Trends & issues in crime and criminal justice

No. 456 May 2013

Australian Government
Australian Institute of Criminology

Cloud computing for small business: Criminal and security threats and prevention measures

Alice Hutchings, Russell G Smith & Lachlan James

Cloud computing refers to the delivery of computer processing infrastructure, operating systems, software and data storage over Internet-based public or private computer networks. The aim is to relieve users of some of the burdens associated with maintaining computers and data storage, while enabling the associated costs to be reduced. Although cloud computing is still developing in popularity and coverage, its use raises a number of crime and security concerns, particularly for small business users. This paper charts the nature of these concerns for small business and reviews the detection, prevention and mitigation measures that may be implemented by small business users and cloud service providers to minimise or negate the risks identified.

Foreword | *Compared with large organisations, small businesses operate in a distinct and highly resource-constrained operating and technical environment. Their proprietors are often time poor, have minimal bargaining power and have limited financial, technical, legal and personnel resources. It is therefore unsurprising that cloud computing and its promise of smoothing cash flows and dramatically reducing ICT overheads is attractive to small business. Cloud computing shifts the delivery and maintenance of software, databases and storage to the internet, transforming them into Pay-As-You-Go services accessed through a web browser. While providing many benefits, cloud computing also brings many risks for small business, including potential computer security and criminal, regulatory and civil liability issues. This paper, undertaken as a collaborative partnership with the ARC Centre of Excellence in Policing and Security at Griffith University, identifies these risks and offers a perspective on how they might be contained so that the benefits of cloud computing do not outweigh the risks for small businesses in the 21st century.*

Adam Tomison
Director

The small business computing environment

The Australian Bureau of Statistics (2001) defines a small business as one employing fewer than 20 people and includes sole proprietorships as well as partnerships without employees. As at June 2011, small businesses represented 96 percent of businesses in Australia (ABS 2012). Small business suffers from what Welsh and White (1981: 32) describe as 'resource poverty' compared with larger organisations. This includes limited in-house specialist technical and/or legal knowledge necessary to evaluate and capture the benefits of new operational services and technologies. It is also a very time-constrained working environment, where personnel frequently work overtime in order to complete necessary tasks. Small business has limited access to financial resources and inconsistent cash flow, as well as limited bargaining power. Arguably, there is a need for greater tolerance to risk, with many Australian small businesses experiencing low survival rates—in any one year, more than 15 percent of all small businesses can be expected to fail (DIISR 2011).

CEPS ARC Centre of Excellence in Policing and Security

Australian Government
Department of Broadband, Communications and the Digital Economy

In relation to information and communications technologies (ICT), small businesses may seek to save costs by using laptop computers, tablet devices and mobile phones for both business and personal use. ICT is also often shared among personnel and small businesses are more likely to have poorly setup and maintained firewalls, virus protection and other security software than their larger counterparts.

Small businesses face a number of computer security threats and may lack the time and/or technical resources to install software updates and patches to fix software and security bugs or address wireless network security, rendering them vulnerable to network exploitation (Hutchings 2012). Finally, small businesses are always on the lookout for new tools and are willing to adopt alternative software applications. These aspects all create vulnerabilities in terms of computer security and safety.

One solution that is gradually being adopted by small business is to make use of so-called 'cloud computing'. Cloud computing includes the delivery of computer processing infrastructure (Infrastructure as a Service—IaaS), operating system platforms (Platform as a Service—PaaS) and/or software, databases and storage as a service (Software as a Service—SaaS) on demand over either a public or private computer network (Mell & Grance 2011). The range of cloud computing services (including some that are provided free of charge) that meet the particular needs of small business is vast and growing rapidly.

There are many benefits to be derived from cloud computing for small business including improvements in cash flow, reduced administrative and personnel overheads, more efficient setup and maintenance of ICT, and improvements in computer security, particularly with respect to the secure storage of sensitive information (Mowbray 2009). Finally, cloud services replace the need for frequent software installation and updates, and their accompanying service downtime.

While cloud computing holds great promise for small business, it does not completely remove all ICT overheads. Small businesses remain tasked with engaging other subscription services, such as an Internet Service Provider. There are also hardware-related costs including:

- purchasing and setting up a modem (ADSL, cable, mobile broadband) to securely connect to the internet via an Internet Service Provider (and where appropriate, establishing a secure wireless local network); and
- purchasing and setting up computer(s), printer(s), backup storage etc.

Businesses also need to purchase, set up and maintain operating system software, security software (eg firewall, anti-virus etc) and other software (eg web browsers).

A number of specific crime risks have been identified in the literature that could affect cloud service providers, cloud computing tenants and the transmission of data between providers and tenants in the small business environment. Many of these vulnerabilities are not unique to cloud computing, but could arise in connection with conventional use of ICT by small businesses and indeed, by larger businesses as well. What is different, however, is the nature of the data that may be stored by small businesses on the cloud and its attractiveness to offenders located in disparate countries. Other vulnerabilities are unique to virtualisation and the multi-tenancy environment of the public cloud.

Methods and aims

This paper presents the findings of a desk-based assessment of English-language, public source literature available over the internet and through subscription-based services to identify current and emerging cloud computing risks and incidents relevant to small businesses. The research was commissioned by the Department of Broadband, Communication and the Digital Economy and undertaken by staff of the ARC Centre of Excellence in Policing and Security and the Australian Institute of Criminology. While the commissioned research had a wider scope, this paper focuses on the crime and security risks that small businesses could face through the adoption of cloud computing and how they might be minimised.

Crime and security risks in the cloud

Compared with computer security incidents affecting corporate systems generally, there have been relatively few attacks reported against cloud service providers. Banham (2012) claims that this is because cloud service providers have stronger security, as they are more concerned about the consequences of reputational damage if data are breached. However, according to Pacella (2011: 70), 'cloud providers often ask their clients to keep attacks quiet'. When not bound by mandatory data breach reporting requirements, as in Australia, cloud computing tenants are likely to want to avoid the publicity associated with data breaches. This may be particularly relevant where the cloud service provider claims no responsibility or liability for breaches of data security or unavailability of data in service-level agreements (Blumenthal 2011). In addition, some attacks may go undetected and in other cases when data breaches are made public, the fact that data were held in the cloud may not be released. It is clear that cloud service providers and vendors are reluctant to publicise the insecurity of their systems and are unwilling to disclose security breaches that occur. However, recent survey research involving cloud tenants, cloud service providers and those who attempt to breach systems has revealed concerning evidence and actual victimisation in connection with cloud computing.

Aleem and Sprott (2013) interviewed 200 ICT professionals worldwide. Respondents' most cited concern regarding the use of cloud computing was security, as reported by 93.4 percent of interviewees. This was considered to be more of a concern than governance (62.3%) and the lack of control over service availability (55.7%). Cloud computing had been implemented by 17 percent of respondents' organisations and eight percent of respondents reported that they had experienced a security breach in the cloud. Respondents reported that the

top two cloud threats were data loss and leakage (73.5%), and account, service and traffic hijacking (60.8%).

According to an international survey of 1,200 companies with over 500 employees in the United States, Canada, the United Kingdom, Germany, Japan and India conducted by Trend Micro (2011), an antivirus and computer security vendor, 43 percent of organisations that reported using cloud computing had experienced a 'security lapse or issue' in the previous 12 months, although the nature of the incident was not disclosed.

Another survey of 103 US and 24 European cloud service providers by the Ponemon Institute (2011) revealed that 62 percent were not confident that the cloud applications and resources they supply are secure. Sixty-five percent of respondents were public cloud providers, while private and hybrid cloud providers comprised 18 percent of the sample each. Of the public cloud providers, only 29 percent were confident or very confident that the cloud applications and resources supplied by their organisation were secure.

A survey of 100 ICT professionals conducted by a computer security vendor at DefCon (a hacker conference held in Las Vegas in 2010) found that 96 percent of respondents believed that the 'cloud would open up more hacking opportunities for them' and 45 percent had 'already tried to exploit vulnerabilities in the cloud' (Fortify 2010: 7).

In the absence of empirical research into the extent of these risks, it is not known at present which are more prevalent or more important than others.

Crime and security risks involving cloud service providers

Examples of the crime and security risks that face cloud service providers are as follows.

Authentication issues

Unauthorised access to cloud computing systems may occur when a username and password combination has been obtained without authorisation. This can occur using a variety of technical and non-technical methods. Social engineering may be targeted towards the cloud service provider by, for example, claiming that urgent access is required but that the password is not working and needs to be reset. Passwords may also be guessed, be left lying around in offices, obtained using keylogging malware, cracked using brute force, or overcome when there are weak password recovery mechanisms, such as answering 'secret' questions where the answers are publicly available (Dlodlo 2011). An example of a social engineering attack is provided in Box 1.

Inadequate authentication checks may not necessarily be attributed to malicious activity, although they may result in data being accessed for nefarious purposes. For example, some incidents in which others are permitted to have access to data stored on the cloud may be inadvertent:

> In June 2011, Dropbox, a popular cloud storage site where approximately 25 million people store their videos, photos, documents, and other files, inadvertently left the site open for four hours on Father's Day. The glitch let anyone log in to customers' accounts with any password (Wright 2011: 20).

Insufficient or faulty authentication checks may also provide opportunities for Uniform Resource Locator (URL) guessing attacks, whereby possible page links are entered to gain access to pages directly, bypassing authentication checks (Grobauer, Walloschek & Stoecker 2011). Data breaches, however they are accomplished, may have significant impact not only on the cloud service provider's tenant, whose data have been accessed, but also on customers who may have trusted that organisation with their personal information:

> In early April, Epsilon announced that its database had been breached by an unknown third party, allowing unauthorised access to the email addresses of its clients' customers (Kunick 2011: 18).

Denial of service attacks

Denial of service (DoS) attacks against cloud service providers may leave tenants without access to their accounts. This can occur by sending a flood of traffic to overwhelm websites to make them inaccessible to legitimate users. When a DoS attack is conducted using a botnet (a network of compromised machines), this is referred to as a distributed denial of service attack, or DDoS. DoS attacks aimed at individual accounts, rather than at all cloud tenants, may also be accomplished by changing the tenant's password or maliciously continuing to enter the incorrect password so that the account becomes locked.

Use of cloud computing for criminal activities

Cloud computing accounts can be created or existing accounts compromised for criminal purposes. New cloud computing accounts may be created with stolen credentials and credit card details, thereby reducing the cost to the offender(s), as well as anonymising

Box 1 Social engineering attack

zzzreyes writes:

> I got an email from my cloud server to reset the admin password, first dismissed it as phishing, but a few emails later I found one from an admin telling me that they had given a person full access to my server and revoked it, but not before 2 domains were moved from my account. I logged into my account to review the activity and found the form the perpetrator had submitted for appointment of new primary contact and it infuriated me, given the grave omissions. I wrote a letter to the company hoping for them to rectify the harm and they offered me half month of hosting, in a sign of good faith. For weeks I've been struggling with this and figure that the best thing to do is to ask my community for advice and help, so my dear slashdotters please share with me if you have any experience with this or know of anyone that has gone through this. What can I do?

Source: http://it.slashdot.org/story/12/04/04/1738220/ask-slashdot-my-host-gave-a-strangeraccess-to-my-cloud-server-what-can-i-do?utm_source=rss1.0moreanon&utm_medium=feed

the offender and creating further difficulties in tracking down the source of the attack, particularly when jurisdictions are crossed. Accounts created or compromised in such a way can be controlled as part of a botnet. In the following example, an existing cloud computing account was compromised and used to run a botnet command and control server:

> Computer World UK reported in December 2009 that a website hosted on Amazon EC2 had been hacked to run the Zeus botnet's command-and-control infrastructure (Blanton & Schiller 2010: np).

Botnet command and control servers can be used to launch DDoS attacks, conduct scams such as click fraud and distribute spam. The processing power of botnets may also be used to conduct brute force attacks to overcome password restrictions. For example, there have been reports that hackers made use of a cloud computing server to launch attacks on Sony's payment platforms in April 2011. This attack resulted in the breach of the personal data (including name, date of birth and email address) of 77 million users across the globe and it was believed that the data of around 11 million credit cards may also have been leaked (Hong Kong Government News 2011).

Cloud computing services may be used for the storage, distribution and mining of criminal data such as stolen personal information or child exploitation material (Cloud Security Alliance 2010). Accounting systems run in the cloud may be attractive for money laundering and terrorism financing activities. The use of cloud computing to conduct illegal activities has had further negative consequences in relation to data access for other legitimate users of the cloud service provider when servers have been seized by a law enforcement agency. Not only may access be disrupted, but the law enforcement agency (international or domestic) may have access to that data in a multi-tenanted environment (Allen 2010).

Illegal activity by cloud service providers

Loss of access to data has also occurred when cloud service providers themselves have allegedly engaged in illegal behaviour. In one case, the cloud service provider's services were stopped due to police action. Kim Dotcom and his colleagues were arrested following allegations the Megaupload cloud storage service he conducted involved illegal piracy. While the service had allegedly been used to swap movies and music files, Megaupload was also a low-cost way of legitimately sharing files and making online backups. When the US authorities closed the service without warning, businesses were unable to access their documents (Bennett 2012).

Attacks on physical security

Cloud service providers' data centres may also be physically attacked, resulting in hardware theft, unauthorised access to servers or loss of access to data. In one case in the United States, two masked men allegedly pistol-whipped a lone staff member during a graveyard shift, holding the worker hostage for two hours while confiscating equipment in a Chicago data centre. The burglars reportedly entered the facility through a fire escape, swiped the staffer's access card through a reader and forced him to perform a fingerprint scan before stealing computer storage equipment (Knapp, Denney & Barner 2011).

Insider abuse of access

Cloud service provider insiders, such as employees, contractors or third party suppliers, may misuse their privileges to disrupt access or to obtain unauthorised access to stored data. Insiders may obtain employment at a targeted cloud service provider, be targeted by organised crime syndicates, abuse their access as the result of becoming discontent in their employment, or become tempted by presented opportunities and the potential perceived gains (Blumenthal 2011). Over half (52.9%) of the ICT professionals surveyed by Aleem and Sprott (2013) indicated that they were concerned about insider threats in the cloud.

Malware

The cloud service providers' servers may be vulnerable to malware infection, including virtual machine-based rootkits (Aron 2011). These risks apply in non-cloud environments as well. Malware infection may result in account names and passwords being compromised, files being accessed and copied, corruption of files or being added to a botnet. There is also the possibility that malware compromising one tenant's virtual machines could then spread to the virtual machines of other tenants.

Side channel attacks or cross-guest virtual machine breaches

'Side channel attacks' or 'cross-guest virtual machine breaches' may result in tenants crossing the shared virtual machine boundaries and accessing the data of other tenants using shared physical resources. Side channel attacks require the attacker's virtual machine and victim's virtual machine to be located on the same physical machine; therefore, these attacks may be random and not targeted towards a specific tenant. However, targeted attacks may still be possible. It has been demonstrated with one cloud computing service provider that co-tenancy could be successfully achieved 40 percent of the time by setting up new accounts while simultaneously manipulating the resource needs of the targeted victim's virtual machines (Ristenpart et al. 2009).

Vulnerabilities in shared technology resources, which is the environment where side channel attacks occur, was listed as one of the top cloud threats by 37.3 percent of the ICT professionals surveyed by Aleem and Sprott (2013).

Vulnerabilities in software applications

Security holes and vulnerabilities may exist in software applications run in the cloud, such as backdoors that bypass normal authentication protocols (Pacella 2011). New vulnerabilities for operating systems, internet browsers and business applications are regularly being identified. Security patches fix vulnerabilities in computer programs, which may be used to gain unauthorised access. However, delays in installing patches may lead to increased exploitation attempts as the vulnerabilities they are fixing are then made known.

Similarly, insecure application programming interfaces, which allow software applications to interoperate with each other by passing login information between them, may provide another attack vector. Of the ICT

professionals surveyed by Aleem and Sprott (2013), 39.2 percent indicated that insecure application programming interfaces were among the top cloud threats.

Web browsers, used to access the internet and cloud service providers, are another type of software application that may be subject to attack. Browser vulnerabilities include cross site scripting whereby code is injected into websites and executed by the browser (Dlodlo 2011). Cross site scripting can be used to hijack sessions by obtaining cookies or authentication credentials by redirecting users to a site impersonating the cloud service provider.

Cryptanalysis of insecure or obsolete encryption

Data stored in the cloud may be encrypted to prevent it from being read if accessed without authorisation. However, encryption can potentially be weakened or broken if insecure or obsolete (Grobauer, Walloschek & Stoecker 2011). Partial information can also be obtained from encrypted data by monitoring clients' query access patterns and analysing accessed positions (Agrawal, El Abbadi & Wang 2011).

Structured Query Language injection

Structured Query Language (SQL) is a programming language used for database management systems. SQL injection attacks targeting web entry forms involve inputting SQL code that is erroneously executed in the database back end (Dlodlo 2011). SQL injection attacks can result in data being accessed and modified without authorisation. Another injection attack is OS injection or command injection, whereby the input contains commands that are erroneously executed by the operating system (Grobauer, Walloschek & Stoecker 2011).

Crime and security risks targeting cloud computing tenants

Phishing

Although, in the context of cloud computing, phishing misrepresents the provider, the attack is directed towards those who may hold an account with that organisation with the aim of obtaining passwords and other identifying information to obtain unauthorised access to data held in the cloud (Dlodlo 2011). Phishing is one example of social engineering in which an email appearing to be from a legitimate organisation is sent directing recipients to a bogus (spoofed) website to enter their login credentials or other personal information.

Domain name system attacks

Cloud computing users may be subject to domain name system (DNS) attacks. The principal use of domain names is to convert an internet protocol resource (a string of numbers) into a readily identifiable and memorable address, such as those used in email addresses and URLs. A variety of DNS attacks are aimed at obtaining authentication credentials from internet users, including cloud service tenants. Pharming and DNS-poisoning involve diverting visitors to spoofed websites by 'poisoning' the DNS server or the DNS cache on the user's computer. Domain hijacking refers to stealing a cloud service provider's domain name, while domain sniping involves registering an elapsed domain name. Cybersquatting refers to registering a domain name that appears to be similar to a cloud service provider, which can be used to conduct phishing scams. Login details can also be obtained by typesquatting, which relies on a user entering the wrong URL and subsequently providing their authentication credentials to a spoofed website.

Compromising the device accessing the cloud

Access to a business's cloud computing account may be achieved if the device accessing the cloud service is compromised, for example, by a keylogger that records keystrokes including usernames and passwords (Banks 2010). Again, malware infections such as this may be random, or individuals within an organisation may be directly targeted with a Trojan—malware designed to look like a legitimate file.

Access management issues

Businesses that fail to restrict their employees' access to cloud computing services after they leave their employment would be vulnerable to having their data accessed, altered, copied, or deleted (Subashini & Kavitha 2011). Former employees may seek revenge against their employer, or steal information for resale or to use in setting up a competing business. Such risks, of course, also exist in the non-cloud computing environment.

Attacks targeting the transmission of data

Session hijacking and session riding

Session hijacking involves the attacker exploiting active computer sessions by obtaining the cookies that are used to authenticate users. This can be achieved by cross site scripting, which involves malicious code being injected into the website, which is subsequently executed by the browser (Dlodlo 2011).

A similar attack called *session riding*, is where websites are exploited using cross site request forgery to transmit unauthorised commands. An attacker 'rides' an active computer session by tricking a user (eg by sending a link) into visiting a manipulated webpage while they are logged into the targeted site. The webpage contains a request that is executed by the website as the user is also sending their authentication credentials. Commands may be used to, for example, manipulate or delete data, reset passwords, add new users or delete existing users, or forward emails (Schreiber 2004).

Man-in-the-middle attacks

In a man-in-the-middle attack, the attacker intercepts traffic between a website and a Browser (Grobauer, Walloschek & Stoecker 2011). This occurs when the browser believes that the attacker is the legitimate website and the website authenticates the attacker as the browser. The attacker can then read and alter the data being transmitted, including account passwords that may be used to login to cloud services.

Network/packet sniffing

Network or packet sniffing involves the interception and monitoring of network traffic (Subashini & Kavitha 2011). Data that are being transmitted across a network, such as passwords, can therefore be captured and read if not adequately

Table 1 Summary of cloud computing crime and security prevention measures

	Technical prevention measures						Physical security					Organisational policies, awareness and training					
	Patching operating systems, internet browsers and software applications	Installing anti-virus, anti-malware tools and firewalls	Implementing multifactor authentication	Encrypting data travelling between the cloud and the browser	Encrypting data stored in the cloud	Intrusion detection and prevention systems and network monitoring	Perimeter security	Shielded server rooms and cages	Surveillance	Access control	Facility access logs	ICT-acceptable use policies	Password policies	User access management policies	BYOD policies	Staff training	Background checks of cloud service provider staff
Crime and security risks involving cloud service providers																	
Authentication issues		✓	✓		✓	✓						✓	✓	✓	✓	✓	
Denial of service attacks and botnets		✓				✓											
Use of cloud computing for criminal activities						✓											
Illegal activity by cloud service providers					✓												✓
Attacks on physical security					✓		✓	✓	✓	✓	✓						
Insider abuse of access			✓		✓	✓			✓	✓	✓						✓
Malware	✓	✓	✓		✓	✓						✓			✓	✓	
Side channel attacks					✓												
Vulnerabilities in software applications	✓	✓	✓		✓	✓						✓					
Cryptanalysis of insecure or obsolete encryption					✓												
SQL injection	✓	✓			✓	✓											
Crime and security risks targeting cloud computing tenants																	
Phishing			✓		✓							✓	✓			✓	
Domain name system attacks	✓		✓		✓							✓	✓			✓	
Compromising the device accessing the cloud	✓	✓	✓		✓	✓						✓	✓		✓	✓	
Access management issues			✓											✓			
Attacks targeting the transmission of data																	
Session hijacking and session riding				✓													
Man-in-the-middle attacks				✓													
Network/packet sniffing				✓													

encrypted. In the cloud environment, this is particularly important as passwords play a critical role in establishing access to the provider's services.

Responding to crime and security threats facing small business

Although the threats identified above may seem somewhat oppressive, there are a number of measures that can be adopted by small businesses as well as cloud providers to detect, prevent and minimise the damage from criminal and security threats in the cloud environment. Table 1 provides an overview of the various methods that are available both to business tenants and cloud computing providers.

Arguably, a single measure can be used to address multiple threats. While the implementation of some measures resides with cloud service providers, such as physical security of data warehouses, others can be undertaken by small business proprietors themselves, particularly when they select a provider and assess the nature of the services they offer. Assessing considerations such as whether data travelling between the cloud and the browser are encrypted, whether multi-factor authentication is offered and the physical security of the data warehouse are all of critical importance.

Technical prevention measures

Technical prevention measures can be adopted by both the small business and the cloud service provider. These include patching operating systems, internet browsers and other software applications to protect against new vulnerabilities and malware, installing anti-virus and malware tools, and installing firewalls to protect against unauthorised access. Cloud computing providers may also implement multifactor authentication to strengthen authentication checks. Encrypting data travelling between the cloud and the browser, as well as encrypting data stored in the cloud, protects against attacks targeting the transmission of data, as well as limiting the effects of unauthorised access. Cloud

service providers may also use intrusion detection and prevention systems and network monitoring.

Physical security

Cloud service providers should, arguably, provide a safe and secure data warehouse that can only be accessed by authorised personnel in order to prevent attacks against physical infrastructure, as well as insider abuse of access. Physical security measures include:

- perimeter security, such as bunkers, gates and fences;
- shielded server rooms and cages that prevent eavesdropping, external scanning and interference via electromagnetic radiation;
- surveillance, such as CCTV and security guards;
- access control, such as swipe cards, turnstiles, biometric authentication and identity cards; and
- maintaining facility access logs.

Cloud service providers should also have effective fire management practices in place and backup power systems to prevent data loss through natural disaster or malicious attacks. While security audits should assess whether appropriate physical security measures are in place, audit rights may be beyond the scope of small businesses.

Organisational policies, awareness and training

Small businesses may implement a number of organisational policies to protect against computer security threats that relate to cloud computing, as well as computer security more generally. These include ICT-acceptable use policies that set out how a business's computer resources should be used, including expectations in relation to personal use, the handling of sensitive information, the installation of applications and the forwarding of emails, which may contain malware.

Password policies set out how often passwords should be changed and their complexity to strengthen authentication checks, while user access management policies set out the access rights for staff, including that access should be discontinued when a staff member leaves an organisation. Employees using their own devices into the workplace should also be subject to organisational policies, as they may be vulnerable to compromise and create more avenues for unauthorised access to cloud services.

Small businesses may also provide training to staff and create awareness about computer security issues. Ensuring staff are well informed may assist in preventing social engineering attacks, such as phishing that are not necessarily protected against by technical measures. Because of the sensitive nature of data stored by cloud service providers, they should also conduct background checks when employing staff as a preventative measure against insider abuse of access.

The AIC's Australian Business Assessment of Computer User Security (ABACUS) revealed that small business respondents were less likely than medium and large businesses to have staff policies or training in place. Only seven percent had ICT-acceptable use policies, 19 percent had account/password management policies, 12 percent had user access management policies and 15 percent provided employee education and awareness programs (Richards 2009).

Service level agreements

Small businesses should be aware of the implications of their cloud service provider's service level agreement, which will address the issues of security, privacy and data control. Service level agreements may also set out requirements for third party audits of cloud service providers.

Cyber and cloud insurance

Existing cyber liability insurance holds out some limited hope of compensating for losses as a result of cybercrime. However, the best hope for broader coverage rests with contingent business interruption insurance adapted to the unique circumstances of cloud computing ('cloud insurance') being developed by new entrepreneurial ventures.

Crime displacement risks

Crime displacement occurs when crime moves to other locations, times, targets, methods, perpetrators, or types of offence, often as the result of crime prevention initiatives. Displacement concerns that relate to cloud computing may include:

- displacement to cloud service providers who do not have strong security measures;
- cloud service providers operating from jurisdictions that do not have applicable criminal provisions, have low criminal penalties, or do not have extradition treaties;
- different methods, for example, if a target is adequately protected against electronic attacks, an offender may coerce an employee through bribery or extortion; and
- displacement to perpetrators who are more highly skilled and perhaps more adept at hiding their offending activities.

Effective crime prevention requires an appreciation of these risks and the use of measures designed to address them.

Conclusions

Compared with larger organisations, small business operates in a distinctive, highly resource constrained environment, rendering the promise of cloud computing to smooth cash flows and reduce ICT overhead highly attractive. However, in adopting cloud computing, it is this distinct operating environment that also renders small businesses vulnerable to criminal and security threats.

In relation to cybercrime risks, while cloud service providers themselves hold much greater appeal to cybercriminals, it is the cloud service provider's small business tenants—who experience disrupted services and hence disruption to their already fragile revenues—that are likely to be the real victims. Lacking policies, procedures and training relating to cyber and network security, small businesses are particularly vulnerable to having account details stolen and their cloud services hijacked. There are, however, technical and commercial practices that can be implemented to reduce at least

Dr Alice Hutchings is a Senior Research Analyst at the AIC.

Dr Russell G Smith is Principal Criminologist at the AIC.

Lachlan James is a Research Associate of the ARC Centre of Excellence in Policing and Security (CEPS), Griffith University.

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

some of the security and crime risks. In the words of Mowbray (2009: 14):

> [I]t is likely that a combination of technical solutions, business practices, and standard contracts between [cloud service providers] and customers will be able to resolve most if not all [cloud computing concerns].

In addition, cyber liability insurance may be able to compensate small businesses for losses as a result of cybercrime in the cloud. Creating a secure cloud computing environment may serve to place small business on substantially the same footing as larger businesses, enabling them to fully capture the true benefits of cloud computing while enduring a more equitable share of the risks.

References

URLs are current at April 2013

Agrawal D, El Abbadi A & Wang S 2011. Secure data management in the cloud. *Databases in Networked Information Systems* 7108: 1–15

Aleem A & Sprott CR 2013. Let me in the cloud: Analysis of the benefit and risk assessment of cloud platform. *Journal of Financial Crime* 20(1): 6–24

Allen J 2010. Data security in a mobile world. *GPSolo* 27(8): 4–6

Aron J 2011. Beware of the botcloud. *New Scientist* 210(2817): 24

Australian Bureau of Statistics (ABS) 2012. *Counts of Australian businesses, including entries and exits.* cat. no. 8165.0. Canberra: ABS

Australian Bureau of Statistics (ABS) 2001. *Small business in Australia.* cat. no. 1321.0. Canberra: ABS

Banham R 2012. Few data breaches in the cloud-for now. *Business Insurance* 46(3): 14

Banks L 2010. *Cyber criminals using cloud to launch attacks, security expert warns*. ComputerWorld. http://www.computerworld.com.au/article/363710/cyber_criminals_using_cloud_launch_attacks_security_expert_warns/

Bennett B 2012. Megaupload raid underlines cloud risks. *NZ Business* 26(2): 54

Blanton S & Schiller C 2010. Is there safety in the cloud? *EDUCAUSE Quarterly* 33(2)

Blumenthal MS 2011. Is security lost in the clouds? *Communications and Strategies* (81): 69–86

Cloud Security Alliance 2010. *Top threats to cloud computing v1.0: Cloud Security Alliance*. https://cloudsecurityalliance.org/research/top-threats/#_downloads

Department of Innovation, Industry, Science and Research (DIISR) 2011. *Australian small business, key statistics*. Canberra: Department of Innovation, Industry, Science and Research

Dlodlo N 2011. *Legal, privacy, security, access and regulatory issues in cloud computing*. Proceedings of the European Conference on Information Management & Evaluation: 161–168

Fortify 2010. Vast scale of cloud hacking. *International Journal of Micrographics & Optical Technology* 28(3): 7–8

Grobauer B, Walloschek T & Stoecker E 2011. Understanding cloud computing vulnerabilities. *IEEE Security & Privacy* 9(2): 50–57

Hong Kong Government News 2011. *LCQ3 information security*. Hong Kong: Hong Kong Government News

Hutchings A 2012. Computer security threats faced by small businesses in Australia. *Trends & Issues in Crime & Criminal Justice* no. 433. Canberra: Australian Institute of Criminology. http://aic.gov.au/publications/current%20series/tandi/421-440/tandi433.html

Knapp KJ, Denney GD & Barner ME 2011. Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly* 28(4): 533–541

Kunick JM 2011. Navigate the cloud. *Managing Intellectual Property* 210: 18

Mell P & Grance T 2011. *The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology*. Gaithersburg: US Department of Commerce/National Institute of Standards and Technology. http://csrc.nist.gov/publications/PubsSPs.html

Mowbray M 2009. The fog over the Grimpen Mire: Cloud computing and the law. *SCRIPTed Journal of Law, Technology and Society* 6(1): 1–15

Pacella RM 2011. Hacking the cloud. *Popular Science* 278(4): 68–71

Ponemon Institute 2011. *Security of cloud computing providers study*. Traverse City: Ponemon Institute. http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

Richards K 2009. *The Australian business assessment of computer user security: A national survey*. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/documents/3/B/3/%7B3B3117DE-635A-4A0D-B1D3-FB1005D53832%7Drpp102.pdf

Ristenpart T, Tromer E, Shacham H & Savage S 2009. *Hey, you, get off my cloud: Exploring information leakage in third-party compute clouds*. Paper presented at the 16th ACM Conference Computer and Communications Security, Chicago

Schreiber T 2004. *Session riding: A widespread vulnerability in today's web applications*. Munchen: SecureNet. http://www.securenet.de/papers/Session_Riding.pdf

Subashini S & Kavitha V 2011. A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1): 1–11

Trend Micro 2011. *Cloud security survey: Global executive summary*. http://newsroom.trendmicro.com/file.php/194/Global+Cloud+Survey+Exec+Summary_Final+%282%29.pdf

Welsh JA & White JF 1981. A small business is not a little big business. *Harvard Business Review* 59(4): 18–32

Wright A 2011. Cloud computing and security. *Toledo Business Journal* 27(11): 20–22