2010

Small Business - A Cyber Resilience Vulnerability

Patricia A H Williams
Edith Cowan University

Rachel J. Manheke
Edith Cowan University

Originally published in the Proceedings of the 1st International Cyber Resilience Conference, Edith Cowan University, Perth Western Australia, 23rd August 2010

SMALL BUSINESS – A CYBER RESILIENCE VULNERABILITY

Patricia A. H. Williams and Rachel J. Manhcke

secau - Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
Trish.williams@ecu.edu.au

Abstract

Small business in Australia comprise 95% of businesses. As a group this means that they contain increasing volumes of personal and business data. This creates escalating vulnerabilities as information is aggregated by various agencies. These vulnerabilities include identity theft and fraud. The threat environment of small business is extensive with both technical and human vulnerabilities. The problem is that the small business environment is being encouraged to adopt e-commerce by the government yet lacks resources in securing its cyber activity. This paper analysed the threats to this situation and found that questions of responsibility by individual businesses and the government are fundamental to the protection of small businesses information. Ultimately this raises the possibility of an undefined and unrecognised major vulnerability for Australia.

Keywords: SME, Small Business, Cyber resilience, vulnerabilities

INTRODUCTION

Around the world the issue of cyber security has been viewed as a national based responsibility with private sector involvement (ITU, 2005). Yet, in Australia the fragmented environment of business, and dependency on many small businesses in the community means that resources, funding and knowledge are compromised. Accurate statistics on cyber incidents are difficult to obtain, however there is no doubt that attack vectors increase daily and that keeping pace with this is a major challenge for small business.

Resilience is the ability to recover and return to an original state, after some event has occurred to disrupt the original state (Collins Compact Australian Dictionary, 1999). For small businesses, cyber resilience is the ability to defend against and to recover should a cyber incident occur and return to a normal functioning state. Further, in the current threat environment to ensure that the work computer is not involved in fraudulent activities such as distributing spam and phishing emails.

Small businesses account for approximately 95% of all businesses operating in Australia (COSBOA). Small businesses are businesses which employ less than 20 people, and including non-employing businesses (ABS, 2001). Non-employing businesses (such as self-employed tradespeople) represent 61% of the small business sector (COSBOA). That is, non-employing businesses are often a single person home based businesses. It is necessary then to take into account when considering the cyber resilience of small businesses, that the home computer is very likely also the small business computer. The issue that arises is that many home computers, and therefore small business computers, are not sufficiently protected against computer threats such as malware and intrusions.

Protecting systems requires multiple layers of security from physical security of equipment, updates of the operating system and application software, to preventing intrusions on the network. In order to improve Australia's cyber resilience, recognition of the vulnerability of small business computers is necessary given the increasing threats introduced by the Internet. 90% of all Australian businesses have internet access and 42% have a web presence (ABS, 2010). This means that almost all businesses in Australia are vulnerable to cyber threats.

Small businesses lack the financial, time and staffing resources available to large organisation (McDermid, Mahncke & Williams, 2009). This is highly significant because the lack of time and knowledge resources means that small businesses behave quite differently to large organizations. Further, small businesses may not seek and adapt information security research to fit their small business needs as larger organisations may do. Further, small businesses are unlikely to employ dedicated Information Communication and Technology (ICT) staff and so keeping up-to-date on information security practices is an added burden on businesses that are already overly

busy and short staffed (McDermid, Mahncke & Williams, 2009). If Google with all their security resources can be attacked then every business in Australia is vulnerable to similar attacks. However, there is a fundamental difference between resources available to small businesses and larger organisations.

NEW AND EMERGENT THREATS

There are additional threats that need to be considered particularly in a small business environment where the very nature of the business is more relaxed and less controlled. One such emerging threat arises if social network sites such as Facebook and Twitter, are used to promote the business are accessed for personal use on a work computer. The threat arises when fictitious hyperlinks are clicked and malicious software (malware) is inadvertently downloaded. Such is the stealth nature of malware in the current threat environment. Where malware, such as viruses, once caused great inconvenience when computers to crashed, they now operated quietly in the background reading system files and utilising user bandwidth to redistribute spam and phishing emails. Further, the virus if not detected by antivirus software may well form part of a botnet.

A botnet is a large group of infected computers that when instructed, collectively harness their resources in an attack, such as a Denial of Service (DoS) attack against a website. Organised crime has moved online and utilise botnets to achieve their unlawful aims. When small business log on to the Internet to conduct e-business, they need to be mindful of this added threat. Botnets can lie dormant on a computer awaiting an instruction to be involved in an online attack. For example, if a website experiences a DoS attack, the legitimate users of the website will be unable to access and utilise these resource as the system is unable to process the flood of requests. The business equally suffers a loss of sales and reputation. If small business computers are infected, then these computers are likely be involved in such online attacks thereby contributing to the problem as a whole. Such botnet attacks could equally target power stations, government websites etc, causing enormous risk, damage and expenditure. In terms of cyber resilience then, it is within the national interest that small business computers are adequately protected.

How are small businesses able to manage the current threat environment when they have limited access to computer security knowledge and financial resources? Ideally, as required of larger organisations, small business need to implement numerous security controls provided within the ISO/IEC 27002 *Information technology - Security techniques - Code of practice for information security management*. However, implementation of this layered approach is no defence against a determined attacker who can bypass these best practice security controls. In this sense, unless a small businesses address security requirements daily by updating antivirus software and analysing network performance, they can not consider themselves to be secure.

Additionally, small businesses may utilise insufficiently configured wireless networks that can be easily penetrated by a determined attacker. PDAs, iPhones and laptops further introduce areas of vulnerability for small businesses. If small business utilise freeware antivirus it may be possible that there is a delay in the release and resultant updating new virus definitions, thereby leaving small business systems vulnerable. Systems that are not regularly patched, especially the browser application introduce add-ons vulnerabilities such as for active x, Flash and Adobe PDF.

Installation of software such as antivirus and Intrusion Prevention (IPS) software, could further protect against intrusion. Intrusion of small business systems could range from a simple scan of the network in order to determine system vulnerabilities or a hacking attack, or as using malicious code to view all files on a computer. The United States Department of Energy (Sperling, 2010) reported experiencing more than 10 million cyber attacks every day. Small businesses are vulnerable to the same security issues as are larger organisations. Countries such as the United States have recognised the role of small business in cyber security and have begun addressing the issue.

THREAT ANALYSIS FOR SMALL BUSINESS

The six areas defined as areas of possible vulnerability are: Personnel Security, Information Assurance, Physical Security, Access Control, Information Systems and Network Security. Information Assurance is not addressed in the ISO/IEC 27002 but has been added to support the electronic collection, capture and management of information within small business such as customer and payment details. Information Assurance includes privacy, confidentiality assurance and information leakage as it relates to information. Although equally important, the more strategic operations provided within ISO/IEC 27002 such as policies, risk management, incident reporting and business continuity management have not been included into these areas of vulnerability.

For the purposes of this paper, the analysis of the operational vulnerability areas was required. The Threat Rank outcomes would inform strategic operations within small business, such as policy development.

In order to analyse the computer security threats to small business a list of current threats was compiled and placed on the top horizontal axis of the Vulnerability Matrix shown in Table 1. A threat is a circumstance which has the possibility of occurring and the potential to cause loss or harm. The technical and human vulnerabilities were placed on the left vertical axis. The areas of possible vulnerability are based in part on the ISO/IEC 27002 *Information technology - Security techniques - Code of practice for information security management*. These best practice recommendations have been operationalised and incorporated into six practical operational areas in order that it may be easily applied to small business (Mahncke, McDermid & Williams, 2010). It is important to note that the threats and areas of vulnerability may not be precisely equal, although for the purpose of this analysis they can be considered to be within an acceptable range given that each threat may affect multiple areas of vulnerability within a system.

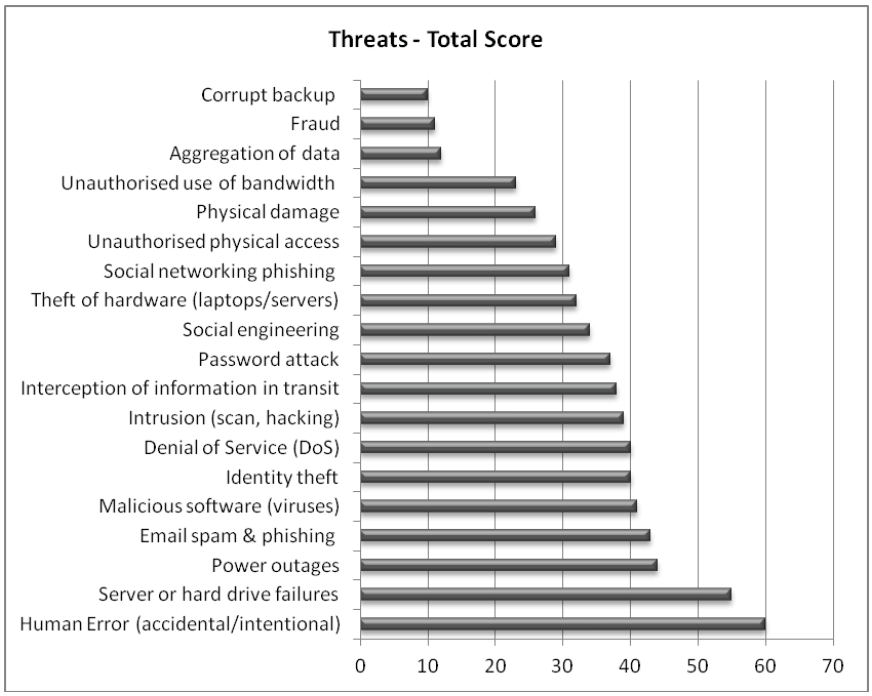
Vulnerability Matrix Threat rating based on worst case scenario should the threat act upon the vulnerability: Blank = Not likely to happen 1 = Unlikely to happen 2 = Might happen 3 = Likely to happen 4 = Very likely to happen 5 = Certain to happen **Threats** **Areas of Possible Vulnerability**	Human Error (accidental/intentional)	Server or hard drive failures	Power outages	Email spam & phishing	Malicious software (viruses)	Identity theft	Denial of Service (DoS)	Intrusion (scan, hacking)	Interception of information in transit	Password attack	Social engineering	Theft of hardware (laptops/servers)	Social networking phishing	Unauthorised physical access	Physical damage	Unauthorised use of bandwidth	Aggregation of data	Fraud	Corrupt backup
1. Personnel Security																			
Internal staff				4		2					4		4						
External third parties				2		1					3		2						
2. Information Assurance																			
Privacy	4			3	2	4		2	3			3		3			5	4	
Confidentiality assurance	5			4	4	3		3	4		3	4	3	5			4	2	
3. Physical Security																			
Physical access	2													3	2				
Equipment security – (PCs, laptops etc)	5											5		5	5				
Environmental security	2	2	5					1				3		3	4				2
4. Access Control																			
User registration	3	5		4	1	5			1		2								
Software access protections	5	5		4	3	5		3	2	5	4		4				3		
Mobile devices access	4	5	3	4	2	4	4		3	5	3	2	4	1	2	4			
External access	3	5	4	3	2	4	4		4	5	4	2	3			4			
5. Information Systems																			
System maintenance (configuration, patching etc)	3	3	3	2	4		2	3								2			3
Backup	4	3	2		1		2	1				4		2	4				3
Email	3	5	5	5	5	3	5	4	3	4	3		2			2			
Internet	5	5	5	4	4	4	5	3	5	4	4		5			2			
Web services (Electronic commerce)	3	5	5	4	4	5	5	5	5	4	3		4			2		5	
6. Network Security																			
Peripheral defences (firewalls)	1		4		3			5		1	1	3		2	2				
Data transmission	1	5			2		5	4	5							4			
Servers	3	5	5		2		5	3		5		2		2	3				2
Wireless and mobile (including protections are configured)	4	2	3		2		3	2	3	4		4		3	4	3			
Total Score (Higher being more significant)	60	55	44	43	41	40	40	39	38	37	34	32	31	29	26	23	12	11	10
Threat Rank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Table 1: *Threat Matrix for Small Businesses*

The matrix provides a method for assessing specific threat types to potential areas of vulnerability. The threats list given is not exhaustive and is intended to give an indication of the current threat environment. The matrix was populated by applying a threat rating scale of 1-to-5 for each threat based on the worst case scenario should the threat act upon the vulnerability. The threat ratings were aggregated and then sorted into the Threat Rank order based on greatest likelihood of that threat acting upon all vulnerability areas.

Each threat type therefore has a maximum total score out of 100 for its potential occurrence in the small business environment, given that there are 20 areas of possible vulnerability which have been defined. This does not incorporate an impact factor, as is usually part of risk assessment, because in doing so often diminishes perception of vulnerability. In this case we are specifically highlighting the vulnerability patterns that exist for small business. Evaluating the potential impact on individual businesses also needs addressing but this cannot be done as straightforwardly as for larger organisations where information may be more protected and existing in a distributed environment. The dependency of smaller businesses on single or smaller networks increases the potential impact of any cyber incident.

The Vulnerability Matrix analysis determined that the highest Total Score for a threat acting upon the areas of vulnerability to be that of human error (additionally depicted in Figure 1). Human error, both intentional and unintentional, therefore has a greater impact on the small business given that it affects many areas of protecting computer systems. Human error can be largely addressed with security awareness training and auditing. Human error was closely followed by server or hard drive failure, and then power outages. If the business has no power or the information on the server or hard drive is unavailable, then the business is unable to operate until the system is restored or a backup restore strategy implemented.



Threats such as malicious software, email spam and phishing, identity theft, intrusion, password attacks and social engineering followed, to name a few. In the matrix aggregation of data is placed as a threat because it is considering the collection of information from multiple sources and using this in some unauthorised manner, such as identity theft. This should not be confused with the security issues that arise from legitimate aggregation and collation of data from multiple sources for business use purposes. This type of justifiable aggregation has a separate set of security issues related to use and access such as privacy and client permissions, confidentiality particularly when shared, and access control management. These threats receive much attention in the media and whilst severe should they occur, affect fewer areas across the total computer system and therefore received a lower Threat Rank. Threats such as fraud, was surprisingly low, however if assessed for impact it would have an enormous impact on an individual. The majority of these threats can be managed by implementing traditional safeguards, staff awareness and security training and managing information made available online.

RESPONSIBILITY FOR SMALL BUSINESS

Bearing in mind the types of threats and potential vulnerabilities to small business security, and the limitations that exist in a small business operating environment, such as lack of time, funding and expertise, the way small business accesses assistance needs to be considered. Small businesses need to be aware of the current computer threat environment. Cybersecurity Watch Survey (Deloitte, 2010) found that most businesses surveyed believed that their current security measures were sufficient to protect them, but lacked awareness of cyber attacks. Whilst such websites as Stay Smart Online (2010) provide Internet awareness training and advice, and the Australian Government has funded various one off projects that touch on security as part of e-commerce, there is no coordinated approach by government to address the growing issue in the small business environment. As with the home user, small business is akin to individuals who are responsible for their computers and connections to the outside world. Similarly, this means that there is limited expertise within small business to deal with security awareness and threat issues. In addition, the costs must be borne by the businesses themselves, which is a disincentive for many businesses where balancing the tradeoffs between security and cost may be difficult to assess and prove.

There are other initiatives that the government could take responsibility for that would improve security for small business: national programs to raise awareness, funding for training which could be through associations such as the Small Business Association in Australia. Further, technology needs greater integration with security instead of leaving users to implement multiple layers of security and manage attacks, developers of hardware and software need to look for ways to incorporate practical and effective security into their technologies. From a broader perspective a greater push to incorporate security into computing technologies and software may also assist those with limited knowledge and access to expertise. Leaving security to the end users is like purchasing a new car and being told to head down the road to have the brakes and airbags fitted; the extra cost and expertise required are effective disincentives to being safe and secure.

CONCLUSION

It may be argued that from a national security perspective, cyber security threats to small business are not a significant risk. Whilst they may cause disruption and inconvenience to the business community, they do not pose a risk to the country as a whole. However, in a country such as Australia, where much of the business and economy is in the hands of small business, and where dependency on critical infrastructure and e-commerce is encouraged, together with the increasing aggregation of data, can we afford to ignore this sector? At what point does it become a national concern? If financial well being is affected, or large groups of society are impacted then it is clearly a national concern. As Westrin (2001) points out, if the flow on from cyber attacks on the business sector that can indirectly adversely affect confidence in e-commerce and subsequently affect the economy.

Perhaps the first step in this is get an accurate picture of exactly what (and which) small businesses in Australia contribute to (or is a fundamental part of) our critical infrastructure. Without this conceptual knowledge, how can we know what needs to be protected? This is already defined for areas such as healthcare where primary and some secondary healthcare providers and allied health providers function already as independent small business. No doubt there are other overlapping and diverse sectors of small business that contribute to Australian critical infrastructure sectors. In the context of small business it potentially impacts the economic fabric of Australian society. Cyber resilience must move from the being just an IT issue to that of a national security issue.

REFERENCES

The Australian Bureau of Statistics. (2007). 8175.0 - Counts of Australian Business Operators. http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8175.02006%20to%202007?OpenDocument

Collins Compact Australian Dictionary. (1999). Resilient. HarperCollins Publishers: Sydney.

Deloitte. (2010). CSO Cybersecurity Watch Survey. Retrieved September 29, 2010 from http://www.deloitte.com/view/en_US/us/Insights/centers/Center-Security-and-Privacy-Solutions/bcdc005f1e056210VgnVCM100000ba42f00aRCRD.htm

McDermid, D. C., Mahncke, R. J., & Williams, P. A. H. (2009). Challenges in improving information security practice in Australian general practice. Edith Cowan University, SECAU Security Research Centre, Australian Information Security Management Conference, Perth, Western Australia.

Sperling, E. (2010). Ten million cyberattacks a day. Retrieved August 11, 2010 from http://www.forbes.com/2010/08/06/internet-government-security-technology-cio-net

Stay Smart Online. (2010). Retrieved August 3, 2010 from http://www.staysmartonline.gov.au/

UTI. (2005). A comparative analysis of cybersecurity initiatives worldwide. Retrieved from http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf

Westrin, P. (2001). Critical information infrastructure protection. in Wenger, A. (Ed.) *The Internet and the Changing Face of International Relations and Security, Information & Security: An International Journal*, *7,* 67–79.

ACKNOWLEDGEMENTS

The authors acknowledge unpublished discourses between ourselves and Associate Professor Donald C McDermid in regards to the development of an information security governance framework to address the areas of vulnerability within small businesses, especially general medical practices.

WHICH ORGANISATIONAL MODEL MEETS BEST PRACTICE CRITERION FOR CRITICAL INFRASTRUCTURE PROVIDERS: AN EXAMINATION OF THE AUSTRALIAN PERSPECTIVE BASED ON CASE STUDIES

Andrew Woodward and Craig Valli

secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

Abstract

While it is recognised that there must be segregation between corporate and process control networks in order to achieve a higher level of security, there is evidence that this is not occurring. Computer and network vulnerability assessments were carried out on three Australian critical infrastructure providers to determine their level of security. The security measures implemented by each organisation have been mapped against best practice recommendations for achieving segregation between process control and corporate networks. One of the organisations used a model which provided a dedicated information security team for provision of security for the process control networks. One of the other organisations relied heavily on outsourcing for their IT security, and a third used in house corporate IT for their process control security. It was found that the organisation using a dedicated IT security team that worked within the process control group achieved the highest level of security when mapped to best practice. This paper concludes that best practice recommendations for critical infrastructure providers should also include guidelines for the organisational structure, and further, that dedicated IT security personnel be placed within the process control group.

Keywords: SCADA security, critical infrastructure protection, organisational model, operational technology, information technology

INTRODUCTION

Process control systems (PCS), of which supervisory control and data acquisition (SCADA) systems are a subset, are used by critical infrastructure operators to regulate and manage the operation of critical systems such as power, water and gas. In addition, these systems control everything from traffic lights through to large scale refineries and mining operations. All critical infrastructure providers also rely upon these systems for safety and reliability, through continuous monitoring and operation. These systems were originally designed around reliability and safety, and if they were network connected they were connected on isolated internal networks for the purposes of control and management; essentially a closed system. Typically in these situations security was not a consideration due to the isolated nature of the systems and their closed nature. It should be remembered that these systems were implemented also in an era when computing and information technology will also largely conducted in isolated installations or laboratories around the globe (Stouffer *et al*, 2008).

With advances in technology, we are becoming increasingly interconnected and interdependent on these connections for the full functioning of modern society. One of the main conduits and enablers for this has been the rapid expansion of the Internet. Correspondingly, as a result of the growth of the Internet there has been a convergence on the TCP/IP protocol suite as the dominant network protocol for business and industry (Steenstrup, 2010). This has seen many hardware and software vendors, including SCADA vendors, align their products with this kind of reality (Igure *et al*, 2006).

The increased interconnection of SCADA systems to corporate networks is a significant threat in itself, enabling and making them accessible to undesirable entities. Be it directed attacks, opportunistic scanning or malfeasant insiders (Jackson-Higgins, 2007), these once stand-alone systems are now vulnerable to a range of new attack vectors. While insider malfeasance may only account for some 20% of attacks against a system, the percentage of the costs related to insider attacks is nearer to 80% (Baker *et al*, 2009). The most infamous of the intentional insider attacks against a critical infrastructure provider is the case of Maroochydore shire. Their SCADA system was attacked by a person who had been employed to install the system after a request for employment was

turned down (Smith, 2001). The attacker stole a laptop when he left which contained all of the tools and codes required to remotely operate the control system, and it took some time for the operators to locate the source of the issues he was causing. Additionally, most security measures are outward facing, and are not intended to detect against insider malfeasance. Insider attack must be a significant concern for CIPs, and gives further weight to the need for internal segregation between control system and corporate networks.

The research reported in this paper was based on the examination of a number of case studies conducted under the Federal Governments computer and network vulnerability assessment (CNVA) program. The CNVA program is an Australian Government grants scheme developed to help ensure the security of Australia's critical infrastructure (TISN 2008).

RECOMMENDED BEST PRACTICE FOR SECURING SCADA

This paper drew on a range of literature in order to create a composite, best practice list of features and strategies for securing process control systems, and as a guideline for measuring the compliance of an organisation against the organisational model. The first piece of literature used for this purpose is the NIST Guide to industrial control system security (Stouffer *et al*, 2008). This guide was produced by the National Institute of Standards and Technology (NIST), a United States Government Organisation, and the guide itself is put forward as recommended best practice by US-CERT. In addition to using the NIST guide as a reference point for determining effectiveness of the organisational structure, a range of other network security best practice measures have also been used including ANSI/ISA-TR99.00.01-2007 Security Technologies for Industrial Automation and Control Systems (ISA, 2007), Idaho National Labs Control Systems Cyber Security – Defense in Depth Guide (INL, 2006).

Table 1: Common methodology used to assess the three organisations. Multiple other methods used for other CNVAs, components of assessment all align with NIST best practice.

Category	*Specific Measures*
Firewall	External
	Multiple
	Multiple (different vendors)
	Firewall rule sets configured correctly
	Firewall OS / firmware patched?
Network Segregation	DMZ between corporate and PCS
	DMZ between Internet and Corporate
	Logical segregation through VLANs and subnets
	Access Control lists on border routers
	Intrusion Detection
Remote Access	Secure authentication method
	Two factor authentication
	RSA token authentication
Documentation	Policies current
	Policy audited or enforced?
	Network topology diagrams current
	Network topology diagrams available