Small to Medium Enterprise Cyber Security Awareness: an initial survey of Western Australian Business

Craig Valli, Ian Martinus and Mike Johnstone
c.valli@ecu.edu.au, i.martinus@ecu.edu.au, m.johnstone@ecu.edu.au
Security Research Institute
Edith Cowan University
Perth, Western Australia, Australia

Abstract

Small to Medium Enterprises (SMEs) represent a large proportion of a nation’s business activity. There are studies and reports reporting the threat to business from cyber security issues resulting in computer hacking that achieve system penetration and information compromise. Very few are focussed on SMEs. Even fewer are focussed on directly surveying the actual SMEs themselves and attempts to improve SME outcomes with respect to cyber security.

This paper represents research in progress that outlines an approach being undertaken in Western Australia with SMEs in the northwest metropolitan region of Perth, specifically within the large local government catchments of Joondalup and Wanneroo. The high order goal of the project was to assist with measures to improve their cyber security resilience and resistance to threats. This paper documents outcomes of an initial survey of SMEs and its implications for interventions to improve information security and make the businesses less susceptible to computer hacking incidents.

Keywords: cyber security, information security, computer hacking, small to medium enterprise

1 Introduction

The largest growth area for targeted cyber attacks in 2012 was SMEs; 31 percent of all attacks targeted them, and they area sustained a 30% increase in attacks overall [1]. These statistics are typical of reports, surveys and studies highlighting the significant threats now being realised on SMEs who use the Internet to conduct business [2]. The effects of cyber attack can destroy businesses financially through loss of bank account details as well as materially through loss of intellectual property or customer data. However, a recent survey by Kasperksy Labs reports that 75% of SMEs believing they are not targets of cybercrime and a further 59% say they have no data of interest for attackers[3].

Due to their need to compete and survive, SMEs are now some of the biggest adopters and users of the Internet and its associated technologies. These technologies include, but are not limited to, social media such as Facebook and Twitter, mobile phones and tablets connected to 3G/4G networks, email, cloud-based applications-often accessing these services on high speed DSL, Cable or Ethernet connections to the Internet [4, 5].

There is little literature available about the ability of SMEs to deploy, use and monitor cyber security countermeasures. Even basic cyber security countermeasures such as virus and malcode scanners are increasingly complex and difficult to set up, except for an experienced IT security professional. Many SMEs simply cannot afford these professional services due to fiscal and time constraints [2, 6].

Vendors have not been insensitive to the need to protect operating systems from attack. Many of the popular operating system vendors have provided firewall solutions as system defaults. However, we posit that most SMEs would not know where to check the configurations of said firewall, or how to respond or report any attacks the firewall may have blocked during the course of its operation.

We asserted an approach that actively engages SMEs to help themselves better secure their enterprises can produce significant benefits for all stakeholders. Our plan was to engage with small to medium enterprises in the Wanneroo and Joondalup local government areas in Western Australia to assist with this new economy threat. The aim of the project pilot was to increase SME knowledge about cyber security issues. In addition to knowledge, our aim is to arm them with the tools and techniques to better protect their business by achieving a lower cyber security risk profile through active utilisation. This paper outlines the issues with respect to small to medium enterprise cyber security and analyses initial findings from the survey instrument used with study participants.

2 The SMESEC project

The SMESEC project actively involves researchers from the ECU Security Research Institute and the relevant staff from the local government, introducing a program to educate small to medium enterprises about cyber security issues they face and the need to address through positive action. This engagement was achieved through a survey and initial awareness raising workshops, leading to intervention driven by the survey's findings. The survey analysis will allow targeted workshops as the main vehicle for the dissemination of information to SMEs on how best to protect their business.

The four stages of the project are as follows:

Stage 1 - Initial survey of small to medium enterprises in the catchment areas
The survey established a baseline of user knowledge about cyber security and also the perceived risk that cyber security presented to their businesses. The anonymous survey was completed online or in face-to-face mode.

Stage 2 Analysis of survey results
An analysis of survey results has been undertaken to find areas of focus to be addressed in the intervention workshop. (The context and content of this paper)

Stage 3 Conduct of the workshop
This is designed to be a two-hour information session examining key issues identified from the analysis of the survey. The aim of the workshop is to enable businesses to utilise existing tools and freely available, robust software to create a more secure and resilient business.

Stage 4 Post workshop survey
This will be conducted with the attendees of stage 3, approximately one to two months after the workshop to assess the impact of the intervention.

3 Initial Survey details

The survey was designed to collect basic information about:

1. Basic demographics - enterprise type, age of respondents

2. Respondents knowledge of cyber security issues

3. Type and numbers of generic device types used on the Internet

4. Any cyber security protections or countermeasures that may be applied to the devices

5. Update frequency for equipment or operating systems

6. User confidence in using certain applications

This information was collected using 17 exploratory questions; the aim was not to make the questionnaire long or protracted, nor overly technical in emphasis. The survey was deployed as an anonymous online survey and all data were acquired in this fashion. The total number of respondents to the survey so far is 50. The survey was distributed via the respective business associations from the local government regions to approximately 1200 individual email addresses.

4 Survey Results

4.1 Basic Population Demographics

The industry profile of the respondents was Retail 12%, Services 44%, Manufacturing 6%, Other 38% and no Primary. The age demographic of respondents was 18-35 year old (18%), 35-45 year old (34%), 45-55(26%) and 55 or over (22%).

4.2 Technology – Profile and Use Practices

The type of devices used to access the Internet in the surveyed SMEs demonstrated a broad mix and number of device types. There is more than one device type used with the average being 2.92 device types per respondent used for business purposes. It is interesting to note that the desktop computer is still the most single used overall piece of IT device at 84% but only marginally. Smartphone usage is 78%, laptops at 74% and tablets at 54% in the respondents businesses.

Access technology was also identified in the study based on potential business and home use. The results were ADSL Modem 62%, ADSL Wireless 54%, 3G/4G Wireless 50% and 2% who did not know (the labels here are truncated for brevity, explanation between the different types of ADSL was provided in the questionnaire to reduce ambiguity).

Inquiry around cyber security countermeasures deployed by the respondents evinced that Firewall 88%, Virus Scanner 86%, Malware Scanner 43%, Spam Killer 35% and 8% did not know what they were using. Of those respondents who have anti-viral countermeasures 12% indicated they never updated, 20% did not know when they update and 8% said less than once a month since they last updated signatures. This profile represents 40% of SME businesses employing a countermeasure and it been largely ineffective due to poor process. Encouragingly though 37% update several times a week, 12% once a week, 2% 2-3 times a month, 8% once a month.

In response to questions about installing updates of operating systems on PCs, the automatic update functionality was used by 64% of respondents, a further 16% were updating at least weekly. Of the remaining 20%, 14% at least update once a month, with 4% less than once a month and 2% not knowing. Of the Smartphone or tablet owners users 92% had installed updates on their devices, with 8% indicating never having done so.

Phishing emails had been sent to 98% of all respondents, with 98% of respondents also asserting that they knew what one was. The type of phishing received by respondents was identified as financial/banking institution related 86%, free prize 78%, lottery 80% and other topics 40%.

One of the key issues is around security of financial transactions in particular Internet banking. Respondents answered questions about their perceptions of security and safety of using banking on the Internet. Of the respondents 4% never felt secure when using Internet banking, with a further 2% rarely feeling secure and 12% sometimes. Nearly half (48%) felt secure most of the time and the remaining 32% feeling always secure.

5 Discussion

5.1 Mobile devices proliferate

Mobile devices combined are the dominant platforms outnumbering PCs two-to-one in the surveyed businesses. This dominance presents some interesting issues for cyber security. It is fair to assume mobile devices would see connectivity to multiple networks and also possible types of network channels. There is safety in assuming that even the simplest usage scenarios of business and home use is a connection to two different networks. In the case of smart phones, the use of multiple channels opens up opportunities for potential exploit or compromise. This would include 802.11 wireless, 3G/4G network and the often forgotten Bluetooth. This protocol is the predominate pairing mechanism when a user is operating their device while in their car.

5.2 Multiple Channel, multiple threat

The respondents clearly identified they are using multiple Internet media types for access to business transactions with a large proportion being mobile. This trend is consistent with usage patterns from Australian Bureau of Statistics reports where mixed use is demonstrable as is the ongoing proliferation and penetration of mobile devices [4, 5]. These mobile devices primarily use wireless transmission for communication to networks and other devices e.g. automotive systems. All wireless transmission is susceptible to interception regardless of technology. Basic physics confirms this assumption. The protection for these wireless systems typically relies on protocols and cryptographic countermeasures which are manifestly insecure.

ADSL-based wireless, and wireless used in these mobile devices is typically 802.11 b/g/n and is known to be insecure[7]. Through deduction and implication, 54% of SMEs are vulnerable to exploitation via known documented 802.11 vulnerabilities. Many wireless transmissions are vulnerable to simple but illegal interception of wireless signal, the technology for extraction of cryptographic keys and subsequent decode are effective and well documented. As early as 2001 this has been occurring for the capture of financial credentials by cyber enabled criminals from wireless enabled technology.

The type and value of information disclosed on wireless can cause SMEs to become attractive targets for cyber criminals. We posit that this is a haven for data relating to identity theft. Given that identity theft is the largest and fastest growing crime types in the world this should be considered by SMEs concerned with protection of customers private details. Of the Wanneroo and Joondalup businesses surveyed, they were vocal in their reaction to ‘old economy’ physical theft, but less aware of the damage of virtual identity theft and the potential for devastating business loss.

The use of personal business devices and subsequently connecting to various outside networks also raises the risk to an SME. Wireless access point (WAP) spoofing techniques are well documented, but awareness is low. Despite an SME providing safe secure networks at the business premise, the level of risk increases dramatically if an employee logs in from a home networks or the “free” wireless at the local cafe, library or city centre ‘hotspot’. SMEs can be seen as a trusted second or third party, and used as "watering holes" to break down the security of other businesses with cyber criminals stalking a business user through the other party[1]. A recent example of customers accessing a Chinese restaurant’s web site to order through the online menu and subsequent infection with malicious code demonstrates this point. The ‘watering hole’ was designed by cyber criminals in order to facilitate an attack on a geographically close oil and gas company[8].

The attendant data leakage possible through a work synchronised/synchronising device being exploited and compromised while in a home/external network scenario was not specifically covered in the survey. This exploitation could occur either through malicious extraction of the data from the device directly using a USB as a result of physical access, or through interception of transmission across insecure or unmonitored network endpoints. There is a colloquial term within cyber criminal networks called “whaling” for the targeting of high worth individuals [9]. It should be noted this high worth often relates to information value not personal financial wealth, making this compromise of most SMEs real and viable.

5.3 Basic cyber security countermeasure use and deployment is lacking

It was disappointing to see firewalls as a primary defence not being utilised fully, given that all contemporary operating systems have firewalls as default configurations. Equally, the use of antivirus is also low given the attendant risk these present for conventional PCs. It is again more alarming when taken in the context for mobile devices when 82% of respondents do not install antivirus. Furthermore on the mobile platforms 94% of all respondents have downloaded applications (apps) from the various vendor based platforms. Given that it is known that these apps, even from “reputable” vendor sites, are vulnerable [10] to exploit due to programming flaws or deliberate insertion of malicious code, this raises the risk to SMEs significantly. There appears to be a “lost in translation” event here around transitioning knowledge from PC environments to smartphone and tablet environments. Further research into the penetration of smartphone apps as small business take up increases would be useful to investigate including the loss of business as a result of those dubious downloads.

5.4 Patch is starting to match message

The survey responses relating to operating system patching indicated that the messages from various initiatives in industry and government around the need to patch systems regularly are potentially being heard[11, 12]. The results show that the automatic update processes when seamless or made to be “set and forget” are elected as a choice by 64% of end users. The implication *ceterus paribus* here for cyber security is that 80% of operating system related vulnerability or exploit code will prove to be ineffective if patched within a week cycle, and 64% as soon as an update is available via automatic update mechanism. This lessens the effective windows for exploit, threat realisation by cyber criminals and ultimately results in a common good outcome for cyber security.

6 Conclusion and Future Work

There is a definite identified need for education and dissemination of cyber security information to SMEs in this project as we move into Phase 3 of the SMESEC project. The initial survey results strongly indicate that there is a pressing need for direct intervention and the wider Wanneroo and Joondalup business group has indicated strong interest in this component through their online and physical enquiry.

This intervention is to be achieved through the facilitation of a targeted practical workshop to enhance understanding and implementation of cyber security countermeasures for SMEs. In addition, post-workshop the provision of supporting process documentation in the form of conventional paper-based and online materials for SMEs is seen as an important support mechanism.

The content of the workshop will be as follows. First, the need to get antivirus countermeasures installed on mobile platforms owned by these SMEs and at the same time reinforcing the messaging about regular patching and updates. This will significantly reduce the risk to the 94% of SMEs who are indicate they are currently using unprotected devices.

Second, considerations about the use of wireless for transmission of critical or sensitive business information across wireless conduits will be explored. This intervention will involve educating the individual business about the significant risk wireless presents when transmitting business data such as email and document attachments. There will be a demonstration of the use of high grade file-based encryption for data storage using for instance

Windows EFS at a file system level. Educating SMEs about the effective use of open source cryptographic solutions such as OpenPGP and Truecrypt to allow for the safe transfer of documents is also incorporated in the workshop agenda.

Finally, a refresher or back to basic assistance on firewall, anti-virus, malware and spam-based applications will close the first stage of the loop, after which point the business community can then become advocates of the process we designed and deployed. The results indicate that SMEs have not transferred skills and knowledge around these technologies to smart phone and tablet in particular and further 'communications' is needed in the marketplace to get the message out there.

As planned in the project, there will be an evaluation of the workshop phase with a post-workshop survey. Furthermore, we are seeking mechanisms to use existing Australian government data on botnet data for instance to demonstrate effectiveness of our interventions. As with any intervention, dissemination to a wider business group beyond the original geographic area is the wider goal.

7 References

[1] Symantec, *Internet Security Threat Report 2013*, 2013, Symantec Corporation.

.[2] J. Hayes and A. Bodhani. (2013) Cyber security - small firms now in the firing line. *Engineering and Technology Magazine*. Vol 8 Issue 6, The Institution of Engineering and Technology: London, UK

[3] W. Ashford. (2013). *SMEs believes they are immune to cyber attack*. Available: http://www.computerweekly.com/news/2240216202/SMEs-believes-it-is-immune-to-cyber-attack-study-shows

[4] Australian Bureau of Statistics, "8153.0 - Internet Activity, Australia, June 2013," Australian Bureau of Statistics, 2013. Available: http://www.abs.gov.au/AUSSTATS/abs@.nsf/allprimarymainfeatures/70EF9515319BAB35CA257CB30013246D?opendocument

[5] Australian Bureau of Statistics, "8166.0 - Summary of IT Use and Innovation in Australian Business, 2011-12" Australian Bureau of Statistics, 2013.

[6] Anonymous. (2013). *SMEs must get better at the cyber security basics, ICAEW tells Parliamentary group on IT*. Available: http://www.icaew.com/en/about-icaew/newsroom/press-releases/2013-press-releases/smes-must-get-better-at-the-cyber-security-basics-icaew-tells-parliamentary-group-on-it

[7] Valli, C. and P. Wolski. *802.11b Wireless Networks Insecure at Any Speed*. in *International Conference on Security and Management - SAM'04*. 2004. Las Vegas: CSREA Press.

[8] N. Perlroth, "Hackers Lurking in Vents and Soda Machines," in *New York Times*, New York Edition, 2014, 8th April, p. A1.

[9] IBM, " X-Force 2011 Mid-Year Trend and Risk Report," IBM 2011.

[10] P. Krill. (2012, 31 March). *Google finally scans malware-ridden Android Market*. Available: http://www.infoworld.com/d/security/google-finally-scans-malware-ridden-android-market-185654

[11] Australian Signals Directorate. (2014). *Strategies to Mitigate Targeted Cyber Intrusions*. Available: http://www.asd.gov.au/infosec/top-mitigations/top35mitigations-2014-table.htm

[12] CERT Australia, "The top cyber security tips for small to medium business," CERT Australia, Australia, 2014. Available: https://www.cert.gov.au/system/files/5/5/CERT-Australia-top-cyber-security-tips-for-small-to-medium-business.pdf