 2009. *The Australian business assessment of computer user security (ABACUS) survey: Methodology report*. Technical and background paper series no. 32. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tbp/21-40/tbp032.aspx

Cisco 2009. *Cisco 2009 annual security report*. San Jose, CA: Cisco Systems Inc

Defence Signals Directorate (DSD) 2010. *Strategies to mitigate targeted cyber intrusions*. http://www.dsd.gov.au/_lib/pdf_doc/intrusion_mitigations_intro.pdf

Forrester 2010. *The value of corporate secrets*. Cambridge, MA: Forrester Research Inc

House of Representatives Standing Committee on Communications (2010). *Hackers, fraudsters and botnets: Tackling the problem of cybercrime*. http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf

Kirk J 2009. ATM malware spreading around the world. *CSO 6 June*. http://www.cso.com.au/article/306524/atm_malware_spreading_around_world

Jack B 2010.Jackpotting automated teller machines redux. Presented at Black Hat Technical Security Conference: US 2010

Lohman T 2010. Card skimming to cost Australia $100 million. *Computerworld* 13 April. http://www.computerworld.com.au/article/342872/card_skimming_cost_australia_100_million/

Microsoft 2010. *Microsoft security intelligence report: volume 8*. http://www.microsoft.com/security/sir/default.aspx

Microsoft 2009. *Microsoft security intelligence report: volume 7*. http://www.microsoft.com/security/sir/default.aspx

O'Connor 2010. Minister backs call for vigilence to combat card skimming. *Media release* 12 April. http://www.ministerhomeaffairs.gov.au/www/ministers/oconnor.nsf/Page/MediaReleases_2010_SecondQuarter_12April2010-MinisterBacksCallforVigilencetoCombatCardSkimming

Payments cards and mobile 2009. *Fraud supplement.* Sept–Oct 2009. www.paymentscards andmobile.com

Ponemon Institute 2010a. *2009 annual study: Australian cost of a data breach*. Michigan: Ponemon Institute

Ponemon Institute 2010b. *2009 annual study: Cost of a data breach*. Michigan: Ponemon Institute

Richards K 2009. *The Australian Business Assessment of Computer User Security: A national survey*. Research and public policy series no 102. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp102.aspx

Richards K & Davis B 2010. Computer security incidents against Australian businesses: Predictors of victimisation. *Trends & Issues in Crime and Criminal Justice* no 399. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi399.aspx

Symantec 2010. *Symantec global internet security threat report: Trends for 2009, Volume XV.* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

Verisign 2009. *Fraud alert phishing—the latest tactics and potential business impact*. https://www.verisign.com.au/ssl/ssl-information-center/ssl-resources/phishing-tactics/phishing-tactics.pdf

Verizon 2009. *2009 data breach investigations report*. http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf