GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Cyber Defense Challenges from the Small and Medium-Sized Business Perspective

GIAC (GSEC) Gold Certification

Author: Aric Asti, aricasti@gmail.com

Advisor: Ovie Carroll

Accepted: November 2017

With 5.7 million SMBs in the United States, it is essential that the risks involving cybersecurity events are identified. Small and medium-sized businesses (SMBs) face different challenges than large enterprises in regard to cybersecurity. The goal of this project was to survey SMBs and reveal organizational barriers that impact the cybersecurity posture of SMBs. An online survey was administered with a final sample size of 22 SMBs. Significant results showed that the top challenges were finances to pay talent, regulatory compliance and professionally available talent. As a result of inadequate information technology (IT) and cybersecurity staffing, 64% of respondents were unaware if a successful cyber-attack had taken place. The significant challenge SMBs face is their security posture and knowing if they have been or are being targeted against a cyber-attack. The main objective of this project was to show the security profile of the typical SMB. Educational, software and hardware tools should be promoted to increase the security posture of SMBs. Further research might focus more on the staffing and dedicated hours of IT and cybersecurity employees.

© 2017 The SANS Institute, Author Retains Full Rights

© 2017 The SANS Institute Author retains full rights.

Cyber Defense Challenges from the Small and Medium-Sized Business Perspective

Identifying who Small and Medium-sized businesses are

According to the Statistics of U.S. Businesses Employment and Payroll Summary: In 2012, there were 5.73 million employer firms in the United States of America. Of those employer firms, 99.7 percent have fewer than 500 workers. Eighty-nine percent have less than 20 workers. (Caruso, 2015). Small and medium-sized businesses (SMBs) are the majority of businesses found in the United States. Therefore, when looking at the number of cyber-attacks on businesses in the U.S., the majority of those attacks are likely to target SMBs.

Cyber-attacks are analyzed and studied to identify the motivation of attacking SMBs. For example, according to the Small Business Administration (SBA), small businesses account for 42% of private-sector payroll (Caruso, 2015). The payroll number is a metric which can be used to compare large and small businesses. To put the private-sector payroll number in perspective, the following examples should be noted which are taken from the U.S. Census Bureau, 2012 Statistics of U.S. Businesses. There are more than 5.7 million SMBs operating in the US (according to the 2012 survey). Those SMBs employ 56 million persons. The annual payroll of those SMBs is $2.2 billion. In contrast, there are more than 18,000 large enterprises made up of more than 500 employees. The large enterprises employ almost 60 million persons (Caruso, 2015) and have an annual payroll of $3.1 billion. A quick number check reveals that the SMB payroll makes up 41.8% of the total annual US payroll – which agrees with the previously cited statistic of 42%. These numbers provide a reference showing how much money may be available to attackers.

Payroll reserves is a highly liquid asset for companies that may be targeted as vulnerable by nefarious actors. A 2015 survey shows that the average money stolen from bank accounts of SMBs was $32,020.56 (NSBA, 2015). According to the Netwrix 2017 IT risk report, 73% of SMBs do not have a separate information security function, compared with only 33% of large

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

enterprises. This data suggests that SMBs may represent a more vulnerable environment for would-be hackers. With a combined payroll of approximately $2.2 billion (Caruso, 2015) SMB payroll represent a potentially lucrative target for hackers seeking to hold data ransom for a $32,000 payday.

The NSBA Year-End Economic Report (2015) provides insight into a typical SMB. Eighty-eight percent of SMB respondents employed between 1 and 99 employees. Sixty-two percent of the respondents reported total payroll between $100,000 and $5 million. Therefore 40% of responding SMBs have less than 99 employees and payroll between $100,000 and $5 million. Forty percent of respondents in the 2013 NSBA Small Business Technology Survey responded that the owner of the company provides all technical support (there was no reporting of this statistic in the NSBA 2015 Year End economic report). Consider all of the business owners' other duties. If there is no dedicated technical staff supporting the SMB, then the SMB is an easier target than a large enterprise that has dedicated technical staff. Combine the lack of technical staff with SMBs expanding their presence on the internet. Thirty-five percent of SMBs reported they would be utilizing a growth strategy of Internet / Expand E-commerce (NSBA, 2015). This fact should be noted as more exposure on the Internet will increase their cybersecurity risk.

Are SMBs being targeted more?

Assuming a hypothesis that SMBs are an easier, yet lucrative, target, are SMBs becoming targeted more frequently? At first glance, there appears to be some conflicting data. In 2015, 58% percent of respondents said they have never been a victim of cyber-attacks, compared with 50% in 2014. This statistic suggests that between 2014 and 2015 SMBs have had less reported cyber-attacks. One possible explanation for the decline from 58% to 50% could be that the SMB doesn't know they've been attacked. Other possible explanations would include different polled respondents or even poor statistical sampling methods. Supporting this idea is Symantec's (2015) report that in 2015, 59% of all spear-fishing attacks were targeting SMBs. Another noteworthy metric is the length of time to resolve a cyber-attack. In 2015, cyber-attacks took longer to resolve than those reported in 2014. In 16% of cases, it took longer than two

© 2017 The SANS Institute Author retains full rights.

weeks to resolve a cyber-attack (NSBA, 2015). These statistics show that SMBs may be being targeted more frequently and the cyber-attacks may be taking more time to resolve, presenting an urgent challenge to the cyber defense of SMBs.

Corroborating Data

The biggest challenge that SMBs face when dealing with cybersecurity can be separated into two topics. The first topic is technical - according to the respondent data, seven and a half hours per month are spent on cybersecurity. The second topic is resource-related, finances to pay professionally available talent (Figure 1). This data is corroborated by other available surveys. According to the *Ponemon Institute Research Report*, when small businesses were asked "What challenges keep your IT security posture from being fully effective?", 67% of respondents reported insufficient personnel (pg. 6). The priority of cybersecurity in an SMB must also be considered. According to Manta (2017), "only 69% of small business owners have controls in place to prevent hacks—meaning 1 in 3 small business owners have no safeguards in place" (para. 6). The same study cited 87% of small business owners did not feel they were at risk of experiencing a data breach (Manta, 2017, para. 2). Finally, Small Business Trends (2017) cites in the Small Business Cybersecurity Prevention Statistics that "51% of small businesses are not allocating any budget at all to risk mitigation" related to cybersecurity. These three separate studies all collaborate the previous data cited. If there is no way to add staff to assist with the solution, consider providing three steps for the existing staff to mitigate the risk of cybersecurity.

Typical SMB technical staffing structure

The goals of this paper are to identify what challenges SMBs face when considering cybersecurity. How are SMBs staffed in terms of their cybersecurity and information technology needs? Which constraints have the most impact from the SMBs perspective? To build a picture of what a typical SMB looks like from a cybersecurity staffing perspective, a survey was conducted that returned 31 participating enterprises. Respondents to the survey who belong to a

© 2017 The SANS Institute Author retains full rights.

business of more than 500 employees were removed from the sample size. This left the survey with twenty-two respondents. The median employee number was 80. The median was used, when analyzing the data, in order to minimize the statistical effect of outliers.

The first question posed in the survey was: "Do SMBs have IT staff, cybersecurity staff or both?". Fifty percent (11) reported they employ dedicated staff for both cybersecurity and IT roles. Eighteen percent (4) reported only dedicated IT staff. Eighteen percent (4) reported outsourced resources. Finally, 9% (2) reported they had no dedicated IT or cybersecurity staff. This data shows the majority of SMBs that responded recognize the need for both skills.

A follow-up question of "Are there separate roles when considering information technology and/or cybersecurity?" Typical roles of information technology include the implementation of support of internal electronic systems. These systems include but are not limited to, e-mail, workstations, servers, network hardware and software used to support business functions. Typical roles of cybersecurity include the detection and prevention of unauthorized persons, data or other electronic communications from negatively impacting the organization. These systems typically include but are not limited to firewalls, intrusion detection systems, intrusion prevention systems, anti-malware, anti-virus. Sixty-four percent of respondents reported "No." Concluding that many of these SMBs have separate staff for the task of IT and cybersecurity, however, they consider IT and cybersecurity to be a joint effort and in the same department.

Respondents were asked to provide the number of staff who provide IT, cybersecurity or a combination of the two services. The survey shows the mean number of employees that are responsible for IT services is 1.5 with 18% (4) reporting they have outsourced their IT service needs. The mean number of employees that are responsible for cybersecurity services is 1. Thirty percent of respondents reported they have outsourced their need for cybersecurity services. The mean number of employees who are responsible for both cybersecurity and information technology services is 1.5 with 22% reporting they have outsourced their need for both services.

The data from these respondents begin to form what the staffing of a typical SMB looks like. If an organization has 80 employees (the mean staff number of respondents), it can be concluded that 54% of those SMBs would have two staff responsible for IT and cybersecurity

© 2017 The SANS Institute Author retains full rights.

services. Forty-six percent of the SMBs would have one staff member for just IT services or utilize an outsourced solution.

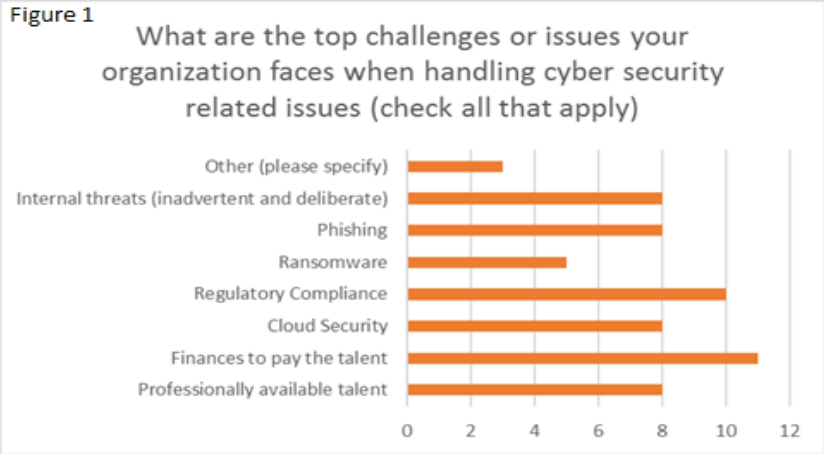
In order to explore the possible challenge of technical staffing, two questions were asked, "Given no constraints, how many full-time equivalent (FTEs) would you like to see for IT?" and "How many FTEs would you like to see for cybersecurity?" The mean for both questions was two (2). According to this data, participants would like to see a combined staff count for both IT and cybersecurity of four (4). The current mean number of staffing for both IT and cybersecurity needs is 2. These numbers show us that respondents report that staffing is half of what would be considered ideal.

The next step was to identify what the top challenge is regarding staffing for the participating enterprises. To provide more insight, the question was asked, "What are the top challenges or issues your organization faces when handling cybersecurity related issues?" In figure 1, the top two challenges reported were finances to pay talent followed by regulatory compliance. Among the next grouping of concerns is the availability of professionally available talent. The challenge of finances to pay talent aligns with the previous respondent data stating staffing populations being half of ideal. Regulatory compliance is responsible for setting the requirements of the technical staff's workload. Professionally available talent also contributes to the staffing issues that were seen previously. To clarify the "other" category there were three responses. Two of the responses mentioned time. One of the respondents stated that only one-third of their time was allocated for cybersecurity, which is not nearly enough to complete the job satisfactorily. The other comment reported lack of support from upper management. The top three responses all correlate to the previously identified issue regarding lack of staff when dealing with cybersecurity issues.

Aric Asti, aricasti@gmail.com

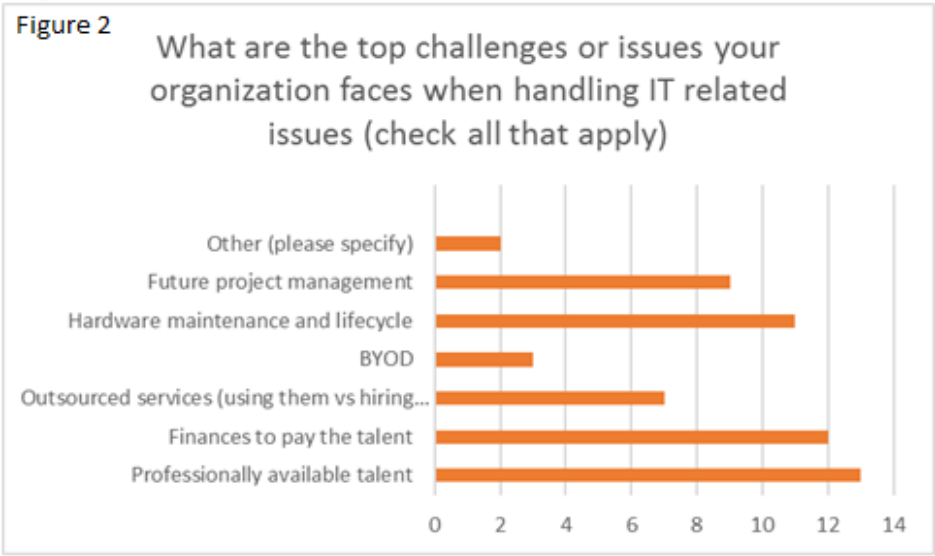
© 2017 The SANS Institute Author retains full rights.

Figure 1



The next question explores challenges when dealing with the IT side of the organization. "What are the top challenges or issues your organization faces when handling IT related issues?" Figure 2 shows professionally available talent ranked the number one issue, followed by finances to pay talent. The third-ranked response is a technical response opposed to a staffing-related response - hardware maintenance and lifecycle. It is important to note that finances to pay the talent were the number one and number two issue faced in both Figures 1 and 2.

Figure 2



According to data from figures 1 and 2, it can be concluded that staffing is a top issue faced by SMBs. There is both an availability challenge as well as a financial one.

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

According to the average SMB, current staff levels are at 50% of ideal. Assuming all of the technical staff are overworked due to job vacancies, consider how internal and external communication and reporting is presented. Respondents were asked "How does your organization present metrics on IT and/or cybersecurity events? Forty-one percent responded they present events verbally. Twenty-seven percent reported a formal meeting that was regularly scheduled. Twenty-seven percent reported that they do not present security events. Five percent of respondents reported that they had a formal meeting, but it was irregularly scheduled. Roughly 70% of respondents have no formality, documentation or other presentation methods in which they present cybersecurity events. These numbers suggest that if a cyber-security event is detected, 7 out of 10 SMBs lack a method in which to disseminate that information. If the presentation of metrics is not a priority (according to the data presented), and presentation of metrics is a form of education, do organizations recognize the need for technical staff to formally educate themselves?

The next question "Do organizations recognize the need for continuing education for IT and/or cybersecurity professionals?" was polled. Nearly 60% of respondents reported their organization requires continuing education for IT and/or Cybersecurity employees. This number suggests that the majority of responding SMBs recognize that there is a need to remain current and educated when it comes to IT and cybersecurity. Therefore, SMBs recognize the need for staff to participate in formal education, however, internal presentation of metrics is not executed in the majority of polled SMBs.

The biggest cybersecurity challenge SMBs face

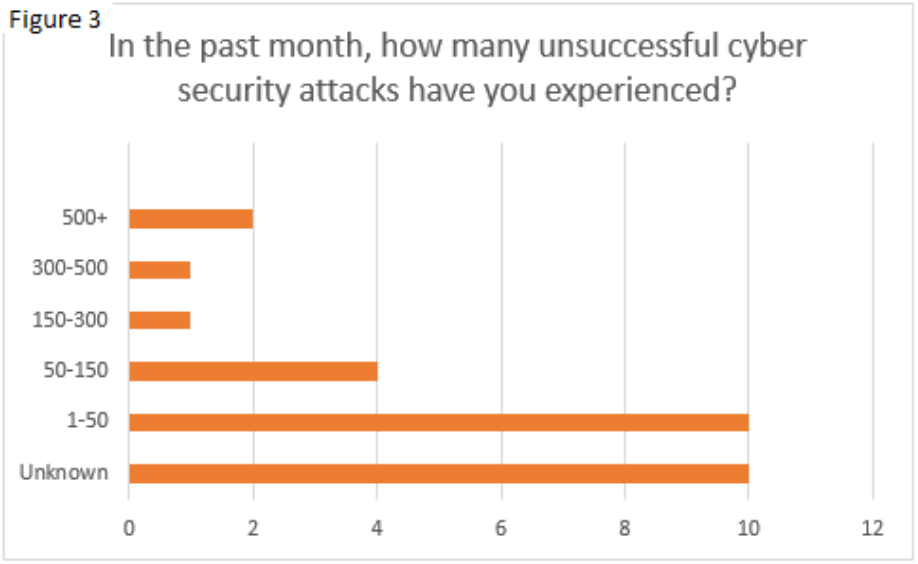
The data from the survey suggests a common staffing situation for SMBs. That situation has a median company employee population of 80. Fifty-five percent of respondents have one dedicated IT employee and one dedicated cybersecurity employee. About 40% of those SMBs report security events verbally, about 30% of them have a regularly scheduled formal meeting, and about 30% of them do not report events at all. Their staffing numbers are about half of what they consider to be ideal.

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

An apparent lack of formal security operations and adequate security staffing becomes apparent in Figure 3 when 41% of respondents were unsure if there had been any unsuccessful security attacks on their organization. Another 41% of respondents report between one and fifty attacks. When considering unsuccessful attacks, it may be argued these are more difficult to detect. If an organization can detect unsuccessful attacks, we can assume they have some sort of security posture. A good example of an unsuccessful cyber-attack would be an alert and blocked traffic by an IDS/IPS (Intrusion detection system / Intrusion prevention system).

Figure 3



In Figure 4, when the question focuses on successful cyber-attacks, the results are more daunting. Nearly 64% of respondents are unaware if they have been successfully attacked. The most significant challenge SMBs face is their security posture and knowing if they have been or are being targeted against by a cyber-attack.

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

Figure 4



The data shows that the majority of SMBs are unaware if they have been the victim of a successful cybersecurity attack. Logically, the next question asked was "How much time does your organization spend on IT and cybersecurity?" To establish a baseline of hours, assume a workweek consists of 40 hours, multiply that by 52 weeks and divide by twelve months. The baseline calculates to 173 available hours per month per FTE.

When asked “How much time does your organization spend on IT (hours per month)?” Calculating the average number of hours per FTE, reported by Respondents, was 99.1. Those hours were calculated by using the previously polled data of how many employees were responsible for IT in the organization. This data shows that 57% of the staff time is dedicated to the core functions of IT. Twenty-seven percent of the respondents didn’t know much time their organization spends on IT.

When considering the question “How many hours does your organization spend on cybersecurity?” the data shows something more daunting. The median number of hours, spent per month, on cybersecurity per responding organization is 7.5 hours. Thirty-two percent reported they did not know how much time was spent. This reinforces the reported data that nearly 64% of organizations are unaware if they have sustained a cybersecurity attack that was successful and 41% are unaware if they have sustained an unsuccessful attack. By only spending

© 2017 The SANS Institute Author retains full rights.

seven and a half hours per month on cybersecurity, it is likely that SMBs are placed at increased risk of cybersecurity.

Mitigate cybersecurity risk by answering 3 questions

When considering the mitigation of risks associated with cybersecurity threats. The first question, "Why mitigate this risk?" suggests assessing which documentation is required for an enterprise's cybersecurity. Specifically, what guides and assessments are used to assist organizations in building policies and procedures? These policies and procedures enable an organization to enforce their mitigation factors and answer the question "Why mitigate this risk?" The second question, "What needs to be secured?" is focused on prioritization. What specific physical and virtual assets contain critical information that needs to be secured? The third question, "How is the mitigation executed?" addresses the technical implementation of securing critical data. How are the technical methods applied in order to secure high priority assets? These three broad questions provide an organization with a plan to mitigate cybersecurity risk without sacrificing already scarce resources.

Why mitigate this risk? The first step of mitigating cybersecurity risk is through ensuring a good security program by building or verifying organic policies and procedures. To assist in building that documentation, the Department of Homeland Security (n.d.) through CERT (Computer Emergency Readiness Team) has specific programs designed. One program is called the C3 Voluntary Program. Within the C3 Voluntary Program, there is the Cyber Resilience Review (CRR). The CRR is a no cost, voluntary assessment to evaluate an organization's information technology resilience. The CRR may be conducted as a self-assessment or as an in-person, facilitated assessment. (Department of Homeland Security[DHS], n.d.-b, para. 1). More information on this program can be found at https://www.us-cert.gov/ccubedvp/self-service-crr. The CRR provides a wealth of information. The CRR Resource Guides provide a framework of documentation that will provide a method for an SMB to construct a well-documented, effective security program. An example of some of the resource guides includes Asset Management, Controls Management, Configuration and Change Management, Vulnerability Management, Incident management and Risk Management. Also within the C3 Voluntary Program is a Leadership Agenda. Although the Leadership Agenda (DHS, n.d.-c) is designed for the business

© 2017 The SANS Institute Author retains full rights.

owner or executive leadership, being able to identify and address the Risks and Plans in that document will demonstrate devotion and maturity to upper management. This documentation along with policy and procedures answer the question of why.

What needs to be secured? The second question transitions from the policy and procedure documentation methodology. It focuses on what actions need to be implemented in order to understand what is happening, technically, in the organization. "The Center for Internet Security's Critical Security Controls for Effective Cyber Defense V 6.1 (CIS Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to thwart the most pervasive attacks. The CIS Controls consist of a relatively short list of high-priority, highly effective defensive actions that provide a 'must-do, do-first' starting point for every enterprise seeking to improve their cyber defense." (Center for Internet Security, 2017a, para. 1).

These are the 20 CIS controls described in Center for Internet Security (2017b):

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges
6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security

© 2017 The SANS Institute Author retains full rights.

19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

These controls can be broken into three groups. The first group consists of controls one through five. Those five controls focus on monitoring the environment. The second group, controls six through eighteen, secure and maintain the organization's security posture by focusing on assessment. The third group, controls nineteen and twenty, focus on improvement on the first eighteen controls. These controls answer the question of "What needs to be secured?"

How is the mitigation executed? The third question addresses the technical execution of mitigation. There are many ways to accomplish this step, many tools from which to choose. There is no right or wrong way, provided the organization is able to observe, detect and mitigate cybersecurity risks. This quick overview is meant to provide an organization with resources that will quickly and efficiently provide some means of monitoring network traffic in order to determine if there is anonymous traffic on the network.

Software-based solutions

Security Onion (SO) is an open source software distribution that includes various tools that can provide insight into the network traffic of an organization. SO can be deployed either by itself or multiple instances of itself - monitoring multiple places of a network at one time. For SO to be able to sniff all traffic from a switch, the port that SO is plugged into must be configured as a trunk port. There is a script that walks the user through the installation of SO. Once those steps have been completed, there are tools such as Enterprise Log Search Archive (ELSA) and Sguil (pronounced squeal) that provide insight into network traffic. SGUIL compares network traffic to certain rules. If the network traffic and the rule match, an alert is generated. ELSA is another tool which allows the user to examine network behavior such as what service and ports certain source and destination IP addresses are utilizing.

Hardware-based solutions

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

There are numerous hardware appliances available. One hybrid appliance is the Cisco Meraki series. These firewalls have a cloud-based configuration making setup and deployment simple. There are two license types for the firewall series: enterprise and advanced security. The enterprise license consists of a base set of features. The advanced security license includes all of the features found in enterprise and various security-focused features including intrusion detection, intrusion prevention, content filtering, geography-based rules, anti-malware and anti-virus features. The Meraki firewalls have several models available. The typical budget for one of the appliances cost around $2,800 per year including license fees. This is much less than the cost of hiring a full-time employee while providing intuitive and efficient interfaces for the overworked technical professional.

Education material ranges from free webinars by industry leaders such as Qualys or Rapid7. Mailing lists such as CERT (FEMA community emergency response team) provide up to date information on security issues through automated emails. There are formal educational programs, for example, SANS is a world-renowned industry leader in the field.

While these resources are beneficial, the most useful, most powerful resource is the prioritization of security from upper management. Management must decisively commit resources to enable, improve, and educate their technical staff. Date from this study shows that nearly 60% of polled SMBs require a formal method of continuing education. Yet there is more to improving the security posture of the organization than just continuing education. In addition to continuing education and professional development, technical staff must be able to articulate their needs, concerns, and direction in a clear, metric-driven model to senior management. According to Bailey, Kaplan and Rezek (2014), “Senior-management time and attention were identified as the single biggest driver of maturity in managing cybersecurity risks—more important than company size, sector, and resources provided.” (para. 8). By answering these three questions - why, what and how - technical staff will have a framework for addressing and mitigating the biggest challenge faced by SMBs: the unknown status of cyber-attacks and lack of technical staffing.

Continuing Research and lessons learned

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

When reflecting on this study's survey, one of the most time-consuming efforts was removing all respondents who work at organizations that are larger than 500 employees. When choosing a survey mechanism, ensure that granular control over the analytics is feasible. While rebuilding the analysis is not very challenging, it can be quite time-consuming. In hindsight, obtaining more detailed information regarding what mechanisms are deployed by SMBS to mitigate cybersecurity risk would have provided an interesting metric. These mechanisms would include but are not limited to anti-virus, intrusion detection/intrusion prevention systems, firewalls, anti-malware, anti-spam and vulnerability assessments. This would have provided an opportunity to correlate both successful and unsuccessful cyber-attacks and deployed security mechanisms.

It can be difficult to build a sizeable enough response rate to suggest a statistical significance of data and findings. There are great concerns regarding spam and cybersecurity such that clicking on a link is usually met with hesitation. The SANS faculty were extremely helpful in promoting the survey. Another useful means is targeting forums. A popular IT forum, Spiceworks, is in use by millions of IT professionals. The survey link was submitted in one of these forums. There was a delay in posting as the link had to be vetted by a moderator. Once the link was approved, the population dataset nearly doubled in twenty-four hours. Future researchers should include targeted forums in which to submit their surveys for data.

If organizations are truly dedicating 7.5 hours per month to cybersecurity, a deeper dive should be conducted as to why. Future research may be able to determine if this is a staffing issue, a priority of work issue, education issue or a possible combination of the three. Attackers have recognized the weaknesses in SMBs and are exploiting them more and more. We must be diligent in sounding the alarm and making sure SMBs are aware of the immediate risk posed to their financial and technical infrastructure.

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

© 2017 The SANS Institute, Author Retains Full Rights

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

Appendix A

Summary of Survey Questions

How many employees are in your organization?

How many employees are responsible for your information technology needs? (computers, email, networking, etc)

How many employees are responsible for your cybersecurity needs? (cyber-attacks, phishing, anti-virus, ransomware, etc)

How many employees are responsible for your information technology needs and your cybersecurity needs?

Does your organization require continuing education for IT / Cybersecurity employees?

Are there separate roles when considering information technology and cybersecurity?

Assuming no constraints……how many FTEs would you allocate for IT (computers, email, networking, etc)?

Assuming no constraints…… how many FTEs would you allocate for cybersecurity (cyber-attacks, phishing, anti-virus, ransomware, etc)

What are the top challenges or issues your organization faces when handling IT related issues (check all that apply)?

What are the top challenges or issues your organization faces when handling cybersecurity related issues (check all that apply)?

How does your organization present metrics on IT and/or cybersecurity events?

In the past month, how many unsuccessful cybersecurity attacks have you experienced?

In the past month, how many successful cybersecurity attacks have you experienced?

In a given month, how many hours has your organization dedicated to IT?

In a given month, how many hours has your organization dedicated to cybersecurity?

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

References

Bailey, T., Kaplan, J., Rezek, C. (2014). *Why senior leaders are the front line against cyberattacks.* Retrieved from https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-senior-leaders-are-the-front-line-against-cyberattacks

Caruso, A. (2015). *Statistics of U.S. businesses employment and payroll summary: 2012*. Retrieved from https://www.census.gov/content/dam/Census/library/publications/2015/econ/g12-susb.pdf

Center for Internet Security. (2017a). *CIS Controls FAQ.* Retrieved from https://www.cisecurity.org/controls/cis-controls-faq/

Center for Internet Security. (2017b). *CIS Controls.* Retrieved from https://www.cisecurity.org/controls/

Department of Homeland Security. (n.d.-a). US-CERT *Resources for small and midsize businesses (SMB).* Retrieved from https://www.us-cert.gov/ccubedvp/smb

Department of Homeland Security. (n.d.-b). US-CERT Assessments cyber resilience review (CRR). Retrieved from https://www.us-cert.gov/ccubedvp/assessments

Department of Homeland Security. (n.d.-c). C3 Voluntary program- Small and midsize business (SMB) leadership agenda. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/smb/Leadership_Team_Agenda.pdf

Manta. (2017). *Are small business owners protecting themselves from cyber-attack?* Retrieved from https://www.manta.com/resources/small-business-trends/small-business-owners-protecting-cyber-attack/

National Small Business Association. (2013). *2013 Small business technology survey*. Retrieved from http://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf

National Small Business Association. (2015). *2015 Year-end economic report*.

Aric Asti, aricasti@gmail.com

© 2017 The SANS Institute Author retains full rights.

Retrieved from http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf

Ponemon Institute Research Report. (2016). *2016 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

Small Business Trends. (2017). *Cybersecurity statistics-Numbers small businesses need to know.* Retrieved from https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

Symantec. (2015). *Internet security threat report (volume 20)*. Retrieved from https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

Netwrix 2017 IT Risk Report (2017) https://www.netwrix.com/SMBs_focus_on_endpoint_security_while_large_enterprises_prioritize_data_security_says_Netwrix_survey.html

© 2017 The SANS Institute Author retains full rights.