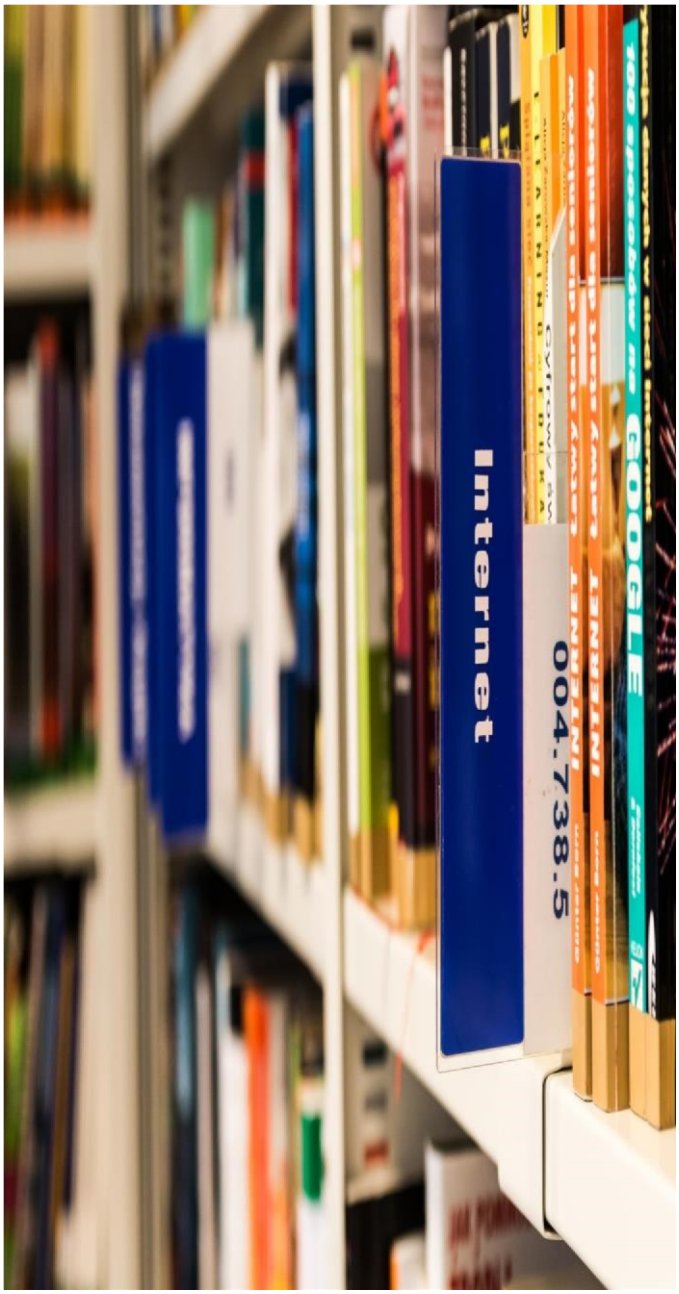

CYBERSECURITY STRATEGY: Policies and Implementation for Medium Size Organizations

Anish Niure
Boxhill Institute

Abstract

This Report Introduce the different scenarios, statistics of the growing cybercrime within the Small and Medium Enterprise in Australia. Cybersecurity not being only the IT matter but overall enterprise-wise concern, how a threat actor can possibly intrude the security culture of an organization. Different types of evolving threat vectors such as Ransomware, Malware, Supply chain attacks, Social Engineering attacks prevailing in the society. The Insiders to State-sponsored threats causes high impact on the security of an Enterprise which mandatories need of effective solution to handle different incidents in the Organization. Formulating different policies, standards and procedures helps organizations for good practices and must consider on all dimensions for secure environment. This report tries to provide include different scenarios and factors for reliable policy. Furthermore, to implement those policies, effective guidelines maintaining compliance, mitigating risks and under being the law how one organization can adopt the proactive mechanisms are discussed in the report.

Table of Contents

Abstract 2

Introduction 3

Why Cybersecurity matters to Small and Medium Enterprises. 4

Threat Landscape: Who is Attacking You? 5

Policies 6

Implementation and Guidelines 11

Conclusion.....13

Introduction

Cybersecurity is emerged as a burning issue, in response, many organizations also seem to evolve from the traditional thinking of cybersecurity governance only as an IT matter, to an enterprise-wide concern. However, the growing landscape of Information Technology has expanded threat, threat actors and threat vectors, has questioned many organizations about their defence layer to protect Confidentiality, Integrity and Availability of their data and service.

Businesses are categorized into different types based on the number of employees and turnover they make annually, and according to Australian Bureau of Statistics (ABS), 99.8 percent of business are small and medium sized [1]. ACSC reports, they receive about 144 reports of cybercrime in a day, which costs about $300 million annual loss. Overall, 62% of the organizations has reported they had experienced cyber security incident at some point, and many were undetected whereas other do not want to open the case because of the fear of reputational risk, above that, many were not found being so much concerned about security strategies, which can be analysed from the report which shows 48% business were spending even less than $500 per year in cybersecurity. Lack of staffs, plan and respond mechanism, guidelines and knowledge in the sector are major issues among small and medium organizations to implement cybersecurity [2].

ACSC [3] provides Eight essential maturity model and [4] gives the strategy for deep analysis and implementation of cybersecurity can be taken as the base to formulate cybersecurity policies and strategies and techniques to carry out those strategies, under being ethics and law of Australia.

Why Cybersecurity matters to Small and Medium Enterprises.

Small and Medium Enterprises are the key drivers of economic activities and more than half of the national revenue is collected by SMEs [5]. While large organizations are comparatively increasing the investment in cybersecurity, SMEs seems lagging, though to maintain overall cybersecurity in a country the policies should start to implement from these industries. Perception towards cybersecurity, financial problem and lack of expertise are the prime causes, however, in this data driven society, the data collected in medium and small organization is equally sensitive, only difference is it is quantitively less, such as personal information, transaction details, sensitive intellectual property information, identity records of costumers and above those most SME acts as the suppliers to the large enterprise, which drives supply chain attacks to large Enterprises, in addition, what if fraudulent actor use the system of SMEs as botnets or just to conduct malicious activity. Many such scenarios had happened in the past such as Target data breach in 2013, recent Netflix ransomware attack and many other [6] [7].

Different types of breach relate different risks, such as financial, reputational, operational, compliance and so on. Organizations comply with PCI DSS regulations and HIPAA requirements, which makes SMEs imposed to maintain cybersecurity.

Threat Landscape: Who is Attacking You?

Report from Australian cybersecurity firm, 43% of cyber-attacks were targeted to SME businesses, where only minimum about 5% businesses' data folders are protected. Ransomware at the top, caused $20 billion lost, with one ransomware in 11 seconds, followed by phishing, hacking, remote access scams and malware attacks [2]. [8] shows, Social Engineering, Business Email Compromise (BEC), Ransomware, Mobile malware, and Supply Chain Compromise as the prominent threats in 20202022.

Have you analysed, how likelihood you can be victim of those threats, because exposing to the internet you are already counted as the threat surface and the type of asset you are owning has increased the risk to be targeted. Simply from Script Kiddies with limited resource and motivation using simple technology can get into your network, think about state sponsored actors and Advance Persistent Threats (APTs), Hacktivists targeting because you can be way for them to get into large Enterprise using large resource. Nonetheless, your competitors or even your employee who are 24 hours monitoring your activities, to revenge you. Moreover, think about the data leaks happen unknowingly, or physically someone robs your systems. Has moving to cloud make you secure or have just increased the threat surface? Is your data exposed to third-parties or shadow IT prevailing in your organization [9].

Further, [10] reports, 76 percent of Australian medium companies are using cloud, and [11] writes SMEs gets data security, Cost Reduction, Disaster recovery, and efficient business plans moving to cloud.

Policies

Policies are high-level statement of management intent. An information security policy is the statement of cybersecurity objectives which includes

- The importance of cybersecurity in an organization,
- Requirements which all members, stakeholders, even third parties comply to follow for the protection of CIA triad,
- Statement of the information possessed by the organization which is designated by staff holding the executive responsible for cybersecurity, commonly, chief information security officer (CISO).

Many organizations tend to have long policies even including the roles and responsibilities of each staff member which meets the needs of that sector; however, they are relatively hard to maintain for long time. Because the policies need to be reviewed and amend in timely manner there is a risk those policies being outdated.

Medium Enterprise organizations varies largely on the sectors of work, resources they own, data they collect and processed and the parties they are involved with. However, this report, purposes the common policies in Information

Security/cybersecurity and provides any organizations ideas about the policies and implementation strategies, based on the policies in [12].

1. Information security policy

Generally, concerns about the confidentiality, integrity, and availability of the data. Policies related to the Data protection, Data Encryption, Data minimization, Data loss prevention and many other techniques are included in this policy. Moreover, the security strategies and different control types such as preventive, detective, or corrective controls needed to an organization. As per the criticality of the data organization can choose to following policies. Some examples that can fits to medium organizations are:

1) Duly verifying every individual coming or going out from the organization or secure premises, and proper authentication and authorization enabled entering the secure rooms with critical data. Fences, alarm, biometric scanners, cc cameras etc.
2) Firewalls, encryption system enabled for the protection of data as the preventive measures for the data in motion or data at rest.
3) Analysing the importance of data, protected with different mechanisms such as hashing, tokenization, masking and so on.
4) Data loss prevention system (DLP) in the systems or network, placed to match and block important data going out to the network and to protect systems form harmful removable devices.
5) Regular use of Intrusion detection system, Security Intrusion Monitoring system (SIEM) placed to identify events detection.
6) Data backup technique with proper encryption in secure servers or cloud for remediation of data loss.

7) Companies can do Cybersecurity Insurance to minimize risk.

2. Acceptable Use Policy [13].

These are the policies with the clear direction or permission to use and access the information resources within an organization or remotely. The regulations can be controlled for the use of User IDs, passwords or tokens, resources regulated or assigned by the organization. The policy should define the conditions, responsibilities, and liabilities for the usage of organization resources. According to different types of organizations, policies can be conducted. Following are some policies for some scenarios:

1) The usage of the provided credentials – Limiting, securing, protecting the given credentials.
2) Usage of software's, regulations for protection from wireless and BYOD systems.
3) Control statements for the unauthorised change, access, breach, or usage of the resources.
4) Delegation of the way to use the communication system such as Email, Software, network in proper way.
5) Handling the data, resources outside the organization network and remotely accessing the organization resources.

3. Data governance, classification, or retention Policies

Data governance Policy clearly state the ownership of information created or used by organization. Different consideration such as data classification standard, data handling Guidelines should be taken formulating these policies. Not every organization comes or have to regulate

with these policies, however, anywhere applicable maintaining these activities protects to be safe from laws and compliance. The main purpose of this policy is,

1) Defining the roles and responsibilities for data creation, usage, conditions and determine the liabilities.
2) Secure and best practices for data protection and management.
3) Ensuring the organization complies with applicable laws, and standards.
4) Documenting the activities while accessing, retrieving, exchanging, reporting, and storing the data
5) Data classification, achieving or deletion policies under being the regulations.

4. Credential Management and Password Policies

Policies for the management of credentials throughout set up a credential to retain the credentials. Policies restricting the specific requirements for employees, third parties help for the credentials management and identification. Credentials are also helpful to maintain access policies in different systems. The complexity, length, and reuse and so on are the essential and best practices. Some policies can be:

1) Disable the root account for remote login.
2) Read only credentials used for different monitoring files or databases to prevent mistakenly execute of files or codes.
3) Password complexity, password managers for the strong password policy.
4) Two factor authentication where possible.

5. Continuous monitoring policy

The policy undertakes the continuous monitoring and informing the employees, visitors, or contractors in the organizations about their activity being monitored, whether it is technical monitoring such as logs or events or the physical activities using cccameras. These types of activities help for the identification, and protection from the unusual behaviour in the organization. Examples:

1) Placing the video cameras and microphones inside and outside of the organizations for analysing activities ongoing in an organization.
2) Informing that they are being monitored by placing hoarding boards.
3) Logging actives using event managers for detection of fraudulent activities done in organizations resources.

6. Change management and change control Policies:

These policies describe the process regarding the reviewing, approving, and implementing the purposed changes to information system for managing both cybersecurity and operational risks.

7. Asset Management:

Asset identification and management in any organization is must to identify, protect, detect, respond, and recover the data. There are different types of assets such as devices, software, network, users. Good policies should be implemented while accepting, tracking the assets and proper disposal policies should regulated by an organization.

8. Code of Conduct/Ethics

Policies about the behaviours that every staff, stakeholders, and affiliates should maintain in the organization. The codes further contain the situations not specified on any other policies.

Above mentioned were different types of policies that are commonly included in information security library of an organization. However, different types of organizations must maintain different types of standards they are with, for the continuity of business and compliance with other third parties, laws and regulations in that country, organizations must adopt their policies accordingly. Furthermore, ISO 27001, [14] is the detail resource for maintaining cybersecurity framework and for guideline for creating policies in cybersecurity.

Implementation and Guidelines

The research done by [6] shows, 80% of SMEs would have serious impact in their business within a week and nearly 60% business would collapse if any crucial cyberattack happens to their organization. No one can deny their system cannot be attacked at this time, however, the response mechanism, plan, and strategy they have taken against the threat can heavily affect the recovery and continuity of their business, because following good practices gives opportunity to become

trustworthy among costumers and improve reputation. Different incident/threats have different types of response, and are always related with Technology, People and Process in the organization. Because we have already said cybersecurity is not only an IT or technical matter, but all processes and people are responsible. For example, to respond volume-based attacks such as phishing, ransomware technical responses are must along with awareness, and to response invoice scam attacks that looks perfectly legitimate, asking to pay the bills, that totally depends on the people and process how the payment system processes, regulations with banks and so on which should be determined by policies.

Furthermore, an organization should create Standards which are mandatory requirements describing the process that an organization will carry out its information policies, In addition, Monitoring procedures describing the process the organization performing the security monitoring activities, the procedures how the organization responds to follow the law infringements, also legal notices to collect digital evidences, nonetheless, the procedures for application and system patching under the organization care and many more. In addition, having proper guidelines help for the ease of deployment of policies.

Often organizations must deal with unforeseen circumstances proper control mechanisms to handle exceptions while adapting new security policies and procedures, for the continuity of the business, should also be provided. To reduce the risk associated with the exceptions to the policies organizations might requires compensating controls. For example, if an organization requires to use outdated version of operating system, to run specific software needed for continuity of business, can deny by the policy and standards, comes as an exception, however, to mitigate the risk by using

the operating in isolated network with limited access can be taken as compensation control.

We cannot unsee the fact that organizations face different types of security compliance requirements. For example, if the organization is associated with PCI DSS, HIPPA, other thirdparty risk managements such as Service Level Agreements (SLAs), Business Partnership agreements (BPAs), Vendor relationship and different criteria from the national and state laws, policies should comply with these factors for the overall risk assessments that affect their operations.

Cyber security strategy helps organizations to take proactive approach to the security because being reactive is time consuming and expensive. The main objective is to attain highest level of precautions without affecting the business continuity and one organization can achieve this following some Frameworks such as ISO 27001 or NIST which as wellknown guidelines that enables to effectively track the progress and evaluate the effectiveness of the measures that is being applied [15].
Finally, the security control verification and quality controls are must to verify that any organization has sufficient security controls and are functioning properly. Conducting security programs with proper procedures for regular internal tests by doing audits and assessments helps for the evaluation of compliance and amendments of cybersecurity policies [16].

Conclusion

In the conclusion, cybersecurity has become the growing concern because of the increased in threat landscape and the cyber threat. Cybersecurity has not only been the technological issue but the overall organizational matter. Maintaining the cybersecurity one organizational should consider from all the dimensions, that a breach can happen. Despite of the growing cyberwarfare, many organizations, specially, small to medium organizations have not successfully able to maintain secure environment in the organization due to lack of proper methodology, staffs and guidelines and the traditional concept of the business owners and stakeholders. However, the reality opposes that for the overall growth of business, maintain cybersecurity is must otherwise it will be hard for one to meet the compliance and continuation of the business. Formulating cybersecurity policy organizations should consider different aspects form different dimensions where information security policy, data governance, data classification, data retention policies, Credential management policy, Password policy, Assets management policies are some crucial policy types. In addition to the policies, organization should consider Standards, Procedures, Guidelines as the supportive regulations in the organizations. Many exceptions and compliance controls are necessary for risk management of unwilling incidents, moreover, the third party's compliance requirements, Service level agreements while dealing with other vendors should be well analysed, well documented and matched with policies under being law of any country is must. Overall, any organizations can map their improvements and achieve strong workflow and measure effectiveness of policies using standards documents such as NIST and ISO 27001. Finally, doing regular audits and assessments help for the evaluation and amendments of cybersecurity policies.

References

[1] Moula, "SME Defination: What is an SME in Australia?," 06 07 2021. [Online]. Available: https://moula.com.au/small-business/sme-definition-australia. [Accessed 30 10 2022].

[2] Australian cyber Security centre, "Cyber Security and," 2021. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2020-07/ACSC%20Small%20Business%20Survey%20Report.pdf. [Accessed 30 10 2022].

[3] Australian Cyber Security Centre, "Essential Eight Maturity Mode," 10 2021. [Online]. Available: https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28October%202021%29.pdf.

[4] Cyber Security Industry Advisory Committee, "Cyber Security Industry Advisory Committee Anual Report 2022," 2022. [Online]. Available: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IACannual-report-2022.pdf. [Accessed 30 10 2022].

[5] CSIRO, "SMEs key to driving growth in Australia Simon Hanson, CSIRO SME Director," 27 06 2022. [Online]. Available: https://www.csiro.au/en/news/news-releases/2022/small-and-medium-businesses-key-to-drivinggrowth-in-australia.

[6] ENSA, "Cybersecurity for smes," ensa.europa.eu, europe, 2021.

[7] imperva, "supply chain attack," imperva, [Online]. Available: https://www.imperva.com/learn/applicationsecurity/supply-chain-attack/. [Accessed 31 10 2022].

[8] B. Tsouvalas, "Cybercrime on the Rise in 2022, after Australians Lost Over $300 million to Scams Last Year," 17 10 2022. [Online]. Available: https://www.savvy.com.au/media-releases/cybercrime-in-australiareport/#:~:text=The%20virus%20crisis%20is%20fuelling,million%20in%20the%20first%20quarter.. [Accessed 30 10 2022].

[9] D. S. Mike Chapple, "Threat LandScape," in *compTIA Security + Study Guide*, sybex, 2022, pp. 19-40.

[10] N. Arboleda, "More Aussie businesses using cloud technology: ABS," 07 06 2021. [Online]. Available: https://www.crn.com.au/news/more-aussie-businesses-using-cloud-technology-abs-565524. [Accessed 30 10 2022].

[11] Chris karapetcoff, "More Reasons to Choose Cloud Computing for Small and Medium Businesses," [Online]. Available: https://computingaustralia.com.au/cloud-computing-for-small-and-mediumbusinesses/#:~:text=Cloud%20computing%20can%20provide%20significant,with%20traditional%20on%2Dpremis e%20infrastructure.. [Accessed 2022 10 30].

[12] M. C. a. D. Seidl, CompTIA Security+ Guide (eight edition), sybex, 2022.

[13] Acme Corporation, "Sample Acceptable Usage Policy," [Online]. Available: https://www.getsafeonline.org/wp-content/uploads/2014/10/Sample_Acceptable_Usage_Policy.pdf.

[14] HighTable, "ISO 27001 Policies Ultimate Guide 2022," [Online]. Available: https://hightable.io/iso-27001-policies/. [Accessed 31 10 2022].

[15] OWASP, "OWASP Cyber Defense Matrix," [Online]. Available: https://owasp.org/www-project-cyber-defense/matrix/. [Accessed 31 10 2022].

[16] D. S. Mike Chapple, "Security Policies, Standards and Compliance," in *CompTIA Security+ Study Guide Eight Edition*, sybex, 2022, pp. 511 - 539.

[17 Z. Thompson, "Australian Budget 2022 bolsters cyber security secto," 30 03 2022. [Online]. Available:
] https://cfotech.com.au/story/australian-budget-2022-bolsters-cyber-security-sector. [Accessed 30 10 2022].