CyberCheck.me: A Review of a Small to Medium Enterprise Cyber Security Awareness Program

Craig Valli, Ian Martinus, Jayne Stanley, and Michelle Kirby

1 Introduction

The CyberCheck.me initiative is a local government and academic engagement project trying to improve cyber security awareness and skills of Small to Medium Enterprise (SME). The initiative utilizes staff from Edith Cowan University (ECU), City of Joondalup (CoJ) and City of Wanneroo (CoW) to manage and run the engagement activities with additional funding from the Australian Centre of Cyber Security Excellence (ACCSE) [1] and WA AustCyber Innovation Hub (WAACIH) [2]. Students from Edith Cowan University and North Metro TAFE (NMTAFE) engage at various business events and forums to disseminate knowledge about cyber security to SMEs. In addition, the SMEs are offered the opportunity to attend a personalized one-on-one cyber consultation to provide them an overview of the potential cyber risks for their business as a result of a detailed cyber health check questionnaire they must complete prior to their consultation. This organized face-to-face engagement is further supported by a public-facing website https://cybercheck.me that has the latest news, and simple guides for securing mobile devices and computers. This chapter will outline the processes undertaken and observed benefits of the CyberCheck.me program, which secured significant funding to increase interactions from 2017.

C. Valli (✉) · J. Stanley · M. Kirby
Security Research Institute, Edith Cowan University, Perth, WA, Australia
e-mail: c.valli@ecu.edu.au; sri@ecu.edu.au

I. Martinus
Western Australian Cyber Innovation Hub, Joondalup, WA, Australia
e-mail: ian@wacyberhub.org

K. Daimi et al. (eds.), *Advances in Security, Networks, and Internet of Things*,
Transactions on Computational Science and Computational Intelligence,
https://doi.org/10.1007/978-3-030-71017-0_17

1.1 The Background

In 2014, ECU, CoJ and CoW commissioned and ran a survey of SME businesses in the respective catchments [3]. The survey was the first of its kind conducted in Australia and possibly the world. The research was action-based and the results from the survey informed the basis for skills intervention workshops that were run in the local government catchments, post survey and publications resulted. The workshop attendances exceeded expectations and a model to further extend the engagement was planned in 2015 which resulted in the CyberCheck.me initiative being launched in early 2016. In 2017, additional funding allowed the program to increase its scope and performance indicators. At present, the program is further consolidating and codifying processes with the objective of continual improvement.

1.2 CyberCheck.me 2019 and Beyond

Since August 2019, six CyberCheck.me pop-ups have been held at various business events and locations with more than 200 SMEs visiting the stands and speaking to the cyber students from ECU and NMTAFE. In addition to this, more than 50 businesses registered their interest with CyberCheck.me to attend a one-on-one free cyber consultation. The consultations have increased in number in 2020. Small businesses can now book a session online after completing the pre-consultation survey. Promotion of the consultations occurs through various online channels. Feedback from the initial consultations has been positive with one business stating, "I have learned a lot. My understanding and vigilance toward cyber security has changed dramatically."

In addition to CoW and CoJ, a number of other local councils are in the pipeline to roll out the initiative taking available outreach to over 700,000 people.

2 The CyberCheck.me Engagement Model

A secure ecosystem for the conduct of cyber-enabled business is an essential underpinning of any digitally enabled economy. One of the issues for SMEs is the ability to access expert help at a reasonable cost. The CyberCheck.me initiative addresses this in that ECU, CoJ and CoW, respectively, have co-funded the provision of expert advice to the city catchments. The model also allows for targeted expert advice and training to be given to SMEs who opt in to deal with their self-identified cyber security issues.

Dissemination of cyber security material for CyberCheck.me is achieved on multiple levels and channels of engagement. The activities for CyberCheck.me are published through the cybercheck.me website, CoJ and CoW Facebook and

Twitter channels, and various ECU twitter channels. Additionally, local government pushes notifications to their respective business associations, such as the Wanneroo and Joondalup Business Associations. Their combined membership exceeds 700 businesses, representing every major industry group and ANZSIC code. The interactive information sessions run at civic facilities such as community libraries as well as at local business events within those primary and secondary centres.

Relevant and easy-to-understand fact sheets have been produced for dissemination to the community. The first is a fan fold brochure that outlines the eight key things people should do to protect themselves. It contains general information that can be applied to a business or anyone in the community. The tips include:

1. Use strong passwords
2. Protect your computer
3. Use email and the web safely
4. Use your mobile devices securely
5. Keep up to date
6. Install AV software
7. Back up your data
8. Use encryption

The brochure also contains information regarding other available online resources to get further advice and information. In addition to this, an animation book was created with cartoon graphics to make the message clear to a wider variety of audiences. The messaging still had a small business focus. The same eight cyber security tips were highlighted, but applied to a business scenario in an easily digestible format. These animation books have proved to be very popular with SMEs who visit, and engaged with, the students at the CyberCheck.Me stand during the events.

Complementing the two guides are single sheet A4 information sheets about securing mobiles through use of pin or pattern, enabling file encryption on computer operating systems and how to use encryption to protect files in transit. These are used also in the face-to-face engagements with people. These sheets use freely available either embedded in the operating system features or freeware/opensource solutions, for example, VeraCyrpt [4] for USB disk encryption.

2.1 Outreach Sessions Uncover Serious Attacks

In 2019, we saw an increase in businesses self-identifying as suffering a significant cyber-attack. Some of these businesses have gone further and told their story in an effort to make others realize they are vulnerable to cyber-attack and the follow-on consequences of weak cyber defence. The attacks have resulted in significant damage to their businesses.

A national insurance company reported a $2 million loss due to a crypto-locker attack that wiped out their entire laptop fleet and servers. This attack further resulted

in the business being offline for 18 days and having to replace over 400 laptops. As the owner of this business said, “Like a burglary, it’s not if it happens, it’s when, and a Disaster Recovery Plan is paramount”.

A small catering and event management business that primarily used a web page as a channel for promoting and securing new business almost never recovered from the cyber attack. As a result of the attack, they had lost view of all customer bookings for the next 12 months, their website completely disappeared from the Internet and the business had to be closed for 2 months and all staff laid off. A common thread in these stories is a failure to patch, backup, antiviral protections and firewalling. The effects of a weak cyber defence were swift and costly.

3 Survey Results Section

Preliminary results (n = 30) from the survey this year would indicate there are still some very troubling patterns and trends being observed in the responses from the SMEs. The survey covered basic demographics, technologies in use to access the Internet, technologies used in the SME, cyber security countermeasures applied to those technologies and devices in the SME, implementation of cyber policies and plans. This following section outlines and discusses some of the key preliminary trends and results uncovered in the survey so far.

3.1 Survey Demographics

The survey had the following demographics. The age of respondents were as follows 18–35 18%, 35–49 50%, 50–64 32%, 65 or older 0%. The following Tables 1, 2, and 3 also outline basic demographics for the SME businesses that have participated in the survey so far.

Table 1 Which industry sector(s) does your business operate in?

Construction	7%	Transport, postal, warehousing	7%
Professional, scientific and technical Services	30%	Rental, hiring and real estate	3%
Financial and insurance Services	10%	Manufacturing	3%
Retail trade	0	Other	40%

Table 2 Business size

Sole proprietor/partnership (non-employing)	60%	Microbusiness (less than 5 employees)	11%
Small business (5–19 employees)	11%	Medium business (20–199 employees)	11%
Large business (200+ employees)	7%		

Table 3 Where they conduct business

Commercial premises	33%	Home	37%
Mobile (e.g. vehicle-mobile tradesperson)	18%	Anywhere/completely virtual	12%

Table 4 Internet access methods (%)

NBN	100	Mobile phone	61	WiFi/wireless	61%
4G/Wireless hotspot	7	NBN satellite	4		

3.2 Business Devices and Access

The devices used to access the Internet by the businesses are desktop computer 68%, smartphone 79%, tablet 46% and laptop 75%. It should be noted that some organisations have multiple devices in use. The following Table 4 outlines how the businesses access the Internet and what technology they use to access it again; some businesses use multiple technologies.

NBN in an Australian context means the Australian National Broadband Network (NBN) which is a high-speed network developed by the Australian government to provide network infrastructure to the nation. It should be of little surprise that NBN is at 100%. It is interesting to note in this survey that all of the respondents are technically in a metropolitan area with some respondents from rural areas using satellite because of physical cable distance issues. This outcome may be as a result of the universal service guarantee to overcome network blackspots which occur with some frequency in certain parts of the metropolitan area. For the first time as well, the use of 4G/wireless hotspots has been registered.

With respect to countermeasures being deployed on devices by device type, there is some stark differences. The following table shows each category of device as per the questionnaire which is PC/laptop, tablet and smartphone.

Authenticating to Devices

To authenticate to computers/laptops, the following percentages were observed in survey response: password 86%, multifactor or two-factor authentication 43%, fingerprint 19%, face recognition 10% and hardware token 4%. For tablets and mobile phones, the following authentication methods were observed: password/PIN 100%, facial recognition 31%, multifactor or two-factor authentication 15% and fingerprint 61%.

Survey respondents answered a question about password policy setting and enforcement thereof, the responses were Yes 45%, Partial 33% and No 22%. When asked if they used a password manager to manage passwords, the responses were Yes 33%, No 41% and "do not know what it is" 26%. This points to a significant gap that needs to be addressed with one third of respondents using a password manager. This type of tool is an effective countermeasure against poor passwords and password strength when used correctly. As this program is tied educating SMEs about cyber security, this is an area for us to focus on. We already have some

materials available and have delivered presentations on why they should be used. This outcome is an indicator that this work needs to continue to educate users on the importance of a password manager for password security.

What was of significant concern is that 73% have shared accounts and 27% do not have shared accounts. From a cyber security and auditing perspective, this is dangerous and needs to be addressed. If this is then coupled with frequent staff turnover and infrequent changing of passwords, this becomes a significant vector for insider attack.

There was an incongruity in the survey in that when asked 80% restrict access to sensitive and critical data which is in direct contrast to 73% of people having shared accounts. This response does not make a lot of sense. The survey also returned that 50% provide basic information security training but this result could be a self-selection effect in the survey; we would not posit that this is not normal.

3.3 Maturity of Wi-Fi Security

Wi-Fi is actively used by 95% of the SMEs surveyed. Of these respondents, only 63% have implemented WPA2 that they can confirm, 8% confirmed No and 29% were unsure. Furthermore, 59% of respondents that had used WPA2 had reset their password to a complex password. Alarmingly, 35% still are using default passwords either provided by the manufacturer or the Internet service provider. Further study will reveal if this is a matter of laziness or a lack of awareness of the dangers of keeping default settings on devices. A strong indication that Wi-Fi is starting to be seen as a significant risk for the SME businesses has seen 38% of the respondents place their Wi-Fi on a separate NBN connection that does not connect to their internal business systems. This question will be modified to further investigate the need for this separation of networks in future surveys.

Approximately 40% of respondents use VPN to protect connections. However, 32% answered No to the use of VPN and 28% were unsure. It could be reasonably argued that 60% of businesses are not using VPN technologies to protect their data; this needs to be addressed. Combining this observed response with 30% of all businesses operating in a mobile or virtual fashion and they are not using VPN. This is a significant risk.

3.4 Applied Countermeasures

One of the simplest things that SMEs can do is install standard countermeasures such as a firewall, some form of antivirus or malware protection, and possibly a spam killer. It should be noted that firewalls are now routinely provided free with all operating systems that are in use in SMEs including but not limited to computers, laptops, PCs, tablets and phones. The following Table 5 outlines a percentage of

Table 5 Applied countermeasures by technology type

Countermeasure	AV	Spam killer	Firewall	Malware
PC/laptop	95%	32%	73%	50%
Phone	34%	5%	58%	21%
Tablet	15%	0%	15%	7%

Table 6 Application of operating systems and vendor patches frequency by hardware platform

Vendor	Auto	Weekly	2–3 a month	Month	Less than monthly	Does not know
PC/laptop	62%	8%	4%	4%	8%	12%
Phone	79%				21%	
Tablet	79%				21%	

Table 7 Updating of antiviral countermeasures frequency by hardware platform

AV	Auto	Week	2–3 a month	Month	Less than month	Never	Does not know
PC	62%	8%	4%	4%	8%		12%
Phone	100%						
Tablet	62%					13%	25

software installed on each given hardware platform of the identified cyber security countermeasures.

As can be seen in Table 5, in the PC/laptop technology 95% of SMEs have now applied antivirus. Microsoft Defender Antivirus with Microsoft Windows 10 [5] has now made its entry into the market and has a good effect, as most SMEs use Microsoft operating systems on their PCs and laptops. The enablement of firewalls is also increasing based on previous similar surveys [3, 6], which is encouraging. What is also trending similar to previous surveys is the lack of antivirus software that is installed on both phones and tablets. Commercial offerings and competent-free versions of antivirus software are available. However, there still seems to be a disconnection on cyber risk when it comes to these devices.

3.5 Applying Updates

The application of updates and patching of operating systems, applications and countermeasures is a critical function in any cyber security program. The figures expressed in Tables 6 and 7 gives us an insight into what SMEs are doing with respect to their software patching of their critical business devices and systems.

It is alarming to see that the automatic update of operating system patches and applications is still not occurring. The percentages in phones and tablets while presenting as high given that phones and tablets by default automatically update, it means that someone has potentially altered this away from good practice. In the case of smart phones and tablets, it could be that the update processes are consuming scant space on memory cards and so users turn them off to save space, a bad idea.

With antivirus being installed on phones at the rate of 34% and tablets at the rate of 15%, it is encouraging to see, however, that those have taken the time to install have left it on to automatically update the antivirus signatures. PCs and laptops have 62% of respondents who have enabled automatic updates. The remaining 38% either do not know or are doing it at such a frequency that they are putting themselves at a higher risk of compromise. This trend is of major concern given the growth of crypto locker-based attacks on the business sector in the past few years. This is only expected to increase.

3.6 Backups Often the Last Great Refuge of Clean Data

In the survey only 50% of respondents indicated that they backup regularly, the remaining 50% backup sometimes, rarely or do not even know about status of backup. This is a very alarming trend in the age of crypto locker-based attacks. A regular routine of backing up important company data is one of the few significant countermeasures that businesses can rely on to recover from these type of cyber attacks.

When we delve into the more granular statistics, the picture is worse for all technologies: computers/laptops 46%, phones 21% and tablets only 15% are backed up. Surprisingly, the backup of network accessible storage (NAS) is higher at 18% than for phones. In, this survey, we asked where they backup their critical data. The use of a cloud service was actually the highest at 37%. This is unsurprising given the tight coupling and bundling offers that modern vendors are placing in their operating systems and the cloud. The use of local USB drives was only 18%, with backup tapes now becoming rapidly arcane with only 3% of businesses using this as a backup media. The use of network-attached storage has grown to replace or supplant tapes with 11% of the respondents backing up to these locations.

These trends and statistics, however, point to a critical problem or failure point in SMEs currently, which is insufficient backup of critical data. Further, the complete lack of any good frequency of backup with only 50% of respondents regularly backing up is of significant concern and needs to be addressed.

3.7 Cyber Security Responses, Planning, Maintenance and Insurance for the Lack Thereof

The authors surveyed the businesses to ascertain if they had sustained a cyber attack 54% of respondents claim they have never suffered a cyber attack. When they identified as being cyber attacked, we asked what remedies they undertook to address and recover from the attack. Thirteen percent (13%) of respondents fixed the problem themselves, a further 25% had their IT support person fix the problem.

Further study on the nature, cost and time taken to remedy the attack might be useful in that it might give some insight into the reliance of micro and small businesses on outsourced IT services.

In terms of reporting the incident to the authorities, no one reported anything to police or law enforcement agencies at all, simply astounding. A mere 8% indicated they reported it to ACORN (Australian CyberCrime Online Reporting Network) [7] or the new replacement site ReportCyber [8] functionality in Australia. This is a significant problem in that crimes go unreported and that government and others cannot get statistics and signals about current state of impacts of cyber attacks on the Australian economy.

A question was asked as to who in the small business was responsible for the cyber security function. Not surprisingly, but nonetheless alarming, 11% of SMEs have no one to carry out this function. Other patterns identified were 4% use a trusted family member, 11% use a specialist cyber security service, 25% use their existing IT support team and 50% look after it themselves. Also, in terms of a cyber response plan only 22% had a cyber response plan, 64% had no plan and 14% indicated they were working on a plan. Of those with plans and processes, 64% did not review any of these processes after they had been developed. This was expected, and in many ways unsurprising.

The marketing of cyber insurance to small business has increased in recent times, with many large global firms entering this potentially lucrative source of new insurance product revenue. In this survey, 20% of respondents had some form of cyber insurance, 55% no insurance and 25% were considering it. Given that most of them did not have information security processes mapped and plans, it would be questionable as to whether they could get cyber insurance as most insurance require some basic policy and process for cyber security to be able to claim. Cyber insurance is quickly moving and evolving component of cyber security, and one that signals the opportunity for a greater awareness of small business governance, risk and compliance (GRC) requirements in the future.

4 Conclusion

The survey is indicating yet again that SMEs need access to easily digestible cyber education. There is a strong role that local government and its local business association and business chamber partners can play to assist a greater awareness of the vital role cyber security plays. As businesses digitally store and transmit data on an increasing basis over a wide range of networks and platforms, their understanding of basic countermeasures and available protections can make them more resilient to cyber-attack and cyber-criminal exploits. There are many concerning trends in this initial analysis, some of which has some relatively simple remedies. Implementation of the simple remedies will significantly increase the cyber security posture and resilience of any small business at little or no cost. The CyberCheck.me platform allows easy access to the basic cyber security countermeasures. The program

is gaining national and international recognition given its blend of face-to-face and online consultations. The success of the program is due to its practical and immediate suggestions to a small business where instant action is possible.

In this age of a wide variety of disruptive and deadly distributed cyber threats to business, the lack of backup being applied to vital business data is of extreme concern. A key focus of the CyberCheck.ME small business awareness training is how to backup critical business data with adequate frequency and assurance. Equally, patching and updating systems and applications are techniques that small businesses need to be aware.

As the practical value of programs customised to suit a small business audience increases, SMEs need to realise in greater numbers that their smart phone and tablets are a critical point of vulnerability. The way in which they use and protect them needs to change in step with the increasing level of risk associated with attacks, whether they be motivated by profit, disruption, fun or all those things.

References

1. Anonymous, Academic Centres of Cyber Security Excellence (ACCSE), May 11, 2020; https://www.education.gov.au/academic-centres-cyber-security-excellence-accse
2. Anonymous, AustCyber, Australian Cyber Security Growth Network Limited, 2020
3. C. Valli, I.C. Martinus, M.N. Johnstone, Small to medium enterprise cyber security awareness: An initial survey of Western Australian business, in *SAM2014 International Conference on Security and Management, Las Vegas, USA*, (2014), pp. 71–75
4. IDRIX, Veracrypt., IDRIX, 2016
5. Microsoft, Microsoft Defender Antivirus, Microsoft, 2019
6. C. Valli, M.N. Johnstone, R. Fleming, A survey of lawyers' cyber security practises in Western Australia, in *2018 ADFSL Conference on Digital Forensics, Security and Law, University of Texas, San Antonia, USA*, (2018), pp. 219–226
7. ACORN, Australian Cybercrime Online Reporting Network (ACORN), 29/09/2017, 2017; https://www.acorn.gov.au/
8. Anonymous, Welcome to ReportCyber, 10th May, 2020; https://www.cyber.gov.au/report