International Journal of Future Generation Communication and Networking
Vol. 13, No. 04, (2020), pp. 1780-1788

Recommendations for Implementing Cyber security Controls in Small and Mid-Sized Businesses in India

Lumena Mukherjee, Pooja Trivedi and Dhanraj Verma

Department of Computer Science & Engineering, Dr. A. P. J. Abdul Kalam University, Indore (M.P.) - 452016
Corresponding Author : Lumena Mukherjee

***Abstract*—** *With the lines between our digital and physical lives getting blurry with every passing day, cyber attacks have emerged as a prime concern for individuals and businesses alike. Most of us live in a bubble of denial that if we are a small business, hackers will not target our systems or data. However, the facts and figures indicate otherwise with more than half the majority feeling helpless to defend themselves against new forms of cyber-attacks.*
As data theft, network breaches, and other forms of security threats keep growing, with attackers specifically targeting underprepared and often defenseless SMBS, we must use the resources available wisely, reform our IT policies to include cybersecurity best practices and make best possible use of available technologies. This paper focuses on understanding the gap by conducting a survey using various security controls and defining financially viable recommendations to safeguard small and mid-sized businesses against cyber attacks..

***Index Terms*—** Cybersecurity Policies, Cybersecurity Solutions for Small Business, Small Business Cybersecurity, Small Business Security in India, SMB Cybersecurity in India**.**

1. INTRODUCTION

1.1 Is There a Need for Cybersecurity in SMBs?

According to the Data Security Council of India, we've been the second most affected country due to cyber attacks between 2016 to 2018, with reports indicating that 60% of affected small businesses close within six months of a breach. Score reports that 43% of cyberattacks worldwide target SMBs. Juniper Research reports that while the security risk is high in the SMB sector, they only account for a meager 13% of the overall cybersecurity market, in terms of expenses on security-driven products. Security analysts project that information breaches will increase three times every year over the next five years with an average annual increase of 9% in terms of budget allocation for cybersecurity. The general lack of awareness and unresponsiveness towards cybercrime, and a false belief that an SMB can fly under the radar of cybercriminals, might cause more harm than we can foresee. According to SiteLock (a website security company), a site is exposed to cyber attacks more than 50 times on average each day. It should come as no surprise that SMBs have emerged as desirable targets for cybercriminals.
It is of utmost importance for businesses to safeguard their data and network from security threats as best as they can.
Cybersecurity usually does not cut it to the budget allocation stage in most SMBs. In this paper we look at some practical ways to implement security through reshaping security policies, creating or building them from scratch where needed, and implementing security checks without making a huge dent on the budget.

ISSN: 2233-7857 IJFGCN

1.2 What Are the Biggest Security Threats Faced by SMBs?

Some of the most common threats faced by small businesses are as follows:

- Ransomware Attacks
- Phishing Attacks
- Privilege Escalation Attacks
- Fraudulent Apps
- Weak Passwords
- DDoS Attacks
- Social Engineering Attacks

1.3 How to Defend Against These Attacks?

Defending against these attacks can be implemented by taking a layered approach to cybersecurity. Apart from deploying solutions and security tools at every level such as on endpoint devices or at perimeters, organizations must also consider how they factor in people and processes along with technology.

People: Cybercriminals can specifically target innocent employees to gain access to sensitive information or undue leverage since they are typically unaware of security best practices. While employees can be one of the biggest security risks, when properly trained and valued, they can also be a huge asset and act as the first line of defense against potential threats.

Processes: There must be strategies in place to proactively prevent any attacks on the organization network and to safeguard all sensitive information. However, the IT team should establish standard procedures to follow in the event of a breach, and develop effective response and recovery plans.

Technology: While there are several security solutions available in the market, selecting the right technology to be deployed in the environment in order to create a security fabric across the network, should be a priority. Layering defenses, deploying deception technology to send attackers on a wild goose chase, leveraging segmentation to limit access to business-critical data are a few ways SMBs can use technology to their advantage.

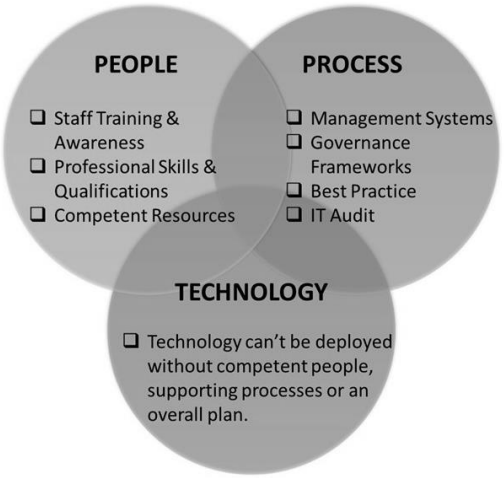

Fig 1: People, Process, and Technology

II. RELATED WORK

M. Rea-Guaman, JA Calvo-Manzano, T. San Feliu proposed "A Prototype to Manage Cybersecurity in Small Companies". In this work, they have identified some management tools of cybersecurity for small businesses based on certain requirements and have described a prototype. [1]

"Cyber Risk for Small and Medium-Sized Enterprises." is a report presented by The Janet & Mark L. Goldenson Center for Actuarial Research, University of Connecticut. The report concentrates on how small businesses can incorporate a cyber risk management plan, including purchasing cyber insurance, to protect themselves from cyber-attacks. [2]

"2019 Global State of Cybersecurity in Small and Medium-Sized Businesses" by Ponemon Institute, is an annual study conducted with a focus on the cyber threats faced particularly by SMBs. It tracks the trends in attacks and breaches, and the preparedness of small-medium sized businesses to defend against and respond to these threats. [3]

Joanna Patterson from Walden University proposed "Cyber-Security Policy Decisions in Small Businesses". In this case study, he surveys small businesses to understand their existing cybersecurity strategies and recommends feasible strategies that can or have successfully prevented cyber attacks. [4]

Jari Flyktman, from JAMK University of Applied Sciences, conducted a study and proposed "Implementing Information Security Management System as a part of business processes". This study attempts to help SMBs to understand and implement ISMS while forming the organization's processes. [5]

Nabila Amrin, from the University of Twente, wrote a paper on the "The Impact of Cyber Security on SMEs". The study was aimed to be a pilot research on surveying SMEs in Europe with respect to their security practices. Sixteen businesses from different business operations were sampled and interviewed on their recent IT security trends (with a focus on Cloud Computing, BYOD), cybercrime victimization, and cybercrime prevention practices. [6]

Ruti Gafni and Tal Pavel from The Academic College of Tel Aviv, Yaffo, Israel conducted an exploratory research on "The Invisible Hole of Information on SMB's Cybersecurity". In this study, investigation covered general mass communication media channels, technological and professional cybersecurity websites, and academic journals, and found that very few studies, articles, and news items were published in this matter. [7]

Syed (Shawon) M. Rahman, Ph.D., and Robert Lackey proposed "E-commerce systems security for small businesses". This paper is a discussion on how attacks are carried out and how a small business can effectively secure their networks with minimum cost. [8]

Jamal Raiyn, from the Computer Science Department of Al-Qasemi, Academic College of Education, Baqa Alqarbiah, Israel, conducted "A survey of Cyber Attack Detection Strategies." This paper introduces, discusses, and compares the different cyber-attack detection strategies and proposes a new scheme for a real-time and short-term response to actual attacks. [9]

The ninth annual cost of cybercrime study, independently conducted by Ponemon Institute LLC, and jointly developed by Accenture, is a report that quantifies the economic cost of cyber attacks. It looks at past and current security trends and projects future costs to enable leaders to best target their funds and resources. [10]

III. PROPOSED RECOMMENDATIONS

We look at the various domains such as asset management, physical security, mobile device management, etc. and recommend basic guidelines that need to be taken into consideration before the formulation of policy documentation at the organization level. The recommendations also deal with how technology

should be deployed in the business environment as well as considerations if remote access is granted to personnel or third party vendors are allowed to connect to the business network.

The work is conducted in phases, starting with an initial survey done using a security assessment questionnaire. This survey helps to establish a baseline level of awareness in business owners, existing security practices, existing IT policies, etc. We work with businesses in the next phases to formulate strategies and policies that can be implemented to safeguard business assets. We look at processes, people and technology, existing insecure practices, and what needs to be improved upon to protect against potential attacks. Towards the end of the study, we conduct an impact analysis and publish findings.

A. Phases of Proposed Work

The proposed work is conducted in four phases:

Phase 1: Conduct a study through a series of surveys and interviews with a sample size of 10-15 business owners to identify the causes that contribute towards the slow adoption rate of cybersecurity practices in the SMB market.

Phase 2: Formulate recommendations for implementing cybersecurity controls in small and mid-sized businesses in India.

Phase 3: Provide actionable inputs that educate and enable small business owners to make informed cybersecurity decisions. Since most business owners are non-technical, it is important to communicate the risks they face with limited usage of technical jargon while describing their threat landscape.

Phase 4: Evaluation of the degree of perception change, awareness levels, openness to adopt and implement cybersecurity best practices in their organization, etc. as a measure for the effectiveness of the study conducted with the control group.

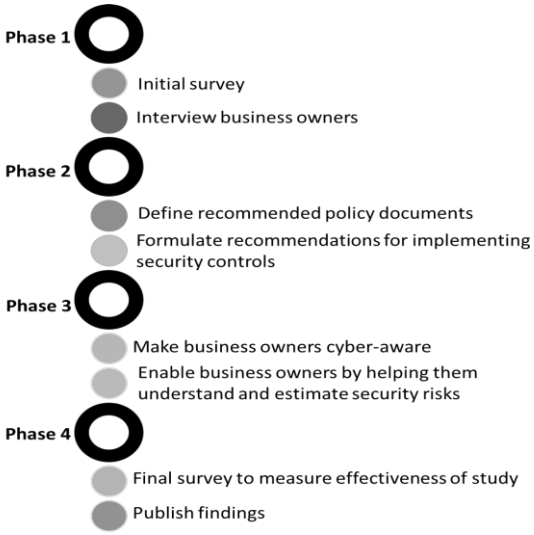

Fig 2: Phases of Study

B. Basic Requirements for Implementation of Proposed Work

- Trained internal IT team to frame security policies for the organization
- Skilled security professional to implement the said policies
- Recommended security tools and solutions
- Third party security service providers to conduct regular VAPT scans and manual testing to identify potential vulnerabilities
- System Admins to implement controls and limit access to resources on a need to know basis

ISSN: 2233-7857 IJFGCN

- IR team, responsible for escalating, handling, and analyzing security incidents in the event of a breach.
- L&D team, responsible for awareness training, internal and external.

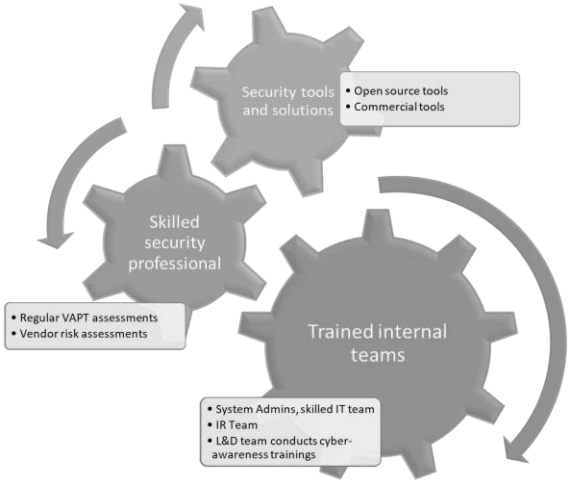

Fig 3: Basic Requirements for Implementation of Security Controls

IV. SURVEY ANALYSIS AND RESULTS

If the sample size of 11 organizations, who were willing to participate in the study, is taken as an approximation of the SMB sector, it leaves room for a lot of improvement for a majority of the security controls that were assessed. While some of the unpreparedness can be chalked up to financial constraints, in most cases it was the lack of awareness, the assumption of safety, and an unwillingness to devote time, effort, or resources to invest in security. The table below is a summary of the level of implementation of each security control, based upon the analysis of the responses received from the survey.

Table 1: Survey Results

Sr. No.	Security Control	Well Imple--mented	Needs Improve--ment	Likely to Imple--ment	Unlikely to Imple--ment
1	Security Policies and Agreements	27.27%	18.18%	27.27 %	27.27%
2	Incident Management and Disaster Recovery	9.09%	9.09%	45.45 %	36.36%
3	Staff Training and Awareness Workshop	18.18%	0.00%	63.63 %	18.18%
4	Data Security	27.27%	0.00%	45.45 %	27.27%
5	Asset Management	54.55%	9.09%	9.09%	27.27%
6	Access Management	27.27%	27.27%	18.18 %	27.27%

ISSN: 2233-7857 IJFGCN

7	Cryptographic Controls	18.18%	27.27%	9.09%	45.45%
8	Technological Competence	54.55%	27.27%	18.18 %	0.00%
9	Patch Management Strategy	9.09%	45.45%	27.27 %	18.18%
10	Technical Vulnerability Management	18.18%	36.36%	18.18 %	27.27%
11	Physical Security Controls	36.36%	9.09%	27.27 %	27.27%
12	Change Management	18.18%	18.18%	45.45 %	18.18%
13	Compliance	0.00%	36.36%	36.36 %	27.27%

Recommendations for Implementing Security Controls in SMBs

The most prevalent threat vectors for small and mid-sized businesses are –

- Weak default passwords,
- Phishing scams,
- Privilege escalation attacks,
- DDoS attacks,
- Information disclosure due to fraudulent apps,
- Insider threats,
- Social engineering attacks,
- Information leakage due to mishandling of sensitive data, etc.

As an SMB, who may or may not be an IT related service provider, financial constraints are only a part of the problem. Lack of effort when it comes to investing time and energy into implementing better open-source technology to secure business networks, and delays in adopting security best practices, goes a long way in building an entire business sector riddled with security loopholes. The recommendations below are only a starting point and have been made keeping in mind the scope of technical expertise of non-IT organizations and financial limitations that may typically prevent SMBs to opt for high-priced enterprise-level security solutions.

1. Training employees to recognize security threats

Security is the responsibility of everybody at an organization starting from an intern to the leadership. Humans are often considered to be the weakest link in security. However, with regular cyber awareness workshops that train employees on recognizing the common pitfalls, differentiating between a legitimate vs. a phony email or a website, and staying aware of the latest trends in security, an SMB can develop a security mindset, with the staff acting as a defensive asset who can ward off cyber-attacks because they're now armed with the knowledge of how to react to any potential threat vector.

2. **Establishing an effective patch management process**

According to a study by Ponemon institute 60% breaches in 2019 involved unpatched vulnerabilities, reminiscent of the Equifax breach, and the infamous Wanna Cry ransomware. Cybercriminals are aware that often companies fail to install patches on a regular basis either because they are laid back or

sometimes because installing patches can break existing systems. However, installing incremental updates can solve this problem so the IT team can test if a new update crashes the existing system. Developers often release security updates to patch newly found bugs and failure to install these updates can potentially cause a breach that could've been easily avoided. Keep your operating systems, applications, any IoT firmware, website software, and plugins updated and secure.

3. Investing in upgrading outdated systems

Installing updates on an obsolete system can only take one so far. While it may not be feasible to have the most recent cutting edge technology, it is important to ensure that an organization's connected devices and systems are reasonably modern and can interface with leading security solutions.

4. **Creating offsite backups for all business-critical data**

In case of a successful breach, having an uncorrupted backup ascertains that the business impact is minimal. Especially if you're reliant on data, or have a web presence, backups are a great way to ensure the least possible repercussions on availability. Create at least three copies of backups, on different media and store at least one offsite or on a third-party platform.

5. Formulating an incident response (IR), business continuity and disaster recovery plan (BCP/DR)

In the event of a breach, an organization's level of preparedness is key to the extent of the impact on business operations and availability. Having a documented incident response plan, with well-defined roles and responsibilities, preliminary point of contact, escalation points, recovery strategies, etc. with steps detailing the procedure to be followed when under attack, will eliminate the pressure of instant decision making, reducing error margins and following a pre-planned recovery process. Documenting BCP and DR plans also assist in the same purpose. However, it is not enough to merely document these policies. Conducting scenario based exercises with employees is equally essential as it prepares them on how to respond to a data breach.

6. Conducting third-party vendor risk assessments

Before giving access to the business network to any external third-party vendor, assess their security posture as they may introduce a foothold for an attacker into the company's networks. If the IT team is not equipped to carry out these assessments, get them trained on ISO 27001 standard. Where possible, seek help from an experienced security professional.

7. Establish security policies and agreements at an organizational level

Draw up well-defined information security policy, data classification policy, data disposal policy, physical security policy, confidentiality agreements, non-disclosure agreements, etc. and get employees and vendors to sign off on them before proceeding with an engagement. Review the policies periodically and ensure that your employees and external vendors understand what these policies entail.

8. Investing in the right technology

For most SMBs, it may not be feasible to invest in an enterprise-grade security solution. However, barring a few, there are plenty of open-source free alternatives that can be deployed. Though in some cases they're not as effective as their commercial counterparts, in most situations, they can get the job done fairly well. At any rate, installing free software is better than having no solution to protect your environment. If you're choosing to implement open-source tools, get your IT team to configure them correctly based upon your requirements.

With many organizations continuing to offer remote work benefits, given the situation of global pandemic, it is best practice to install network perimeter security solutions as well as endpoint solutions on host systems. For instance, a network DLP (data loss prevention) will not be able to prevent information leakage from a laptop that's connected to the user's home network. Deploying an endpoint DLP solution,

and blocking the usage of removable media and USB ports, to safeguard against any unauthorized transfer of data, will also prove to be effective.

Recommended open-source security solutions:

The list of tools listed below are either completely free or at least offer a community edition that businesses can choose to explore. There may be restrictions on using the community edition for commercial purposes, depending on the software. So, one must be sure to read the license agreement beforehand.

- Firewall/router– pfsense (https://www.pfsense.org/)
- IDS/IPS – Snort (https://www.snort.org/)
- Vulnerability scanner – Vega(https://subgraph.com/vega/)
- DNS filtering – Quad9 (https://www.quad9.net/)
- DV SSL/TLS Certificates – Let's Encrypt (https://letsencrypt.org/)
- VPN – OpenVPN (https://openvpn.net/community-downloads/)
- Logging and Monitoring – Fluentd (https://www.fluentd.org/download); Apache Flume (https://flume.apache.org/download.html)
- Firewalls with Unified Threat Management functionalities – OPNsense (https://opnsense.org/), Endian Firewall Community (https://sourceforge.net/projects/efw/)
- Antivirus – ClamAV (https://www.clamav.net/downloads)
- Anti-ransomware – Avast (https://www.avast.com/c-ransomware-protection-tool; https://www.avast.com/en-in/ransomware-decryption-tools)
- Other Tools: Apptrana (https://apptrana.indusface.com/) - A web security solution that comes with four services integrated into a single platform – auto scanner, WAF, CDN, and managed services. The basic plan can be tried out free of cost.

9. Get rid of default passwords and implement a strong password policy

In the past, enforcing a strong password policy referred to password strength (minimum 8 characters long), complexity (using lowercase, uppercase, special characters, numbers), periodical changing of password, etc. However, nowadays passphrases ("Hide Keyboardart Mosquitowandgel Insignia") are considered more secure since they're longer, unique, and in most cases easier to remember. Alongside passphrases, using multi-factor authentication that relies on secure factors like using a software-based authenticator instead of an OTP via SMS, can also prevent unauthorized access. It is still vital to avoid reusing passwords across multiple accounts. Consider using a password manager where you only need to remember the master key while the software inputs the other passwords for you. The passwords are encrypted and stored by the password manager and almost none of them store your master key. Hence even if the password manager gets hacked, the attacker can't use your passwords. However, since the master key is stored at the user's end, if your device gets infected by malware that, for example, logs keystrokes, all your accounts may get compromised. Implementing account lockouts after a certain number of unsuccessful tries may also work for you.

When it comes to default login passwords such as the ones in the web interface of IoT devices, or to your website portal, etc. ensure these are changed in accordance with your password policy.

10. Implementing a strong access control policy and physically restricting unauthorized access to computer systems and devices

Access control refers to prevention of unauthorized access to your systems and resources. It entails allowing access to sensitive resources on a need basis that gets revoked once the requirements is fulfilled, verifying if the user requesting access is not only authenticated but also authorized to access the resource,

ISSN: 2233-7857 IJFGCN

etc. Implement an access control list, consider using an identity and access management solution, and use a VPN when connecting to the business network. Administer user accounts on the principle of least privilege, refrain from using administrative accounts except when essential, and regularly review user permissions and decommission old, unused accounts.

V. CONCLUSION

As already discussed, SMBs have developed into easy targets for attackers due to a lack of awareness and initiative from the leadership board and the general apathy towards cybercrime. Small businesses do not invest in security the same way as large corporate firms due to budget constraints, business environment constraints, and internal inefficiencies. However, SMBs form an integral part of our nation's economy and need to be protected against data theft and network breach. Additionally, finding the right resources to implement security checks within the organization can be exhausting due to the shortage of trained personnel in the security industry. According to an estimate by cybersecurity ventures, there will be 3.5 million unfilled cybersecurity jobs globally by 2021. If we look at India specifically, NASSCOM estimates 1 million cybersecurity professionals will be needed here by 2020 and if past trends are any indication, this gap will only continue to grow. We attempted to assess a few such SMBs and provide recommendations for cybersecurity policies and controls that can be implemented in small and mid sized businesses.

REFERENCES

1. "A Prototype to Manage Cybersecurity in Small Companies." – M. Rea-Guaman, JA Calvo-Manzano, T. San Feliu.
2. "Cyber Risk for Small and Medium-Sized Enterprises." – The Janet & Mark L. Goldenson Center for Actuarial Research, University of Connecticut.
3. "2019 Global State of Cybersecurity in Small and Medium-Sized Businesses" – Ponemon Institute, October 2019
4. "Cyber-Security Policy Decisions in Small Businesses" – Joanna Patterson, Walden University.
5. "Implementing Information Security Management System as a part of business processes" – Jari Flyktman
6. "The Impact of Cyber Security on SMEs" – Nabila Amrin, University of Twente
7. "The Invisible Hole of Information on SMB's Cybersecurity" – Ruti Gafni, Tal Pavel, The Academic College of Tel Aviv – Yaffo, Israel.
8. Rahman, S., & Lackey, R. (2013). E-Commerce systems security for small businesses. International Journal of Network Security & Its Applications, 5(2), 193-210. http://dx.doi.org/10.5121/ijnsa.2013.5215
9. Raiyn, J. (2014). A survey of cyber-attack detection strategies. International Journal of Security & its Applications, 8(1), 247-255. http://dx.doi.org/doi:10.14257/ijsia.2014.8.1.23
   Ninth annual cost of cybercrime study – Independently conducted by Ponemon Institute LLC, and jointly developed by Accenture,
   https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf