Trends & issues in crime and criminal justice

No. 433 February 2012

Australian Government
Australian Institute of Criminology

Computer security threats faced by small businesses in Australia

Alice Hutchings

In this paper, an overview is provided of computer security threats faced by small businesses. Having identified the threats, the implications for small business owners are described, along with countermeasures that can be adopted to prevent incidents from occurring. The results of the Australian Business Assessment of Computer User Security (ABACUS) survey, commissioned by the Australian Institute of Criminology (AIC), are drawn upon to identify key risks (Challice 2009; Richards 2009). Additional emerging threats relating to wireless internet, cloud computing and spear phishing are also outlined, as well as the risks relating to online fraud.

The small business sector is important to Australia; comprising the largest part of the business sector, they are a key employer and contributor to the economy. As at June 2010, small businesses (defined as having less than 20 employees) made up 95.6 percent of Australian businesses (ABS 2010). The majority (62.7%) of small businesses were sole operators, employing no staff; 25.3 percent employed one to four staff and 11.9 percent employed five to 19 staff (ABS 2010). As at June 2009, small businesses employed 48 percent of private sector staff (DIISR 2011). The Department of Innovation, Industry, Science and Research (2011) estimated that in 2008–09, small businesses contributed approximately 34 percent of private industry value to the economy.

Having an online presence enables small businesses to expand the reach of their products and services to a wider range of potential consumers. A 2010 Australian survey, which included 1,436 small business respondents, found that 96 percent owned a computer, 94 percent were connected to the internet, 60 percent had a website, 43 percent took orders for products and services online and 53 percent received payments online (Sensis Pty Ltd 2010). Some small businesses conduct the majority of their trade online, with 19 percent of businesses with up to four staff reporting that more than half of their total goods and services income in 2007–08 came from online business; this figure was 10.3 percent for businesses with five to 19 employees (ABS 2009).

The ABACUS survey

The ABACUS survey was comprised of a random sample of small, medium and large businesses. Businesses were surveyed to examine the nature and extent of computer security incidents. Of the 4,000 respondents to the survey, 3,290 (82.3%) were small businesses. Compared with their proportion in the Australian business population, small businesses were under-sampled. However, the survey was weighted according to industry type and business size so that the data provided by each participant was proportionate in relation to the broader population being sampled. Challice (2009) provides an overview of the research methodology.

Foreword | *The internet is an affordable and effective place for small businesses to sell and promote their goods and services. However, the internet also provides opportunities for fraudulent behaviour and unauthorised access to business and client data. Attacks on the computer system of a business can have immediate and ongoing effects, such as targeting customers for identity crimes or infecting website visitors with malicious software. It is contended that small businesses in Australia have been slow to implement security technology and policies that may protect their information systems, making them vulnerable to current and future threats. In this paper, an attempt is made to educate small business owners about the risks that they face and the mitigation strategies they could employ to make their organisation safer.*

Adam Tomison
Director

Results of the survey were congruent with previous findings, confirming that small businesses in Australia have embraced the use of technology, with 92 percent using it to some extent during 2006–07 (Richards 2009). Most small businesses reported the use of personal computers (85%) and laptops (54%). Presumably due to smaller staffing levels, fewer small businesses reported the use of a local area network (43%), wide area network (9%) or virtual private network (10%) than medium and large businesses (Richards 2009).

During 2006–07, 14 percent of small businesses reported having experienced one or more computer security incidents (Richards 2009). Of these, 83 percent experienced one to five incidents, eight percent experienced six to 10 incidents and nine percent experienced more than 10 incidents. Negative outcomes were reported by 75 percent of small businesses following the most significant computer security incident. These included:

- corruption of hardware or software (42%);
- corruption or loss of data (31%);
- unavailability of service (38%);
- non-critical operational losses (24%);
- non-critical financial losses (12%);
- critical financial losses (5%);
- theft of business, confidential or proprietary information (5%);
- theft or loss of hardware (4%);
- harm to reputation (4%);
- critical operational losses (4%);
- website defacement (2%); and
- other (1%; Richards 2009: 69).

When a computer security incident occurred, the average loss to a small business was $2,431 (Richards 2009).

The Australian and New Zealand Standard Industrial Classification was used to determine the industry sectors covered by the survey (Richards 2009). The ABACUS results indicated that each industry sector experienced a relatively even proportion of computer security incidents (Richards 2009).

This paper is part of a suite of publications using data from the ABACUS survey. These publications have examined predictors of victimisation (Richards & Davis 2010) and the threats faced by the financial and security industry (Choo 2011). Fact sheets have also provided summaries of the number of incidents faced by Australian businesses (AIC 2009a), the proportion of incidents by industry sector (AIC 2009b) and the types of computer security tools used by Australian businesses (AIC 2009c). Although four years can be a long time in the cyberworld, the ABACUS survey data remains one of the few sources of information on the computer security risks faced by small business.

Threats

Small businesses may lack the expertise to identify and deal with computer security incidents (Williams & Manhcke 2010), making them an attractive target for online offenders (Verizon 2011). An overview of some of the threats faced by small businesses, including the nature of the threat and potential outcomes, is provided in the following section. Scenarios include malware infection, wireless internet misuse and session hijacking, online fraud, compromised websites, denial of service attacks, phishing, spear phishing, unauthorised access and risks associated with cloud computing. While this overview is not exhaustive, it aims to increase awareness of the types of vulnerabilities small business operators may face.

Malware

Malware, or malicious software, includes viruses, worms, keyloggers, spyware, trojans and botware (see definitions in Table 1). Potential outcomes of malware infection include account names and passwords being compromised, which may lead to fraudulent activity; files being accessed and copied, and corruption of hardware or software resulting in computer downtime or a slowed computer network (Furnell 2010). Botware may also result in the infected computer being used as part of a botnet (a network of compromised machines), which among other things, can be harnessed to send spam and conduct denial of service (DoS) attacks (Ianelli & Hackworth 2006), consuming bandwidth in the process. If a computer infected with botware is found to be sending spam, the internet service provider may disconnect or suspend the internet connection (IIA 2005).

Common ways that computers become infected with malware include visiting websites or opening email attachments (Furnell 2010). Malware is reportedly the most prevalent computer security issue affecting small businesses in Australia, with 65 percent of small businesses experiencing one or more computer security incident involving a virus or other malicious code and 44 percent reporting spyware infections (Richards 2009). Half (50%) of small business who reported one or more computer security incident identified viruses, malicious code and spyware as causing the greatest financial loss and 60 percent identified these incidents as being the most significant (Richards 2009).

Wireless internet vulnerabilities

Many small businesses, particularly in the hospitality sector, are now offering free public wireless internet connections to attract customers. Other businesses that utilise wireless local area networks may inadvertently leave their connections open or use weak encryption. Four issues relating to wireless connections are considered here—session hijacking, man-in-the-middle attacks, their use to anonymise the commission of further offences and unauthorised access to data held on servers.

Users of wireless connections are at risk of having their sessions hijacked, leaving their accounts accessible to other network users without their knowledge. This occurs when the cookies, used to authenticate the user, sent by an unencrypted website are intercepted and used to impersonate the account holder (Dacosta et al. 2011).

An example of a man-in-the-middle attack in this context involves the use of a proxy who intercepts traffic between a website and the browser over an unencrypted wireless connection. This occurs when the browser believes that the proxy is the legitimate

Table 1 Malware definitions

Name	Definition
Virus	A self-replicating program that is spread by opening infected files and uses up available memory
Worm	A self-replicating program that spreads automatically and uses up available memory
Keylogger	A program that records users' keystrokes
Spyware	A program that can monitor computer activity
Trojan	Malware disguised as legitimate software, such as a game
Botware	A program that connects a computer to a botnet and enables it to be controlled remotely

Source: Grabosky 2007

website and the website authenticates the proxy as the browser (Knights et al. 2006). The proxy can then read and alter the data being transmitted, including account passwords.

Wireless internet may also be misused to access and download illegal content such as pirated software, music or movies, child pornography, or to commit further criminal activities such as hacking, conducting fraudulent activities, DoS attacks or sending spam (Selvadurai, Islam & Gillies 2009). As well as having their bandwidth used, the wireless connection provider may initially be suspected of conducting these activities, and if no user agreements are in place for public access, could potentially be held liable (Selvadurai, Islam & Gillies 2009).

Open or poorly encrypted wireless connections could also leave information stored on computers on the same network vulnerable to access and misuse. In one such attack in 2007, an American retail store had 45 million credit and debit card accounts compromised (Lawton 2010).

Online fraud

There are a number of scams that small businesses may be vulnerable to and many of these are being committed over the internet or by email. Some of the online scams targeting businesses are card-not-present fraud, overpayment and upfront fee scams.

Compromised credit card details may be used online for fraudulent card-not-present transactions, where account information is used without the authority of the cardholder. If the cardholder has abided by their financial institution's terms of use, they will generally be reimbursed for their loss (Shelly & Jackson 2008). However, generally the merchants are liable for the fraudulent transaction (Shelly & Jackson 2008). The Australian Payments Clearing Association Limited (2010) reported that in 2009–10, the cost of card-not-present fraud in Australia amounted to $62.7m.

Overpayment scams involve ordering goods and the scammer paying more than the agreed amount using a counterfeit or dishonourable cheque, or money order or stolen credit card. The seller is then out of pocket if they post the goods and refund the overpaid amount before the payment is cleared (ACCC 2008).

Advance fee scams also target goods being sold online. In this variation, the seller is asked to pay the buyer's agent for the cost of shipping or insurance, which they are promised will be repaid, along with payment for the item, however the money is never received (ACCC 2011).

Compromised websites

Web servers may become compromised and used to host prohibited material without the knowledge of the site owners (Moore, Clayton & Anderson 2009). Arrests of 92 Australians in 2008 occurred after they apparently accessed child exploitation images hosted on a hacked website (Arup 2008). Compromised web servers may also deliver malicious software, which infects visitors to the site without their knowledge, known as a 'drive-by download' (Egele et al. 2009). Websites can also be defaced to include misleading or malicious content.

Having a compromised website may affect a business in a number of ways. Businesses may experience a loss of reputation if their website cannot be trusted for the integrity of its contents. Websites hosting malicious or illegal material may be added to search engine blacklists, so that people searching for a business receive a warning that the website may be harmful (Larsen 2010). There is also the possibility that websites compromised for the purpose of hosting illegal content such as child exploitation material may be blocked by internet filters, such as the one proposed by the Australian Government (EFA 2010). For small businesses trading or advertising online, these consequences could be significant.

Two percent of small businesses that had experienced a computer security incident reported experiencing an incident involving the business's web application (Richards 2009). This was defined as

> any malicious or destructive incident that involves a business's website. This may include placing unauthorised information on a website or preventing it from being used as intended (Richards 2009: 97).

Although low compared with other types of reported computer security incidents, the actual incident rate may be higher if businesses are not aware that their websites have been compromised.

Denial of service attacks

As mentioned earlier, computers infected with botware can be controlled remotely for the commission of further criminal activities, including DoS attacks. A DoS attack may be conducted by sending a flood of traffic, resulting in websites becoming overwhelmed and inaccessible to legitimate users (Ianelli & Hackworth 2006). DoS attacks can also target hardware or software applications, for example, by shutting down the power supply (TISN 2006). Four percent of small businesses that had experienced a computer security incident in 2006–07 reported a DoS attack (Richards 2009).

DoS attacks may be launched against businesses for a number of reasons including extortion, competition, protest or revenge. Online extortion typically consists of a sample DoS attack, followed by a threat that a larger scale attack will follow if payment is not provided (Ianelli & Hackworth 2006). Business competitors may organise DoS attacks against their opponents in order to obtain financial benefit by attracting their clients (TISN 2006). Protestors may use DoS attacks to object to practices such as animal testing. Revenge DoS attacks may also take place when an employee is dismissed or a job applicant is unsuccessful (TISN 2006).

Phishing and spear phishing

Phishing refers to fraudulently obtaining login credentials or personal information by appearing to be a legitimate company, such as a bank. Typically victims are contacted by email and directed to a bogus website to enter their personal information. Of the small businesses that had experienced a computer security incident in 2006–07, 24 percent reported a phishing attack. This could involve the business being fraudulently represented as well as receiving phishing emails (Richards 2009).

Spear phishing is conducted with the aim of gaining access to the business's computer system. Spear phishing differs from phishing in that rather than targeting a large number of prospective victims, a specific business owner or a business's employees are selected. The attack is tailored to enhance its perceived legitimacy, such as appearing to come from a service provider that the business deals with. Further, as spear phishing emails are directed towards a small number of individuals rather than many recipients, they may be less likely to be detected and blocked by email filters (Sheng 2009).

Unauthorised access

Unauthorised access of computer systems may occur in a number of ways, including

exploiting software weaknesses and vulnerabilities, malware infection or obtaining passwords. The outcomes of unauthorised access could include, for example, obtaining client information for the commission of further identity theft or fraud offences, or obtaining copies of business tenders for competition purposes. Eight percent of small businesses who experienced a computer security incident in 2006–07 reported that their networks had been accessed without authorisation, five percent reported theft or breach of proprietary or confidential information and three percent reported the sabotage of their network or data holdings (Richards 2009).

Employees have knowledge of a business's computer systems and, while they may have legitimate access to those systems, there is the potential for unauthorised use. Businesses that are slow in restricting access after terminating someone's employment may find that their systems have been sabotaged. In 2006–07, six percent of small businesses who had experienced a computer security incident reported insider abuse of access (Richards 2009).

Cloud computing risks

Cloud computing refers to the access to network storage and applications online. These services are stored on servers in large data warehouses and are accessed via the internet, with users paying providers only for what they use (Choo 2010). Cloud computing offers a number of benefits to businesses. For example, data and applications can be accessed anywhere and there are cost benefits in not having to purchase, maintain, install and update hardware infrastructure or software applications (Choo 2010; DSD 2011). It is predicted that the uptake of cloud computing will increase, with Choo (2010: 2) asserting that

> cloud computing also offers significant computing capability and economy of scale that might not otherwise be affordable to business, especially [for] small and medium enterprises that may not have the financial and human resources to invest in IT infrastructure.

However, there are risks associated with the use of cloud computing. For example:

- providers may be vulnerable to malware infection and attacks that result in unauthorised access to the data held in their servers;
- if internet connectivity is lost, businesses would be unable to access their data or applications;
- businesses lose control over the security of their data;
- data may be misused by rogue providers;
- data may be insecurely transmitted, stored or processed by the provider; and
- legal jurisdictional issues may arise when the provider is foreign owned or the data are stored or transmitted overseas (Choo 2010; DSD 2011).

Crime prevention

Just as retail stores take steps to ensure that their premises are secure with the use of locks, security alarms, surveillance cameras or anti-theft devices, so can businesses operating in the online environment. Basic precautions that small businesses can take to help protect themselves against loss of reputation, time and money include technical countermeasures, such as security patches and antivirus tools, as well as organisational policies directed towards improving the security culture within the business. An overview of some of the commonly used crime prevention strategies are outlined below. Further information is available from the Australian Government's Stay Smart Online (2010) website.

Security patches

New vulnerabilities for operating systems, internet browsers and business applications are constantly being identified. Security patches fix vulnerabilities in computer programs that may be used by hackers to gain unauthorised access. Patches also fix software bugs and improve computer performance. Patches can be installed on a test computer to ensure that they do not change or remove functionality that could interfere with normal business functions. It is important to ensure that patches are installed soon after they are made available as the vulnerabilities they are fixing are then made known, potentially leading to increased exploitation attempts. This can be facilitated by ensuring that the auto update function is enabled (Stay Smart Online 2010). However, only seven percent of small businesses reported in the ABACUS survey that they used automated patch management to update their computer security, with five percent managing patches manually (Richards 2009).

Firewalls

According to the ABACUS survey, 70 percent of small businesses use firewalls to protect their computer systems (Richards 2009). Firewalls provide a barrier between the computer and the internet, protecting them from unauthorised access. Firewalls can also be used inside a network to restrict access to certain systems or services. Hardware firewalls include routers with firewall capabilities or a computer that acts as a buffer, and are generally used for computer networks, while software firewalls protect individual computers (Stay Smart Online 2010). Many operating systems have firewalls that can be enabled and some antivirus programs also offer this feature.

Antivirus and malware tools

Analysis of the ABACUS survey showed that 84 percent of small businesses were using antivirus software, 63 percent used anti-spam, 58 percent used anti-spyware and 33 percent used anti-phishing tools (Richards 2009).

It is important to ensure that antivirus tools are reputable. Scareware refers to fake anti-malware applications that typically appear as a computer pop-up advising that there is a (non-existent) problem with the computer that requires rectifying for a cost (Cluley 2010). It should also be recognised by businesses that anti-malware tools do not provide a complete antivirus/malware solution as they respond reactively to known threats. Stealth malware even attempts to trick antivirus software into thinking that it is not there (Chen & Abu-Nimeh 2011). Businesses can, however, ensure that anti-malware subscriptions are renewed when required, that the software is kept up to date and that computers are scanned regularly.

Fraud detection and prevention

Businesses trading online can take steps to help ascertain if orders are genuine. Stay Smart Online (2010) provides advice about what to look out for in suspect orders, how to check if an order is likely to be fraudulent and steps that a business can take to prevent against fraud.

Offering a secure site for customers to enter personal information, including account names and passwords and particularly payment details, helps ensure that their data and customer accounts are protected. Secure websites use digital certificates to ensure that data travelling between it and

the browser are encrypted, so that it cannot be read if intercepted. Secure sites also advise the web browser that the domain name details match those provided on the certificate, thereby providing reassurance that the website is legitimate. However, only 13 percent of small businesses responding to the ABACUS survey reported that they used digital certificates (Richards 2009).

Staff policies, awareness and training

IT-acceptable use policies set out how a business's computer resources should be used (Stay Smart Online 2010). As well as outlining expectations in relation to things such as personal use of resources and the handling of sensitive information, these policies may cover the installation of applications or the forwarding of emails that may contain malware.

A user access management policy sets out the access rights for staff on a business's computer system. Restricting administrative privileges prevents the installation of malware and minimises the extent of damage done if users' accounts are compromised (AusCERT 2008). Similarly, limiting staff access to only the files that they require will minimise insider abuse of access or the damage caused by unauthorised access. A policy that ensures that system access is discontinued when a staff member leaves an organisation will also assist in preventing malicious attacks.

Account/password management policies set out how often passwords used to access accounts should be changed, their complexity and length (Richards 2009). Employee education and awareness programs include courses and seminars to inform staff about computer security issues (Richards 2009).

Small business respondents to the ABACUS survey were much less likely than medium and large businesses to report having staff policies or training in place. Only seven percent had IT-acceptable use policies, 12 percent had user access management policies, 19 percent had account/password management policies and 15 percent provided employee education and awareness programs (Richards 2009).

Physical security

The physical security of computer systems can be enhanced by ensuring that servers are kept in secure rooms and that staff computers are not easily accessible by others. Guidelines for the use of portable business equipment may also be integrated into staff policies.

Small business respondents to the ABACUS survey indicated that 20 percent kept their servers in secure rooms, 28 percent limited access to workstations, 16 percent physically secured laptop computers and seven percent secured wireless devices (Richards 2009).

Conclusion

Computer security may not be a high priority for small businesses, however, the outcomes of a security incident, such as websites not being accessible and loss of reputation can have a significant impact on a business. This is particularly the case for businesses conducting the majority of their trade or advertising online.

It is also important to recognise that the harm caused by computer security incidents can extend beyond damage to business. For example, there is also the increased proliferation of malware, botnets and identity crimes when websites and computer systems are compromised. The cost of a multifaceted security strategy that is regularly reviewed and updated may be trivial compared with the financial and intangible losses following a computer security incident and may not necessarily be that difficult to enact. A cost-effective strategy could consist of the implementation and regular review of:

- *technical prevention measures*—ensuring application and operating system patches are up-to-date and automated, enabling firewalls, using effective anti-malware software, providing secure sites so that customers can provide their personal information safely and restricting administrative privileges for IT systems;
- *organisational policies and staff training*—informing employees about the proper and secure use of business resources, password management and user access; and
- *physical security*—restricting access to IT hardware and infrastructure.

As demonstrated in this paper, small businesses in Australia still have some way to go to ensure that they remain safe in the ever-changing online environment. The risks for businesses and their online customers are likely to change and potentially increase. Therefore, it is advantageous for a business to take steps now to implement a security strategy and ensure that it is kept up to date to address future threats.

Acknowledgements

The ABACUS study was funded under the Attorney-General's Department's Proceeds of Crime fund and conducted by the Social Research Centre, Melbourne.

Assistance in preparing this paper was provided by Dr Russell G Smith.

References

All URLs correct as at September 2011

Arup T 2008. More arrests as child porn net closes. *The Age* 6 June. http://www.theage.com.au/national/more-arrests-as-child-porn-net-closes-20080605-2mbz.html

AusCERT 2008. *Protecting your computer from malicious code.* Brisbane: University of Queensland. http://www.auscert.org.au/render.html?it=3352

Australian Bureau of Statistics (ABS) 2010. *Counts of Australian businesses, including entries and exits.* cat. no. 8165.0. Canberra: ABS. http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/4B1441D347457CF6CA2577C2000F0A05/$File/81650_jun%202007%20to%20jun%202009.pdf

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

Australian Competition & Consumer Commission (ACCC) 2011. *Selling goods through the internet or classifieds?* Canberra: ACCC. http://www.scamwatch.gov.au/content/index.phtml/itemId/777292

Australian Competition & Consumer Commission (ACCC) 2008. *The little black book of scams.* Canberra: ACCC. http://www.scamwatch.gov.au/content/index.phtml/itemId/726050

Australian Institute of Criminology (AIC) 2009a. Computer security incidents experienced by Australian businesses. *Crime Facts Info* no. 191. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/cfi/181-200/cfi191.aspx

Australian Institute of Criminology (AIC) 2009b. Industry sector and the prevalence of computer security incidents against Australian businesses. *Crime Facts Info* no. 192. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/cfi/181-200/cfi192.aspx

Australian Institute of Criminology (AIC) 2009c. Top 10 computer security tools used by Australian businesses. *Crime Facts Info* no. 193. Canberra: AIC. http://www.aic.gov.au/publications/current%20series/cfi/181-200/cfi193.aspx

Alice Hutchings is a 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. 133
Ethics approval no. PO114
Dataset no. 105

Australian Payments Clearing Association Limited (APCA) 2010. *Payment fraud statistics: Summary of results.* Sydney: APCA. http://www.apca.com.au/Public/apca01_live.nsf/ResourceLookup/Payment_Fraud_Statistics_20090_PrintFriendly.pdf/$File/Payment_Fraud_Statistics_20090_PrintFriendly.pdf

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

Chen TM & Abu-Nimeh S 2011. Lessons from stuxnet. *Computer* 44(4): 91–93

Choo K-KR 2011. Cyber threat landscape faced by financial and insurance industry. *Trends & Issues in Crime and Criminal Justice* no. 408. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/401-420/tandi408.aspx

Choo K-KR 2010. Cloud computing: Challenges and future directions. *Trends & Issues in Crime and Criminal Justice* no. 400. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/381-400/tandi400.aspx

Cluley G 2010. Sizing up the malware threat—key malware trends for 2010. *Network Security* (4): 8–10

Dacosta I, Chakradeo S, Ahamad M & Traynor P 2011. *One-time cookies: Preventing session hijacking attacks with disposable credentials.* Georgia: Georgia Institute of Technology. http://smartech.gatech.edu/bitstream/handle/1853/37000/GT-CS-11-04.pdf?sequence=1

Defence Signals Directorate (DSD) 2011. *Cloud computing security considerations.* Canberra: Department of Defence. http://www.dsd.gov.au/infosec/cloudsecurity.htm

Department of Innovation, Industry, Science and Research (DIISR) 2011. *Small business and independent contractors.* Canberra: DIISR. http://www.innovation.gov.au/AboutUs/KeyPublications/Documents/InnovationPortfolioFactSheets.pdf

Egele M, Wurzinger P, Kirda E & Kruegel C 2009. *Defending browsers against drive-by downloads.* Presented at Conference on Detection of Intrusions and Malware & Vulnerability Assessment: Milan. https://eldorado.tu-dortmund.de/bitstream/2003/26299/1/01-06.pdf

Electronic Frontiers Australia (EFA) 2010. *Submission to the Department of Broadband, Communications and the Digital Economy 'Mandatory internet service provider (ISP) filtering: Measures to increase accountability and transparency for refused classification material' consultation*. North Adelaide: Electronic Frontiers Australia. http://www.dbcde.gov.au/submissions/20100316_11.34.55/211-Main%20Submission_EFA.pdf

Furnell S 2010. Hackers, viruses and malicious software, in Jewkes Y & Yar M (eds), *Handbook of internet crime*. Devon: Willan Publishing: 173–193

Grabosky P 2007. *Electronic crime*. New Jersey: Pearson Education

Ianelli N & Hackworth A 2006. *Botnets as a vehicle for online crime.* Presented at 1st International Conference on Forensic Computer Science: Brazil. http://www.icofcs.org/2006/ICoFCS2006-pp03.pdf

Internet Industry Association (IIA) 2005. *Internet industry spam code of practice: A code for internet and email service providers.* Canberra: IIA. http://www.acma.gov.au/webwr/telcomm/industry_codes/codes/iia%20spam%20code%20dec%202005.pdf

Knights L, Fonceca M, Mack G & Woodward A 2006. *Risks and responsibilities in establishing a wireless network for an educational institution.* http://igneous.scis.ecu.edu.au/proceedings/2006/aism/Knights%20et%20al%20-%20Risks%20and%20responsibilities%20in%20establishing%20a%20wireless%20network%20for%20an%20educational%20institution.pdf

Larsen K 2010. Search for security. *Infosecurity* 7(1): 32–35

Lawton G 2010. Fighting intrusions into wireless networks. *Computer* 43(5): 12–15

Moore T, Clayton R & Anderson R 2009. The economics of online crime. *Journal of Economic Perspectives* 23 (3): 3–20

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

Selvadurai N, Islam MR & Gillies P 2009. Unauthorised access to wireless local area networks: The limitations of the present Australian laws. *Computer Law & Security Review 25*(6): 536–542

Sensis Pty Ltd 2010. *Sensis e-business report: The online experience of small and medium enterprises.* Melbourne: Telstra Corporation Limited. http://about.sensis.com.au/IgnitionSuite/uploads/docs/Sensis%20e-Business%20Report%20September%202010%20FINAL.pdf

Shelly M & Jackson M 2008. Doing business with consumers online: Privacy, security and the law. *International Journal of Law and Information Technology* 17(2): 180–205

Sheng XS 2009. *A policy analysis of phishing countermeasures.* Pittsburgh: Carnegie Mellon University. http://gradworks.umi.com/3383412.pdf

Stay Smart Online 2010. *Small and medium business. Canberra*: Commonwealth of Australia. http://www.staysmartonline.gov.au/small_and_medium_business

Trusted Information Sharing Network (TISN) 2006. *Denial of service/distributed denial of service: Managing DoS attacks.* Barton: Attorney-General's Department. http://www.dbcde.gov.au/__data/assets/pdf_file/0011/41312/DoS_Report.pdf

Verizon 2011. *2011 data breach investigations report.* Verizon. http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

Williams PAH & Manhcke RJ 2010. *Small business—A cyber resilience vulnerability.* Presented at International Cyber Resilience Conference: Perth 2010. http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1013&context=icr&sei-redir=1#search=%22Small+business+:+A+cyber+resilience+vulnerability%22