# BUSINESS DOMAIN-SPECIFIC LEAST CYBERSECURITY CONTROLS IMPLEMENTATION (BDSLCCI) FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMES)

by

Shekhar Ashok Pawar, DBA Research Scholar

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

AUGUST, 2022

BUSINESS DOMAIN-SPECIFIC CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMES)

by

Shekhar Ashok Pawar, DBA Research Scholar

APPROVED BY

Dr. Ivana Nobilo, Ph. D., Chair

Anna Provodnikova

Dr. Anna Provodnikova, Ph. D., Co-Chair

Dr Hemant Palivela, Ph.D, Research Supervisor

RECEIVED/APPROVED BY:

<Associate Dean’s Name, Degree>, Associate Dean

## Dedication

THIS DISSERTATION IS DEDICATED TO ALL SMALL AND MEDIUM ENTERPRISES WHO ARE WILLING TO IMPROVE CYBERSECURITY POSTURE BUT NOT ABLE TO FIND A SUITABLE ROADMAP THAT WILL BE SUITABLE FOR THEIR BUSINESS DOMAIN AND INVESTMENTS.

## Acknowledgments

Firstly, I want to thank my organization, “GrassDew IT Solutions,” for providing me with the platform to work for many years in the cybersecurity domain in many countries, where I have gained knowledge of ground-level problems faced by different organizations when it comes to cybersecurity implementation. I also want to thank my teammates, my clients, and my mentors for their continuous support and motivation in this journey. Secondly, I want to thank the dissertation chair of my research and supervisor, Professor Dr. Hemant Palivela, for the continuous support, advice, comments and criticism, and encouragement throughout this dissertation's development. Thirdly, I take the opportunity to thank SSBM management and staff for granting me the opportunity to study at a high-caliber business school and all the doctoral students and colleagues for their contributions during the study. I wish to thank all the enterprises who contributed with their valuable inputs to this research study. Without their true input of crucial cybersecurity information on their own, I could not have gathered knowledge of real problems and further pointed solutions. Finally, I want to share that my wife Poonam, my son Omkar, and my parents also helped me in many ways when I was engaged in my studies after office working hours and I was allowed to focus on my research studies, pulling quite a large amount of quality family time. I also want to share my deep gratitude towards the lotus feet of my beloved master, Osho, for blessed teachings related to the meditation journey which have helped me to remain focused and witness this success. I want to dedicate this research to all of them.

# ABSTRACT

## BUSINESS DOMAIN-SPECIFIC CYBERSECURITY FRAMEWORK FOR SMALL AND MEDIUM ENTERPRISES (SMES)

Shekhar Ashok Pawar
2022

Dissertation Chair: Dr Ivana Nobilo
Co-Chair: Dr Anna Provodnikova

SMEs (Small and Medium Enterprises) are the most important contributors to the global economy, accounting for over two-thirds of worldwide job opportunities and more than half the GDP of the developed economies. It is also very visible through various cyber-attack statistics and news that they are the most vulnerable to cyber threats, with major consequences for their continued existence if successful cyber-attacks by cybercriminals are carried out. With the existence of different ecosystems reliant on them, there is a growing need to defend the entire SME segment from cyber threats. There are currently no solid security standards or frameworks in place for any organization, given the large number of cyber-attacks targeting SMEs followed by successful cybercrimes. It is one of the main reasons this research was more interested in identifying probable gaps in their adoption. There is a need to comprehend the issues that the SME segment faces, particularly in terms of planning and successfully implementing cybersecurity standards, frameworks, or controls to be cyber secure. This research thesis will be a good attempt to shed light on the current cybersecurity posture having various controls implemented within different types of SMEs, as well as the challenges they are facing about the same. This research will try to find the reason that is preventing them from deciding, planning, and implementing cybersecurity controls. I would like to thank the top management of one hundred and fifteen SMEs who voluntarily participated in the research survey conducted by us. In addition, based on the analysis of their valuable inputs and keeping the core cybersecurity principles at the center of the new implementation strategy, this research study will present a recommended solution that will assist any SME by providing a few directions to overcome the obstacles they are encountering in enhancing their cybersecurity posture. According to the research findings, more than half of SMEs lack cybersecurity standards or structures. It was interesting to know that their top four obstacles which are stopping them from going ahead with the implementation of cybersecurity controls are (i) cost involved in implementing cybersecurity controls, (ii) lack of resources to implement and maintain, (iii) not finding a roadmap to invest in cybersecurity control implementation, and (iv) available cybersecurity standards or frameworks need a big investment. To design the recommended solution for the SMEs, research interviews were conducted among the top management of SMEs to understand the critical assets contributing to their business. This research also gave a few more inputs about important components they are more concerned about. Taking these inputs while providing the recommended solution to the problems identified, research has considered a few unavoidable or must-have cybersecurity controls implementation and safeguarding BDSMCA based on domain-wise prioritization of Confidentiality, Integrity, and Availability (CIA triad). This strategic solution design can help SMEs in a particular business domain. The Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI) framework is the probable recommended solution as a result of the research, which is the actual step-by-step

implementation of cybersecurity controls, contributing to each and/or multiple areas in the CIA triad considering BDSMCAs.

# KEYWORDS

Small and Medium Enterprise (SME), cybersecurity, cybersecurity controls, physical controls, logical controls, technical controls, administrative controls, business domain

## LIST OF ABBREVIATIONS

**AI**: Artificial Intelligence

**BDSC Framework**: Business Domain-Specific Cybersecurity Framework

**BDSLCCI**: Business Domain-Specific Least Cybersecurity Controls Implementation

**BDSMCA**: Business Domain-Specific Mission Critical Asset

**BDSMCAS Level**: Business Domain-Specific Mission Critical Asset Security Level

**BFSI**: Banking, Financial Services, and Insurance

**CC**: Common Criteria

**CI**: Critical Infrastructure

**CIA triad**: Confidentiality, Integrity, and Availability triad

**CIS**: Critical Infrastructure System

**COBIT**: Control Objectives for Information and Related Technology

**CSCRM**: Cyber Supply Chain Risk Management

**DCS**: Distributed Control System

**DiD**: Defense in Depth

**EMR**: Electronic Medical Record

**ERP**: Enterprise Resource Planning

**FERPA**: Family Educational Rights and Privacy Act

**FISMA**: Federal Information Security Modernization Act

**FMEA**: Failure Mode Effect Analysis

**FMCG**: Fast-Moving Consumer Goods

**FTA**: Fault Tree Analysis

**GDPR**: General Data Protection Regulation

**GRC**: Governance, Risk Management, and Compliance

**HIPAA**: Health Insurance Portability and Accountability Act

**HMI**: Human Machine Interface

**HHM**: Hierarchical Holographic Modeling

**ICS**: Industrial Control System

**ICT**: Information and Communications Technology

**IIoT**: Industrial Internet of Things

**IoT**: Internet of Things

**ISO**: The International Organization for Standardization

**MCA**: Mission Critical Asset

**MOCCI Level**: Minimum Overall Cybersecurity Controls Implementation Level

**NIST**: National Institute of Standards and Technology

**NIST CSF**: NIST Cyber Security Framework for Critical Infrastructure

**OCTAVE**: Operationally Critical Threat, Asset, and Vulnerability Evaluation

**OS**: Operating System

**OT**: Operating Technology

**PII**: Personally Identifiable Information

**PLC**: Programmable Logic Controller

**PRA**: Probabilistic Risk Assessment

**R&D**: Research and Development

**RTU:** Remote Terminal Unit

**SCADA**: Supervisory Control And Data Acquisition

**SME**: Small and Medium Enterprise

**SSE-CMM**: System Security Engineering-Capability and Maturity Model

**VAPT**: Vulnerability Assessment and Penetration Testing

**VM:** Virtual Machine

TABLE OF CONTENTS

# LIST OF TABLES

## LIST OF FIGURES

# CHAPTER I:
# CONCEPTUAL FRAMEWORK

## 1.1 Introduction

According to the World Trade Organization, SMEs account for more than 90% of the business population, 60% to 70% of employment, and 55% of developed economies' GDP (WTO, 2016). There are over 400 million SMEs in the world, which are the backbone of the global economy. The most evident existing challenges among most SMEs across various countries are a lack of cash, a lack of experienced top management, and a lack of technical skilled resources for ICT (PETKOVSKA, 2015; Duan, 2002; Emine, 2012; Farsi, 2014; Moeuf, 2017; Muriithi, 2017; Ramukumba, 2014; Khalique, 2011). Recent decades have seen increased exposure of SMEs to cyber threats due to the increase in the use of digitalized platforms. It is important to protect, sustain and grow the SME segment as it plays a key role in the global economy. This research is going to focus on identifying the root causes of why SMEs are not able to protect themselves against cyber-attacks.

## 1.2 Emergence and justification of the problem

The general business sector has moved into the digital era over the previous few decades, but cyber threats have increased globally as a result. SMEs now have a bigger attack surface than ever before since many of them are gradually shifting away from traditional methods and toward greater use of the Internet and cloud to meet their digital needs. SME's have a "one in two" probability of experiencing a cyber breach, according to the NCSC (SENSEON, 2019). According to recent figures, cybercriminals are targeting 43 percent of small businesses, and it's crucial to note that

60 percent of small firms that are victims of such cyber-attacks close their businesses within six months. According to statistics, cybercrime costs small and medium businesses more than $2.2 million every year (Shepherd, 2019). Every SME is trying to expand its IT assets due to the increasing demand for digitization for any business to go to the next level. As a result of this, SMEs are now more vulnerable to cyber threats. Cybercriminals are not just targeting SMEs, but they are also posing the greatest threat to the SMEs' dependent ecosystem and hence threatening the global economy. Many hacks can wreak havoc on SMEs' long-term viability and growth by causing financial and reputational losses in a variety of sectors. Existing cybersecurity standards and regulations are extremely good, but "why they are not beneficial to SMEs" needs to be examined, especially with the increasing number of cyber-attack victims SMEs. Motivation, capacity, opportunity, and impact all play a role in the threat to the SME segment (Blyth, 2001). Insignificant, mild, moderate, substantial, or catastrophic impacts are all possible when it comes to cybercrime. A negligible impact implies that no actual loss has occurred, even if improper use of the item has occurred; it can simply be ignored. A mild asset loss with no business impact is classified as a minor impact. Even these can be given a low priority rating. The moderate impact produces business disruption and has a medium impact. The substantial or catastrophic impact is far more serious since it can hurt the enterprise in different ways. It must be addressed immediately by putting in place remedies. To avoid disastrous consequences caused by a new cyber danger that the organization has not yet recognized, enterprises must have up-to-date information about the current and ongoing cyber risks. It is important to study the various gaps faced by SMEs while implementing cybersecurity controls to protect themselves against rising cyber-attacks, as those are a threat to the ecosystem which is dependent on the SME segment.

### 1.3 Statement of the problem

SMEs play an important role in global employment opportunities, GDP, and the global economy. These organizations are facing many cyber threats with growing digitization. It is important to know if there are any issues faced by these organizations while implementing a good cybersecurity posture to protect themselves against such threats. This study will focus on identifying numerous cybersecurity implementation gaps in the SME segment, which are contributing to rising cyber threat risk and inflicting damage to the economy established by SMEs.

### 1.4 Definitions of the terms used in the study

Generally, an SME can be characterized as a non-subsidiary, independent firm that employs a particular number of employees, also based on a yearly turnover range. This term has different meanings in different nations. It indicates that SMEs are critical for job creation and economic growth and that if they are struggling, it will negatively impact both of these factors, as well as GDP.

Invoking the existing broader definition of a cyber threat for an organization (NIST - Cyber Threat - Definition, 2018), a cyber threat for an SME can be defined as an unauthorized access/destruction/disclosure/modification of information and/or denial of service on an SME's information system that has the potential to negatively impact its operations, its mission/functions/reputation/image, its assets/individuals associated with it, other organizations linked to it, or even its impact on a specific state/country. Invoking the current broader definition of cyber risk for an organization (NIST - Cyber Risk - Definition, 2018), a cyber threat for an SME can be defined as an unauthorized access/destruction/disclosure/modification of information and/or denial of service on an SME's information system that has the potential to negatively impact its operations, its mission/functions/reputation/image, its assets/individuals associated with it, other organizations linked to it, or even the impact on a specific state/country.

In a nutshell, the risk is a function of asset value, vulnerability, and the possibility of exploiting that vulnerability (Ayyub, 2001; Bavisi, 2009; Bernd, 2007; Ciampa, 2004; Denning, 2003; Dhillon, 2000; Dondo, 2007; ITU-T, 2005; Katsikas, 2009; Parker, 2002; Perfilieva, 2011; Shaurette, 2002; Walker, 2009; Whitman, 2005; Zadeh, 1975; Zimmerman, 1995). It can be written as below.

$$\textbf{Risk}_{\textbf{threat}} = f\,(\textbf{Threat}_{\textbf{asset}}, \textbf{Vulnerability}_{\textbf{threat}}, \textbf{Asset Value})$$

Threat agents can be divided into several kinds based on their intent and methods for pursuing the victim. Threat agents performing cybercrime or malicious activities might be hired by unethical competitors of the enterprise or other unethical entities with different purposes. Insider threat agents include partners, company employees, contractors, vendors, maintenance team, security team, security guards, operations workers, and cleaners, among others. Worms, trojan horses, logic bombs, viruses, and other non-target-specific threat agents are examples of various creations which are created by cybercriminals to perform malicious activities on their victims. Terrorist threat agents can be political, religious, or anarchists. Media, activists, political entities, religions, governments, the general population, extremists, vandals, and enthusiasts are all examples of ESA threat agents. Cybercriminal gangs that are involved in organized crime are also threat agents. Fire, flood, lightning, vermin, wind, sand, frost, earthquakes, and other natural calamities are examples of natural disaster threats. By learning from the COVID-19 pandemic, a pandemic can also be deemed a natural disaster too. Apart from all these nation-states, specific threat agents are also active. Any threat agent must have three things to exploit any vulnerability in an enterprise or asset: capability, opportunity, and motivation (Vidalis, 2005).

### 1.5 Objective of the study

Direct input from SMEs will be taken into account in this study via a research survey. Top management, c-level executives, directors, and SME owners are among the survey's participants. In addition, this study survey was carried out across a variety of company categories. A gap analysis of the SME segment's present cybersecurity posture and the targeted minimum cybersecurity maturity level they should achieve to reduce cyber threat risks. Because SMEs play such a vital part in the global economy, ongoing innovation is even more important for them. SMEs have a significant impact on the competitiveness and economic prosperity of the country to which they belong (PETKOVSKA, 2015).

**Specific Aims**

- To listen to the top management of SMEs to understand the current cybersecurity control implementation within their organization
- Identify the security risks by assessing gaps in current cybersecurity implementation within SMEs
- To provide a structured recommended solution that should be solving problems identified in research studies by taking few inputs from SMEs

### 1.6 Delimitations of the study

This research will consider organizations that fall under the SME segment regardless of their location. It will try to get insights about the internal cybersecurity posture of the participant SME, which is internal as well as somewhat confidential information about the organization that will be difficult for the top management to share.

### 1.7 Educational implications and significance of the study

Information security and cybersecurity are frequently used interchangeably. Although this is not the case, there is an overlap between these terms. According to the ISO definition, "cybersecurity" means maintaining the CIA Triad requirement for information in cyberspace. It goes on to explain that cyberspace is made up of tangible entities that are linked to or connected to the internet. In a nutshell, information security is the protection of data as an asset from cyber threats and vulnerabilities, whereas cybersecurity is the protection of cyberspace and all assets present in that cyberspace (Bay, 2016). It's vital to remember that cyberspace encompasses not just entities linked to the internet, but also entities communicating with one another without using the internet. One of the subgroups is Cyberspace, which is part of the Internet. There are two types of cyber assets, or ICT assets: tangible and intangible. Information, data, intellectual property, goodwill, reputation, a market image, service, software programs, and applications are examples of intangible assets. Hardware, storage media, equipment, machines, prints, and end-users are examples of tangible assets (Ozier, 2002).

Asset value changes depending on the relevance of the asset to the company. Asset value may be determined even using the CIA triad. It is determined by the cost, sensitivity, and criticality of the asset, as well as the amount of maintenance and administrative effort required for the same (Fisch, 2000). Viruses, unauthorized access, theft of the organization's proprietary information, DoS attack, insider threat, laptop theft, financial fraud, misuse of a public-facing web application, system penetration by unauthorized entities, wireless network abuse, sabotage, telecommunication fraud, website defacement, and many other security issues can affect cyberspace (Fenz, 2005). Furthermore, relationships between high-level layers of physical objects, systems, applications, people, and processes shape cyberspace as a whole. In short, cyberspace is incomplete without taking into account people, processes, and technology, as well as their interactions with each other, and whether or not they are connected to the internet (Daras, 2018). This study will aid in determining the fundamental, or root-level, difficulties that SMEs face in protecting cyberspace. The survey will try to find a few new ground-level implementation statistics of cybersecurity controls among different SMEs and will try to comprehend cybersecurity control level implementation gaps, in addition to valuable inputs from various existing research literature available to date. The goal of this study is to find hidden pointers that will help SMEs articulate problems and offer solutions.

# CHAPTER II:
# REVIEW OF LITERATURE

## 2.1 Introduction: Background of Existing Cybersecurity Standards for Enterprises

Today, every business considers ISO/IEC 27001, which is widely used for defining ISMS (information security management system) requirements (ISO, 2013). There are 114 controls in ISO 27001:2013, which are related to 14 different security domain objectives (Shojaie, 2014). ISO/IEC 27002:2013 is a set of instructions that aid in the application of the controls outlined in ISO 27001:2013 (Sukmaji, 2021). ISO 27001 provides extensive coverage of each clause, which is backed up by specific security objectives and measures. The COBIT maturity model is primarily utilized in IT governance, with a focus on auditing, procedural awareness, and adaptability (Nasser, 2017). NIST also offers a useful structure for cybersecurity, with five basic tasks that begin with "Identify," then "Protect," then "Detect," then "Respond," and lastly "Recover" (Keller, 2019). NIST has released a framework for small and medium businesses (SMBs) that is based on these five functions once again (Swenson, 2016). NIST Special Publication 800-53 Revision 4 distributes approximately 900 or more distinct security controls from 18 control families, assisting in risk reduction, information protection, the overall cybersecurity framework, and security standards (Bodeau, 2013). The NIST CSF is the most recent framework for a risk-based approach. There are five functional domains, 22 categories, and 98 subcategories within them (Almuhammadi, 2017). The implementation of the NIST framework still requires a significant amount of resources, and several areas have yet to be effectively mapped within it. Since smaller organizations are still doubtful about their potential as attack targets, they see little point in adopting the framework where they think that there is little or no risk of occurrence (GAO, 2018). Even so, there are a few gaps in this framework, and it is still improving (Alsinawi, 2018). According to the Zero Trust concept, businesses should not trust any outside or internal connections to their systems but should instead verify anything that tries to connect (Pratt, 2018). When developing apps, processes, or data handling methods, many businesses, regardless of their various areas, rarely consider the necessity for isolation. The traditional perimeter is dissolving in today's fast-paced digital era. As it is a data and identity-centric paradigm, zero trust assists businesses in overcoming a variety of security difficulties (Kindervag, 2016). Zero Trust Security protects any enterprise from the inside out, but it will cost a lot of money and demand a high level of cybersecurity maturity to deploy. Along with the aforementioned, there are a plethora of other cybersecurity standards, principles, and frameworks that, when effectively implemented, not only reduce cyber-attack risks but also take an enterprise towards good cyber security maturity. The survey will discuss a few of the earlier studies that identified several challenges that SMEs have while implementing information security standards like CC, SSE-CMM, and ISO/IEC 27001. The problems found could make it difficult for SMEs to execute a robust security policy to protect their data and online services. The security objectives of IT goods or system operational settings are more important to CC (Bialas, 2011). While CC can be quite beneficial for analyzing the security of IT goods, the studies point out that the method is time-consuming. Due to the dynamic nature of business, enterprises do not have time to develop the CC's protection profile, wait for vendors to prepare their goal for the evaluation, and then ask a testing laboratory to accredit the product. As a result of the same, the CC's overall procedure is lengthy, costly, and inconvenient for enterprises. SSE-CMM is divided into two sections: System Security Engineering (SSE) and Capability Maturity Model (CMM). SSE-CMM is made up of eleven process areas, each of which is mapped to one of five CMM levels. Initial, repeatable, defined, managed, and optimized are the five maturity levels. The organization adopts IT reactively at first, which means there is no prior preparation. If a business follows a pattern for completing operations connected to managing IT governance without a well-defined or formal approach, it is termed repeatable or maturity level 2. When an organization has formal written standard operating procedures that are followed by all stakeholders throughout the business, it is considered to be at maturity level 3. An organization is deemed level 4 or at the management level if it has quantitative measures or various indicators that help measure particular objectives of every application in IT. An organization is considered optimal or at level 5 if it has embraced IT governance best practices (Kurniawan, 2018). According to the findings, SSE-CMM does not describe specific processes. Instead, it provides suggestions that can be used regardless of the procedures that are carried out. As a result, the new modified version of the standard, which combines e-Business processes with security engineering activities, may be useful for evaluating the maturity of security practices in e-Business firms. Also, the ISO/IEC 27001 standard permits enterprises to design their information security management systems, but it does not specify any technique or method for doing so (ISMS). On the other hand, few enterprises are discouraged by this because they lack security expertise and the ability to construct an ISMS (Alqatawna, 2019). When the survey tried to highlight current cybersecurity standards or framework references to what they serve to enterprises, some of them appeared as shown in Figure 2.1.  It has several cybersecurity controls which need to be satisfied to qualify for a particular standard or framework, which might not be relevant to the business domain that the enterprise is working in.

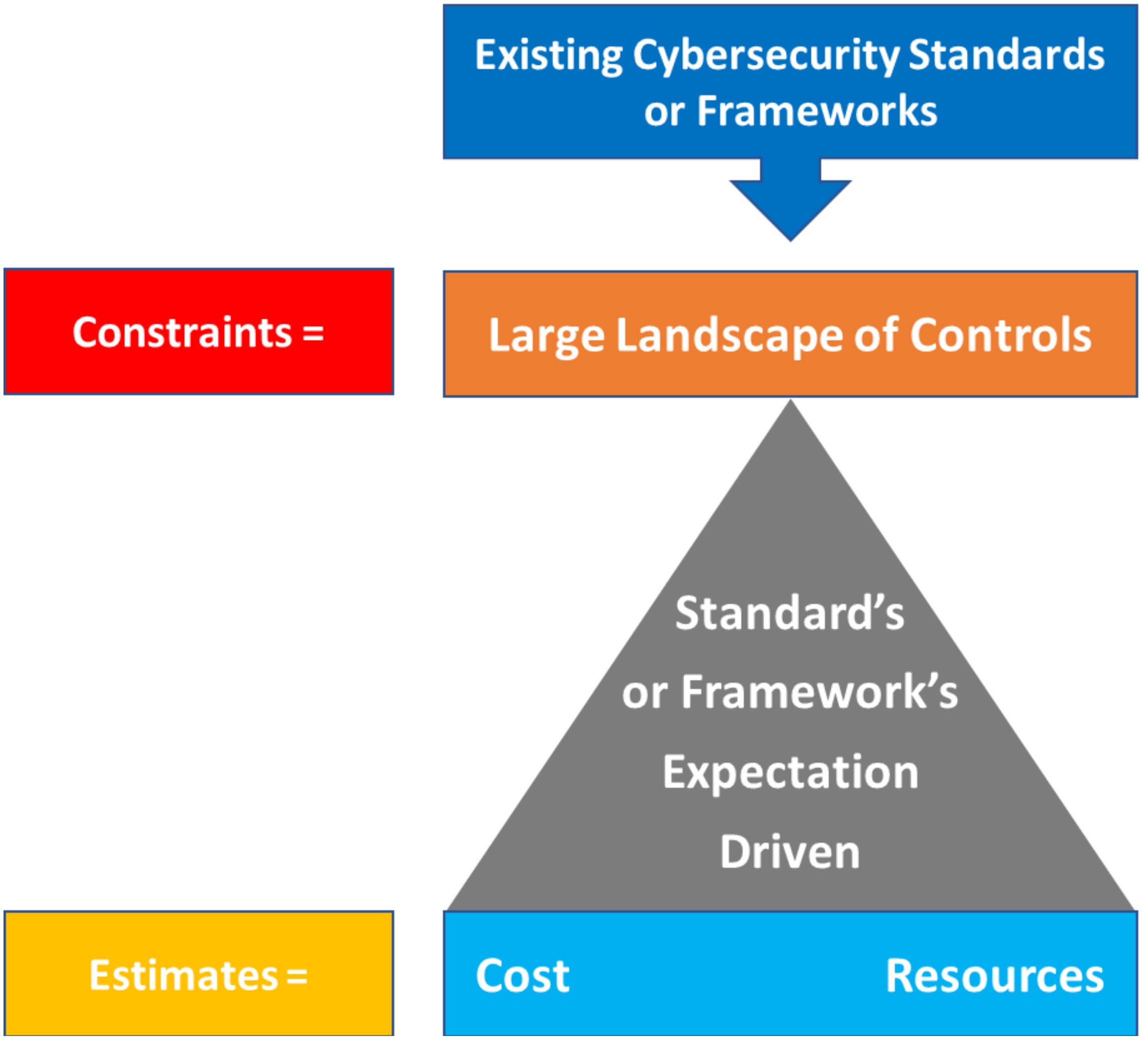

Existing Cybersecurity Standards or Frameworks
Constraints =
Large Landscape of Controls
Standard's or Framework's Expectation Driven
Estimates =
Cost
Resources

*Figure 2.1*
*Existing Standards or Framework*

### 2.1.1 Core Cybersecurity Concepts

For more than four decades, the CIA triad has always been a vital contributor to successful security designs. It's hardly surprising that it will hold its value in the long run.

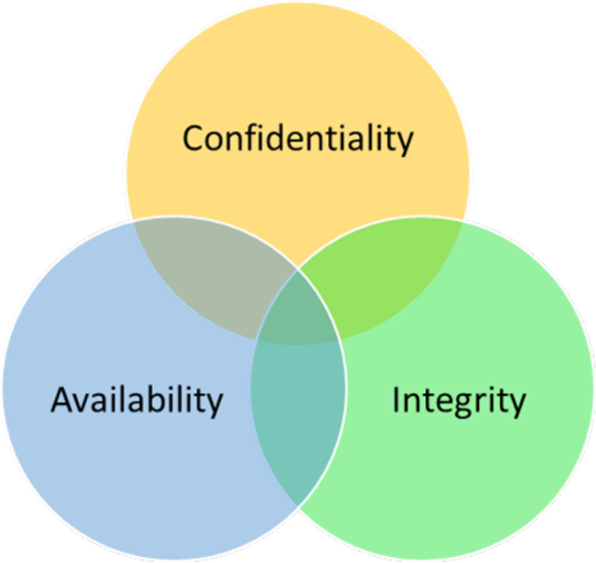


*Figure 2.2*
*CIA Triad*

The CIA triad can yet satisfy other criteria of sociotechnical security literature. Authenticity, Non-repudiation, Responsibility, Personal Integrity, and Ethicality, for example, can all be satisfied by Integrity in the CIA triad. Integrity and availability are used to ensure that the specification is correct. Confidentiality and integrity are the foundations of trust. Identity management can also be accomplished by all three members of the CIA triad. Classic security models such as the Bell-LaPadula, Biba, and Clarke Wilson Security Model have had a strong presence for the past 50 years. The Bell-LaPadula security model focuses on maintaining confidentiality, whereas the Biba model focuses on increasing integrity, and the Clarke Wilson Security Model is a more advanced model that aids in maintaining integrity in a well-formed transaction. The CIA triad serves as the foundation for all of these concepts (Samonas and Coss, 2014). Without the CIA triad, none of the security models can be constructed. By applying the CIA at both the organizational and individual levels, information security issues can be reduced. Individuals are in charge of the organization's human layer of DiD as well as its strategic information security posture should be strengthened for information security (Yee, 2021). From top to bottom, the same can be true for every company's cybersecurity deployment. Furthermore, any organization that tries to satisfy one of the CIA triad's elements will naturally contribute to at least a small part of the other two – as seen in the Venn diagram of Figure 2.2. The CIA triad can still satisfy other criteria of sociotechnical security literature. Authenticity, Non-repudiation, Responsibility, Personal Integrity, and Ethicality, for example, can all be satisfied by Integrity in the CIA triad. Integrity and availability are used to ensure that the specification is correct. Confidentiality and integrity are the foundations of trust. Identity management can also be accomplished by all three members of the CIA triad. Classic security models such as the Bell-LaPadula, Biba, and Clarke Wilson Security Model have had a strong presence for the past 50 years. The Bell-LaPadula security model focuses on maintaining confidentiality, whereas the Biba model focuses on increasing integrity, and the Clarke Wilson Security Model is a more advanced model that aids in maintaining integrity in a well-formed transaction. The CIA triad serves as the foundation for all of these concepts (Samonas and Coss, 2014). Without the CIA triad, none of the security models can be constructed. By applying the CIA at both the organizational and individual levels, information security issues can be reduced.

Individuals are in charge of the organization's human layer of DiD as well as its strategic information security posture should be strengthened for information security (Yee, 2021). From top to bottom, the same can be true for every company's cybersecurity deployment. Furthermore, any organization that tries to satisfy one of the CIA triad's elements will naturally contribute to at least a small part of the other two – as seen in the Venn diagram of Figure 2.2.

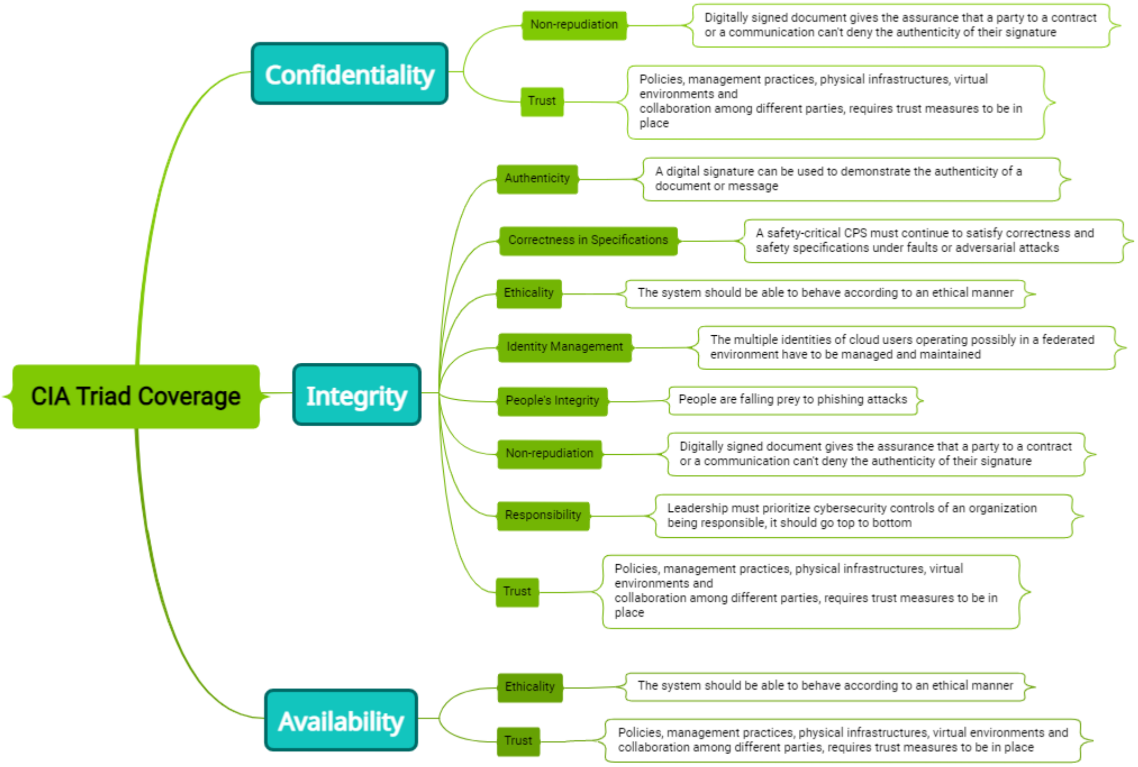

CIA Triad Coverage
Confidentiality
Non-repudiation
Digitally signed document gives the assurance that a party to a contract or a communication can't deny the authenticity of their signature
Trust
Policies, management practices, physical infrastructures, virtual environments and collaboration among different parties, requires trust measures to be in place
Integrity
Authenticity
A digital signature can be used to demonstrate the authenticity of a document or message
Correctness in Specifications
A safety-critical CPS must continue to satisfy correctness and safety specifications under faults or adversarial attacks
Ethicality
The system should be able to behave according to an ethical manner
Identity Management
The multiple identities of cloud users operating possibly in a federated environment have to be managed and maintained
People's Integrity
People are falling prey to phishing attacks
Non-repudiation
Digitally signed document gives the assurance that a party to a contract or a communication can't deny the authenticity of their signature
Responsibility
Leadership must prioritize cybersecurity controls of an organization being responsible, it should go top to bottom
Trust
Policies, management practices, physical infrastructures, virtual environments and collaboration among different parties, requires trust measures to be in place
Availability
Ethicality
The system should be able to behave according to an ethical manner
Trust
Policies, management practices, physical infrastructures, virtual environments and collaboration among different parties, requires trust measures to be in place

*Figure 2.3*
*CIA Triad Coverage*

If confidentiality lags, it will be harmful due to "disclosure." If Integrity lags, it will increase the possibility of "alteration," and if Availability is neglected, it will add to "destruction" (Stajano, 2002). Security goals can be mapped against confidentiality, integrity, and availability for any asset (Kure, 2019). As displayed in Figure 2.3, the CIA Triad can be mapped to additional important tenets of cybersecurity such as authenticity, correct specifications, ethicality, identity management, people's integrity, non-repudiation, responsibility, and trust. This diagram also shares a little more information with an example for each additional tenant. Even more, such tenets can be mapped to this cybersecurity core concept (Samonas, 2014; Vegh, 2015; Nguyen, 2021; Trentesaux, 2021; Hamlen, 2011; Khan, 2020; Aldini, 2002; Hathaway, 2012; de Oliveira Albuquerque, 2016).

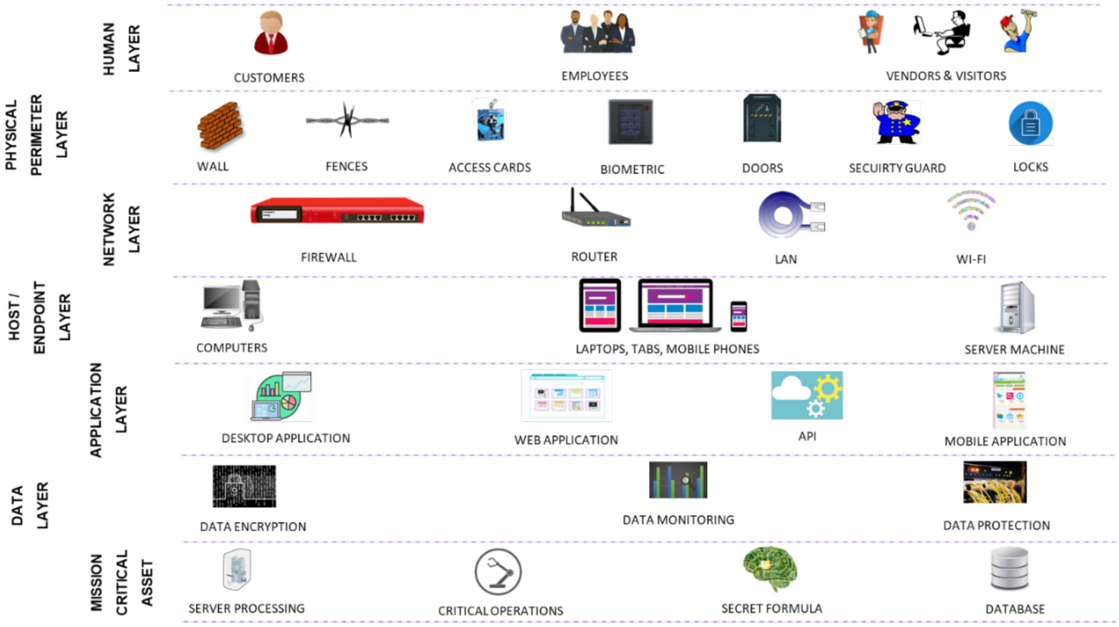


*Figure 2.4*
*Different Layers considered in Defense in Depth Concept*

Defense in Depth (DiD) is a concept developed by the National Security Agency (NSA) of the United States. It was initially more useful for military strategy, which is why it is sometimes referred to as a "castle" approach. It establishes principles and best practices for safeguarding assets like physical infrastructure, processes, and IT systems in the areas of people, operations, and technology. Later on, this conceptual model was adopted by a variety of businesses, including the layered approach to cybersecurity. DiD, also known as the "Security in Depth" strategy in the digital era, refers to a holistic protective approach for cybersecurity deployment on many levels, as shown in Figure 2.4. These are the levels at which data or information might be in various stages, such as data at rest, data in transit, or data in use. Each layer's goal is to improve an organization's security by decreasing vulnerabilities that could lead to cyber threats. It lowers the likelihood of a successful cyber-attack (Paloma, 2008). If a cybercriminal succeeds in breaching the security of one layer, it will make unethical behaviors more difficult as breaching the next layer will be a new problem, and so on. As seen in Figure 2.5, the MCA is at the heart of all security levels. The definition of mission-critical for any company may vary depending on the assets it has in cyberspace. Different forms of vulnerabilities and threats play a big role in deciding whether or not to keep a key asset (May, 2006; Kure, 2019). Data Layer Security can be strengthened by encrypting important information in the database and taking regular backups of the critical database. Endpoints include laptops, desktop computers, servers, and even mobile phones. Endpoint protection software and network-level devices should be used to protect them. To improve Application Layer Security, it must have been built from the ground up utilizing optimal security coding techniques. Unauthorized access to an organization’s network should be avoided to safeguard network security. Physical and digital perimeter security should both be secured with adequate measures to prevent the greatest number of threats. Humans are always seen as the weakest link in successful cyber-attacks, whether it's due to insider threats or a lack of security knowledge. Employees or other stakeholders can make or break any technology or process the enterprise has successfully implemented. As a result, the security layer that motivates individuals to decrease risks is critical (GOZTEPE, 2014). Cybersecurity is more of a socio-technical issue, with social essentials being people linked with the enterprise (Haastrecht, 2021).

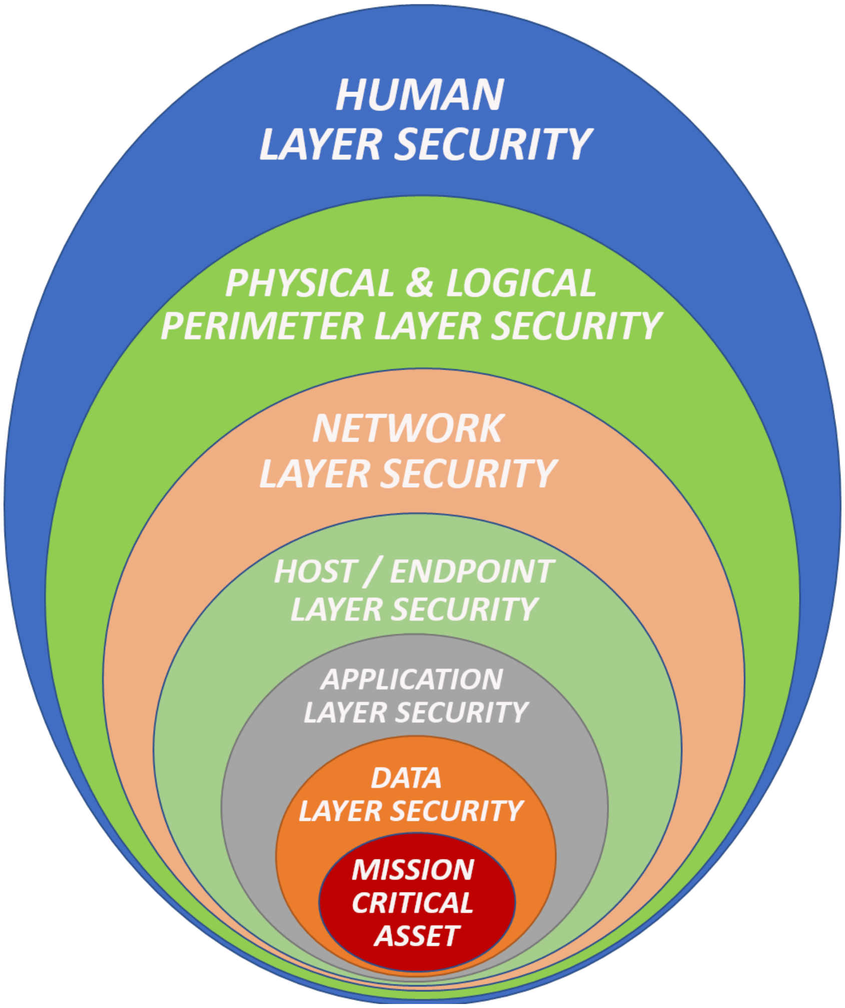

HUMAN LAYER SECURITY
PHYSICAL & LOGICAL PERIMETER LAYER SECURITY
NETWORK LAYER SECURITY
HOST / ENDPOINT LAYER SECURITY
APPLICATION LAYER SECURITY
DATA LAYER SECURITY
MISSION CRITICAL ASSET

*Figure 2.5*
*Defense in Depth (DiD) Approach*

Industry 4.0 has brought a revolution in manufacturing enterprises through increased implementation of IoT and cloud computing. In Industry 4.0, the factory perimeter includes manufacturing (production), logistics, supervision, R & D, living area, external physical, and external virtual. It further considers business impacts due to cybersecurity threats filtered by risk areas contributed by loss of confidentiality, integrity, or availability. The denial of service kind of cyber-attacks impacts the availability, causing loss of production time, violation of commercial agreements with customers, quality degradation of work parts, and service theft. Sabotage of the critical infrastructure of the factory's machines or components damages the machines on shop floors, degrades the quality of products, violates commercial agreements with clients of products, and also violates standards and regulations in the field of safety. Theft of industrial secrets or cyber-espionage can hamper confidentiality. It can reduce the competitive advantage of the enterprise. It also damages the reputation or image of the enterprise in the market. It can be even worse, as it can contribute to the violation of commercial agreements with the industrial partners of data (MULLET, 2021).

Any SME should have certain cybersecurity controls to strengthen people, processes, and technology areas. Any security framework or standard is incomplete if it fails to address the maximum issues in these three. The minimum cybersecurity controls for SMEs should provide at least some level of possible protection at each layer shown in Figure 2.5. It will help in defense-in-depth, but the survey will propose that instead of having all layers prioritized at the start, any SME should have the first level of layers prioritized, followed by increased coverage of layers with time.

### 2.1.2 Business Domain-Specific Mission Critical Asset

No cybersecurity framework or standard can guarantee that any organization will be 100 percent cyber secure after its implementation, but they will always try to keep cyber threat risk to a minimum (Florakis, 2020). For any asset, security objectives can be mapped against confidentiality, integrity, and availability. For example, the power distribution system has various critical assets, which include different software, SCADA, hardware, etc. Within the SCADA system, its subcategories such as ICS, HMI computers, RTU, PLC, industrial software applications, and Windows OS require high integrity and availability. The workstation and substation ethernet devices of SCADA need high availability rather than integrity and confidentiality. Production

ICS networks and ICS specifications need high confidentiality and availability. SCADA database software requires high confidentiality, high integrity, and high availability. In correlation with the CIA and its dependent factors, the SCADA system can be considered the most critical asset in the power distribution system (Kure, 2019). It should be remembered as a fact that practically any cybersecurity risk is never “zero”. If any SME can identify their Business Domain-Specific Mission Critical Assets (BDSMCAs), it will be the first successful step toward the resolution of the challenges they are facing. For any service-oriented business model such as an e-commerce platform, availability is very important, followed by the integrity of information through activities such as electronic payments (Gehling, 2005). Ramakrishnan (2010) considers confidentiality one of the most crucial elements in the BFSI domain. In the digital world, BDSMCA is mostly crucial data, information, or important systems handling it. It differs for each SME, mostly based on its business domain. The asset which has the maximum value, the highest risks, and a major impact on the SME’s core business can be treated as BDSMCA. For example, BDSMCA in the industry that deals with healthcare can be Electronic Medical Record (EMR) software; in the BSFI industry, it will be a net-banking transaction or financial records kind of web portal; in the E-Commerce sector, it will be shopping web and mobile app online presence; for the innovative manufacturing industry, product design ideas, methodology, and research material might be more valuable assets than anything else, and so on. Most of the time, mission-critical assets are information-related. There have been a few studies recently on "Information Assets" areas, and improving their effective management in different environments and systems can be managed mostly through cybersecurity awareness among human beings working in or for an enterprise (Evans,2020).

On the other hand, it is important to consider top management's inputs while deciding on the prioritization of the CIA as it might differ from the business point of view. If an e-commerce domain enterprise has been listed on the stock market, if confidentiality or integrity is lost in any information security breaches, it will lead to damage to reputation and even legal suits. From a business management perspective, availability might not be the highest priority in this case (Das, 2012).

Also, if possible, enterprises can consider CIA-related control implementation as well for BDSMCA.

### 2.1.3 Changing Priorities of CIA Triad based on Business Domain

Further, during a closer look at each SME's domain – it will be apparent that each domain has at least one key asset on which its existence depends. On the evaluating asset area reference to a particular domain of SME, it will be observed that each one of those has different priorities on the CIA Triad, which is changing the reference to the most damage they should be afraid of in their domain.

Each domain will have different priorities based on the demand and importance of a particular aspect. This aspect can be mapped to either all from people, processes, or technology. In other words, it will explain the need for either physical, logical, or administrative controls. Also, it will point towards specific expectations of confidentiality, integrity, or availability.

Refer to Appendix C, where the second part of the research interviewed top management of SMEs from the different business domains, to understand their business prioritized BDCA and prioritization of CIA. Figure 2.7 shows all the inputs gathered from various business domains. Figure 2.6 which is a subset of Figure 2.7, shows the manufacturing domain-related inputs received during these interviews. The

BDCAs for this domain are Design Drawings, Innovative Technology Design, Own Chipset, and Technical Knowledge, as demonstrated.

According to top management, the most crucial factor for these BDCAs is secrecy, followed by honesty and availability. Similarly, the Robot, Medicine Formulae, Software Technology Server, and Supply Chain Network algorithms are some of the other BDCAs, with senior management prioritizing integrity over confidentiality and availability. SME's top management, automated machinery, and tools were all BDCA in a few manufacturing areas. In addition, BDCA availability was deemed the most important factor, followed by secrecy and integrity. Quality control, line operation, and software of detector tolerance range were also mentioned as BDCA for this domain's top management. In addition, the highest priority for the same was integrity, followed by availability and confidentiality.

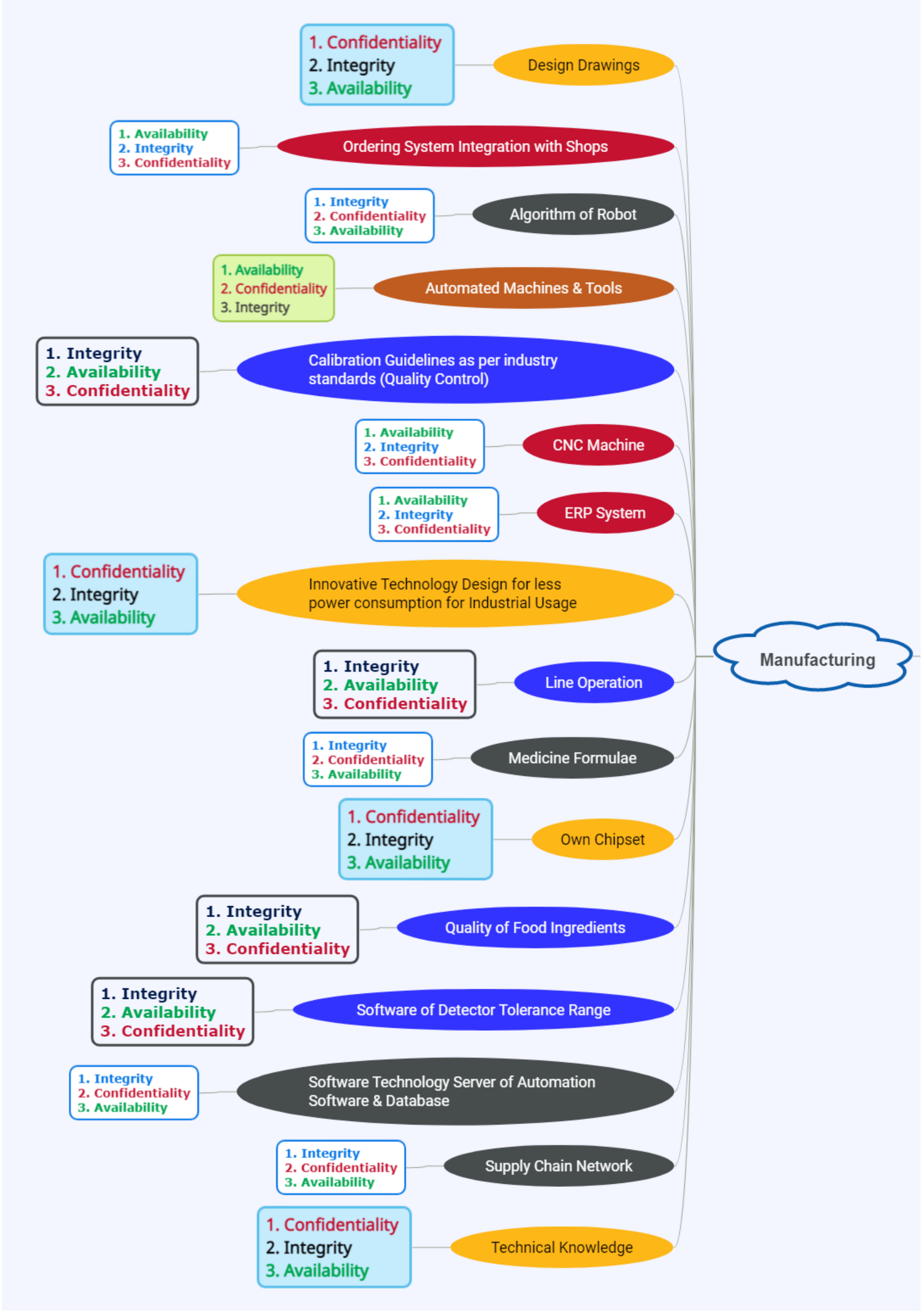


*Figure 2.6*
*BDSMCA & CIA Prioritization in Manufacturing Domain*

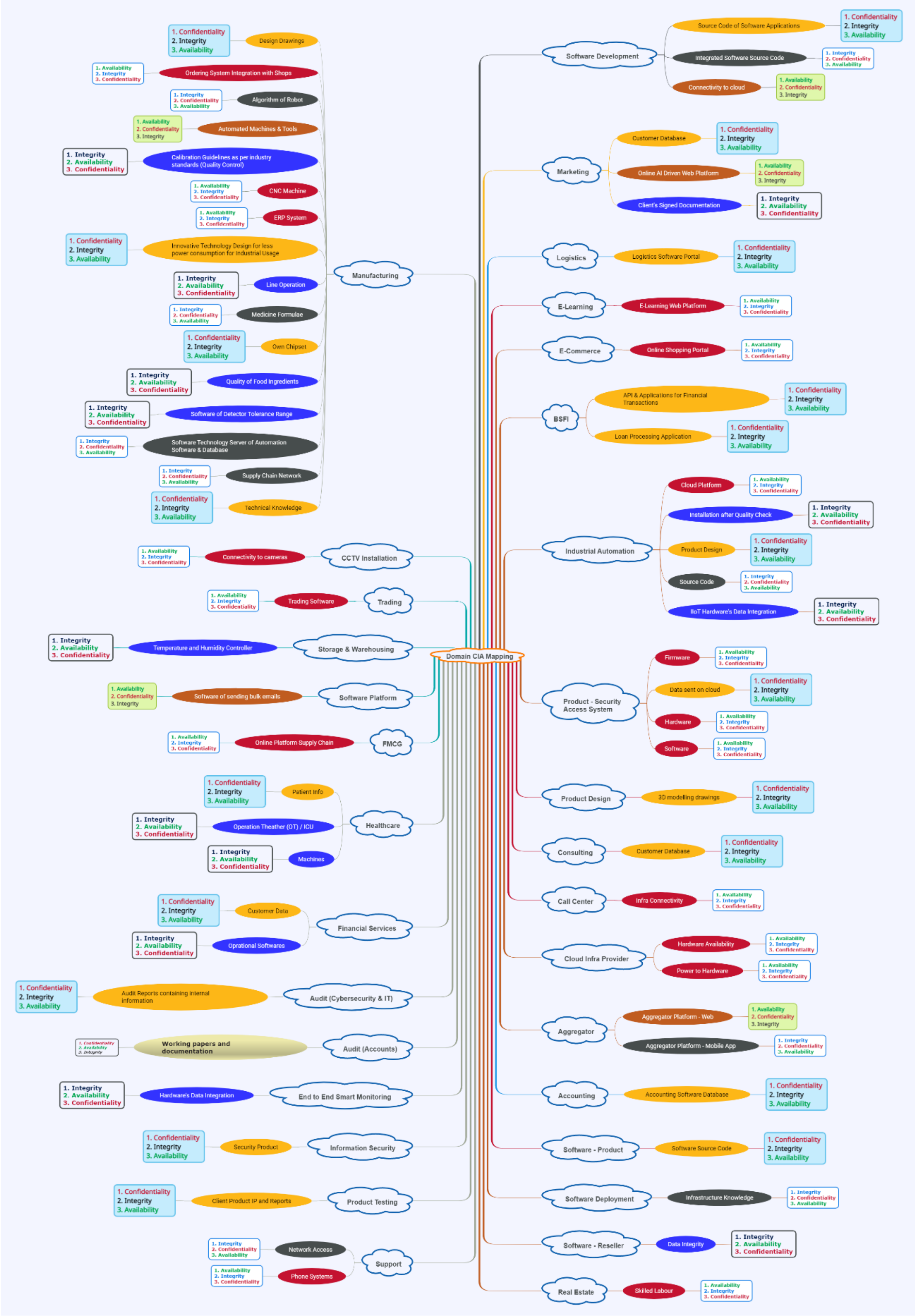

Domain CIA Mapping
Manufacturing
Design Drawings
1. Confidentiality
2. Integrity
3. Availability
Ordering System Integration with Shops
1. Availability
2. Integrity
3. Confidentiality
Algorithm of Robot
1. Integrity
2. Confidentiality
3. Availability
Automated Machines & Tools
1. Availability
2. Confidentiality
3. Integrity
Calibration Guidelines as per industry standards (Quality Control)
1. Integrity
2. Availability
3. Confidentiality
CNC Machine
1. Availability
2. Integrity
3. Confidentiality
ERP System
1. Availability
2. Integrity
3. Confidentiality
Innovative Technology Design for less power consumption for Industrial Usage
1. Confidentiality
2. Integrity
3. Availability
Line Operation
1. Integrity
2. Availability
3. Confidentiality
Medicine Formulae
1. Integrity
2. Confidentiality
3. Availability
Own Chipset
1. Confidentiality
2. Integrity
3. Availability
Quality of Food Ingredients
1. Integrity
2. Availability
3. Confidentiality
Software of Detector Tolerance Range
1. Integrity
2. Availability
3. Confidentiality
Software Technology Server of Automation Software & Database
1. Integrity
2. Confidentiality
3. Availability
Supply Chain Network
1. Integrity
2. Confidentiality
3. Availability
Technical Knowledge
1. Confidentiality
2. Integrity
3. Availability
CCTV Installation
Connectivity to cameras
1. Availability
2. Integrity
3. Confidentiality
Trading
Trading Software
1. Availability
2. Integrity
3. Confidentiality
Storage & Warehousing
Temperature and Humidity Controller
1. Integrity
2. Availability
3. Confidentiality
Software Platform
Software of sending bulk emails
1. Availability
2. Confidentiality
3. Integrity
FMCG
Online Platform Supply Chain
1. Availability
2. Integrity
3. Confidentiality
Healthcare
Patient Info
1. Confidentiality
2. Integrity
3. Availability
Operation Theather (OT) / ICU
1. Integrity
2. Availability
3. Confidentiality
Machines
1. Integrity
2. Availability
3. Confidentiality
Financial Services
Customer Data
1. Confidentiality
2. Integrity
3. Availability
Oprational Softwares
1. Integrity
2. Availability
3. Confidentiality
Audit (Cybersecurity & IT)
Audit Reports containing internal information
1. Confidentiality
2. Integrity
3. Availability
Audit (Accounts)
Working papers and documentation
1. Confidentiality
2. Availability
3. Integrity
End to End Smart Monitoring
Hardware's Data Integration
1. Integrity
2. Availability
3. Confidentiality
Information Security
Security Product
1. Confidentiality
2. Integrity
3. Availability
Product Testing
Client Product IP and Reports
1. Confidentiality
2. Integrity
3. Availability
Support
Network Access
1. Integrity
2. Confidentiality
3. Availability
Phone Systems
1. Availability
2. Integrity
3. Confidentiality
Software Development
Source Code of Software Applications
1. Confidentiality
2. Integrity
3. Availability
Integrated Software Source Code
1. Integrity
2. Confidentiality
3. Availability
Connectivity to cloud
1. Availability
2. Confidentiality
3. Integrity
Marketing
Customer Database
1. Confidentiality
2. Integrity
3. Availability
Online AI Driven Web Platform
1. Availability
2. Confidentiality
3. Integrity
Client's Signed Documentation
1. Integrity
2. Availability
3. Confidentiality
Logistics
Logistics Software Portal
1. Confidentiality
2. Integrity
3. Availability
E-Learning
E-Learning Web Platform
1. Availability
2. Integrity
3. Confidentiality
E-Commerce
Online Shopping Portal
1. Availability
2. Integrity
3. Confidentiality
BSFI
API & Applications for Financial Transactions
1. Confidentiality
2. Integrity
3. Availability
Loan Processing Application
1. Confidentiality
2. Integrity
3. Availability
Industrial Automation
Cloud Platform
1. Availability
2. Integrity
3. Confidentiality
Installation after Quality Check
1. Integrity
2. Availability
3. Confidentiality
Product Design
1. Confidentiality
2. Integrity
3. Availability
Source Code
1. Integrity
2. Confidentiality
3. Availability
IIoT Hardware's Data Integration
1. Integrity
2. Availability
3. Confidentiality
Product - Security Access System
Firmware
1. Availability
2. Integrity
3. Confidentiality
Data sent on cloud
1. Confidentiality
2. Integrity
3. Availability
Hardware
1. Availability
2. Integrity
3. Confidentiality
Software
1. Availability
2. Integrity
3. Confidentiality
Product Design
3D modelling drawings
1. Confidentiality
2. Integrity
3. Availability
Consulting
Customer Database
1. Confidentiality
2. Integrity
3. Availability
Call Center
Infra Connectivity
1. Availability
2. Integrity
3. Confidentiality
Cloud Infra Provider
Hardware Availability
1. Availability
2. Integrity
3. Confidentiality
Power to Hardware
1. Availability
2. Integrity
3. Confidentiality
Aggregator
Aggregator Platform - Web
1. Availability
2. Confidentiality
3. Integrity
Aggregator Platform - Mobile App
1. Integrity
2. Confidentiality
3. Availability
Accounting
Accounting Software Database
1. Confidentiality
2. Integrity
3. Availability
Software - Product
Software Source Code
1. Confidentiality
2. Integrity
3. Availability
Software Deployment
Infrastructure Knowledge
1. Integrity
2. Confidentiality
3. Availability
Software - Reseller
Data Integrity
1. Integrity
2. Availability
3. Confidentiality
Real Estate
Skilled Labour
1. Availability
2. Integrity
3. Confidentiality

*Figure 2.7*
*BDSMCA & CIA Prioritization for various Business Domains*

Let's take an example of three domains of SME as shown in *Table 2.1*.

*Table 2.1*
*Business Domain Prioritization of CIA Triad*

| SME's Domain | Business Domain-Specific Mission Critical Asset (BDSMCA) | Prioritized Risk Level causing biggest loss by damage to CIA Triad (1 = first top most priority) | | |
|---|---|---|---|---|
| | | *Confidentiality* | *Integrity* | *Availability* |
| BSFI | Financial Transaction Web Portal | 1 | 2 | 3 |
| E-commerce | Online Sales Web Portal | 3 | 2 | 1 |
| Pharmaceutical | Pharmaceutical Drug Manufacturing Process | 3 | 1 | 2 |

Here I take into consideration three different domains along with the key asset on which an SME is executing its business. As shown in the table of examples, if it considers SMEs from the BSFI domain, the important asset may be financial transactions and related stuff on their net banking kind of portal. Here, the highest priority for them will be confidentiality as compared to integrity and availability (AL-ALAWI, 2020). Continuing more in this area, if confidentiality is hampered, this kind of SME will have a serious impact on their customer, their reputation, and so on. If a transaction facility is unavailable for an extended period, this is preferable to losing confidentiality. In BSFI, if confidentiality is not maintained, it will provide a window for alteration of transactions impacting the integrity of the same.

Similarly, for the e-commerce domain or such kinds of SMEs, the enterprise will be more concerned about availability, followed by priority fulfilment for confidentiality and integrity. In previous research, it is evident that the criticality of this domain is centered on accessing the applications and network (Sutton, 2008). This domain has more focus on providing consumers with what they want and whenever they want (Guynes, 2011). Other than specific compliance needs, if one sees the broader picture, then this domain is not more concerned about the damage they can cause by disclosure or alteration. For example, in the case of the pharmaceutical industry, for medicine manufacturing purposes, different minerals, animal-derived materials, and botanicals are processed, considering very critical parameters. A few decades ago, these processes were manual or human-driven, but with the industrial revolution, they are now automated. The operations such as milling, blending, crushing, pressing into the desired pill shape, and packaging at a high volume level with the highest quality parameters are expected. Any change in a parameter may be life-threatening for consumers. The manufacturing of pharma products demands high integrity (Arden, 2021). For pharmaceutical SMEs, integrity might be more important than confidentiality and availability if one compares areas of the CIA Triad in the broader sense. It is because the information on drugs or other products is very sensitive. Such sensitive information should be captured and kept away from alteration by unauthorized entities.

### 2.1.4 Cybersecurity Control Types

There are three major categories of cybersecurity controls: physical, technical/logical, and administrative controls. Each category has many different controls, each with a specific purpose towards satisfying either or multiple purposes of prevention, detection, deterrence, recovery, and correction (Kim, 2011). For defense in depth of selected layers wherever there is relevance, SMEs need to map minimum cybersecurity controls to get a satisfactory level, lowering the risk. To fulfil the prioritized area of the CIA Triad, SMEs must map maximum controls and functions to the same. They can even find overlap of controls in a few functions, which will help them to achieve multiple objectives in one control implementation.

*Table 2.2*
*Few Cybersecurity Control Key Categorization*

| | | Control Types | | | | |
|---|---|---|---|---|---|---|
| | | **PREVENTIVE** | **DETECTIVE** | **DETERRENT** | **RECOVERY** | **CORRECTIVE** |
| Control Implementation Method | PHYSICAL (Structure used to prevent/deter | Construction planning for the site, Fences, Gates, Locks, Lighting, Fire prevention mechanisms (gas suppression, wet pipe, dry pipe, pre-action, etc.), Alarm systems (thermal, motion-based, etc.), Electronic emanation, Security Guards, Guard Dogs, Media Storage Security like Safe, Bulletproof and laminated Windows, Turnstiles, Mantrap, Physical security awareness, and training, warning signs | Lighting, Alarm systems, Guard Dogs, Broken Glass, Tamper Seals, Fingerprints, Physical Inventory Count, Receipts, Vouchers | CCTV, Surveillance Camera, Security Guards, Guard Dogs | Disaster Recovery Site | Repair Physical Damage, Re-issue Access Cards, Hot-warm-cold sites for Disaster Recovery, Heater and AC, Humidity Control |

| | | | | | |
|---|---|---|---|---|---|
| LOGICAL/TECHNICAL (Technology for controlling the access and/or usage of | Encryption, System certification process, Endpoint Protection, Data backups, Virus scanners, Email Security, Firewall, IPS / IDPS, MFA solution, Antivirus software, Security Information, And Event Management (SIEM) | Intrusion Detection Prevention Systems (IDPS) Logs, High-availability systems detection (HA failure detection), Verification of digital signatures, Biometrics for identification, network sensors, diagnostic utilities, forensics, Honeypots Analysis, CCTV, and surveillance camera | A proxy server that redirects a user to a warning page when a user attempts to access a restricted site | System Restoration, Backups for Application /Database Recovery, Server clustering, Rebooting, Key escrow, Insurance, Redundant equipment, Fault-tolerant systems, Failovers | Patch a System, Terminate a Process, Reboot a System, Quarantine a Virus, Data Restoration from Backups, File Repair Utilities, High-availability systems detection (HA failure detection), Redundant Network Routing, Server Images |
| ADMINISTRATIVE (Human factors of security) | Employee Hiring/Termination policies, Job Description, Business Contracts, Service Level Agreements (SLA), Laws & Regulations, Risk Management, Acceptable User Policy (AUP), Project Management, System Documentation, Training and Awareness, Disaster preparedness and recovery plans, Separation of Duties, Data Classification, Escort and Visitor Control, Fixing open security issues identified in Cybersecurity audits | Review Access Rights, System Logs, Unauthorized Changes, Physical Inventory Checks, Cybersecurity Audits, Mandatory Vacations, Exception Reporting, Control Self-Assessment, Oral Testimony, Risk Assessment, run-to-run totals, check numbers | A strict security policy stating severe consequences for employees if it is violated | Contingency Plans (ref to BCP), Drills | Business Continuity Plan, Disaster Recovery Plan, Incident Response Plan, Fixing open security issues identified in Cybersecurity audits, Termination Procedures, Outsourcing, Insourcing, Implementing recommendations of prior audits, lessons learned, property and casualty insurance |

For example, nowadays, endpoint protection software has built-in anti-virus, anti-spyware, anti-ransomware, data loss prevention, device control, full disc encryption, etc. It can meet the requirement for multiple technical controls to prevent a wide range of risks. If an SME is doing vulnerability assessment and penetration testing (VAPT) as a detective control to identify open issues in its assets, followed by fixation of those open issues, it will help in detective, preventive, and corrective functions. SMEs need to invest in minimum physical, logical/technical, and administrative controls to safeguard the prioritized area of CIA Triad for maximum risk coverage of BDSMCA. Table 2.2 lists a few of the key security control types. Preventive controls aid in the prevention of cyber threat problems; detective controls aid in the detection of problems or malicious activities; and corrective controls aid in the repair of detected irregulates or issues (Cannon, 2016). Deterrent controls avoid small threats by discouraging attackers with their visible presence in the system, whereas recovery controls help to get back to normal after an incident (Harris, 2016).

### 2.1.5 Fail-Safe and Fail-Secure: Unavoidable Consideration for Cybersecurity Controls' Implementation

Along with cybersecurity, human safety is the most important thing, which cannot be ignored in any case. In the improved cybersecurity standards, implementation of controls is done taking into consideration the “Fail-Safe” and “Fail-Secure” concepts. The term "fail-safe" encourages avoiding any scenario where any human being’s life or property is not in danger when it fails. (Siewert,2019). For example, a server room where all important data is stored – always has the best physical controls like access controls implemented for doors. With proper access control or the process of allowing a specific authorized person in and out, these doors are increasing physical perimeter cybersecurity levels. Say, if that server room catches fire by any accident or other possible valid reason, the fail-safe concept will unlock the doors of that room to ensure quick escape for any person working inside it and allow firefighters to get inside the room to save other lives. In such cases, the fail-secure takes second place because the fail-safe must take precedence. Also, IoT devices play an important role in many SMEs, where they contribute more to safety and security (Riahi, 2014). There are multiple technical ways of designing security layers that can help in making sure that fail-secure will be auto-triggered during situations like this without impacting fail-safe. Cyber resilience thinking helps in designing systems to fail safely. Hence, many countries embed resilience thinking as a national-level cybersecurity strategy. In studies conducted in the Asia Pacific, SME owners appeared to be vulnerable groups in the national cybersecurity strategies of countries like Australia, Japan, New Zealand, the Philippines, Singapore, and South Korea (Thinyane, 2020).

### 2.1.6 Governance, Risk Management, and Compliance Requirements

At any level of implementation of controls for mission-critical assets, the minimum possible governance, risk management, and compliance (GRC) should be deployed to make cybersecurity perfect. For IT governance, ISO 38500 or COBIT are widely used (Brandis, 2019). COBIT focuses on generic processes for IT governance and IT management. It has five processes related to governance under the domains of Evaluate, Direct, and Monitor (EDM). COBIT has thirteen Align, Plan, and Organize (APO) processes, ten Build, Acquire, and Implement (BAI) processes, six other Deliver, Service, and Support (DSS) processes, and three Monitor, Evaluate, and Assess (MEA) processes for IT management (Devos, 2015). Governance is the unique stream of management in any organization. ISO 38500 provides a clear difference between those; it applies to all kinds and all sizes of organizations. Good governance assures all stakeholders of the enterprise about the standard being followed by it. It also guides the top management. ISO 38500 provides six principles that focus on a clear understanding of responsibilities for IT; planning of IT; acquiring IT validity; ensuring IT performs well; ensuring IT conforms with formal rules; and ensuring IT use respects human factors (Feltus, 2012). For BDSMCA, governance will provide the overall system of rules, practices, and standards that will be a guide for SMEs.

Risk management will be the process of identifying potential threats to the BDSMCA of SMEs and taking steps to reduce or eliminate them. The different threat agents who can harm cybersecurity can be broadly categorized into human threat agents, technological threat agents, and environmental threat agents. To provide a solution to risk by different threat agents, the risk management process has different methodologies and steps based on the approach it (Meszaros, 2017). There are various methods for risk assessment in IT operations (OPS), and each one has different approaches, benefits, and lagging areas. NIST, FAIR, IT-Grundshutz, OCTAVE, IRAM, EBIOS, RISK WATCH, MEHARI, MAGERIT, CRAMM, Methods NBU, and Methods Korchenko are a few basic methods used for risk assessment. The NIST is a heuristic approach that provides maximum details of the information assets and is helpful for a wide range of enterprise sizes. But this risk analysis requires a long time and a few features of its lagging automation. FAIR is based on a probability approach and is suitable for large enterprises, providing comprehensive analysis. IT. Grundshutz is a heuristic approach that is costly and demands lots of knowledge of its process. Being flexible, it can be used for any organization or any type of asset. OCTAVE is suitable for SMEs and it is fast to implement. On the negative side, it lags in automation. Instead of being technology-specific, this heuristic approach is focused on operational risks and security practices. IRAM is an informative, approach-based risk method that is easy to implement. The high cost of licenses and their tight coupling to existing information assets makes it difficult. The EBIOS method uses an informative approach where it is suitable for many users, making it useful only for government or commercial organizations. Risk watch is an informative approach method that gives flexibility and high efficiency with ease of use. It has costly licenses and only focuses on the software and technical levels. MEHARI is a heuristic approach that provides an analysis of formulas and parameters. It is only applicable to ISO-based systems. Magerit is a heuristic approach-based method of quantifying with systematic analysis. It gives results based on data that is dependent on human factors. CRAMM is a probability-based method that provides detailed information about risk exposures. It again has costly licenses and has the limitation of only working for existing information assets. Methods: NBU uses an informative risk-based approach and provides a detailed analysis of resources. It is only designed for the specific Ukrainian banking system. Methods Korchenko is again an informative approach, which not only describes application feature principles but also allows for expanding feature space to describe new classes. It is not providing coverage for financial losses from sales of threats. (P, 2018). With continuous improvement, the OCTAVE Allegro method was introduced in June 2007. OCTAVE Allegro is different as compared to previous versions of it, as it primarily focuses on information security. It has eight steps. In the first step, it establishes risk measurement criteria. In the second step, it develops an information asset profile. The third step is focused on identifying information asset containers. The fourth step is used to identify areas of concern. The fifth step identifies threat scenarios. The next step identifies risks. In the seventh step, an analysis of risks is done. Finally, in the last step, which is the eighth step, the selection of a mitigation approach is considered (Caralli, 2007; Ralston, 2007). SCADA and DCS are considered CIs in Industrial Automation, where HHM, FTA, FMEA, PRA, attack trees, and vulnerability trees are risk assessment techniques that can be used for those (Ralston, 2007). Recent research also demonstrates new ways in which digital threat-based cybersecurity risk assessment is possible for SMEs. Such an assessment is designed with data models and data sources in mind, with cyber threats at the forefront (Haastrecht, 2021). Even enterprises can use simple methods to calculate cybersecurity risk, then use risk matrixes or risk scores. Any enterprise leader or its top management knows their business priorities and risks. They can prepare simple methods with a scale to show a measurable improvement (Hubbard, 2012).

From the compliance perspective, enterprises and cybersecurity teams must be aware of different laws and regulations that are relevant to them. In the United States, FISMA forces agencies within the federal government to develop, document, and implement a holistic cybersecurity program for those with whom HIPAA has established compliance by protecting medical information through privacy and security rules. FERPA, which is a federal law that protects the education records of students, There are generally big penalties associated with compliance requirements, so they cannot be ignored at all (Harris, 2019). In Europe, GDPR has brought a change in protecting data privacy, which refers to information that can identify a person. It applies to all organizations in Europe and organizations dealing with PII data of European people around the globe. Many times, SMEs are late in implementing certain compliances like GDPR due to a lack of proper knowledge (Freitas, 2018). Compliance will be the set of processes and procedures that an SME should have in place to make certain that it is meeting all legal and regulatory requirements (Asnar, 2011).

### 2.1.7 Cybersecurity Controls Implementation by either Self, Cloud, or Vendor

SME's BDSMCA can be partially or fully managed and hosted within SME's premise, or it can be on the cloud or outsourced to an external vendor. This will have an impact on the efforts required to achieve the required cybersecurity control implementation. Many times, enterprises have very good cybersecurity controls in place, but due to the lack of cybersecurity implementation of connected entities to their environments, which are in less control, they face cyber threats. Also, if an SME has its infrastructure on a physical premise, the cloud, or is not needed due to outsourcing, that should be considered while designing cybersecurity controls. It does not mean that risk is reduced for SMEs; it simply means that risk should be properly maintained at a low level in any case. To become more efficient and productive, many SMEs are becoming attracted to adopting ICT. As SMEs generally have a shortage of financial resources required for ICT, an alternate solution for them is cloud computing. It provides a cost-effective solution for achieving their goals (Tan, 2009). SMEs should not ignore cloud security, where components of the cloud such as OS, web server, applications, VM, VM monitor, host, etc. need to be protected (Hong, 2019). In CSCRM, each entity must be cyber secure. If a vendor is developing software for an SME, that software's source code security audit must be done before it is accepted as part of the enterprise's business. Information security and other relevant audits of vendors are essential while SMEs are dealing with external relationships (Boyson, 2014). Sometimes business partners of SMEs can act as insiders, as they get access to crucial information or any similar asset of the enterprise (Oyebisi, 2020).

## 2.2 Related Work

The growth of IoT devices and mobile devices in SME shops from the shop floor to the top floor is ongoing, making improvements in data exchange capabilities over the internet. The cyber-attack surface for businesses is growing as a result of the new digital era. Cybersecurity auditing approaches such as periodic penetration testing can assist SMEs in identifying open vulnerabilities and developing plans to address them. Recently Jibran Saleem et al. identified that ransomware, data breaches, phishing attacks, smart grid attacks, IoT attacks, and even state-sponsored attacks are becoming more common in SMEs (Saleem, 2017). According to studies performed by Nabila Amrin, malicious HTML emails, web server compromise, data loss on portable devices, employees' careless use of the internet, wi-fi, or publicly available networks, poor configuration management, insider threats, cyber-attacks exploiting open vulnerabilities, and a lack of contingency planning are some of the most common cyber threats that SMEs face. These attacks are carried out using compromised assets such as end-point operating systems, devices used to open emails, a website or its server, portable devices, databases at the organization, employee-owned devices within an organization, and an enterprise's entire network, IT infrastructure, and policies (Amrin, 2014). As the outcome of the recent study for SMEs in Kenya by Eric Muhati, businesses face two key hurdles when it comes to implementing cybersecurity. One was a lack of sufficient funds, and another was a lack of leadership support for cybersecurity implementation, which could be because they have other business-related issues that are a priority for them (Muhati, 2018). As per the recent survey of SMEs in the United Kingdom by Andrew Rae et al., roughly 73 percent had trouble accessing cybersecurity information to adapt. One-third of businesses did not consider cyber-attacks and data loss a significant risk (Rae, 2019). According to a recent Middle

East survey by Nadir Ahmed et al., approximately 56% of SMEs are aware of cybersecurity. In addition, the majority of SMEs have experienced one to five cyber-attacks in the previous five years. Endpoint security solutions are used by 12.45 percent of SMEs, and firewalls are used by 10.2 percent of SMEs. It is clear that about half of SMEs are either going to utilize cloud computing solutions or are not interested in doing so (Ahmed, 2021). As per the recent study of SMEs in developing nations such as South Africa by Salah Kabanda et al., challenges to implementing cybersecurity in SMEs include a lack of management support owing to other company objectives, a low budget, and a lack of resources with technical skills and cybersecurity tools (Kabanda, 2018).

According to the existing data, the expense of implementing well-known cybersecurity frameworks, the time it takes to apply them, and a lack of sufficient guidelines or security knowledge to understand the roadmap to becoming a cyber-secure organization appear to be major roadblocks for SMEs. Another issue to note is that no framework offers a starting point or implementation stages for SMEs to decide on early cybersecurity policies. Furthermore, none of the standards or frameworks are intended to provide appropriate cybersecurity safeguards for SMEs' business domain-specific assets. Every SME has different specialized goals, and “what should be safeguarded from cyber-threats” varies depending on those aims. Existing standards or frameworks aren't focused enough on SMEs' business goals or specific domain demands. This research aims to identify the key issues that SMEs face when it comes to implementing cybersecurity safeguards. It will also strive to come up with a new cybersecurity framework design that will break down the deployment of cybersecurity controls into a step-by-step process while maintaining the business goals of the SME’s domains at the forefront of the recommended solution.

### 2.3 Summary

There is tremendous cybersecurity-related knowledge of core concepts, research, and discussions available now. This information will be useful in identifying gaps and making recommendations in the following sections.

# CHAPTER III:
# METHODOLOGY

## 3.1 Overview of the Research Problem

It is evident through various statistics and existing literature that SMEs are building blocks of the global economy and those are undergoing damage because of various cyber threats. There are already well-established cybersecurity standards for enterprises across the world, but "why" SMEs are facing cyber threats is the biggest question. Looking at the criticality of the global need for the SME segment, researchers decided to gather input from SMEs through a well-designed research survey to understand their current state and the problems they are facing concerning cybersecurity controls.

In the third quarter of the year 2021, the research survey was conducted among SME segments focusing on different key business domains. Even though the cybersecurity posture of an organization is very crucial, 115 SMEs voluntarily participated in this survey.

This research was designed for understanding adopted cybersecurity standards or frameworks, the level of cybersecurity controls implementation, what kind of cyber threat experience they have undergone and further trying to understand what is stopping SMEs to implement cybersecurity controls to safeguard their enterprise and mission-critical assets.

## 3.2 Operationalization of Theoretical Constructs

Although there are different methodologies to proceed with research, initially it chose the quantitative method, which is a research survey. The suitable participants for this survey were chosen as top management, c-level executives, directors, and similar as it has few insights about the internal cybersecurity posture of the enterprise. All the inputs collected from SMEs will be analyzed to understand the gaps present in the existing implementation of overall cybersecurity controls or even the gaps in existing cybersecurity standards or frameworks to satisfactorily fulfil required cybersecurity posture needs. Once gaps are found, the new recommended solution will be designed to bridge them. For research studies, a few hundred SMEs were approached from July 2021 to September 2021. Out of those, only 115 SMEs shared valuable inputs in this survey as information about cybersecurity implementation has been a very sensitive and crucial area of any enterprise. Later, to give proper recommendations to SMEs, it was again decided and chose the qualitative method, which is research interviews. The research's second part conducted interviews with 109 top management of SMEs in different business domains. It helped us to understand their views on what their business priorities are and which assets they want to protect, with more reference to the same.

### 3.3 Research Purpose and Questions

The sole goal of this study is to obtain first-hand input from leaders of SMEs working in various disciplines and regions. This study isn't only about identifying holes; it's also about recommending a solution to help SMEs solve their problems while simultaneously enhancing their cybersecurity posture.

**Specific Aims:**

- To collect direct input from SMEs to understand current cybersecurity control implementation and listen to the problems faced by those enterprises, do the overall gap analysis of the cybersecurity posture within SMEs and risks associated with the same design a structured, recommended solution that can be a new framework to address the resolution of the identified problems.

**Research Questions:**

- Does SME have any cybersecurity standards or frameworks adopted?
- What kind of physical, logical (or technical), and administrative controls does SME have implemented?
- How much effort do SMEs put towards cybersecurity awareness among employees?
- What are the major cyber threats experienced by SMEs?
- What is the biggest problem faced by SMEs while implementing cybersecurity controls?

**Hypothesis:**

- The study hypothesizes that there is a gap between expectations set by existing cybersecurity standards or frameworks, which are not in alignment with the requirements for the specific domain of an SME or the overall benefit for SMEs to relate to or invest in the same.

### 3.4 Research Design

This study uses a quantitative technique and a research survey to address the proposed questions. This research survey has to be created in a more engaging approach to get a few internal insights about SMEs' cybersecurity posture as well as the top problem areas they are encountering while planning or implementing cybersecurity policies. This will also allow the research study to be more diverse and look at multiple viewpoints of the reality of cybersecurity adoption by SMEs, resulting in a better understanding of the issue under study. The research outcome will try to propose a recommended remedy for the highlighted concerns based on existing basic cybersecurity ideas. The main goal of this study is to figure out why SMEs are becoming more vulnerable to cyber threats, as well as to learn how SMEs feel about cybersecurity in general.

In the research survey, participants who are SME leaders, mostly c-level executives such as CEO, CTO, CISOs, etc will be considered. The questions and their purposes in the research survey are listed below.

**Q1. How old are your Small and Medium Enterprises (SMEs)?**

Since how long the participant SME do exist in the market is going to penetrate more deep understanding of business maturity concerning the cybersecurity maturity, hence a question being asked to SME representatives to choose any of the options from - (a) Less than a year, (b) Between one to three years, (c) Between three to five years, (d) Between five to ten years, and, (e) More than ten years.

**Q2. Does your organization have any of the below standards or frameworks implemented?**

Many standards and frameworks are being adopted by organizations globally. To check which of those got adopted by participant SMEs, the survey provided the facility to choose multiple options among (a) ISO 27001, (b) NIST Cybersecurity Framework (CSF), (c) PCI DSS, (d) HIPAA, (e) FINRA, (f) GDPR, and (g) Other. The survey kept the flexibility to share the input in the textbox by choosing the “Other” option if SMEs are using any other framework or standard which is not present in the options provided in optional answers to this question.

**Q3. Does your organization have security controls in place?**

Regardless of the answer to the above question Q2., the survey captured input to identify any security controls that SMEs have already implemented. For this question, the survey provided three options, which are: (a) Yes, (b) No, and (c) Maybe.

**Q4. If the answer to the above question Q3 is YES, please select PHYSICAL Security controls already in place.**

Even though it is sensitive information for SMEs to disclose which physical controls have been implemented in their organization, the survey asked the participant SMEs to choose any or multiple answer options among the following: (a) Fences, (b) Gates, (c) Guards, (d) Security badges, (e) Access cards, (f) Biometric access controls, (g) Security lighting, (h) CCTVs, (i) Surveillance cameras, (j) Motion sensors, (k) Fire suppression, (l) Environmental controls like HVAC and humidity controls, and, (m) Other. Survey has asked participants to add "NA" in the answer textbox, choosing the option "other" if the participant SME has no physical controls in place. If they had any physical security control which is not listed in the options provided in the answer, they could choose the answer option "other" and be asked to add their physical control or list of such kinds of controls in the answer textbox.

**Q5. If the answer to the above question Q3 is YES, please select TECHNICAL Security controls already in place**

Even though it is sensitive information for SMEs to disclose which technical controls have been implemented in their organization, the survey asked the participant SMEs to choose any or multiple answer options among the following: (a) Security Policies,

(b) Security Procedures, (c) Security Guidelines, and (d) Other. Survey has asked participants to add "NA" in the answer textbox, choosing the option "other" if the participant SME has no technical controls in place. If they had any technical security control which is not listed in the options provided in the answer, they could choose the answer option "other" and be asked to add their technical or logical control or list of such kinds of controls in the answer textbox.

**Q6. If the answer to the above question Q3 is YES, please select ADMINISTRATIVE controls already in place**

Even though it is sensitive information for SMEs to disclose which administrative control has been implemented in their organization, the survey asked the participant SMEs to choose any or multiple answer options among the - (a) Security Policies, (b) Security Procedures, (c) Security Guidelines, and, (d) Other. The survey has asked participants to add "NA" in the answer textbox, choosing the option "other" if the participant SME has no administrative controls in place. If they had any administrative security control which is not listed in the options provided in the answer, they could choose the answer option "other" and be asked to add their administrative control or list of controls in the answer textbox.

**Q7. How frequently is Security awareness training conducted for employees?**

Training in security awareness for employees helps organizations in many ways to be cyber secure. Hence, the survey checked it with this question having one of these options to be chosen as an answer- (a) Never, (b) Once a Year, (c) Once Every Six Months, (d) Once Every Three Months, (e) Monthly, and (f) Once Every Month. To capture any other input related to security training that might not be present in the options survey provided in the answer, an option with “other” has a textbox for input from SME participants.

**Q8. Which are the biggest problems you are facing while implementing or deciding/planning to implement Cybersecurity Controls for your organization?**

To hear from SMEs about what is the biggest problem they are facing in terms of cybersecurity implementation, the survey tried to capture their inputs in any or multiple options to be chosen as answers among (a) Cost Involved in Implementing Cybersecurity Controls, (b) Not Sure Which Cybersecurity Controls to Implement, (c) Lack of resources to implement and maintain, (d) Other business priorities are more important, (e) Not finding a roadmap to invest in cybersecurity control implementation, (f) Available cybersecurity standards or frameworks need big investment, and, (g) Other. To capture any other problem an SME wants to share but is not present in the options survey provided in the answer, an option with “Other” has a textbox for input from SME participants.

**Q9. Has your organization undergone any cyber-attack?**

To understand the seriousness of the cyber attack issues, the survey tried to listen to SME participants about if they had faced any cyber-attacks since they started their enterprise business journey. For this question, the survey provided three options, which are: (a) Yes, (b) No, and (c) Maybe.

**Q10. Which kind of cyber-attack did your organization face?**

In continuation of question Q9, the survey attempted to determine which cyber attack SMEs faced by providing answer options in which they could select any or all of the following: (a) Insider Threats, (b) Ransomware, (c) Malware Attacks, (d) Web

Attacks, (e) Phishing Attacks, (f) Man-in-the-middle (MITM) Attack, (g) Denial-of-Service (DoS) Attack, and (h) Other. To capture any other cyber-attack that SMEs face but is not present in the options survey provided in the answer, an option with "Other" has a textbox for input from SME participants.

**Q11. As an SME, what is your expectation from security standards or framework?**

To listen to the SME participants, the survey asked an open question to understand their expectations of cybersecurity standards or frameworks. The research will discuss more of what was witnessed in the SME segment in the upcoming sections.

### 3.5 Population and Sample

These research participants were chosen from diverse business domains such as Banking, Financial Services and Insurance (BFSI), E-commerce, IT industry, Logistics, Manufacturing, SAAS, Telecommunication, Education, FMCG, Hospitality, Insurance, Media, Pharmaceuticals, and a few other domains. The other domains were cold storage & warehousing, consulting, distribution of primary packaging materials, executive coaching, hospitality, legal and accounting services, manpower supply (human resources), maritime, marketing consultant, oil industry, renewable energy, exports, and travel platform. Using this research methodology to try to understand insights into existing cybersecurity posture, information about cyber threats SMEs have undergone, and such few sensitive internal information, there will be a more likely reluctance to participate by top management such as C-Level Executives, Directors, etc.

Table 3.1 shows the sample size selected for this research and the actual response received from the participant SMEs. While research approached a total of

350 top management SMEs, only 115 volunteered to participate in these research studies.

*Table 3.1*
*Sample Selection and Actual Response*

| SME's Domain | Sample Size | Actual Response |
|---|---|---|
| Banking, Financial Services, and Insurance (BFSI) | 20 | 11 |
| E-commerce | 20 | 6 |
| IT industry | 50 | 38 |
| Logistics | 20 | 4 |
| Manufacturing | 20 | 8 |
| SAAS | 20 | 5 |
| Telecommunication | 20 | 4 |
| Education | 20 | 3 |
| FMCG | 20 | 4 |
| Hospitality | 20 | 4 |
| Insurance | 20 | 4 |
| Media | 20 | 5 |
| Pharmaceutical | 20 | 2 |
| Other | 60 | 17 |
| ***Total*** | **350** | **115** |

As shown in figure 3.1, the maximum responses were received from IT industry participants, followed by BFSI, E-Commerce, and manufacturing enterprises.

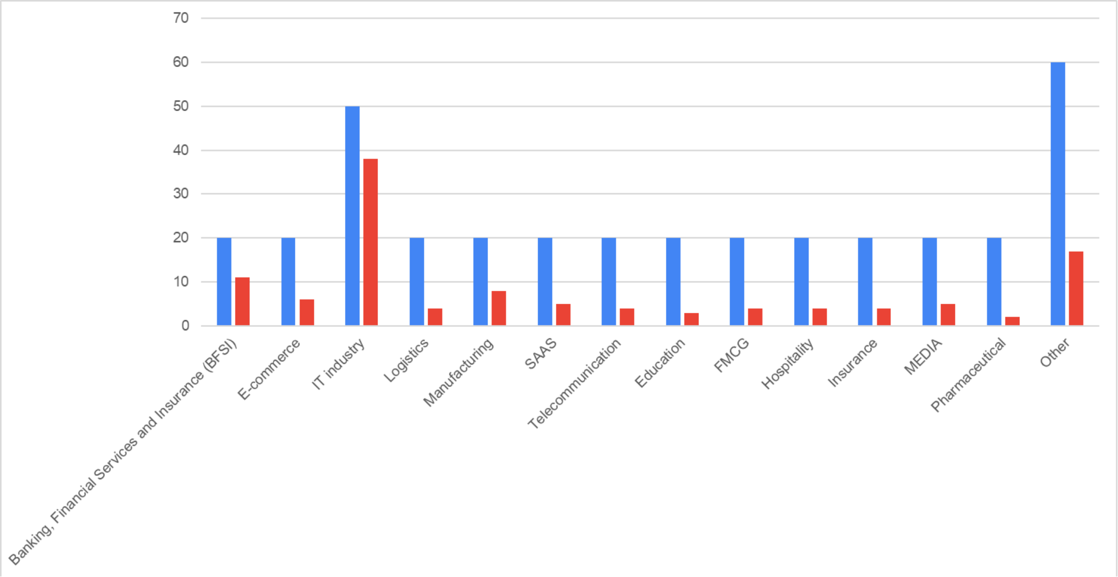


*Figure 3.1*
*Sample Selection and Actual Response*

### 3.6 Participant Selection

SME's top management, who are involved in decisions, execution, and other areas of cybersecurity, were approached to capture correct inputs. Many of the directors, owners, c-level executives (such as CEO, CISO, CTO, etc.), business unit (BU) heads, etc., working in SMEs are considered the right and authorized participants to share the valuable inputs for this research.

Also, participant SMEs were carefully chosen to gather input from different business domains.

### 3.7 Instrumentation

The top management of SMEs communicated via social media messaging like LinkedIn messages, mobile device text messages, emails, etc. Questions and respective answer options were designed in a digital format. The data inputs were digitally recorded for better studies. In the latter part, the research interviews were conducted by phone and voice calls.

### 3.8 Data Collection Procedures

The survey was designed in such a way that participants could complete it for a maximum of 15 to 20 minutes. The format of questions and answers was kept simple and easy for the participants. Whatever was not applicable or if the participant wanted to share other inputs which were not part of the options provided in the answer, an additional textbox was provided as part of such an answer list for capturing their valuable inputs. Data is collected once the participant submits the form. Later, it was extracted in the form of a tabular format for further analysis and study. Similarly, research interview data was captured as notes.

### 3.9 Data Analysis

For data analysis, Microsoft Excel, as well as the Power BI tool, were used. The data captured in digital format will be pulled, and then using the mentioned tools, will try to create pivot tables or datasets required for the study of a particular question's response. I converted it into a graphical format for ease of understanding. Depending on years of existence and many such criteria, I tried to create multiple sub-datasets to prepare a low-level understanding of the valuable inputs from participants.

### 3.9 Research Design Limitations

This research design was for the understanding of internal cybersecurity posture and problems, and as it was sensitive information, most of the top management declined to participate. Even though I approached around a few hundred prospective participants, only 115 participants agreed to share their valuable inputs for this research.

This research is carried out only for SMEs, not for any other enterprises. Also, as the target participants of this research were mostly c-level executives, directors, and owners, it was difficult to get their valuable time for the proper input.

### 3.9 Conclusion

To conclude this chapter, research would like to throw light again on the existing literature, which explains many cyber threats to SMEs. This research got an opportunity to gather input from top management of various SMEs through a well-designed research survey to understand their current state and the problems they are facing concerning cybersecurity controls. Even though the cybersecurity posture of an organization is very crucial, 115 SMEs voluntarily participated in this survey. Also, during the solution design, 109 top management of SMEs participated in the research interviews to share direct inputs.

# CHAPTER IV:

# RESULTS

## 4.1 Age of Small and Medium Enterprises (SMEs)

The results from the survey of SMEs from different domains have been very helpful in understanding good and pain areas as it pertains to cybersecurity implementation for them.

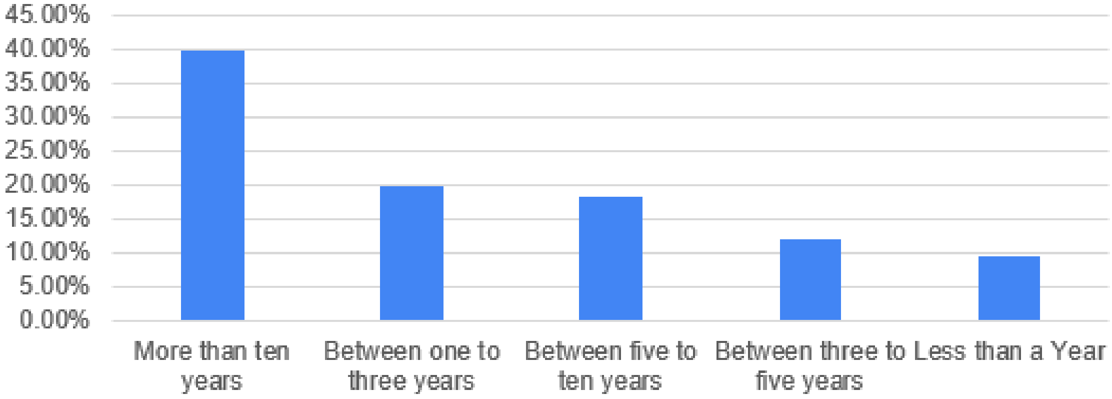


*Figure 4.1*
*Age of SME participated in Survey*

The majority of SMEs with more than ten years in business (around 40 percent), as shown in Figure 4.1, voluntarily participated in this important survey. In addition to that age group, more than 18% of SMEs aged 5 to 10 years old took part. Approximately 20% of SMEs had an execution period of one to three years. Approximately 12% of SMEs have been in operation for three to five years. Less than 10% of the SMEs that took part in the survey had been in operation for less than a year.

## 4.2 Current State of Implemented Standards or Framework in SMEs

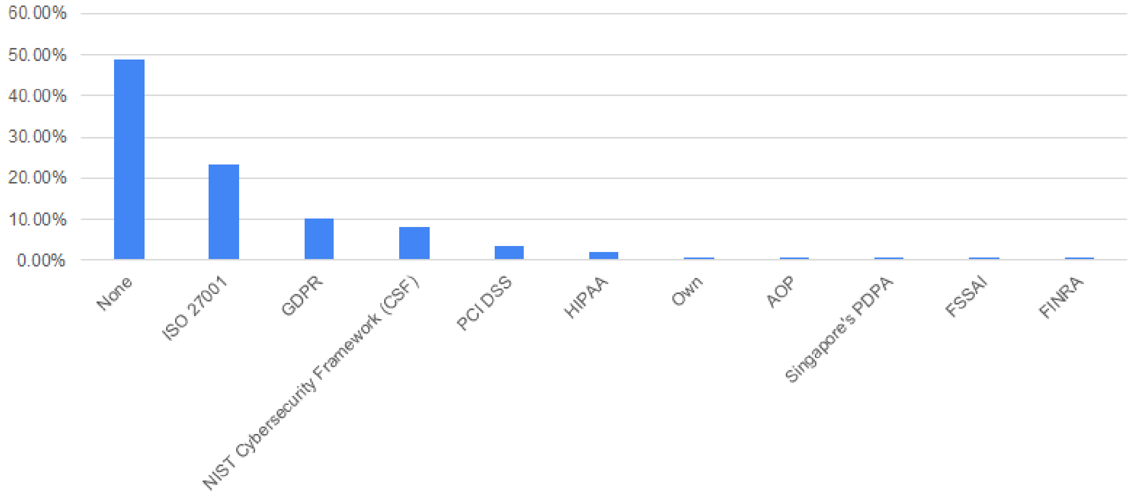


*Figure 4.2*
*Security Standards / Frameworks Implemented in SMEs*

Figure 4.2 shows that approximately 49 percent of SMEs lack cybersecurity standards or frameworks, leaving them vulnerable to cyber threats. There must be issues that are preventing them from adopting those. Only 23% of SMEs have implemented ISO 27001, 10% have implemented GDPR, and 8% have accepted the NIST Cybersecurity Framework (CSF).

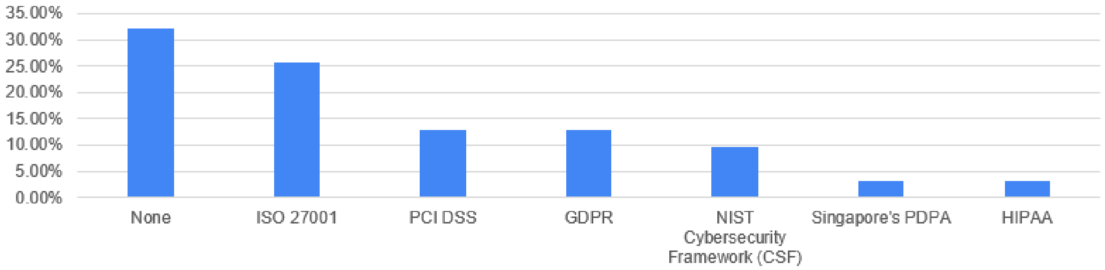


*Figure 4.3*
*Security Standards / Frameworks Implemented in SMEs having existence between 5 to 10 years*

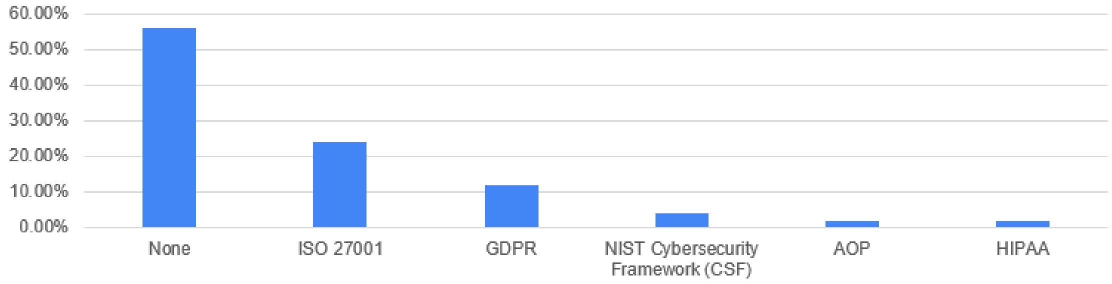


*Figure 4.4*
*Security Standards / Frameworks Implemented in SMEs having more than 10 years of existence*

Figure 4.3 shows that more than 32% of SMEs between the ages of 5 and 10 do not have any cybersecurity standards or procedures in place. Furthermore, 56 percent of SMEs with an average age of more than ten years lack security, according to Figure 4.4.

It also indicates there is something that is stopping SMEs from adopting the available cybersecurity standards or frameworks, which should be revealed.

### 4.3 Current State of Security Controls in SMEs

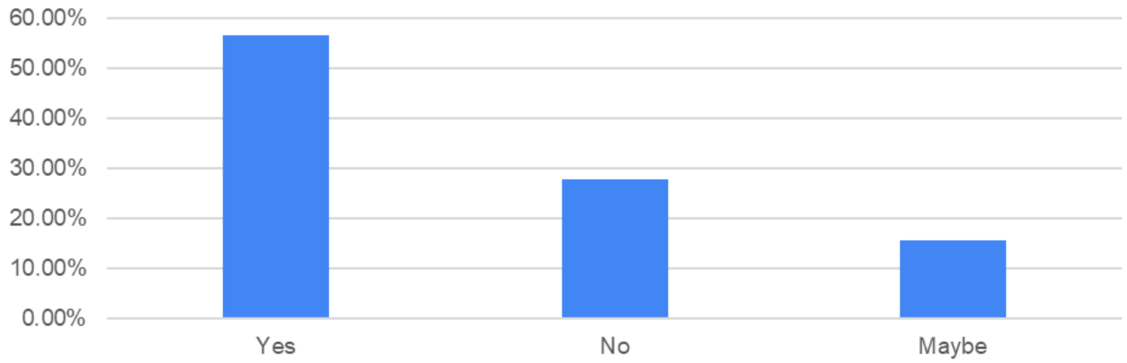


*Figure 4.5*
*Any Security Controls Implementation for SME*

Even if a company hasn't adopted any existing cybersecurity standards or frameworks, there's a good probability they've established some form of security measures. As previously said, nearly half of SMEs said they don't have any kind of standard or framework in place during the survey, and only a handful more said they have any form of cybersecurity measures in place on their own. Figure 4.5 shows that roughly 56 percent of SMEs have implemented security controls, either on their own or as part of the standard or framework they have embraced.

It shows that many SMEs are not even aware of the cybersecurity controls and their implementation. Also, around 28% of the SMEs do not have any cybersecurity controls implemented.

## 4.4 Current State of Physical Security Controls in SMEs

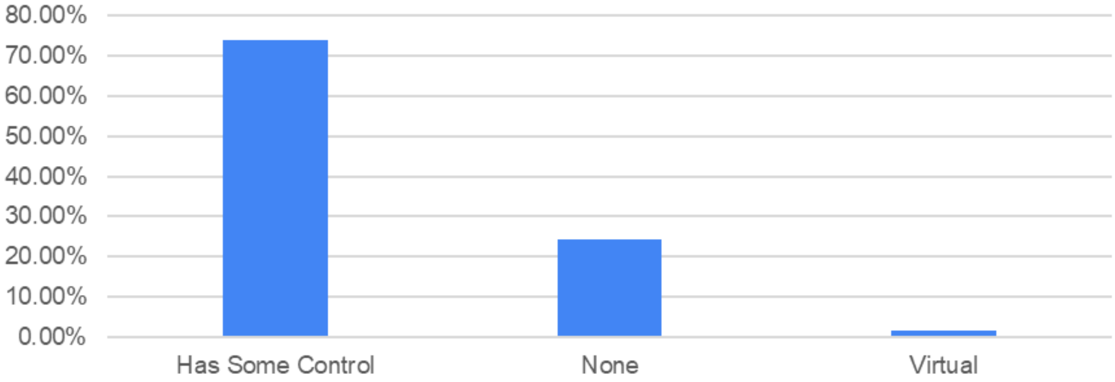


*Figure 4.6*
*State of Physical Security Controls Implementation among SMEs*

Figure 4.6 shows that more than 20% of SMEs with some cybersecurity measures do not have any physical controls in place.

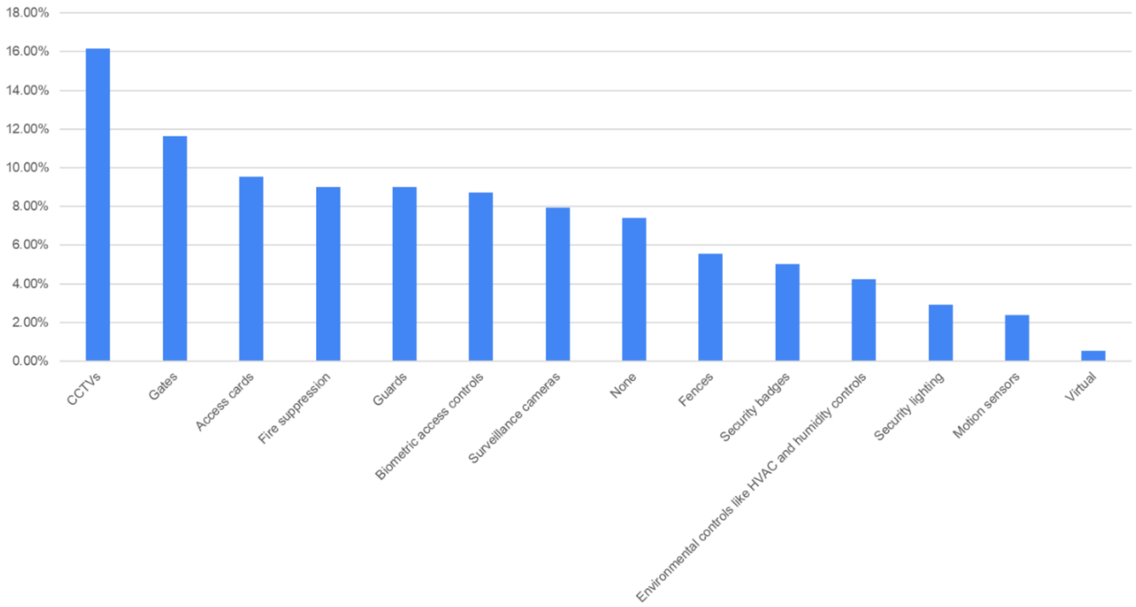


*Figure 4.7*
*Physical Security Controls Implementation among SMEs*

Figure 4.7 shows that more than 7% of SMEs lack any mechanism that could be classified as physical controls. The most popular physical controls, according to my research, were CCTVs, physical gates, and access cards.

### 4.5 Current State of Technical Security Controls in SMEs

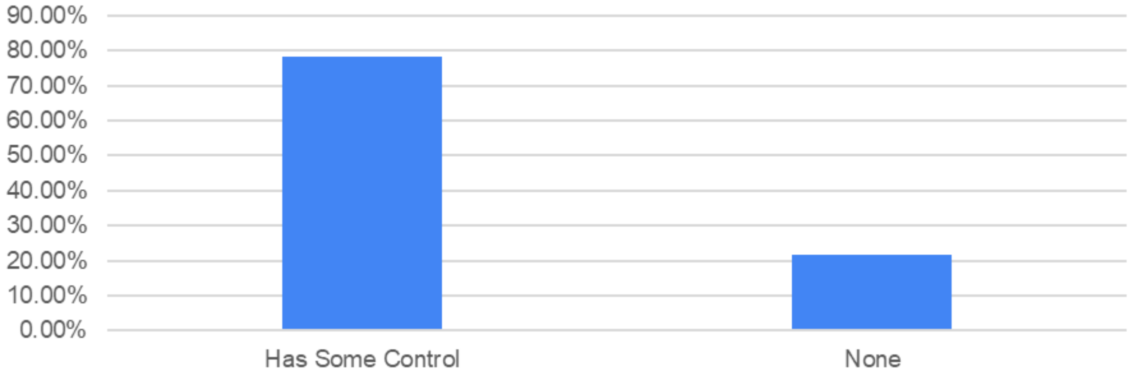


*Figure 4.8*
*State of Technical Security Controls Implementation among SMEs*

Furthermore, as shown in figure 4.8, 20% of SMEs with some cybersecurity measures in place have no technical controls in place.

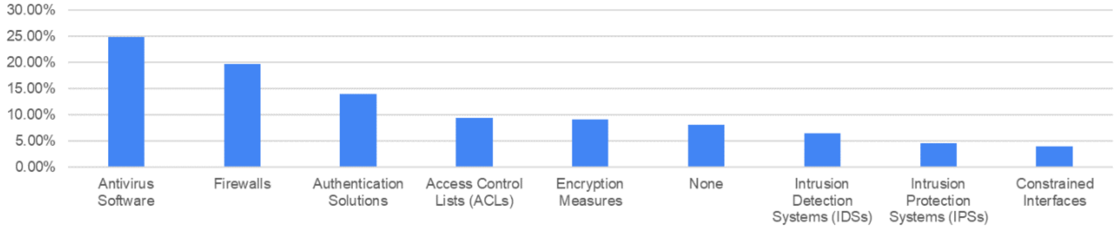


*Figure 4.9*
*Technical Security Controls Implementation among SMEs*

Figure 4.9 shows that more than 7% of SMEs do not have any technical or logical controls. Antivirus software and a firewall were also found to be the most preferred technological measures.

### 4.6 Current State of Administrative Security Controls in SMEs

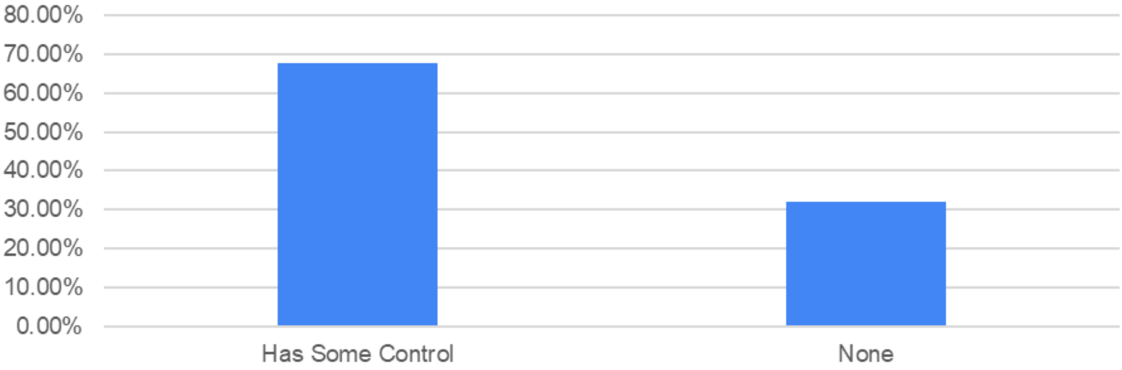


*Figure 4.10*
*State of Administrative Security Controls Implementation among SMEs*

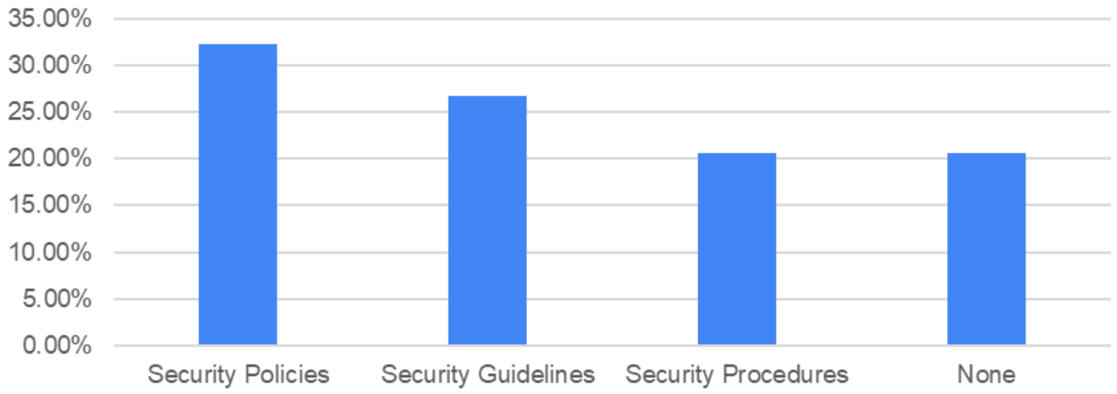


*Figure 4.11*
*Administrator Security Controls Implementation among SMEs*

Figure 4.10 shows that more than 30% of the SMEs who claimed to have minimal controls in place do not have any administrative controls. According to Figure 4.11, more than 20% of SMEs do not have any security policies, processes, or guidelines in place as administrative controls. Furthermore, while a large percentage of SMEs have security policies in place, security procedures and standards are not up to par.

### 4.7 Frequency of Security Awareness Training for Employees in SMEs

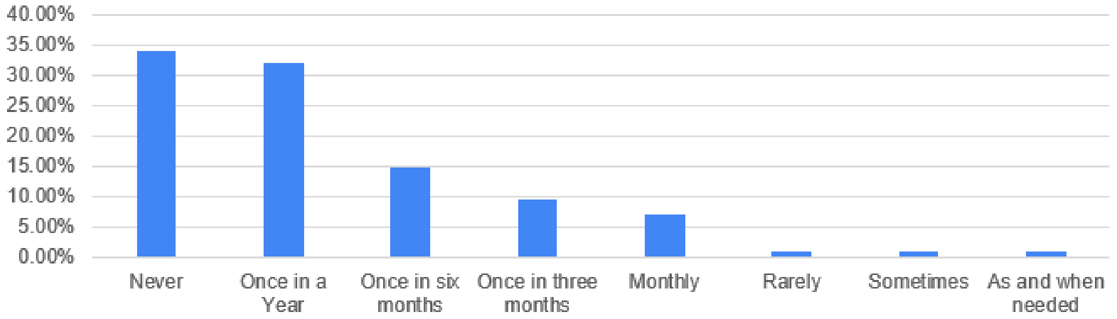


*Figure 4.12*
*Frequency Security Awareness Training for Employees in SME*

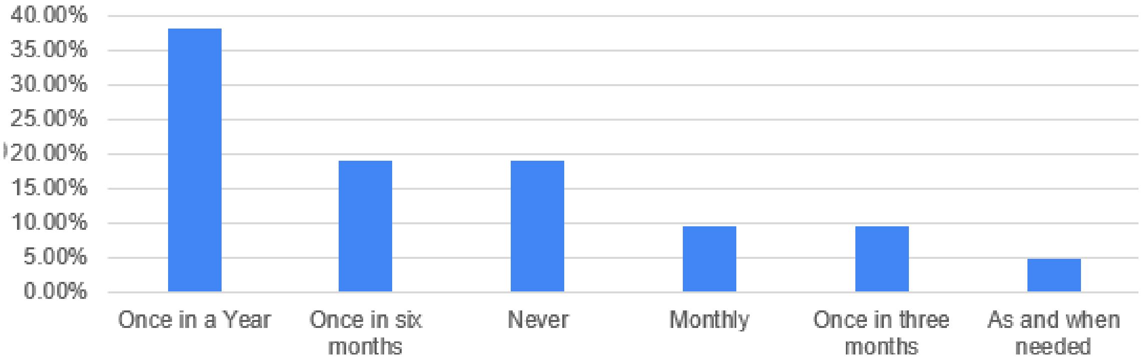


*Figure 4.13*
*Frequency Security Awareness Training for Employees in SMEs* having Existence between 5 to 10 years

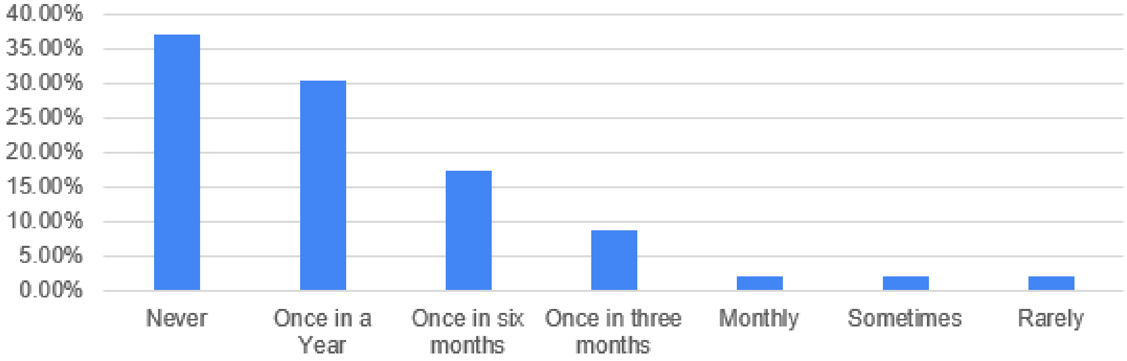


*Figure 4.14*
*Frequency Security Awareness Training for Employees in SMEs* has Existence for more than 10 years

Figures 4.12, 4.13, and 4.14 show that roughly 34 percent of all SME's have never provided security awareness training to their employees. 37% of SMEs with more than ten years in business and 38% of SMEs with five to ten years in business said they had never received such training.

### 4.8 The biggest problems faced by SMEs while implementing or deciding/planning to implement Cybersecurity Controls

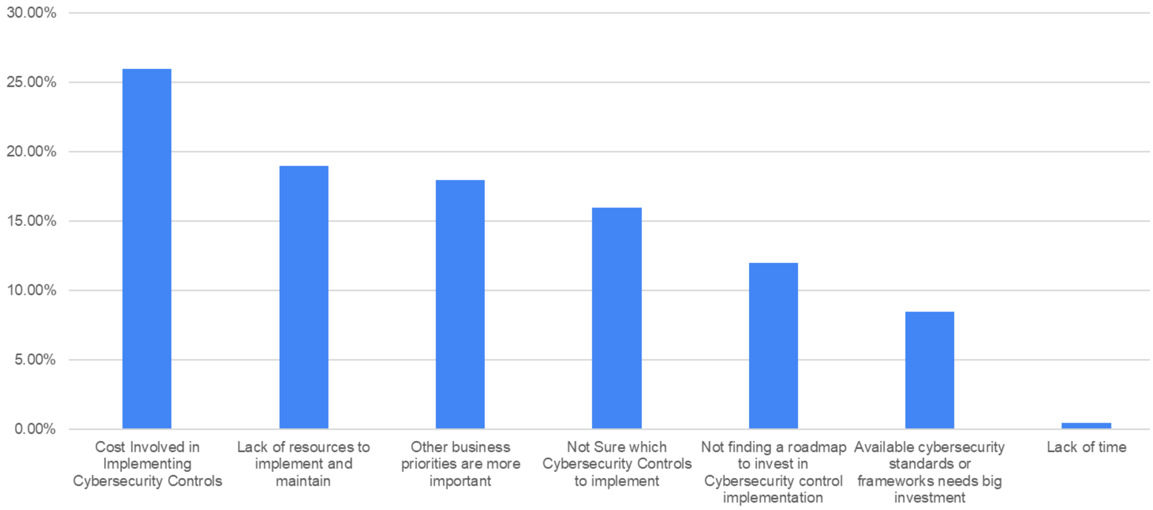


*Figure 4.15*
*The biggest problems faced by SMEs while implementing or deciding/planning to implement Cybersecurity Controls*

When being asked about problems faced during cybersecurity implementation, SMEs believe they have financial difficulty, a lack of resources, and other essential business priorities when it comes to implementing and maintaining cybersecurity, as shown in Figure 4.15.

### 4.9 Experience of Cyber-Attacks Faced by SMEs

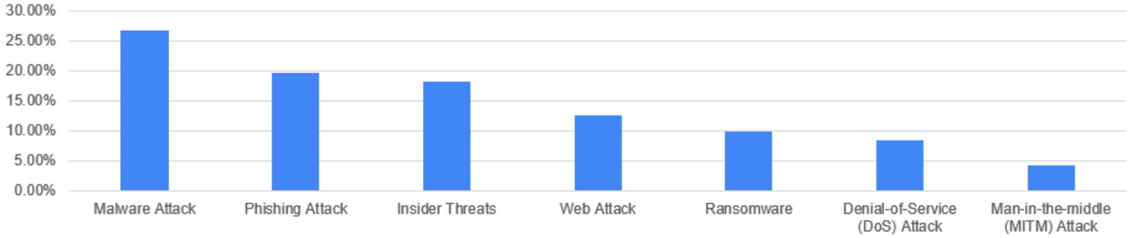


*Figure 4.16*
*Cyber threats faced by SMEs*

Figure 4.16 shows that malware assaults, phishing attacks, insider threats, web attacks, and ransomware are the top five areas of worry for SMEs who have experienced cyber-attacks. Apart from this, a few SMEs identified DoS and MITM assaults as the least dangerous cyber-threats.

### 4.10 Expectations of Security Standard or Framework from SMEs

During the survey's summary, I received input about expectations of security standards or frameworks for their business. Several SMEs asked if they needed simple steps to implement toward cybersecurity adoption, citing their concerns about security, safety, and avoiding data theft, among other things.

### 4.11 Triangulation of the Results

A technique for improving the validity and trustworthiness of research findings is triangulation. While validity is concerned with how precisely a study represents or evaluates the notions or concepts being explored, credibility relates to how trustworthy and convincing a study is. Triangulation can assist in ensuring that basic biases brought on by the use of a single method or a single observer are addressed by combining theories, methods, or observers in a research study. To provide readers with a more complete explanation, triangulation also makes an effort to examine and describe complex human behaviour in a variety of ways. This method, which may be applied to both quantitative and qualitative studies, allows for the validation of data (Noble and Heale, 2019).

As shown in figure 4.17, triangulation offers a choice of datasets to explain various elements of an interesting phenomenon, which might enhance research. It also aids in debunking cases where a dataset invalidates an assumption made using data from another. When one set of findings supports another set, it might help confirm a hypothesis. Triangulation, in the end, can assist in explaining a study's findings. The idea that approaches yielding the same outcomes increase the confidence in the research findings is at the heart of triangulation. It helps to validate the hypothesis.

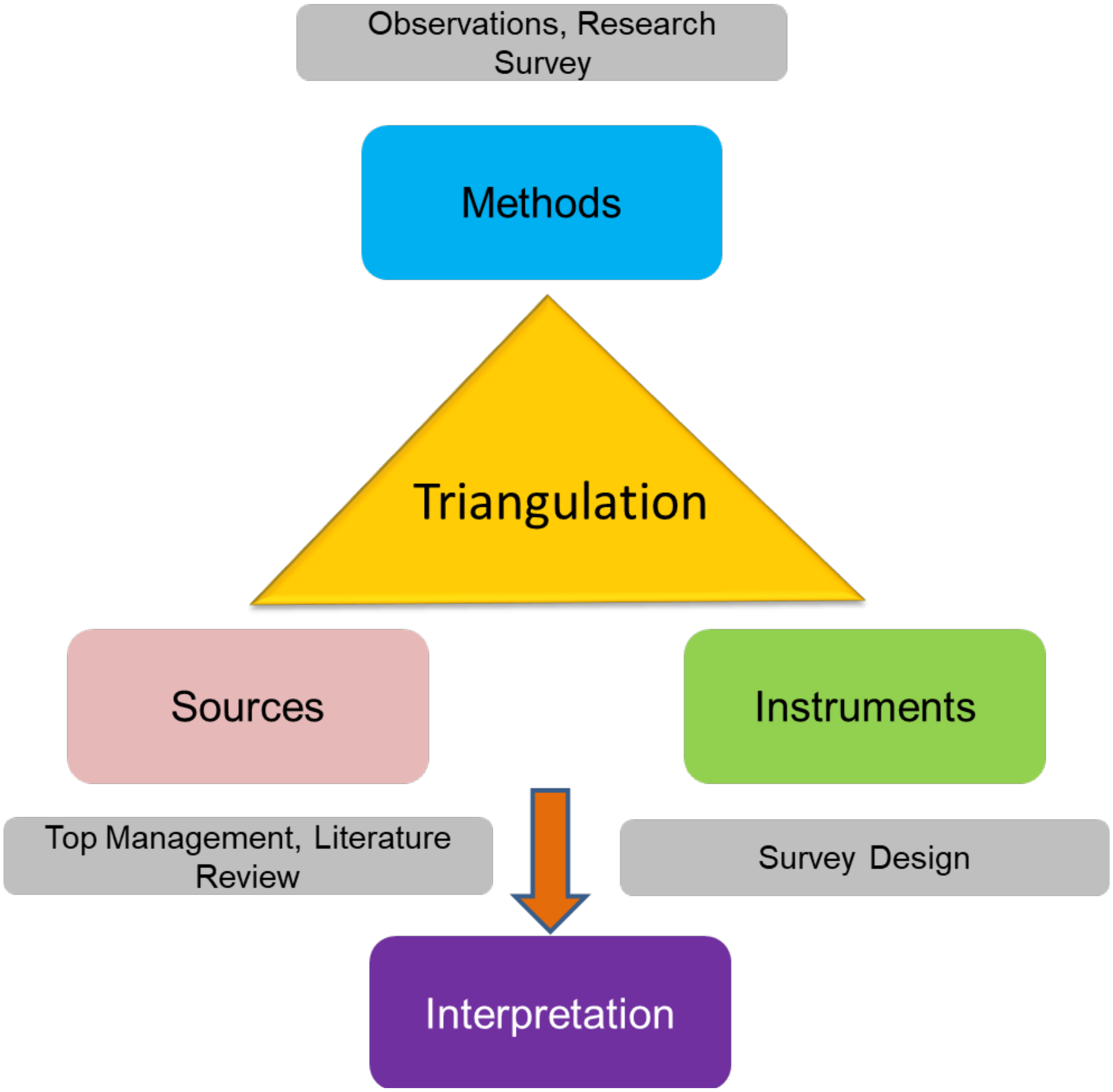


*Figure 4.17*
*Triangulation of the Results*

### 4.12 Data Analysis on Survey Data

I have done some statistical analysis on the survey data, which was gathered from different audiences working in different types of industries. The data was gathered through a survey to understand the current scenarios of SME's, how they are functioning, and what types of security protocols are being followed. The survey data shows the different attributes gathered from the individuals like core of the industry, age of the SME, what type of standards or framework is implemented, whether the SME is having security controls placed, and if there are any security controls, then what type of security controls and how many controls they have. In addition to that, I have verified if there are any technical and administrative controls have been placed or not. The data also shows us the frequency of security awareness training conducted for employees in the company. Lastly, I have gathered some information on what types of problems are being faced while planning or implementing cybersecurity controls. Then I asked whether the company has suffered any cyberattacks or not, and if a cyberattack is happening, then what type of cyberattack has happened.

I conducted exploratory data analysis on this data in order to gain some insights into the data and determine what types of inferences can be drawn from it. I conducted exploratory data analysis on this data in order to gain some insights into the data and determine what types of inferences can be drawn from it. Hence, I have started with some basic data analysis. I have seen that there are a lot of SMEs that are older than 10 years and have taken part in the survey. Figure 4.18 shows the data distribution. Hence, I have started with some basic data analysis. I have seen that there are a lot of SMEs that are older than 10 years and have taken part in the survey. Figure 4.18 shows the data distribution.

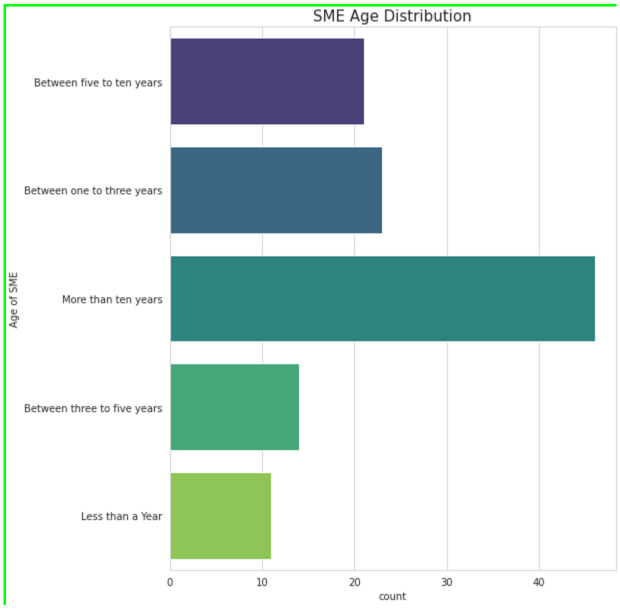


*Figure 4.18*
*Data Distribution : Age of participant SMEs*

The people who took part in the research survey were industry working professionals, and most of them were directors, owners, or C-level executives. Figure 4.19 shows the data distribution of the different roles.

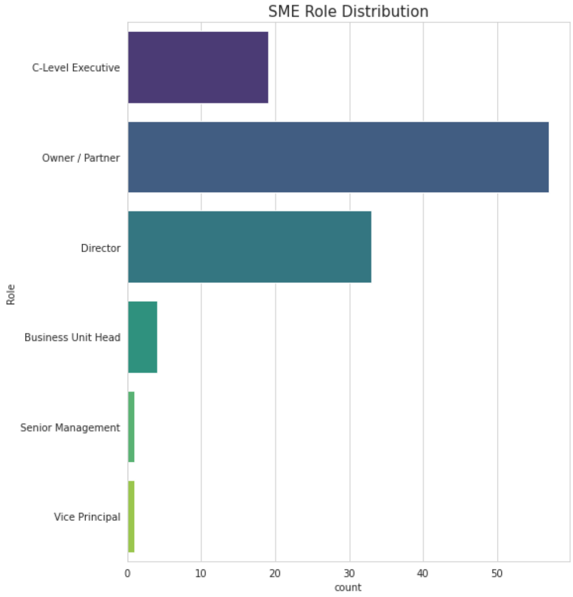


*Figure 4.19*
*Data Distribution : Participant's Role in SME*

It is very important to understand what frameworks or standards a particular SME has implemented, as this will give a better understanding of security controls in the organization. If SME's have standards or frameworks, they must have better security control implementation. Figure 4.20 shows the data distribution of available standards or frameworks implemented in the SMEs. It can be seen that most of the SME's are having ISO 27001 cybersecurity frameworks implemented, and most of those don't have any frameworks or any standards implemented.

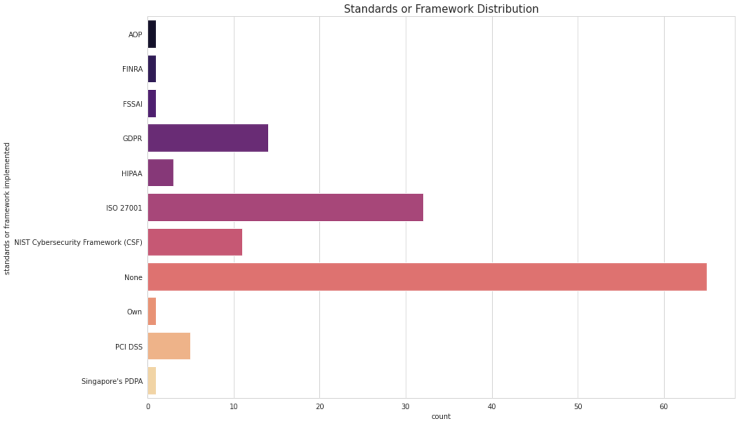


*Figure 4.20*
*Data Distribution : Standards or Frameworks adopted by SME*

The data distribution in Figure 4.21 shows us the basic idea of how many companies are actually using cybersecurity controls. According to the statistics shown below, I can infer that there are a lot of companies using cybersecurity controls, but most of these companies are not using security controls or are not fully aware of the same.

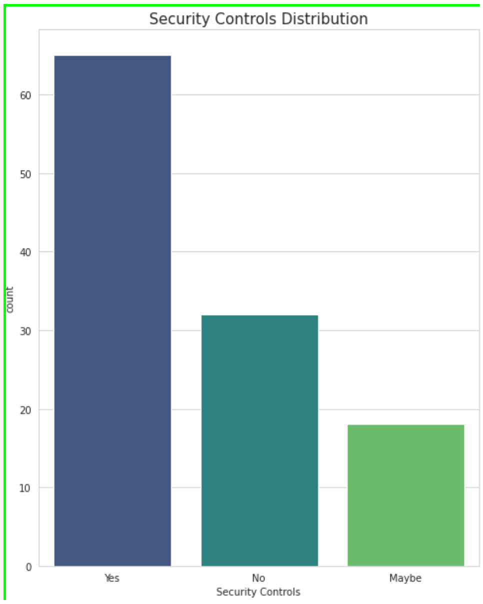


*Figure 4.21*
*Data Distribution : Security Controls Implementation by SME*

I gathered labelled data based on the conditions to see if their companies have undergone any cyberattacks because I need to identify if a particular company will undergo a cyberattack based on some conditions, such as the number of security controls implemented at them and the type of security controls implemented. The following data distribution in figure 4.22 shows if a SME has undergone a cyberattack and how many SMEs have not faced it. I can see that there are many SMEs who have not faced any cyberattacks, and there are a few who have faced cyberattacks or are not even aware of whether they have faced any such cyber attacks. According to this analysis, I can infer that there is an imbalance between the two classes.

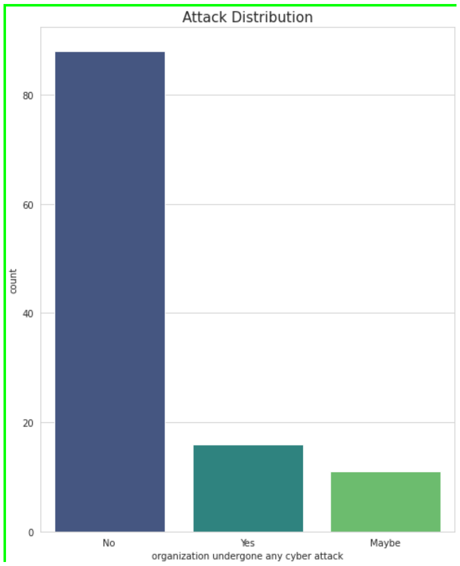


*Figure 4.22*
*Data Distribution : Cyber Attacks on SME*

During the analysis of cybersecurity controls, there are different controls in an organization, like physical security controls, technical security controls, and administrative controls. To protect structures and the equipment inside, physical security controls are used. In other words, they allow authorised visitors or entities but restrict those who are unauthorized. Even while an organization's network and other cybersecurity controls are crucial, physical security threats and breaches must be avoided in order to protect the organization's technology, data, and any employee with access to the facility. Organizations or facilities are vulnerable to theft, vandalism, fraud, and other physical security risks if SME don't have related controls in place. The data distribution in figure 4.23 shows that the different physical controls used in SMEs and the top most are CCTV's, gates, access cards, biometric access, access controls, and surveillance cameras, which are the basic and most used security controls used.

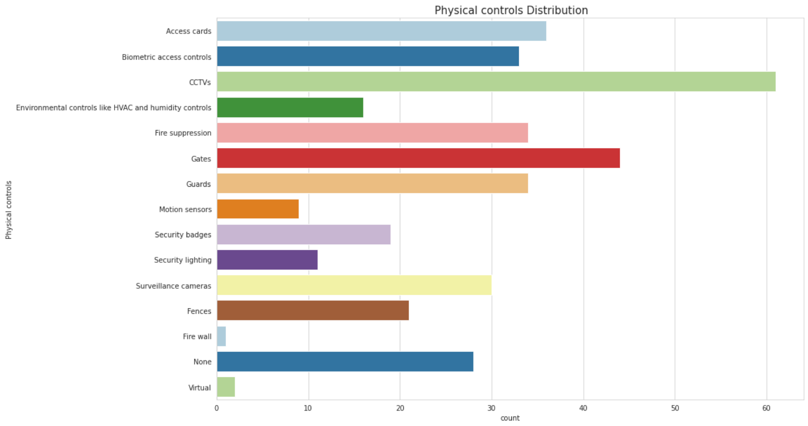


*Figure 4.23*
*Data Distribution : Physical Controls by SME*

A system is protected from cyberattack by the hardware and software components of technical controls. Firewalls, intrusion detection systems (IDS), encryption, and identification and authentication methods are a few examples of such technical controls. Technical controls' hardware and software components work together to protect a system from cyberattacks. The data distribution in figure 4.24 shows the top most commonly used technical security controls used in companies. By analysis of the data distribution, I can see that antivirus software, firewalls, and authentication solutions are the most popular security solutions.

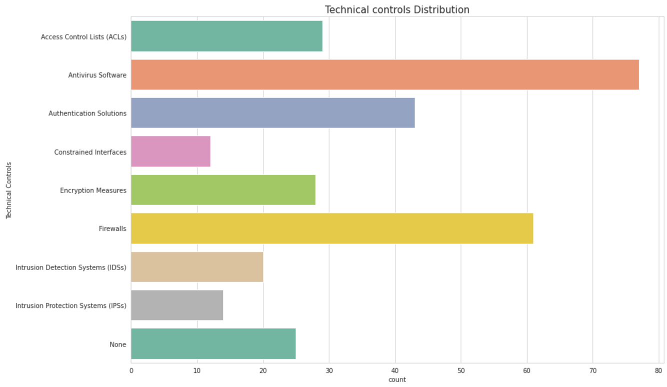


*Figure 4.24*
*Data Distribution : Technical Controls by SME*

Administrative controls specify the human elements of security. It includes all levels of employees within an organisation and determines who has access to what information and resources using methods like relevant education and knowledge, strategies for hiring and firing staff, recovery and disaster readiness plans, personnel accounting and registration. The data distribution in figure 4.25 shows that security policies and security guidelines are the most commonly used security controls in an organization.

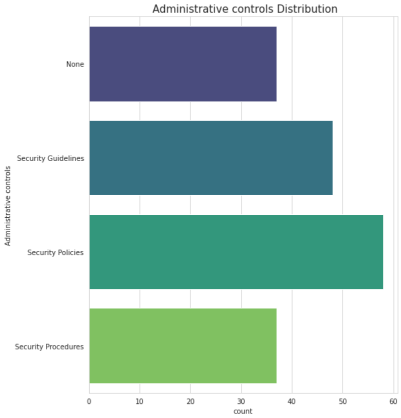


*Figure 4.25*
*Data Distribution : Administrative Controls by SME*

Different cyber attacks affect organizations' critical resources, and there are different cyber attacks because of which the resources get affected. While predicting if a SME has undergone any cyber attack, I also need to analyse what type of cyberattack can happen. By visualising the data distribution in figure 4.26, I can infer that malware attacks, phishing attacks, and insider threats contribute to the most common attacks.

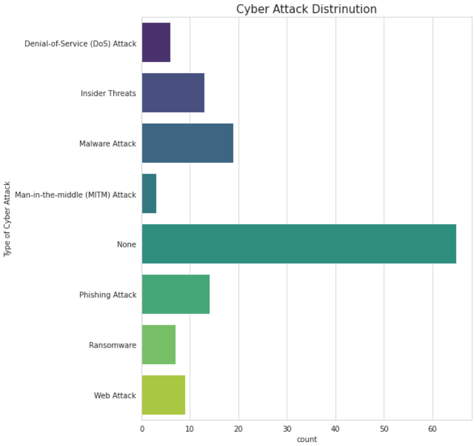
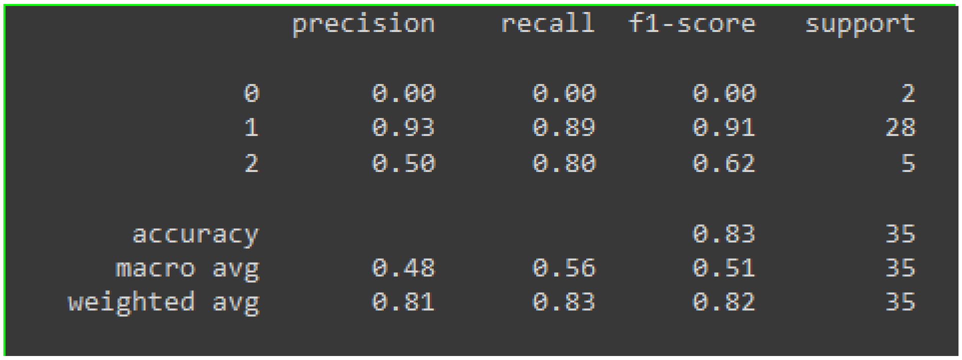


*Figure 4.26*
*Data Distribution : Types of Cyber Attacks Faced by SME*

I have used the survey data to predict if a company will undergo a cyberattack or not. As a result, I used various features, such as the age of SMEs, the types of different cybersecurity controls used by SMEs, and whether or not they use security controls. My hypothesis states that if an SME is using security controls, then there is a high chance that it will not undergo a cyber attack. There will be a possibility of avoiding any cyberattack based on the security controls and measures undertaken.

To support my hypothesis, I have built a classification algorithm to predict if a SME will undergo a cyber attack or not. Here, 0 means “May Be”, 1 means "No", and 2 means “Yes”. Hence, according to the classification report, I can infer that there is a high accuracy that a company will not undergo a cyber attack and there is a lower chance that it will undergo a security attack. Figure 4.27 shows us the classification report of the Classification Algorithm.



```
              precision    recall  f1-score   support

           0       0.00      0.00      0.00         2
           1       0.93      0.89      0.91        28
           2       0.50      0.80      0.62         5

    accuracy                           0.83        35
   macro avg       0.48      0.56      0.51        35
weighted avg       0.81      0.83      0.82        35
```

*Figure 4.27 Classification Report of the Classification Algorithm*

## 4.13 Summary

As a result of the foregoing findings of the study survey, it is clear that more than half of SMEs are completely behind in terms of cybersecurity posture implementation. Furthermore, SMEs with limited cybersecurity controls are still unable to protect people, processes, and technology sectors from cyber threats as a whole. In the next chapter, research will go through what it has seen in the SME category in greater detail.

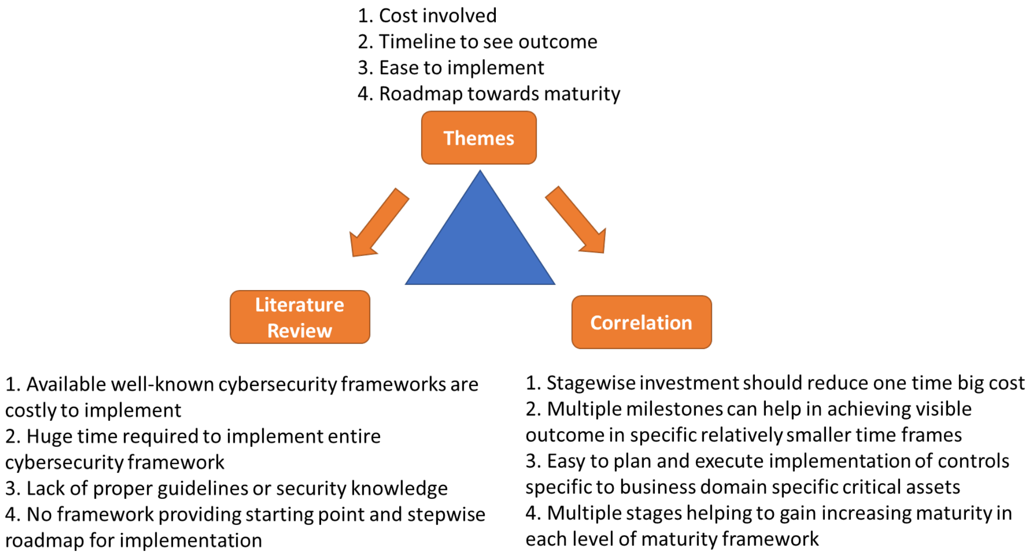
# CHAPTER V:

# DISCUSSION

## 5.1 Discussion of Results

For SMEs, implementing cybersecurity controls should be a well-structured process that contributes to their company's domain-specific demands. If cybersecurity measures have a tangible advantage in the business domain, they will attract more SMEs and persuade them to invest in their implementation. Many times, top cybersecurity standards or frameworks force businesses to implement a comprehensive set of controls, many of which aren't relevant to their industry. Each business domain has its own set of vital assets that the company relies on to execute its operations.

Also, as shown in triangulation figure 5.1, I have shared the link between the themes, correlations, and literature discussions. It will be further discussed in sections 5.3 and 5.4.



1. Cost involved
2. Timeline to see outcome
3. Ease to implement
4. Roadmap towards maturity

1. Available well-known cybersecurity frameworks are costly to implement
2. Huge time required to implement entire cybersecurity framework
3. Lack of proper guidelines or security knowledge
4. No framework providing starting point and stepwise roadmap for implementation

1. Stagewise investment should reduce one time big cost
2. Multiple milestones can help in achieving visible outcome in specific relatively smaller time frames
3. Easy to plan and execute implementation of controls specific to business domain specific critical assets
4. Multiple stages helping to gain increasing maturity in each level of maturity framework

*Figure 5.1*
*Linking the themes, correlations, and literature discussions*

This chapter will go into the specifics of the research findings, as well as a review of the existing literature and a suggested conceptual framework.

### 5.2 Discussion of Research Questions

The valuable inputs from participant SMEs in this section referring to the questions of the research survey will be discussed in the following subsections.

#### 5.2.1 Age of Small and Medium Enterprises (SMEs)

It was noteworthy that nearly two-thirds of the participants experienced SMEs. It demonstrates that SMEs with a longer history were more eager to give more information and discuss the issues they must have encountered along the way. Also, in the coming responses to the research questions, one will observe the value of the inputs sharing the lag in the implementation of the overall cybersecurity posture of the SMEs.

#### 5.2.2 Current State of Implemented Standards or Frameworks in SMEs

There are several mature cybersecurity standards and frameworks that are already leading the market in terms of cybersecurity control implementations. If such measures are not in place, it simply signifies that the organization lacks an organized defense against cyber attacks. If cybercriminals can take advantage of this major weakness inherent in particular SMEs, it can result in financial loss or even damage their reputation in the market, lowering their total brand value. More than 50% of SMEs do not have any kind of cybersecurity framework or standards adopted, which is a big risk.

#### 5.2.3 Current State of Security Controls in SMEs

Regardless of the response to question Q2, the survey gathered information to see if SMEs have already implemented any security controls. The survey supplied three options for this question: (a) Yes, (b) No, and (c) Maybe. It wanted to check if SMEs had adopted a particular standard or framework without actual implementation of cybersecurity controls for the same. More than 55% of SMEs have implemented security controls, either independently or as part of the standard or framework that they have adopted. More than 10% of SMEs were unsure whether their organization had any cybersecurity controls in place. It shows a lack of skills for understanding cybersecurity controls. The remaining SMEs did not have any cybersecurity controls in place. This means that 45 percent of SMEs are at risk of cybercrime.

### 5.2.4 Current State of Physical Security Controls in SMEs

Physical security controls are security measures that are implemented in physical structures to prevent or dissuade unauthorized entities from accessing a company's valuable assets. Physical security is crucial because, despite its low probability, it often results in significant damage. Natural disasters, supply system concerns, politically motivated crises, and even man-made problems can all obstruct it. Floods, earthquakes, storms or tornadoes, fires, and other natural disasters are beyond human control. Unauthorized access, explosions, vandalism, fraud, and other man-made hazards are frequently totally or partially insider threats. Supply systems can produce challenges such as power outages or communication disruptions. Even deadly, politically motivated crises such as strikes, riots, civil disobedience, and terrorist attacks can compromise physical security. Gates, biometrics, motion alarm systems, thermal alarm systems, closed-circuit surveillance cameras, security guards, security dogs, picture ID, and other physical security controls are examples. Lack of physical controls will contribute to weaknesses that can be used by hackers to gain access to internal assets of the organization, such as IT systems and critical data.

### 5.2.5 Current State of Technical Security Controls in SMEs

Technical or logical controls are used to ensure the security of information or important data throughout the physical structure and via the organization's network. They employ technology as the basis for regulating access or use. The most commonly used technical controls include network authentication, antivirus software, file integrity auditing software, encryption mechanisms, smart cards, and access control lists (also known as ACLs). If technical control's implementation is improper, any cyber-criminal or unauthorized user may access important data, IT devices, and applications.

### 5.2.6 Current State of Administrative Security Controls in SMEs

Security policies assist the company in defining a set of broad concepts, whilst standards are utilized to establish minimum requirements for achieving the goal. The simplest criteria for determining eligibility for security clearance is locking down the operating system of an employee's laptop or desktop when he or she is absent. Guidelines are suggested best practices that are not required to be followed in their current form but that assist employees or other stakeholders in the business in following the rules in various instances. Procedures are steps defined in clear and logical language that take into account legal requirements to adopt policies that will be applied in the company. This makes it easier for stakeholders or employees to do the task safely. Security controls that define well-defined processes, procedures, and required guidelines for driving all stakeholders of the organization come under administrative controls. People's involvement is required to succeed in the implementation of overall cybersecurity for any organization, and security controls that define well-defined processes, procedures, and required guidelines for driving all stakeholders of the organization come under administrative controls. This type of control includes disaster preparedness, disaster recovery plans, employee recruiting through resignation, separation of roles, and many more areas. Some of the most significant administrative controls are training and awareness. Administrative controls also supply crucial plans to assist businesses. Any firm must have an Incident Response (IR) plan in place to respond to a cyber threat and avoid the negative effects of a successful cyber-attack (Naseer, 2021). SMEs must capture such incidences in a suitable format, followed by an issue report outlining the detailed cause identification and a roadmap for problem resolution. Generally, administrative controls control the behavior or change the way of working of the people of the organization. As human beings are considered the weakest link to carry out any cyber-attack, these controls are very important to get implemented.

### 5.2.7 Frequency of Security Awareness Training for Employees in SMEs

Cybercriminals invest a lot of time and effort into developing more complex assaults on an organization's essential assets, and it becomes clear over time that the most vulnerable link for them is its employees or stakeholders. Even if a small business invests in the best technical tools and processes, it still requires human leadership. The largest hazard to the SME is if those working within or for it are circumventing cybersecurity measures in any way. Therefore, employees in any SME will play a critical part in the effective implementation of cybersecurity; therefore, having security policies and associated areas is insufficient; instead, instilling the importance of cybersecurity in each employee's behavior and actions is more critical (Li, 2021). As a result, cybersecurity awareness training that emphasizes the importance of the subject is necessary. SME risks are reduced by more cybersecurity awareness training each year. Even firms must have a policy requiring new workers to complete security awareness training and be aware of the organization's environment and assets before being granted access. When SMEs' staff are well-involved and given cybersecurity awareness training, they become the first line of defense against cyberattacks (Ponsard, 2019). As explained in earlier sections, human beings are the weakest link in carrying out any cyber-attack. Cybersecurity awareness training for employees and other stakeholders is the most important tool to equip them with skills and knowledge to avoid being a victim of cyber-attack tricks.

### 5.2.8 The biggest problems faced by SMEs while implementing or deciding/planning to implement Cybersecurity Controls

The first step in every journey is always more important than the rest. Cybersecurity is a broad topic for any business, and evolving umbrellas of relevant controls can assist them. It also necessitates a large budget as an investment and a large number of resources to be achieved. The majority of cybersecurity standards work on the basis that enterprises either implement them entirely or don't. No levelled method can provide investors with confidence. Looking at these top three issues, it's clear that SMEs don't believe investing in cybersecurity would help them achieve their business objectives. Lack of knowledge, inability to identify a path to invest step by step in cybersecurity control implementation and available cybersecurity standards or frameworks are all challenges that prevent them from moving forward with the implementation of existing cybersecurity controls. In particular, the time necessary to establish total cybersecurity safeguards is cited by SMEs as the last issue.

### 5.2.9 Experience of Cyber-Attacks Faced by SMEs

Malware attacks are cyber-attacks that are carried out with the help of malicious software. Malware includes ordinary computer viruses, worms, trojans, adware, malvertising, and other spyware, to name a few. Technical safeguards are less effective against phishing attempts because emails can overcome firewalls, two-factor authentication, and other security measures. Furthermore, restricting a few processes that are open to receiving emails from the general public, such as the human resource management team receiving resumes from job hopefuls, is challenging. To avoid such cyber-attack techniques, all users of any organization must have a higher level of cybersecurity awareness (source: Hong, 2012). Insiders, who might be employees, vendors linked with the firm, or even stakeholders, can frequently obtain access to critical assets in the environment. Such a person is frequently involved in cybercriminal operations directed against that organization. Insider risks are becoming increasingly prevalent in recent cyber-attacks. Individuals working for businesses must follow well-established cybersecurity policies as this threat is exhibited by human behavior, in which an individual or group begins by ignoring, manipulating, neglecting, or committing malevolent acts without adhering to those policies (Greitzer, 2011). Devices owned by the organization, such as laptops or desktops, can have appropriate restrictions installed, but devices owned by workers, stakeholders, vendors, guests, or even visitors, such as smartphones, desktops, or laptops, require a "Bring Your Own Device (BYOD)" policy. Tools that use these privately owned devices can pose a danger to small businesses. The BYOD strategy also aids in the reduction of insider threats (Baillette, 2018). Nowadays, employees who are either enterprise staff or borrowed from vendors do not have a lifelong contract with any enterprise. Any company's internal knowledge is critical information. It's also true that these stakeholders can't contribute to the company if they don't have enough information. It's crucial for knowledge management's cybersecurity. Enterprises must strike a balance between the degree of freedom and security safeguards when it comes to knowledge management. Regular training, motivation, recognition, the enterprise attitude toward employees, specific methods to minimize the disclosure of enterprise knowledge to external organizations, and proper treatment for any process infraction are all critical (Popescul, 2011). Web applications and their security have become increasingly important since many firms have transitioned to a cloud-based environment. Cybercriminals use web attacks to gain access to, disrupt, or leak information flow that is essential to an organization's survival. One of the major technical areas that should be highlighted in relevant rules implemented by the organization is basic vulnerabilities such as the implementation of authentication and authorization utilizing user credentials flow. During security awareness training, basic cyber hygiene recommendations such as selecting complicated passwords, using multiple passwords for different online apps, and so on should be enforced (Bang, 2012). As a result, web platforms hold information about employees and consumers, and data leaking has several ramifications, such as being used in phishing attempts or requiring a ransom to avoid being exposed on black sites. Many SMEs contributed vital information on the cyber-attacks they are facing. Nowadays, hackers target an organization's servers to obtain a copy of data before encrypting the entire server's data. Later, they demand a ransom to prevent the data they have on them from being leaked and/or to obtain a decryption key to restore the server's data to its original state. A few hackers try to overload the target organization's network, rendering it inaccessible to authorized users, which is known as a denial-of-service attack. A Man-In-The-Middle attack on data in transit occurs when cybercriminals can read and/or change information flow references to any organization at a separate location.

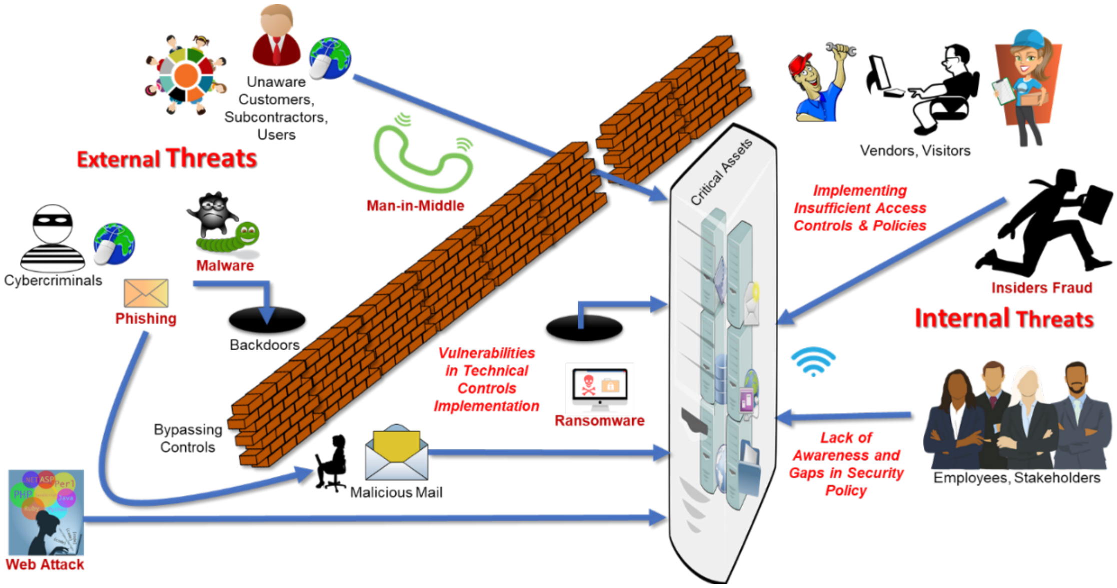


*Figure 5.2*
*Cyber threats landscape faced by SME*

Figure 5.2 shows that malware attacks, phishing assaults, insider threats, web attacks, and ransomware are the top five areas of worry for SMEs who have been victims of cyber-attacks. Malware, phishing, ransomware, online attacks, and man-in-the-middle attacks can all be stopped with appropriate technical controls, but cybersecurity awareness training can also help to reduce the risk of falling victim to phishing attempts. Insider dangers can be reduced by strong rules, relevant technology controls, and physical controls. Policies, rules, and procedures acting as administrative controls can improve the effectiveness of technical or physical controls, forming a solid cybersecurity wall that protects an organization's important assets. Figure 18 depicts these points graphically, showing a few critical areas that are responsible for cyber-attacks that SMEs are most vulnerable to. IoT systems are transforming the way data is collected in the digital world today. Beginning with deeply embedded devices that can be injected into the human body to record inputs for data mining, IIoT in the smart factory is confronted with advanced technology and cybersecurity difficulties (Abbasi, 2019; Chen, 2018). IIoT or IoT-based devices are more vulnerable to data security concerns. If the integrity or availability of essential systems is dependent on such devices playing a significant part in workplace safety or life support equipment. It has the potential to endanger human life or destroy physical assets (Boye, 2018). SCADA systems, which are a combination of hardware and software, assist modern businesses in controlling different industrial operations at multiple locations. It also aids in the monitoring, collection, and processing of real-time data by interacting with various IoT devices, such as pumps, valves, motors, and sensors. It has a significant function to play, and it also interacts with HMI software. Using its logging mechanism to record events is also beneficial to the industry. SCADA systems are built on the architecture of PLCs and/or RTUs. If the SCADA system is unavailable for even a short period, it will have a significant impact on the entire organization. As a result, the first critical issue to examine is the availability of SCADA (Papa, 2011). Insider attacks, backdoors, social engineering, conventional operating systems on which it runs, numerous access points, multiple failure points, less changing legacy systems, protocols used for communication, weaknesses in OT, and so on are all areas where SCADA systems can be exposed to cyber-attacks (Nazir, 2017). Data at rest, access control, user privacy, query privacy, query computation integrity, collaborative query execution, SLA, auditing, multi-tenancy, virtualization, and other security challenges are all too frequent in cloud systems. These are growing difficulties for both businesses and cloud providers (Samarati, 2016).

### 5.2.10 Expectations of Security Standard or Framework from SMEs

It was enlightening to learn about the present state of cybersecurity control implementation and how it contributes to cyber risk exposure for SMEs, as well as the challenges they face when planning or implementing cybersecurity controls.

## 5.3 Discussion of Hypothesis

During the research, it was found that SMEs are lagging in the implementation of physical, technical, and administrative controls. Also, there were gaps in the various important implementations within the organization such as frequent cybersecurity awareness training for employees. Also, research has shown that very few SMEs have adopted existing cybersecurity standards and frameworks.

This study hypothesizes that the existing cybersecurity posture of the SME segment organizations is not in a good state due to various issues while considering cybersecurity implementation.

### 5.3.1 Cybersecurity implementation is costly

Implementing cybersecurity controls in accordance with existing leading standards or frameworks necessitates a significant financial and other resource investment. It is one of the biggest issues faced by SMEs. During an analysis study of the top issues faced by SMEs, it is evident that the top management of such enterprises is not able to relate or see the benefit towards the top goals of their business from the investment made in cybersecurity standards implementation. It is because each business domain is different and has a unique business-critical asset. If such a critical asset gets threatened, it may cause serious issues for the SME's sustenance or growth.

### 5.3.2 Cybersecurity implementation needs huge time

During research analysis, it is also evident that many cybersecurity standards have a long list of cybersecurity controls that require a long time frame. Top management needs to invest in a long timeline to see actual implementation and its benefits.

### 5.3.3 Ease of implementation is missing

All the available standards or frameworks are lagging behind to provide a starting point to start implementation of cybersecurity controls. Also, this long list of control implementation requirements requires lots of effort by skilled resources, which is difficult for SMEs.

### 5.3.4 No road map towards maturity

Existing cybersecurity standards or frameworks are not providing staged implementation of the controls. There is no roadmap or motivation for the top management of the SME to go ahead with the implementation of the various cybersecurity controls that will help their business goals.

### 5.3.5 Hypothesis conclusion

During the research studies, it was evident that there is a gap between expectations set by existing cybersecurity standards or frameworks, which are not in alignment with the requirements for the specific domain of SME or the overall benefit for SMEs to relate to or invest in the same.

## 5.4 BDSLCCI Framework

The Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI) will be based on the implementation of the least cybersecurity controls for mission-critical assets following DiD and CIA Triad priorities. It is divided into three steps that will lead to its successful implementation. The BDSLCCI framework implementation journey is broken down into seven steps, as indicated in Figure 5.3, which are further detailed in the following sections.

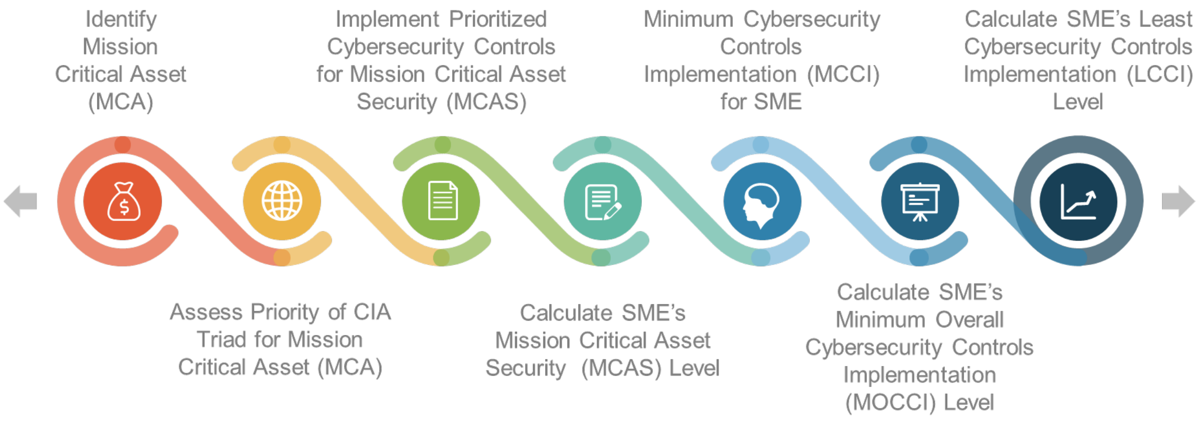

Identify Mission Critical Asset (MCA)
Implement Prioritized Cybersecurity Controls for Mission Critical Asset Security (MCAS)
Minimum Cybersecurity Controls Implementation (MCCI) for SME
Calculate SME's Least Cybersecurity Controls Implementation (LCCI) Level
Assess Priority of CIA Triad for Mission Critical Asset (MCA)
Calculate SME's Mission Critical Asset Security (MCAS) Level
Calculate SME's Minimum Overall Cybersecurity Controls Implementation (MOCCI) Level

*Figure 5.3*
*Seven Steps of Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI)*

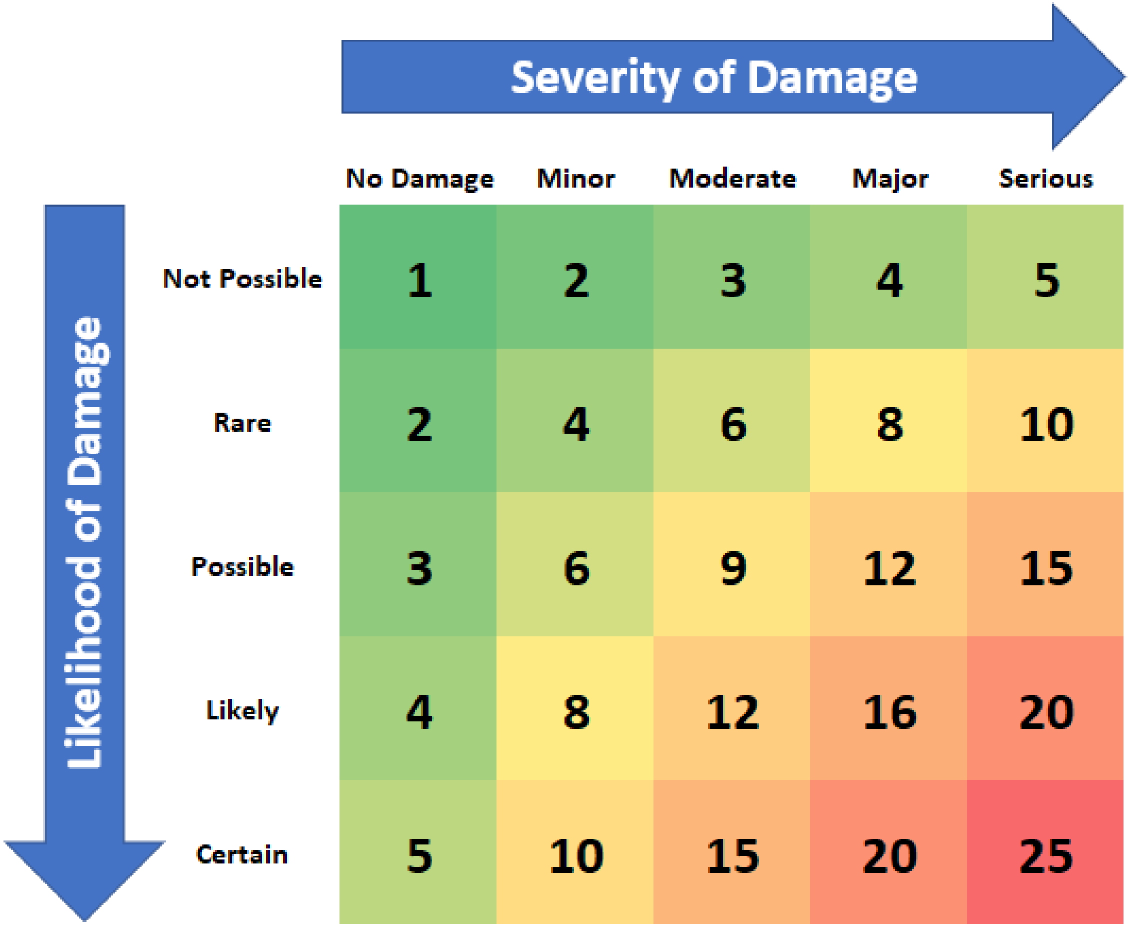
### 5.4.1 Identify Business Domain-Specific Mission-Critical Asset (BDSMCA)

Identify Mission Critical Asset (MCA)

Mission Critical Asset = [Maximum Value] + [Highest Risks] + [Big Impact]

*Figure 5.4*
*Step 1 – Identify Business Domain-Specific Mission Critical Asset (BDSMCA)*

Business Domain-Specific Mission A Critical Cyberspace Asset (BDSMCCA) is any asset in an SME's cyberspace that will have the greatest negative impact on its business if damaged in any or all areas of the CIA. For an SME, BDSMCCA might be an information asset or other key asset with the greatest value and a direct or indirect tie to the company's main operation. If it is breached by cybercriminals, it may have a significant influence on the survival of SMEs. In general, fraudsters continue to analyze such assets to carry out sophisticated cyber-attacks for financial gain, information leakage, acts for the benefit of competitors, and even cyber terrorism. In information security, the value of an information asset can be determined by taking into account the potential for loss due to the exploitation of confidentiality, integrity, and availability (Tatar, 2012). Even BDSMCCA can benefit from the same CIA areas.


Severity of Damage
Likelihood of Damage

| | No Damage | Minor | Moderate | Major | Serious |
|---|---|---|---|---|---|
| Not Possible | 1 | 2 | 3 | 4 | 5 |
| Rare | 2 | 4 | 6 | 8 | 10 |
| Possible | 3 | 6 | 9 | 12 | 15 |
| Likely | 4 | 8 | 12 | 16 | 20 |
| Certain | 5 | 10 | 15 | 20 | 25 |

*Figure 5.5*
*Risk Matrix*

"An effect" is the direct or indirect monetary value that will be required to repair the loss in the respective CIA triad. SME can use quantitative or qualitative analysis approaches to identify risk assessments, which may differ domain-wise or based on the criticality of an asset or even the amount of such assets. For example, risk assessment methodologies for CIS, SCADA, and DCS, for example, will differ from those for e-commerce websites (Patel, 2008). For ERP, E-commerce, or other key assets, a cybersecurity risk analysis model can even use fuzzy decision theory to evaluate each viable alternative in terms of related criteria, as well as fault tree analysis focused on safety and dependability (Henriques, 2018).

Based on the organization's goals and objectives set by management, the risk is also defined by finding answers to four questions, which are: What could go wrong? (2) How likely is it to go wrong? (3) If it goes wrong, what is the impact on the organization? (4) What is the organization’s management opinion on it? (Wall, 2011). An assessment that considers the maximum value and maximum negative impact aids in determining how much damage a key asset can do. Following that, as illustrated in Figure 5.5, the chance of damage and degree of damage can be utilized to calculate a risk rating. BDSMCCA will be applied to critical assets with the highest risk rating number.

SMEs must make a list of all valuable assets to locate the BDSMCCA among them. They can utilize a variety of approaches to link assets to essential business processes.

### 5.4.2 Assess Priority of CIA Triad for Business Domain-Specific Mission Critical Asset (BDSMCA)

$$n(CuIuA) = n(C) + n(I) + n(A) – n(C\cap I) – n(I\cap A) – n(A\cap C) + n(C\cap I\cap A)$$

Assess Priority of
Confidentiality (C),
Integrity (I) and
Availability (A) from
CIA Triad for Mission
Critical Asset (MCA)

*Figure 5.6*
*Step 2 - Assess Priority of CIA Triad for Business Domain-Specific Mission Critical Asset (BDSMCA)*

Once the SME has a clear understanding of one (or a few) BDSMCA, the next stage is to determine what the CIA Triad's cybersecurity priority should be. It will vary depending on the SME domain, as stated in the preceding sections. Even SMEs can choose numerous CIA Triad regions if the chosen BDSMCA has demand for it, as indicated in Table 5.1.

*Table 5.1*
*CIA Mapping with BDSMCA*

| **Damage To** | **Possible Cyber Threats** | **Potential Risks to BDSMCA** |
|---|---|---|
| Confidentiality | Which are cyber threats contributing to disclosure? | List of number of risks if disclosure happens |
| Integrity | Which are cyber threats contributing to alteration? | List of number of risks if alteration happens |
| Availability | Which are cyber threats contributing to destruction? | List of number of risks if destruction happens |

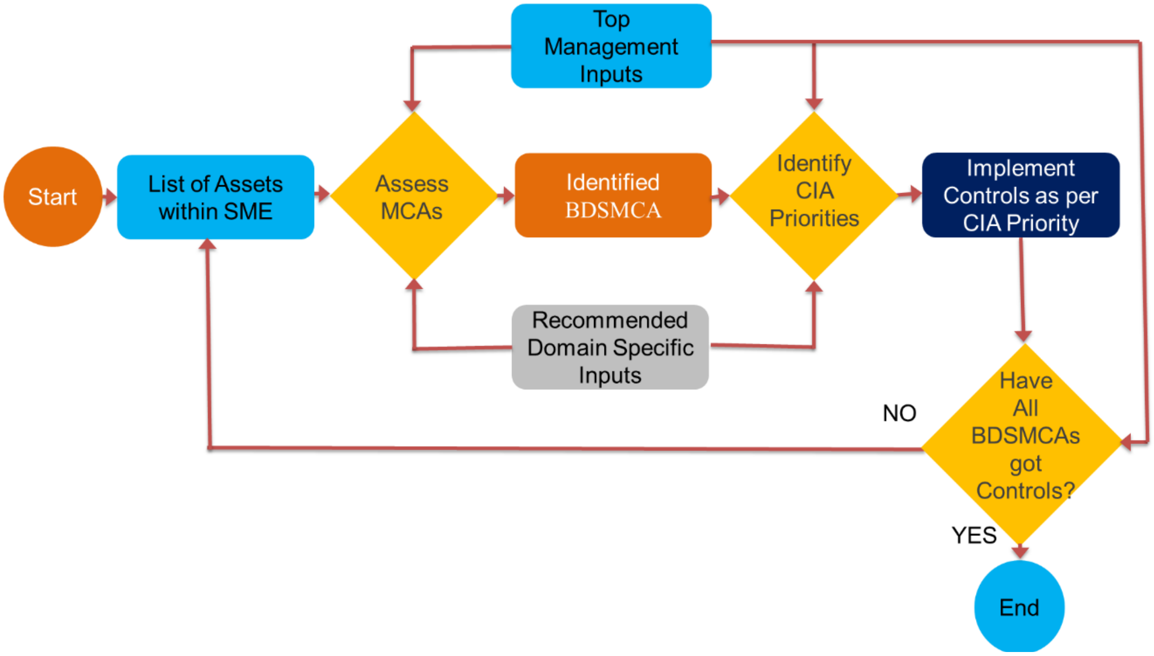
### 5.4.3 Implement Prioritized Cybersecurity Controls for Business Domain-Specific Mission Critical Asset Security (BDSMCA)

Implement Prioritized Cybersecurity Controls for Mission Critical Asset Security (MCAS)

Implementation for MCAS =
[Physical Controls] + [Technical Controls] + [Administrative Controls]

*Figure 5.7*
*Step 3 - Implement Prioritized Cybersecurity Controls for Business Domain-Specific Mission Critical Asset Security (BDSMCAS)*

SME should begin planning how to continue with prioritized cybersecurity controls for BDSMCA as soon as possible, as it is a crown jewel for it. Aside from that, top management, along with all-important stakeholders' involvement, should be sketched out for a complete plan. Actions should be taken to ensure that selected specialist areas of security measures are implemented without flaws.



Top Management Inputs
Start
List of Assets within SME
Assess MCAs
Identified BDSMCA
Identify CIA Priorities
Implement Controls as per CIA Priority
Recommended Domain Specific Inputs
NO
Have All BDSMCAs got Controls?
YES
End

*Figure 5.8*
*The flow of BDSMCA Implementation*

As shown in Figure 5.8, the top management of SMEs can be involved in prioritizing the BDSMCA as they know their domain and its criticality well.

### 5.4.4 Calculate SME's Business-Domain-Specific Mission Critical Asset Security (BDSMCAS) Level

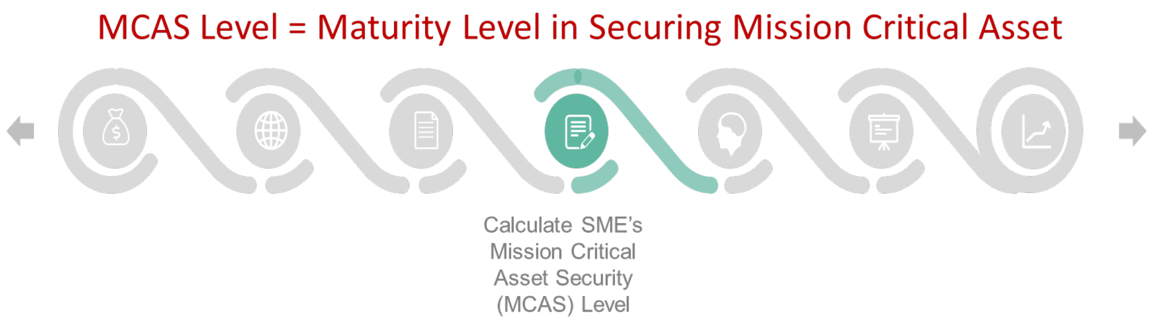

MCAS Level = Maturity Level in Securing Mission Critical Asset
Calculate SME's
Mission Critical
Asset Security
(MCAS) Level

*Figure 5.9*
*Step 4 - Calculate SME's Business Domain-Specific Mission Critical Asset Security (BDSMCAS) Level*

In light of the preceding sections, SMEs must deploy BDSMCAS cybersecurity controls. Levels of least cybersecurity controls for SMEs can be calculated as Mission Critical Asset Security Levels based on increasing cybersecurity controls' adoption in incremental order in the CIA Triad (BDSMCAS Level).

*Table 5.2*
*SME's Business Domain-Specific Mission Critical Asset Security Level (BDSMCAS Level)*

| **Ref to Business Domain-Specific Mission Critical Asset, SME's Primary Focus On** | **GRC Implemented** | **BDSMCAS Level** |
|---|---|---|
| Either of Confidentiality, Integrity, or Availability | YES | 1 |
| Either of Confidentiality and Integrity, Integrity and Availability or Confidentiality and Availability | YES | 2 |
| All Confidentiality, Integrity & Availability | YES | 3 |

According to Table 5.2, if only one part of the CIA Triad is implemented, it is BDSMCAS Level-1; if two aspects are implemented, it is BDSMCAS Level-2; and if all aspects are implemented, it is BDSMCAS Level-3.

### 5.4.5 Minimum Overall Cybersecurity Controls Implementation (MOCCI) for SME

Minimum Overall
Cybersecurity
Controls
Implementation
(MCCI) for SME

MOCCI = Controls Securing Most Vulnerable Areas For High Impact

*Figure 5.10*
*Step 5 - Minimum Overall Cybersecurity Controls Implementation (MOCCI) for SME*

As mentioned in the findings section, outcome research gained insight into the major issues that SMEs face. To begin, SMEs must address the security of three layers: the human layer, the physical and digital perimeter layer, and the host/endpoint layer. Aside from that, if the SME has network devices that are visible to the public, network security rules must be in place.

Also, if it has public-facing applications that access data or information, such as APIs, Web Portals, or Mobile Apps, that application and data layer security must be prioritized.

SMEs must then concentrate on safeguarding the internal network layer and internal application layer, followed by a greater focus on the internal data layer. As illustrated in Figure 5.11, the top management of SMEs will play a critical role in ensuring that each layer of DiD adheres to the fewest cybersecurity controls.

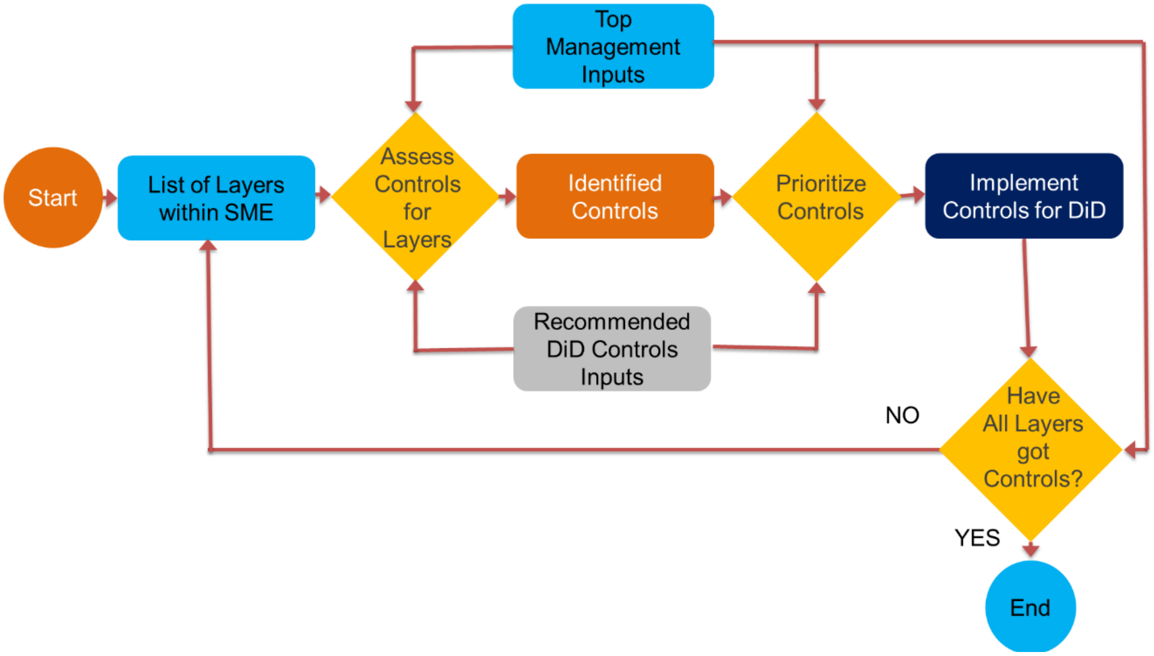

Top Management Inputs
Start
List of Layers within SME
Assess Controls for Layers
Identified Controls
Prioritize Controls
Implement Controls for DiD
Recommended DiD Controls Inputs
NO
Have All Layers got Controls?
YES
End

*Figure 5.11*
*Critical Role of Top Management during Implementation*

### 5.4.6 Calculate SME's Minimum Overall Cybersecurity Controls Implementation (MOCCI) Level

MOCCI Level =
Maturity Level in Securing Overall Assets from Common Vulnerabilities

*Figure 5.12*
*Step 6 - Calculate SME's Minimum Overall Cybersecurity Controls Implementation (MOCCI) Level*

SMEs must satisfactorily implement cybersecurity measures for the human layer, physical and digital perimeter layer, and host/endpoint layer security at the first level, which can be classified as "MOCCI Level 1," as indicated in Table 5.3. If the SME has network devices that are visible to the public, network security rules must be in place.

Also, if it has public-facing applications that access data or information, such as APIs, Web Portals, or Mobile Apps, that application and data layer security must be prioritized.

*Table 5.3*
*SME's Minimum Overall Cybersecurity Controls Implementation (MOCCI) Level*

| **Ref to DiD, SME's Primary Layer Security Implementation Focus On** | **GRC Implemented** | **MOCCI Level** |
|---|---|---|
| Human Layer Security<br>+ Physical & Digital Perimeter Security<br>+ Host/Endpoint Security<br>+ Public-Facing Network Security<br>+ Public-Facing Application Layer Security<br>+ Public-Facing Data Layer Security | YES | 1 |
| All Security Implementation in MOCCI Level 1<br>+ Internal Network Layer Security<br>+ Internal Application Layer Security | YES | 2 |
| All Security Implementation till MOCCI Level 2<br>+ Internal Data Layer Security | YES | 3 |

SMEs must focus on safeguarding the internal network layer and internal application layer at MOCCI Level 2. In MOCCI Level 3, the focus might shift to internal data layer security.

### 5.4.7 Calculate SME's Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI) Level

In this seventh step, research is striving to provide the best solution with targeted cybersecurity measures that will alleviate SMEs' pain points while also lowering their risk of exposure to cyber threats. While each of the CIA triads makes a unique contribution to cybersecurity for a business or its valued assets, they are also interconnected and overlap in some ways. As a result, while all three parts of the CIA cannot be disregarded, they can be prioritized based on demand in the SME area.

Calculate SME's
Least Cybersecurity
Controls
Implementation
(LCCI) Level

LCCI Level = Maturity Level in Securing Overall Assets
= [MCAS Level] + [MOCCI Level]

*Figure 5.13*
*Step 7 - Calculate SME's Business Domain-Specific Least Cybersecurity Controls Implementation (BDSLCCI) Level*

The BDSLCCI level can be estimated based on the attained BDSMOCCI and BDSMCAS levels. Refer to Table 5.4 for more information.

*Table 5.4*
*SME's Business Domain-Specific Least Cybersecurity Controls Implementation Level (BDSLCCI Level)*

| **BDSMCAS Level** | **MOCCI Level** | **BDSLCCI Level** |
|---|---|---|
| 1 | 1 | 1 |
| 2 | 1 | 2 |
| 1 | 2 | 2 |
| 2 | 2 | 3 |
| 3 | 2 | 4 |
| 2 | 3 | 4 |

| | | |
|---|---|---|
| 3 | 3 | 5 |

Only BDSLCCI Level 1 will be considered a Level 1 if an SME has adopted both MOCCI Level 1 and BDSMCAS Level 1.If any of the BDSMOCCI or BDSMCAS Levels do not meet the requirements for Level 1, BDSLCCI will not be at Level 1.

If either BDSMOCCI or BDSMCAS Levels are required for BDSLCCI Level 2, the others will remain at Level 1. Both the BDSMOCCI and BDSMCAS Levels must be at Level 3 for BDSLCCI Level 3.

If either BDSMOCCI or BDSMCAS Levels are required for BDSLCCI Level 4, the others will remain at Level 2. In addition, both MOCCI and BDSMCAS Levels must be at Level 3 for BDSLCCI Level 5.

### 5.5 AI ML-Based Software to Predict Cybersecurity Controls for SME

As for the ease of the recommended solution part, the implemented software has step-by-step guidance for SMEs willing to implement cybersecurity controls. As shown in Figure 5.14, AI and ML are used to help in the prediction of the relevant cybersecurity controls.

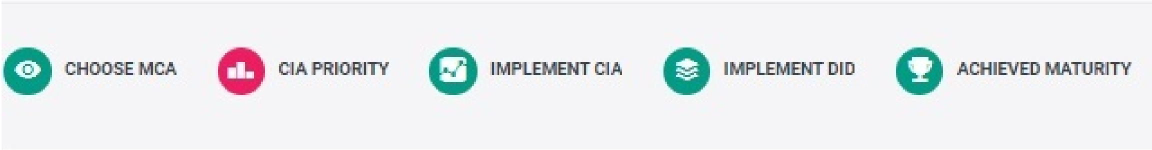


*Figure 5.14*
*Step-wise Implementation in Web Application*

#### 5.5.1 Responsible AI to Predict Cybersecurity Controls for SMEs

While selecting the appropriate controls for cybersecurity implementation, AI should help with the ethical standards. Hence, this is mapped to responsible AI principles, which are part of the methodology for deploying Artificial Intelligence approaches in real life while maintaining model explainability and responsibility (Abir et al., 2022). As illustrated in Figure 5.15 (Clarke, 2019), ten basic concepts of responsible AI can be mapped to cybersecurity control implementation. When it comes to the first principle of responsible AI, "Assess positive and negative impacts and implications," it's crucial to grasp the goal of each critical asset in an SME's specific business sector. Then, to meet the CIA Triad or DiD criteria, the same must be mapped to cybersecurity controls and features. It is vital to describe the benefits of the selected controls and/or their characteristics. Also, by incorporating ongoing input and feedback from SMEs, the process of mapping cybersecurity measures and their characteristics for SMEs with similar business areas can be improved. SMEs should also get as much advice as possible to maximize their benefits. It is also vital to maintain transparency in regards to justifying negative impacts and necessary safeguards, as well as providing specific controls and/or their features to SMEs. AI should be built in such a way that it always shares options for reaching the same goals with fewer risks or side effects.

The second principle, "Complement humans," relates to improving people's abilities to aid in the SME's stronger cybersecurity posture. It should also include cybersecurity controls that will assist individuals in performing better operations rather than directly replacing them. The third principle, "Ensure human control," should be regarded as a zero-day assault, and with the emergence of new cyber tricks, it is critical not to automate the cybersecurity domain. Many effective cyber-attacks have identified humans as the weakest link. Employees should be instructed on what to do and what not to do while working in the field. Furthermore, all SMEs' stakeholders' data should be protected during cybersecurity implementation. Maintain a human-friendly, individual-centered environment inside SME.

The fourth principle, "Ensure human safety and wellbeing," should prioritize the deployment of cybersecurity measures, with "Fail-Safe" being prioritized first, followed by "Fail-Secure," even though both are critical from distinct perspectives. For example, if a fire breaks out in a server room containing a significant database, even though it is a vital database that should be protected by physical doors with access restrictions, it is critical to unlock doors to prevent human deaths or injuries. In this case, organizations must assess whether another solution for database security is required.

The fifth principle is to ensure consistency with human values and human rights, with the intended AI helping framework ensuring that human rights legislation is not overlooked while implementing cybersecurity regulations. It should also consider gathering feedback from individuals on cybersecurity controls in place, analyzing those controls regularly, and improving them to make them more human-friendly without jeopardizing cybersecurity.

The sixth principle, providing openness and auditability, ensures that all stakeholders are aware of the controls and/or features provided by this cybersecurity framework. Under the seventh responsible AI principle, "Embed quality assurance," the framework should ensure that data collected from various SMEs is constantly evaluated and made more useful in the implementation of cybersecurity controls, ensuring that the best possible cybersecurity is delivered. It must also give an honest assessment of the controls and/or features implemented.

The eighth responsible AI principle is to demonstrate robustness and resilience, which requires SMEs to undertake an audit concerning the applied cybersecurity controls, where people, processes, and technology will be evaluated and improved over time. To comply with the ninth principle, "Ensure accountability for obligations," roles and responsibilities must be properly understood by everyone, with SMEs ensuring good communication for any cyber-attack event, complaint, appeal, damaging errors, and so on during the implementation of the framework. According to the tenth responsible AI principle, “Enforce, and accept the enforcement of, liabilities and sanctions,” it is critical to guarantee that processes inside SMEs handle any cyber-attack incident, complaint, appeals, damaging errors, and other cybersecurity controls more efficiently. It should also ensure that SMEs are well-positioned to meet the demands of external stakeholders in their eco-system or specific region/country.

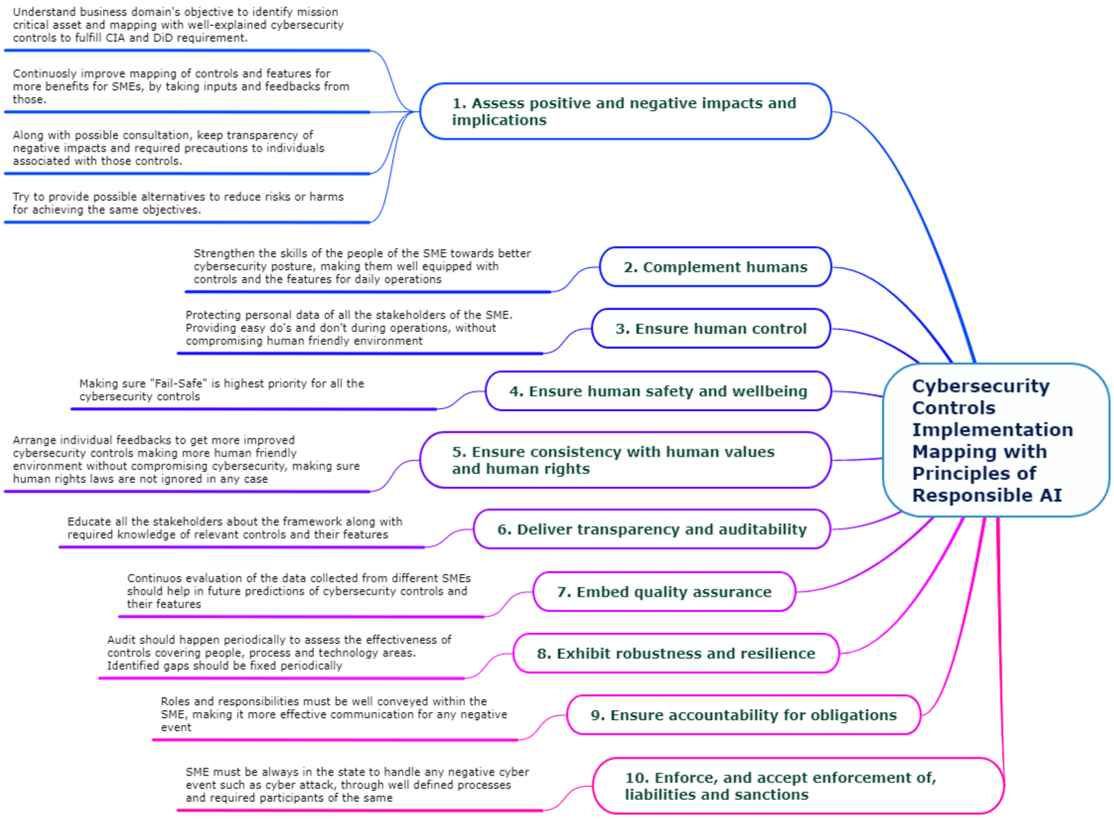

Cybersecurity Controls Implementation Mapping with Principles of Responsible AI
1. Assess positive and negative impacts and implications
Understand business domain's objective to identify mission critical asset and mapping with well-explained cybersecurity controls to fulfill CIA and DiD requirement.
Continuosly improve mapping of controls and features for more benefits for SMEs, by taking inputs and feedbacks from those.
Along with possible consultation, keep transparency of negative impacts and required precautions to individuals associated with those controls.
Try to provide possible alternatives to reduce risks or harms for achieving the same objectives.
2. Complement humans
Strengthen the skills of the people of the SME towards better cybersecurity posture, making them well equipped with controls and the features for daily operations
3. Ensure human control
Protecting personal data of all the stakeholders of the SME. Providing easy do's and don't during operations, without compromising human friendly environment
4. Ensure human safety and wellbeing
Making sure "Fail-Safe" is highest priority for all the cybersecurity controls
5. Ensure consistency with human values and human rights
Arrange individual feedbacks to get more improved cybersecurity controls making more human friendly environment without compromising cybersecurity, making sure human rights laws are not ignored in any case
6. Deliver transparency and auditability
Educate all the stakeholders about the framework along with required knowledge of relevant controls and their features
7. Embed quality assurance
Continuos evaluation of the data collected from different SMEs should help in future predictions of cybersecurity controls and their features
8. Exhibit robustness and resilience
Audit should happen periodically to assess the effectiveness of controls covering people, process and technology areas. Identified gaps should be fixed periodically
9. Ensure accountability for obligations
Roles and responsibilities must be well conveyed within the SME, making it more effective communication for any negative event
10. Enforce, and accept enforcement of, liabilities and sanctions
SME must be always in the state to handle any negative cyber event such as cyber attack, through well defined processes and required participants of the same

*Figure 5.15*
*Cybersecurity Controls Implementation Mapping with Principles of Responsible AI*

### 5.5.2 AI for BDSMCAS Level Implementation

In this software design, ML logic has used a multiclass classification trainer, which is the SdcaMaximumEntropyMulticlassTrainer provided by ML.NET. For it, input values are provided as a list known as "features", whereas the predicted output value is known as "Label". Features are business domain and MCA in the case of this software. It provides a prioritized CIA component as a label (Microsoft, 2022).

As shown in Figure 5.16, any SME can register the web application where it will specify its business domain during the registration process. Based on the business domain, through simulated data points, the software will predict what should be the ideal number of MCAs for the SME. If SMEs don’t agree with the predicted MCA, they can add a new MCA for their business domain. It will be further treated as a new input for AI/ML logic for further predictions. Based on Business Domain and MCA, the software will also help in predicting the prioritization of the components of the CIA triad. SMEs can either modify the recommended prioritization or accept it as is. Based on MCA and the prioritized component of the CIA triad, the software will display the list of cybersecurity controls SMEs need to implement to satisfy the same. Based on the implementation of the controls, the SME’s BDSMCAS level is calculated and saved to the database.

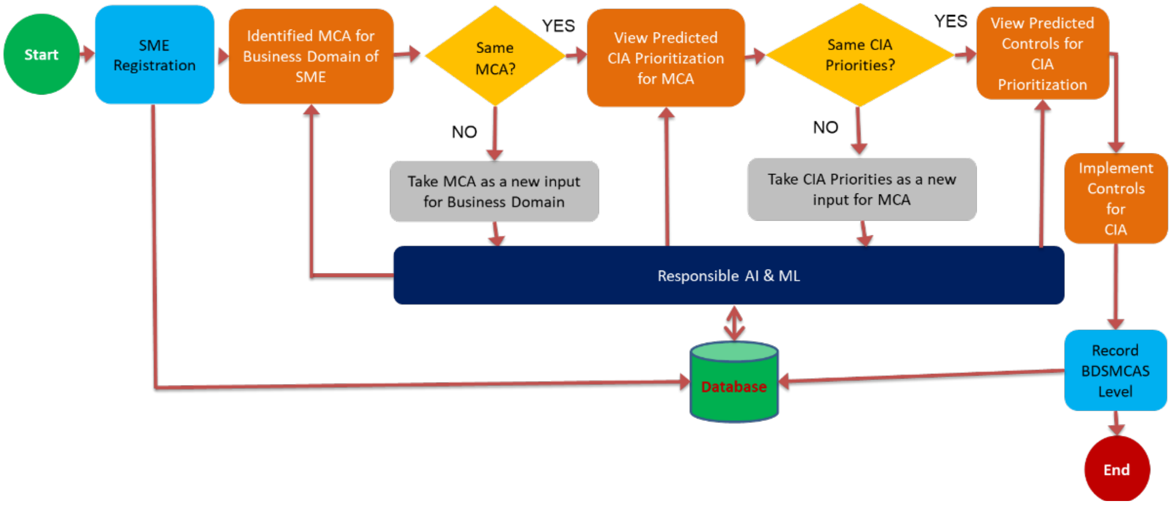

Start
SME Registration
Identified MCA for Business Domain of SME
Same MCA?
YES
NO
View Predicted CIA Prioritization for MCA
Same CIA Priorities?
YES
NO
View Predicted Controls for CIA Prioritization
Take MCA as a new input for Business Domain
Take CIA Priorities as a new input for MCA
Implement Controls for CIA
Responsible AI & ML
Database
Record BDSMCAS Level
End

*Figure 5.16*
*AI for BDSMCAS Level Implementation*

Research is working on the implementation of a web-based software having predictive data pulled by processes developed in AI and ML software. Any SME can register by providing key information such as its business domain and mission-critical assets. Taking it as input, the software predicts the prioritization in the CIA triad, relevant cybersecurity controls, and their specific features. For research recommendation solutions, the implementation of a web-based software having predictive data pulled by processes developed in AI and ML software. Any SME can register by providing key information such as its business domain and mission-critical assets. Taking it as input, the software predicts the prioritization in the CIA triad, relevant cybersecurity controls, and their specific features.

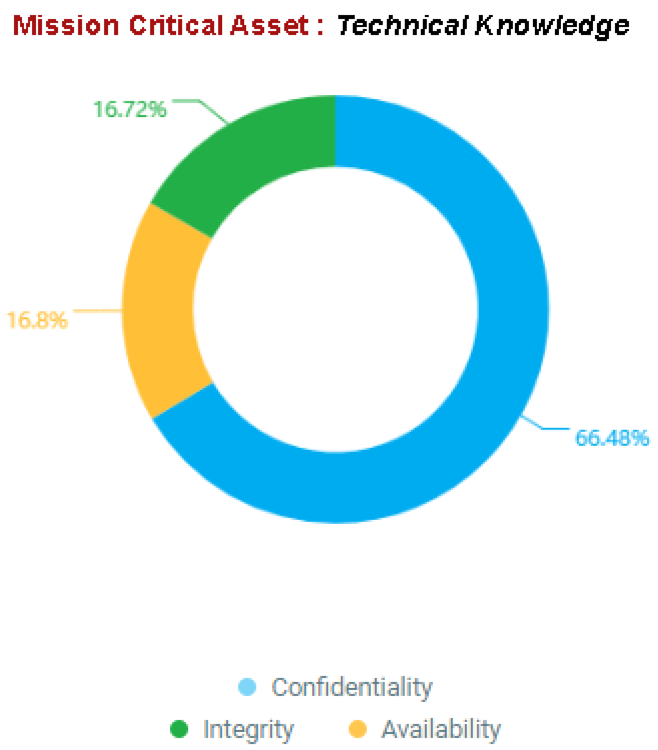
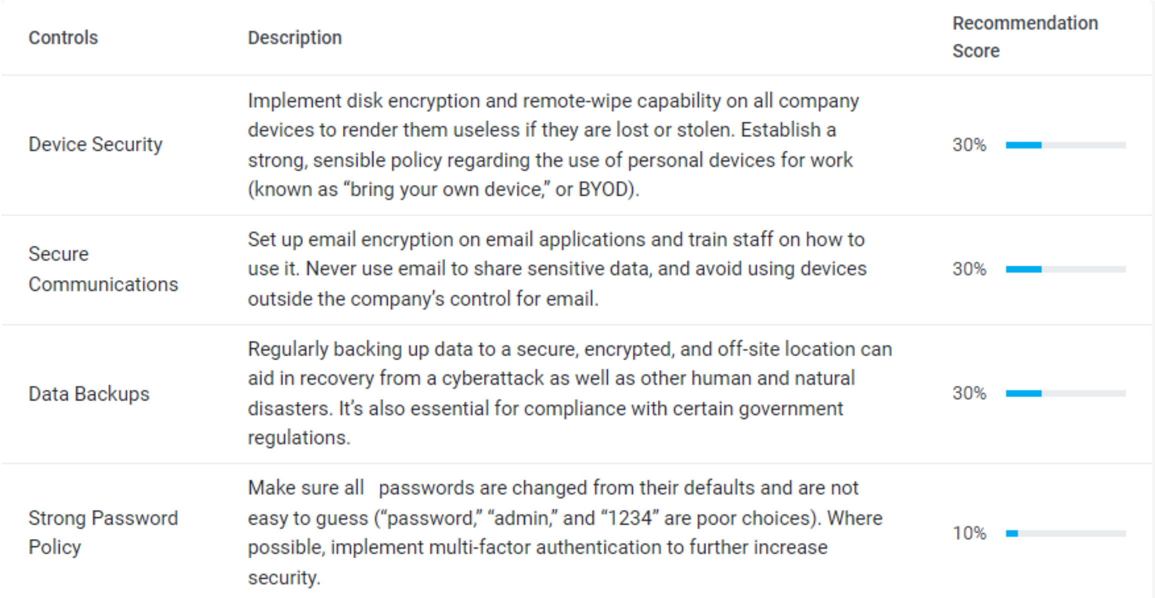


*Figure 5.17*
*Web Application Flow Screenshot showing priority of components in CIA Triad*

The information captured during research is used as initial input data, which is a business domain, its BDSMCA, and prioritization in the CIA triad components. Here the ML software part is using a multiclass classification algorithm. A supervised ML task is used to predict the class (in this case, the CIA triad's three components, which are confidentiality, integrity, and availability) of an instance of data. The input of this algorithm is a set of labeled examples. Each one of them starts as text data. It is then run through the Term Transform, which converts it to the Key (numeric) type. The output of a classification algorithm is a classifier, which is further being used to predict the class of new unlabeled instances (Alaiz-Moreton et al., 2019; Mustaqeem, Anwar, and Majid, 2018). Firstly, it helps in predicting prioritized components in the CIA triad based on particular BDSMCA. This algorithm also predicts the CIA triad prioritisation and cybersecurity controls mapping, categorizing those controls according to their importance in confidentiality, integrity, and availability.



| Controls | Description | Recommendation Score |
|---|---|---|
| Device Security | Implement disk encryption and remote-wipe capability on all company devices to render them useless if they are lost or stolen. Establish a strong, sensible policy regarding the use of personal devices for work (known as "bring your own device," or BYOD). | 30% |
| Secure Communications | Set up email encryption on email applications and train staff on how to use it. Never use email to share sensitive data, and avoid using devices outside the company's control for email. | 30% |
| Data Backups | Regularly backing up data to a secure, encrypted, and off-site location can aid in recovery from a cyberattack as well as other human and natural disasters. It's also essential for compliance with certain government regulations. | 30% |
| Strong Password Policy | Make sure all passwords are changed from their defaults and are not easy to guess ("password," "admin," and "1234" are poor choices). Where possible, implement multi-factor authentication to further increase security. | 10% |

*Figure 5.18*
*Web Application Screenshot showing Recommended Cybersecurity Controls for Particular BDSMCA and Confidentiality as priority*

For example, refer to Figure 5.17, which highlights one of SMEs' BDSMCA. It shows confidentiality is the highest priority. Furthermore, as shown in Figure 5.18, the software can pull required cybersecurity controls to fulfil the security requirements for the same. Similarly, it will help SMEs implement cybersecurity controls for integrity and availability in further steps. Similarly, this software also recommends the least cybersecurity controls to be implemented to satisfy DiD within an SME. Collectively, this software will provide the maturity level as a result. SMEs need to refer to this software and keep on improving the maturity level of cybersecurity implementation.

### 5.5.3 AI for MOCCI Level Implementation

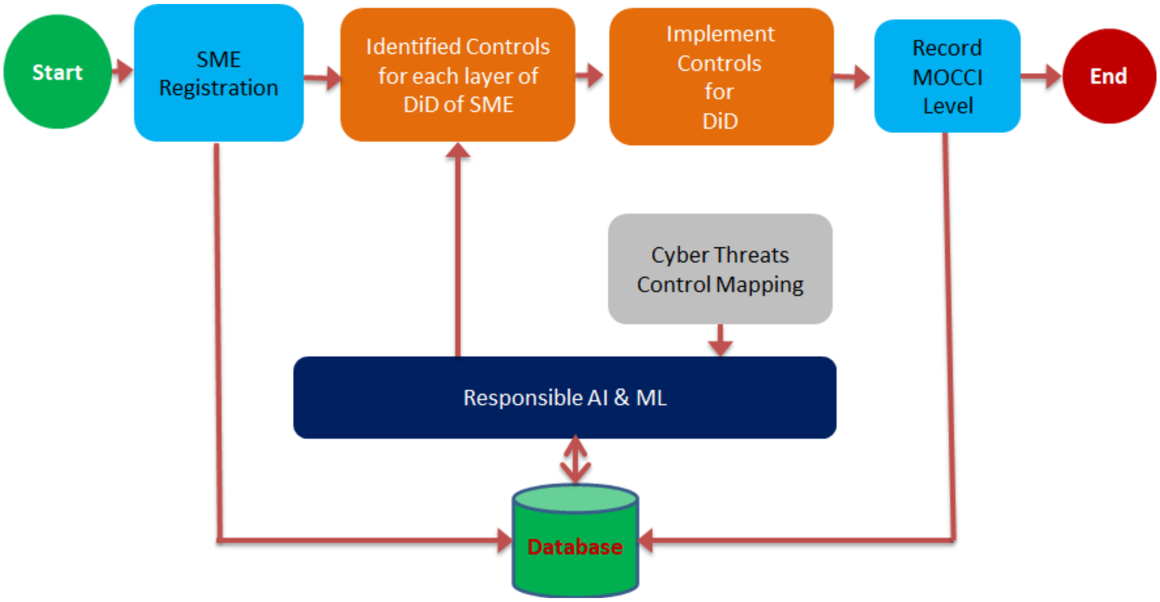

Start
SME Registration
Identified Controls for each layer of DiD of SME
Implement Controls for DiD
Record MOCCI Level
End
Cyber Threats Control Mapping
Responsible AI & ML
Database

*Figure 5.19*
*AI for MOCCI Level Implementation*

As shown in Figure 5.19, the software will also predict the least cybersecurity controls for each layer of the DiD. Different cybersecurity threats will be studied continuously to decide which controls are most important for each layer of DiD. The latest AI ML logic helps in reinventing the weightage for each control in a particular layer of DiD based on the latest cyber threat landscape. SMEs need to achieve a certain level of implementation of those controls to qualify for the particular MOCCI level. This is also retained in the database.

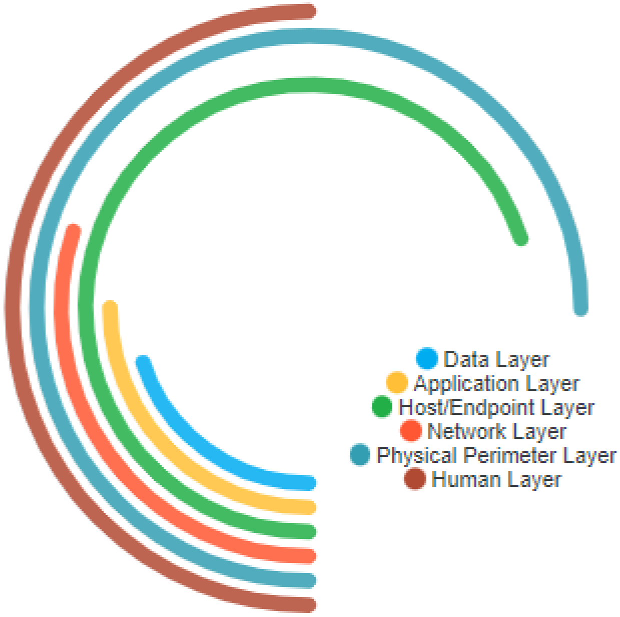


*Figure 5.20*
*Cybersecurity Controls Implementation for DiD Levels*

As shown in Figure 5.20, even software can show the achieved minimum level of cybersecurity control implementation for DiD layers.

# Chapter VI:

# SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

## 6.1 Summary

It's astonishing to see that SMEs have been victims of cyber attacks for years but have received very little attention in terms of resolving the ground-level cybersecurity issue. It was observed that SMEs lack the resources needed to establish a strong cybersecurity posture; they are lost in finding the right stepwise direction; other business priorities prevent them from investing in cybersecurity, and SMEs require the simplest starting points that can also assist them in attaining their business priority goals.

## 6.2 Implications

Rather than having "NO" cybersecurity controls, which exposes about 100 percent of cyber-threat risks, it is preferable, to begin with, the bare minimum of cybersecurity measures advocated in this study. It will undoubtedly assist SMEs in protecting their primary business domain objectives and continuing to improve their cybersecurity maturity.

One of the most important inputs for developing cybersecurity measures should be top management's consideration of business interests. At a high level, contemporary cybersecurity standards or frameworks typically have a broad landscape of controls that they must meet to satisfy the implementation of a cybersecurity posture that meets the standard's or framework's desired expectations. The current recommended solution, as a new framework, represents a paradigm shift in the journey of upgrading SMEs' cybersecurity posture, as depicted in Figure 6.1. This new framework provides a domain-specific security posture, which aids in the protection of the organization's important asset areas.

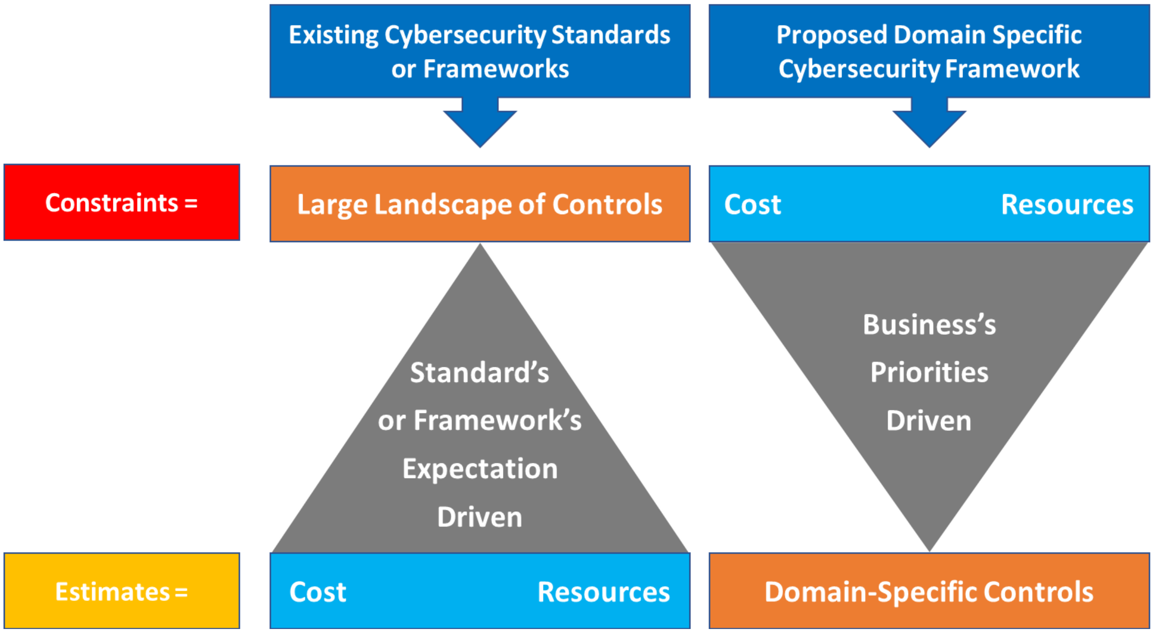

Existing Cybersecurity Standards or Frameworks
Proposed Domain Specific Cybersecurity Framework
Constraints =
Large Landscape of Controls
Cost
Resources
Business's Priorities Driven
Standard's or Framework's Expectation Driven
Estimates =
Cost
Resources
Domain-Specific Controls

*Figure 6.1*
*Paradigm Shift in New Framework*

Most cybersecurity standards and frameworks include a set of measures that should be adopted by any organization, regardless of its size, staff strength, business domain concerns, or other resources. Many times, even a few controls are insufficient for SMEs with a specialized business domain, deterring them from pursuing the implementation of such standards or frameworks. Many SMEs have yet to take the initial step toward cybersecurity, which means they are vulnerable to escalating cyber attacks. Few SMEs are even aware that they have been cyber-attacked. They'll need encouragement and motivation to climb the ladder of acceptable cybersecurity control implementation. Top management should see the link between their cybersecurity investment and achieving optimal protection for their business goals while avoiding cyber dangers.

### 6.3 Recommendations for Future Research

This new cybersecurity framework, which was created for the benefit of a specific SME business domain, can also be further improved to be used for the cybersecurity of micro and large businesses.

### 6.4 Conclusion

During this research study, I found that there are various gaps and issues which are stopping SMEs to implement a good cybersecurity posture. To avoid being hacked, SMEs must follow at least the bare minimum and step-by-step cybersecurity implementation suggestions. There are a few schools of practical thought that can help SMEs solve existing difficulties quickly. Rather than implementing cybersecurity measures at random or not at all, any SME can prioritize the adoption of controls based on the areas outlined in this research.

To conclude the discussion, below are the key points.

1) Determine BDSMCA for SME's Domain

2) Implementing SME’s Domain Specific Security Demand considering all important factors specified

3) Must-Have Minimum Baseline Controls should be implemented for the entire SME

4) Calculating the BDSLCCI Level

5) Keep on improving your BDSLCCI Level

The preceding discussion offers recommendations for the prioritization of cybersecurity controls that SMEs should implement. It is worth repeating that the remaining two components of the CIA are as critical as the CIA triad areas for dividing cybersecurity controls into small parts for ease of SME, but they can be improved at a later stage of cybersecurity control planning and investment. Also, unique compliance requirements for the domain in which SMEs operate should not be overlooked. BDSLCCI Level 1 provides effective cyber-threat security for SMEs, reducing malware, phishing, insider threats, web attacks, ransomware assaults, and a few other dangers to a certain extent. Furthermore, BDSLCCI Level 2 provides higher cybersecurity than BDSLCCI Level 1 and other levels. Level 5 of the BDSLCCI can be considered the best minimal cybersecurity controls for SMEs to apply. SMEs can also pick another mission-critical asset and continue to create controls for each one.

# APPENDIX A

## SURVEY COVER LETTER

This study's research questions are focused on the core question, which is: What is the current cybersecurity posture of SMEs and what are the issues they are facing regarding the implementation of cybersecurity controls?

1. How old are your small and medium enterprises (SMEs)?
2. Does your organization have any of the below standards or frameworks implemented?
3. Does your organization have security controls in place?
4. If the answer to the above question is YES, please select PHYSICAL Security controls already in place
5. If the answer to the above question is YES, please select TECHNICAL Security controls already in place
6. If the answer to the above question is YES, please select ADMINISTRATIVE controls already in place
7. How frequently is Security awareness training conducted for employees?
8. Which are the biggest problems you are facing while implementing or deciding/planning to implement Cybersecurity Controls for your organization?
9. Has your organization undergone any cyber-attack?
10. Which kind of cyber-attack did your organization face?
11. As an SME, what is your expectation from security standards or framework?

## APPENDIX B

## BACKGROUND INFORMATION OF RESEARCH SURVEY PARTICIPANTS

| Core Business of SME | Participant's Role in SME | SME's Country | Number of Years of SME's Existence |
|---|---|---|---|
| IT industry | C-Level Executive | India | Between five to ten years |
| IT industry | Owner / Partner | India | Between one to three years |
| Banking, Financial Services and Insurance (BFSI) | Director | India | Between one to three years |
| MEDIA | Director | India | More than ten years |
| Manufacturing | Director | Russia | Between one to three years |
| IT industry | C-Level Executive | Russia | More than ten years |
| IT industry | Owner / Partner | India | Between one to three years |
| IT industry | Owner / Partner | India | More than ten years |
| Manufacturing | Owner / Partner | India | More than ten years |
| IT industry | C-Level Executive | United Arab Emirates | Between one to three years |
| IT industry | Owner / Partner | India | Between three to five years |
| HR | Owner / Partner | Norway | Less than a Year |
| Executive Coaching | Owner / Partner | United Arab Emirates | Between three to five years |
| IT industry | Owner / Partner | India | More than ten years |
| Distribution of primary packaging material | Owner / Partner | India | More than ten years |
| Insurance | Owner / Partner | India | More than ten years |
| Exports | Owner / Partner | India | More than ten years |
| Manufacturing | Director | India | More than ten years |
| IT industry | Owner / Partner | Israel | Between five to ten years |
| Consulting | C-Level Executive | Ghana | More than ten years |
| Finance Services | Owner / Partner | India | More than ten years |
| E-commerce | Director | United Kingdom | Between three to five years |
| Logistics | Director | Sweden | Between three to five years |

| | | | |
|---|---|---|---|
| Pharmaceutical | C-Level Executive | Sweden | More than ten years |
| Logistics and Supply Chain Management | Director | United Arab Emirates | More than ten years |
| E-commerce | Director | United States | More than ten years |
| IT industry | C-Level Executive | Australia | Between five to ten years |
| IT industry | Owner / Partner | India | More than ten years |
| IT industry | Owner / Partner | India | Less than a Year |
| Cold Storage & Warehousing | Director | India | More than ten years |
| IT industry | Business Unit Head | Australia | Between five to ten years |
| IT industry | Owner / Partner | India | Between five to ten years |
| IT industry | Director | United States | Between five to ten years |
| Maritime | Director | India | Between one to three years |
| E-commerce | Owner / Partner | India | Between one to three years |
| FMCG | C-Level Executive | India | More than ten years |
| Media | Owner / Partner | South Africa | Less than a Year |
| Finance Services | Director | India | Less than a Year |
| IT industry | Director | Singapore | Between one to three years |
| Manufacturing | Owner / Partner | India | More than ten years |
| E-commerce | Owner / Partner | Russia | Less than a Year |
| Online Services and marketing | Senior Management | Sri Lanka | Between three to five years |
| Telecommunication | Owner / Partner | India | More than ten years |
| Manufacturing | Owner / Partner | India | Between three to five years |
| Telecommunication | Owner / Partner | India | More than ten years |
| Finance Services | Owner / Partner | India | Between one to three years |
| IT industry | Business Unit Head | India | Between five to ten years |
| B2C SaaS Hyper Mobility and Fintech consumer services | C-Level Executive | Indonesia | Between five to ten years |
| IT industry | Owner / Partner | India | More than ten years |
| IT industry | Owner / Partner | India | Between one to three years |
| Telecommunication | Owner / Partner | India | Between three to five years |
| Banking, Financial Services and Insurance (BFSI) | Owner / Partner | India | Between three to five years |
| Manufacturing | C-Level Executive | India | More than ten years |

|  |  |  |  |
|---|---|---|---|
| IT industry | Director | India | Between five to ten years |
| Hospitality | Owner / Partner | India | Between three to five years |
| Construction | Director | India | Between three to five years |
| Banking, Financial Services and Insurance (BFSI) | Director | India | More than ten years |
| Legal Services | Owner / Partner | India | Between five to ten years |
| IT industry | Director | India | More than ten years |
| FMCG | Owner / Partner | India | Between five to ten years |
| Logistics and Supply Chain Management | Owner / Partner | Bangladesh | Between five to ten years |
| Oil Industry | C-Level Executive | United States | More than ten years |
| Finance Services | Owner / Partner | Nigeria | Between one to three years |
| SAAS (Software Development in areas of business process automation for SMB and SME) | C-Level Executive | India | Between three to five years |
| Distributor | Owner / Partner | India | Between one to three years |
| Hospitality | Owner / Partner | India | More than ten years |
| Finance Services | Director | India | Less than a Year |
| Manufacturing | Owner / Partner | India | More than ten years |
| IT industry | Director | United States | Between one to three years |
| Logistics | Owner / Partner | India | Between one to three years |
| Finance Services | Owner / Partner | Cyprus | More than ten years |
| IT industry | C-Level Executive | India | More than ten years |
| IT industry | Director | India | More than ten years |
| EduTech | C-Level Executive | United States | More than ten years |

| | | | |
|---|---|---|---|
| FMCG | Owner / Partner | India | Less than a Year |
| Construction | Owner / Partner | India | Between one to three years |
| Hospitality | Owner / Partner | India | Between three to five years |
| IT industry | Owner / Partner | India | Between five to ten years |
| Renewable Energy | Owner / Partner | India | Between five to ten years |
| Telecommunication | Owner / Partner | India | Between one to three years |
| IT industry | Owner / Partner | India | Less than a Year |
| Manpower supply (Human resources) | Director | India | Between five to ten years |
| IT industry | Director | India | More than ten years |
| IT industry | C-Level Executive | India | Between five to ten years |
| E-commerce | Director | India | Less than a Year |
| IT industry | Owner / Partner | India | Between one to three years |
| IT industry | C-Level Executive | India | Between one to three years |
| Media | C-Level Executive | India | More than ten years |
| Manufacturing | Owner / Partner | India | More than ten years |
| Travel / Tech | Director | Australia | Between five to ten years |

| | | | |
|---|---|---|---|
| Pharma | Director | United States | More than ten years |
| SAS services (Software platform for Insurance brokers) | Director | United States | Between five to ten years |
| IT industry | C-Level Executive | India | Between three to five years |
| Education | Vice Principal | India | More than ten years |
| Healthcare | Business Unit Head | India | Between five to ten years |
| MEDIA | C-Level Executive | India | More than ten years |
| FMCG | Owner / Partner | India | More than ten years |
| Construction | Owner / Partner | Kenya | More than ten years |
| Online Services and marketing | Business Unit Head | India | Between one to three years |
| Legal and Accounting Services | Owner / Partner | India | Less than a Year |
| IT industry | Director | Ireland | Between five to ten years |
| Media | Owner / Partner | India | More than ten years |
| IT industry | Director | United States | Between three to five years |
| IT industry | Director | India | Between one to three years |
| IT industry | Owner / Partner | India | More than ten years |
| Marketing Consultant | Owner / Partner | India | Less than a Year |
| IT industry | Director | India | Between one to three years |
| IT industry | Owner / Partner | India | More than ten years |
| Banking, Financial Services and Insurance (BFSI) | Director | India | Between one to three years |
| E-commerce | Director | Australia | More than ten years |
| Healthcare | Director | India | Between one to three years |

| | | | |
|---|---|---|---|
| IT industry | Owner / Partner | India | Between five to ten years |
| Insurance | Owner / Partner | India | More than ten years |
| Hospitality | Owner / Partner | India | More than ten years |
| Finance Services | C-Level Executive | India | More than ten years |

# APPENDIX C

## INFORMATION FROM THE RESEARCH INTERVIEW

The following are the high-level inputs received from top management, such as directors, CEOs, and C-Level Executives of SMEs when asked about the Business Domain-Specific Mission Critical Asset (BDSMCA) for their business domain, followed by prioritization of the Confidentiality, Integrity, and Availability for BDSMCA. In this qualitative analysis, SMEs participating were from countries like India, Dubai, Iran, China, Russia, and the USA.

| **Number of Participants** | **Business Domain** | **Business Domain-Specific Mission Critical Asset (BDSMCA)** | **Prioritization on a scale of 1 to 10 (1 being lowest and 10 being highest)** | | |
|---|---|---|---|---|---|
| | | | **Confidentiality** | **Integrity** | **Availability** |
| 12 | Manufacturing | Design Drawings | 10 | 8 | 6 |
| 10 | Software Development | Source Code of Software Applications | 10 | 8 | 6 |
| 7 | Marketing | Customer Database | 10 | 8 | 6 |
| 3 | Manufacturing | Ordering System Integration with Shops | 5 | 6 | 10 |
| 3 | Aggregator | Aggregator Platform - Web | 8 | 6 | 10 |
| 2 | Real estate | Skilled Labor | 1 | 1 | 10 |
| 2 | Logistics | Logistics Software Portal | 10 | 8 | 6 |
| 2 | E-Commerce | Online Shopping Portal | 6 | 8 | 10 |
| 2 | Consulting | Customer Database | 10 | 6 | 8 |
| 2 | Audit (Cybersecurity & IT) | Audit Reports containing internal information about the organization | 10 | 8 | 6 |
| 1 | Trading | Trading Software | 6 | 8 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | Support | Network Access | 8 | 10 | 6 |
| 1 | Support | Phone Systems | 6 | 8 | 10 |
| 1 | Storage & Warehousing | Temperature and Humidity Controller | 5 | 10 | 9 |
| 1 | Software Platform | Software for sending bulk emails | 8 | 6 | 10 |
| 1 | Software Development - Cloud Infra Based | Connectivity to cloud | 8 | 6 | 10 |
| 1 | Software Development | Integrated Software Source Code | 8 | 10 | 6 |
| 1 | Software Deployment | Infrastructure Knowledge | 8 | 10 | 6 |
| 1 | Software - Reseller | Data Integrity | 6 | 10 | 8 |
| 1 | Software - Product | Software Source Code | 10 | 8 | 6 |
| 1 | Sales & Marketing | Client's Signed Documentation | 7 | 10 | 9 |
| 1 | Product Testing | Client Product IP and Reports | 10 | 8 | 6 |
| 1 | Product - Security Access System | Data sent on cloud | 10 | 8 | 6 |
| 1 | Product - Security Access System | Firmware | 6 | 8 | 10 |
| 1 | Product - Security Access System | Hardware | 6 | 8 | 10 |
| 1 | Product - Security Access System | Software | 6 | 8 | 10 |
| 1 | Product - Design | 3D modeling drawing | 10 | 8 | 6 |
| 1 | Marketing - Web Platform | Online AI-Driven Web Platform | 8 | 6 | 10 |
| 1 | Manufacturing | Algorithm of Robot | 8 | 10 | 6 |
| 1 | Manufacturing | Automated machines and tools | 8 | 6 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | Manufacturing | Calibration Guidelines as per industry standards (Quality Control) | 5 | 10 | 5 |
| 1 | Manufacturing | CNC Machine | 6 | 8 | 10 |
| 1 | Manufacturing | ERP System | 5 | 6 | 10 |
| 1 | Manufacturing | Formula of Beverage | 10 | 8 | 6 |
| 1 | Manufacturing | The formula of various ice-creams programmed in systems | 10 | 8 | 5 |
| 1 | Manufacturing | Innovative Technology Design for less power consumption for Industrial Usage | 10 | 8 | 6 |
| 1 | Manufacturing | Line Operation | 6 | 10 | 8 |
| 1 | Manufacturing | Medicine Formulae | 8 | 10 | 6 |
| 1 | Manufacturing | Own Chipset | 10 | 8 | 6 |
| 1 | Manufacturing | Quality of Food Ingredients | 6 | 10 | 8 |
| 1 | Manufacturing | Software of Detector Tolerance Range | 6 | 10 | 8 |
| 1 | Manufacturing | Software Technology Server of Automation Software & Database | 8 | 10 | 6 |
| 1 | Manufacturing | Supply Chain Network | 8 | 10 | 6 |
| 1 | Manufacturing | Technical Knowledge | 10 | 8 | 6 |
| 1 | IT Consulting | Skilled Employees | 0 | 0 | 0 |
| 1 | Information Security | Security Product | 10 | 8 | 6 |
| 1 | Industrial Automation | IIoT Hardware's Data Integration | 6 | 10 | 8 |
| 1 | Healthcare | Machines | 6 | 10 | 8 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | Healthcare | Operation Theater (OT) / ICU | 5 | 10 | 8 |
| 1 | Healthcare | Patient Info | 10 | 8 | 6 |
| 1 | FMCG | Online Platform Supply Chain | 6 | 8 | 10 |
| 1 | Financial Services | Customer Data | 10 | 8 | 6 |
| 1 | Financial Services | Operational Software | 6 | 10 | 8 |
| 1 | Fabrication of various designs | Customer Designs | 0 | 0 | 0 |
| 1 | End-to-End Smart Monitoring | Hardware's Data Integration | 6 | 10 | 8 |
| 1 | Electrical contracting | Skilled Labor | 0 | 0 | 0 |
| 1 | E-Learning | E-Learning Web Platform | 6 | 8 | 10 |
| 1 | Cloud Infra Provider | Hardware Availability | 6 | 8 | 10 |
| 1 | Cloud Infra Provider | Power to Hardware | 6 | 8 | 10 |
| 1 | CCTV Installation | Connectivity to cameras | 6 | 8 | 10 |
| 1 | CCTV & Firewall Installation | Technical Knowledge | 0 | 0 | 0 |
| 1 | Call Center | Call Center Infra Connectivity | 6 | 8 | 10 |
| 1 | BSFI | API & Applications for Financial Transactions | 10 | 8 | 6 |
| 1 | BSFI | Loan Processing Application | 10 | 8 | 6 |
| 1 | Industrial Automation | Cloud Platform | 6 | 8 | 10 |
| 1 | Industrial Automation | Installation after Quality Check | 6 | 10 | 8 |
| 1 | Industrial Automation | Product Design | 10 | 8 | 6 |
| 1 | Industrial Automation | Source Code | 8 | 10 | 6 |

| | | | | | |
|---|---|---|---|---|---|
| 1 | Audit (Accounts) | Working papers and documentation | 10 | 6 | 8 |
| 1 | Financial Consulting | none | 0 | 0 | 0 |
| 1 | Aggregator | Aggregator Platform - Mobile App | 8 | 10 | 6 |
| 1 | Accounting | Accounting Software Database | 10 | 8 | 6 |

## GLOSSARY – CYBER-THREATS

**Phishing Attack:** Humans or their emotions are targeted in social engineering attacks to capture, manipulate, or involve them in hostile behaviors that can lead to more cyber attacks (Kromholz et al., 2015). Phishing is the most common social engineering assault, in which hackers write fake messages and send them to people in any organization to make them victims of cyber tricks. In most situations, a message with a malicious attachment or an external URL to malicious websites is sent to the email account (Hong, 2012). Hackers try to play a physiological game by getting the victim to focus on the activity indicated in the email. In most cases, malware files disguised as resumes are delivered to the organization's HR management email addresses, which tend to be the weakest point for subsequent hacking attempts. More than 90 percent of cyber-attacks begin with a phishing attempt. Emotional motivators and enticing email contexts are used in these attacks to boost the success rate of targets (PhishMe, 2018). Phishing attacks are being carried out as a campaign on leaked databases of contact information. However, they can be mitigated by an organizational cybersecurity awareness training culture and a lack of cybersecurity measures.

**Insider Threat:** As the term "insider" implies, it is immoral conduct committed by trusted individuals, such as workers, partners, vendors, or others, that harms the organization or engages in illicit operations for the profit of an individual or group. Insider attacks in the digital realm can result in information leakage, an increase in cybercriminal surveillance, or even damage to an organization's systems, infrastructure, or network (Greitzer, 2011).

**Malware Threat**: The word "malware" is made up of two parts: the first is the word "malicious," and the second is the word "software." Malware is given multiple names depending on the family it belongs to. Lollipop, Simda, Gatak, and Obfuscator are some of the most well-known malware families. ACY, Ramnit, and other viruses, worms, Trojan horses, adware, backdoors, and other malware categories are the most common (Ronen, 2018). Each type of malware has distinct characteristics that can aid in classification. Anti-malware systems that can detect behavior more precisely and in less time are providing improved protection against it (Zolkipli, 2011).

**DoS and DDoS Attack**: In the case of a denial-of-service (DoS) attack, cybercriminals try to flood a server with traffic to make it unavailable to desired users by consuming the maximum possible resources required for its function. In a similar way, a distributed denial-of-service (DDoS) attack is simply a DoS attack itself, but here cybercriminals use multiple sources of IP addresses, which are nothing but computers or servers, to flood a targeted resource. Hence, DDoS is much more difficult to prevent as compared to DoS attacks (Mahjabin, 2017).

**Man-in-the-middle (MITM) Attack**: Cybercriminals can intercept, tamper with, send, or receive data between the sender and recipient systems in a MITM attack (Mallik, 2019).

**Ransomware Attack**: Ransomware is a combination of the terms "ransom" and "malware." In this type of attack, cyber thieves encrypt the intended victim's system and then demand a ransom in exchange for a decryption key that allows them to restore it (Tandon, 2019). Nsb Locker, CTB Locker, Crypto Locker, CryptoWall, Torrent Locker, TeslaCrpt, WannaCry, Maze, Locky, Bad Rabbit, GoldenEye, Petya, and other ransomware have been around for more than a decade (Hong, 2018; Liao, 2008).

**Web Attack**: A Web Attack occurs when cybercriminals use the weaknesses of a website or web application to steal data, capture sensitive information, and so on (Kapodistria, 2021). The Open Web Application Security Project (OWASP), a non-profit organization, offers advice on how to avoid such web attacks. It updates its top 10 cyber danger list regularly, based on cyber-attack statistics, to assist software developers in implementing secure coding standards (Wichers, 2017).

## GLOSSARY – CYBERSECURITY CONTROLS

**Business Continuity Plan (BCP):** It specifies how an organization will continue to operate in the event of an unanticipated service interruption. It's more extensive than a disaster recovery plan, as it includes contingencies for business processes, assets, human resources, and business partners - all aspects of an organization that could be impacted.

**Closed-Circuit Television (CCTV):** Video surveillance is another term for CCTV. It is a camera, recorder, direct connection, and video connectivity device. It's usually connected to a wireless or wired network, which allows audio and video to be sent. Night vision capabilities are included in today's modern CCTV cameras, allowing them to capture images in low or dim light.

**Intrusion Detection System (IDS):** It is a hardware device with a software application or individual software that detects policy infractions, as well as any suspicious or malicious acts, by continuously monitoring the system, network activities, and other factors. It can assess the open vulnerabilities in a system's configuration, recognizing distinct attack patterns or harmful behaviors. (1) Host-based IDS (HIDS) and (2) Network-based IDS are the two primary types of IDS based on their solution approach (NIDS). The Network Interface Card (NIC) on NIDS is set to promiscuous mode, and the relevant software is installed. On a workstation or a server, HIDS looks for malicious or unusual activities (Jabez, 2015).

# REFERENCES

Abbasi, Ali, et al. "Challenges in Designing Exploit Mitigations for Deeply Embedded Systems." IEEE Xplore, 1 June 2019, ieeexplore.ieee.org/abstract/document/8806725.

Abir, W.H., Uddin, M.F., Khanam, F.R., Tazin, T., Khan, M.M., Masud, M. and Aljahdali, S. (2022). Explainable AI in Diagnosing and Anticipating Leukemia Using Transfer Learning Method. Computational Intelligence and Neuroscience, [online] 2022, p.e5140148. doi:10.1155/2022/5140148.

Ahmed, Nadir Naveed, and Krishnadas Nanath. "Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System." Journal of Cyber Security and Mobility, vol. 13, no. 3, 27 May 2021, 10.13052/jcsm2245-1439.1032.

Alaiz-Moreton, H., Aveleira-Mata, J., Ondicol-Garcia, J., Muñoz-Castañeda, A.L., García, I. and Benavides, C. (2019). Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol. Complexity, 2019, pp.1–11. doi:10.1155/2019/6516253.

AL-ALAWI, Prof. Adel Ismail, and Ms. Sara Abdulrahman AL-BASSAM. "The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector." Journal of Xidian University, vol. 14, July 2020, www.researchgate.net/profile/Adel-Al-Alawi/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector/links/5f288580299bf134049ebe88/The-Significance-of-Cybersecurity-System-in-Helping-Managing-Risk-in-Banking-and-Financial-Sector.pdf.

Aldini, A. and Gorrieri, R. (2002). Security Analysis of a Probabilistic Non-repudiation Protocol. [online] Available at: http://www.cs.unibo.it/gorrieri/Papers/papm02.pdf.

Almuhammadi, Sultan, and Majeed Alsaleh. "Information Security Maturity Model for Nist Cyber Security Framework." Computer Science & Information Technology (CS & IT), 25 Feb. 2017, csitcp.net/paper/7/73csit05.pdf, 10.5121/csit.2017.70305.

Alqatawna, Ja'far. "The Challenge of Implementing Information Security Standards in Small and Medium E-Business Enterprises." Journal of Software Engineering and

Applications, vol. 07, no. 10, 2014, pp. 883–890, www.scirp.org/html/7-9301952_49991.htm, 10.4236/jsea.2014.710079.

Alsinawi, Baan. "Is the NIST Cybersecurity Framework Enough to Protect Your Organization?" Www.isaca.org, 14 June 2018, www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization.

Amrin, Nabila. "The Impact of Cyber Security on SMEs." Essay.utwente.nl, 14 Aug. 2014, essay.utwente.nl/65851/.

Arden, N. Sarah, et al. "Industry 4.0 for Pharmaceutical Manufacturing: Preparing for the Smart Factories of the Future." International Journal of Pharmaceutics, vol. 602, 1 June 2021, p. 120554, www.sciencedirect.com/science/article/pii/S0378517321003598, 10.1016/j.ijpharm.2021.120554.

Asnar, Y.; Massacci, F. A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process Approach; Springer: Berlin/Heidelberg, Germany, 2011; pp. 152–184.

Ayyub, B. M. Elicitation of Expert Opinions for Uncertainty & Risks, CRC Press LLC, 2001.

Baillette, Paméla, et al. "Bring Your Own Device in Organizations: Extending the Reversed IT Adoption Logic to Security Paradoxes for CEOs and End Users." International Journal of Information Management, vol. 43, Dec. 2018, pp. 76–84, www.sciencedirect.com/science/article/pii/S0268401218305966, 10.1016/j.ijinfomgt.2018.07.007.

Bang, Youngsok, et al. "Improving Information Security Management: An Analysis of ID–Password Usage and a New Login Vulnerability Measure." International Journal of Information Management, vol. 32, no. 5, Oct. 2012, pp. 409–418, 10.1016/j.ijinfomgt.2012.01.001.

Bavisi, S. "Penetration Testing," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 369-382.

Bay, Morten. “WHAT IS CYBERSECURITY? In Search of an Encompassing Definition for the Post-Snowden Era.” frenchjournalformediaresearch.com, June 2016.

Cannon, David L., et al. CISA: Certified Information Systems Auditor Study Guide, 4ed (SYBEX). Wiley, 1 Jan. 2016, pp. 179–182.

Bernd, Moller., and Reuter, Uwe. Uncertainty Forecasting in Engineering, Berlin: Springer, 2007.

Bialas, Andrzej. “Common Criteria Related Security Design Patterns for Intelligent Sensors—Knowledge Engineering-Based Implementation.” Sensors, vol. 11, no. 8, 17 Aug. 2011, pp. 8085–8114, 10.3390/s110808085.

Blyth, A. J. C., L. Kovacich (2001). “Information Assurance: Computer Communications & Networks”. UK, Springer-Verley.

Bodeau, Deb, et al. “Cyber Resiliency and NIST Special Publication 800-53 Rev.4 Controls Sponsor: NIST.” 2013.

Boye, Carolina, et al. Cyber-Risks in the Industrial Internet of Things (IIoT): Towards a Method for Continuous Assessment. 2018.

Boyson, Sandor. “Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT Systems.” Technovation, vol. 34, no. 7, July 2014, pp. 342–353, 10.1016/j.technovation.2014.02.001.

Brandis, Knud, et al. “Governance, Risk, and Compliance in Cloud Scenarios.” Applied Sciences, vol. 9, no. 2, 17 Jan. 2019, p. 320, www.mdpi.com/2076-3417/9/2/320/pdf, 10.3390/app9020320.

Caralli, Richard, et al. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. 2007.

Chen, Baotong, et al. “Smart Factory of Industry 4.0: Key Technologies, Application Case, and Challenges.” IEEE Access, vol. 6, 2018, pp. 6505–6519, ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8207346, 10.1109/ACCESS.2017.2783682.

Ciampa, M. Security Awareness: Applying Practical Security in Your World, Thomson Learning Inc., 2004.

Clarke, R. (2019). Principles and business processes for responsible AI. Computer Law & Security Review, 35(4), 410–422. https://doi.org/10.1016/j.clsr.2019.04.007.

Daras, Nicholas. "On the Mathematical Definition of Cyberspace." Theoretical Mathematics & Applications, vol. 8, no. 1, 2018, pp. 1792–9709, www.scienpress.com/Upload/TMA/Vol%208_1_2.pdf.

Das, Saini, et al. "Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics." Journal of Information Privacy & Security, vol. 8, no. 14, 2012, pp. 33–36, www.researchgate.net/profile/Saini-Das/publication/236576825_The_stock_Market_response_to_public_announcement_of_information_security_breach_on_a_firm_An_Exploratory_study_using_firm_and_attack_characteristics_Journal_of_Information_Privacy_Security_84_2012_27-/links/00b7d53b2a40e83bf0000000/The-stock-Market-response-to-public-announcement-of-information-security-breach-on-a-firm-An-Exploratory-study-using-firm-and-attack-characteristics-Journal-of-Information-Privacy-Security-84-2012.pdf.

de Oliveira Albuquerque, R., García Villalba, L.J., Sandoval Orozco, A.L., de Sousa Júnior, R.T. and Kim, T.-H. (2016). Leveraging information security and computational trust for cybersecurity. The Journal of Supercomputing, [online] 72(10), pp.3729–3763. Available at: https://link.springer.com/article/10.1007%2Fs11227-015-1543-4.

Denning, D. "Cyber-Security as an Emergent Infrastructure," in Bombs & Bandwidth: The Emerging Relationship between IT & Security, The New Press, 2003.

Devos, Jan, and Kevin Van De Ginste. Towards a Theoretical Foundation of IT Governance -the COBIT 5 Case. 2015.

Dhillon, Gurpreet, and Backhouse, James. "Information System Security Management in the New Millenium," Communications of the ACM, vol. 43, no. 7, 2000.

Dondo, Maxwell. A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System. Defense R&D Canada -- Ottawa, 2007.

Duan, Yanqing, et al. "Addressing ICTs Skill Challenges in SMEs: Insights from Three Country Investigations." Journal of European Industrial Training, 26 Sept. 2002, pp. 430–441, d1wqtxts1xzle7.cloudfront.net/43951112/Addressing_ICTs_skill_challenges_in_SMEs20160321-13038-1tw6wyv-with-cover-page-v2.pdf.

Emine, Dahi. “Financial Challenges That Impede Increasing the Productivity of SMEs in Arab Region.” Journal of Contemporary Management, 12 July 2012, web.archive.org/web/20180422063946id_/http:/www.bapress.ca/jcm/jcm2012-2/Financial%20Challenges%20That%20Impede%20Increasing%20the%20Productivity%20of%20SMEs%20in%20Arab%20Region.pdf.

Evans, Nina, and James Price. “Development of a Holistic Model for the Management of an Enterprise’s Information Assets.” *International Journal of Information Management*, vol. 54, Oct. 2020, p. 102193, 10.1016/j.ijinfomgt.2020.102193.

Feltus, Christophe. “Introducing ISO/IEC 38500: Corporate Governance in ICT.” ITSMF Jaarcongres 2008 (2012), 2012, pp. 27–28, www.academia.edu/download/45983421/Introducing_ISO_IEC_38500_Corporate_Governance_in_ICT.pdf.

Farsi, Jahangir Yadollahi, and Mohammad Toghraee. “Identification the Main Challenges of Small and Medium Sized Enterprises in Exploiting of Innovative Opportunities (Case Study: Iran SMEs).” Journal of Global Entrepreneurship Research, vol. 2, no. 1, 2014, p. 4, journal-jger.springeropen.com/articles/10.1186/2251-7316-2-4, 10.1186/2251-7316-2-4.

Fenz, Stefan. “Cyberspace Security: A Definition and a Description of Remaining Problems.” 2005.

Fisch, E.A. & G.B. White, Secure Computer & Networks: Analysis, Design & Implementation, Boca Raton: CRC Press, 2000.

Florakis, Chris, et al. “CYBERSECURITY RISK.” NBER WORKING PAPER SERIES, Dec. 2020, pp. 23–31, www.nber.org/system/files/working_papers/w28196/w28196.pdf.

Freitas, Maria da Conceição, and Miguel Mira da Silva. “GDPR Compliance in SMEs: There Is Much to Be Done.” Journal of Information Systems Engineering & Management, vol. 3, no. 4, 10 Nov. 2018, 10.20897/jisem/3941.

GAO, The Government Accountability Office's. "GAO Reports Challenges and Successes in Cybersecurity Framework Adoption." Www.vnf.com, 5 Mar. 2018, www.vnf.com/gao-reports-challenges-and-successes-in-cybersecurity-framework.

Gehling, Bob, and David Stankard. "ECommerce Security." Citeseerx.ist.psu.edu, 2005, citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.6130&rep=rep1&type=pdf.

Globalnaps. "Small & Medium-Sized Enterprises." National Action Plans on Business and Human Rights, National Action Plans on Business and Human Rights, 3 Nov. 2017, globalnaps.org/issue/small-medium-enterprises-smes/.

GOZTEPE, Dr. Kerim, et al. "CYBER DEFENSE in DEPTH: DESIGNING CYBER SECURITY AGENCY ORGANIZATION for TURKEY." Journal of Naval Science and Engineering, vol. 10, no. 1, 2014, pp. 1–24, www.researchgate.net/profile/Kerim-Goztepe/publication/274733863_Cyber_Defense_In_Depth_Designing_Cyber_Security_Agency_Organization_For_Turkey/links/55290b710cf2779ab78e45a4/Cyber-Defense-In-Depth-Designing-Cyber-Security-Agency-Organization-For-Turkey.pdf.

Greitzer, Frank L., and Ryan E. Hohimer. "Modeling Human Behavior to Anticipate Insider Attacks." Journal of Strategic Security, vol. 4, no. 2, 2011, pp. 25–48, www.jstor.org/stable/26463925.

Guynes, Carl S., et al. "E-Commerce/Network Security Considerations." International Journal of Management & Information Systems – Second Quarter 2011, vol. 15, no. 2, 2011, clutejournals.com/index.php/IJMIS/article/download/4147/4202.

Haastrecht, Max van, et al. "A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs." The 16th International Conference on Availability, Reliability and Security, 17 Aug. 2021, 10.1145/3465481.3469199.

Hamlen, K., Liu, P., Kantarcioglu, M., Thuraisingham, B. and Yu, T. (2011). Identity management for cloud computing. Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '11.

Harris, Mark A., and Ronald Martin. "Promoting cybersecurity compliance." Cybersecurity education for awareness and compliance. IGI Global, 2019. 54-71.

Harris, Shon, and Fernando Maymi. CISSP All-In-One Exam Guide, Seventh Edition Hardcover. McGraw-Hill Education, 16 July 2016, pp. 10–13.

Hathaway, M. (2012). Leadership and Responsibility for Cybersecurity. [online] Available at: https://www.belfercenter.org/sites/default/files/legacy/files/71-80-hathaway.pdf.

Henriques de Gusmão, Ana Paula, et al. "Cybersecurity Risk Analysis Model Using Fault Tree Analysis and Fuzzy Decision Theory." International Journal of Information Management, vol. 43, Dec. 2018, pp. 248–260, www.sciencedirect.com/science/article/pii/S026840121830077X, 10.1016/j.ijinfomgt.2018.08.008.

Hong, Jason. "The State of Phishing Attacks." Communications of the ACM, vol. 55, no. 1, 1 Jan. 2012, p. 74, 10.1145/2063176.2063197.

Hong, Jin B., et al. "Systematic Identification of Threats in the Cloud: A Survey." Computer Networks, vol. 150, 26 Feb. 2019, pp. 46–69, www.sciencedirect.com/science/article/abs/pii/S1389128618308259, 10.1016/j.comnet.2018.12.009.

Hong, Sunghyuck, et al. Ransomware Attack Analysis, and Countermeasures of Defensive Aspects. 2018, www.koreascience.or.kr/article/JAKO201809538046711.pdf, 10.22156/CS4SMB.2018.8.1.139.

Hubbard, Douglas, and Richard Seiersen. How to Measure Anything in Cybersecurity Risk. 2012.

IBM Security. "Regional and Industry Differences Showed Some Big Swings from 2019." [ebook] p. 12. Capita, IBM Security, 6 Aug. 2020, www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

ISO. "ISO/IEC 27001 Information Security Management." ISO, 2013, www.iso.org/isoiec-27001-information-security.html.

ITU-T. "International Telecommunications Union (ITU) - Telecoms Standards Recommendation X.805." ITU, Geneva, 2005.

Jabez, J., and B. Muthukumar. “Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach.” Procedia Computer Science, vol. 48, 2015, pp. 338–346, 10.1016/j.procs.2015.04.191.

Kabanda, Salah, et al. “Exploring SME Cybersecurity Practices in Developing Countries.” Journal of Organizational Computing and Electronic Commerce, 13 July 2018, pp. 269–282, www.researchgate.net/profile/Salah-Kabanda-2/publication/326385562_Exploring_SME_cybersecurity_practices_in_developing_countries/links/5cd56c2ea6fdccc9dd9d5ae4/Exploring-SME-cybersecurity-practices-in-developing-countries.pdf.

Katsikas, S. K. "Risk Management," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 605-625.

Khalique, Muhammad. “Challenges for Pakistani SMEs in a Knowledge-Based Economy.” Indus Journal of Management & Social Sciences, vol. 5, no. 2, 2011, pp. 74–80, d1wqtxts1xzle7.cloudfront.net/6314806/7-2-Khalique-Malasia-Challenges_for_Pakistani_SMEs_in_a_Knowledge_-Based_Economy-0-with-cover-page-v2.pdf.

Khan, N.A., Brohi, S.N. and Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. [online] Available at: https://www.techrxiv.org/ndownloader/files/22624319.

Kindervag, John. No More Chewy Centers: The Zero Trust Model of Information Security Vision: The Security Architecture And Operations Playbook. 2016.

Krombholz, Katharina, et al. “Advanced Social Engineering Attacks.” Journal of Information Security and Applications, vol. 22, June 2015, pp. 113–122, 10.1016/j.jisa.2014.09.005.

Kure, Halima Ibrahim, and Shareeful Islam. “Assets Focus Risk Management Framework for Critical Infrastructure Cybersecurity Risk Management.” IET Cyber-Physical Systems: Theory & Applications, 3 June 2019, repository.uel.ac.uk/download/5d69579c168f1eaa29a5f75e5eae08ffe96ab8c6bce1bd427c00e7a589aefd95/1885444/IET-CPS.2018.5079.pdf.

Kurniawan, Endang, and Imam Riadi. “SECURITY LEVEL ANALYSIS of ACADEMIC INFORMATION SYSTEMS BASED on STANDARD ISO 27002: 2013 USING SSE-CMM.” International Journal of Computer Science and Information Security (IJCSIS), vol. 16, no. 1, Jan. 2018, www.researchgate.net/profile/Imam-Riadi-2/publication/323029044_Security_level_analysis_of_academic_information_systems_based_on_standard_ISO_270022003_using_SSE-CMM/links/5a7d699c458515dea40f96f0/Security-level-analysis-of-academic-information-systems-based-on-standard-ISO-270022003-using-SSE-CMM.pdf.

Li, Ling, et al. “Investigating the Impact of Cybersecurity Policy Awareness on Employees’ Cybersecurity Behavior.” International Journal of Information Management, vol. 45, Apr. 2019, pp. 13–24, www.sciencedirect.com/science/article/pii/S0268401218302093, 10.1016/j.ijinfomgt.2018.10.017.

Mahjabin, Tasnuva, et al. “A Survey of Distributed Denial-of-Service Attack, Prevention, and Mitigation Techniques.” International Journal of Distributed Sensor Networks, vol. 13, no. 12, Dec. 2017, p. 155014771774146, 10.1177/1550147717741463.

Mallik, Avijit. “MAN-IN-THE-MIDDLE-ATTACK: UNDERSTANDING in SIMPLE WORDS.” Cyberspace: Jurnal Pendidikan Teknologi Informasi, vol. 2, no. 2, 10 Jan. 2019, p. 109, 10.22373/cj.v2i2.3453.

Microsoft (2022). SdcaMaximumEntropyMulticlassTrainer Class (Microsoft.ML.Trainers). [online] docs.microsoft.com. Available at: https://docs.microsoft.com/en-us/dotnet/api/microsoft.ml.trainers.sdcamaximumentropymulticlasstrainer [Accessed 1 Jun. 2022].

Moeuf, Alexandre, et al. “The Industrial Management of SMEs in the Era of Industry 4.0.” International Journal of Production Research, 8 Sept. 2017, www.researchgate.net/profile/Robert-Pellerin/publication/319612802_The_industrial_management_of_SMEs_in_the_era_of_

Industry_40/links/5c34e1ec92851c22a364b770/The-industrial-management-of-SMEs-in-the-era-of-Industry-40.pdf.

Muhati, Eric. Factors Affecting Cyber-Security in Kenya -A Case of Small Medium Enterprises. 2018.

MULLET, VALENTIN, et al. “A Review of Cybersecurity Guidelines for Manufacturing Factories in Industry 4.0.” IEEE ACCESS 2021, vol. 9, 3 Feb. 2021, ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9345803.

Muriithi, Samuel. AFRICAN SMALL and MEDIUM ENTERPRISES (SMES) CONTRIBUTIONS, CHALLENGES and SOLUTIONS Future Business Model for 21st Century View Project the IMPACT of COVID-19 on AFRICAN SMES, POSSIBLE REMEDIES and SOURCE of FUNDING View Project. 2017.

Mustaqeem, A., Anwar, S.M. and Majid, M. (2018). Multiclass Classification of Cardiac Arrhythmia Using Improved Feature Selection and SVM Invariants. Computational and Mathematical Methods in Medicine, 2018, pp.1–10. doi:10.1155/2018/7310496.

Nguyen, L. and Gupta, V. (2021). Towards a framework of enforcing resilient operation of cyber-physical systems with unknown dynamics. IET Cyber-Physical Systems: Theory & Applications.

Noble, H. and Heale, R. (2019). Triangulation in research, with Examples. Evidence Based Nursing, [online] 22(3), pp.67–68. doi:10.1136/ebnurs-2019-103145.

Oyebisi, David, and Kennedy Njenga. “Behaviour of Outsourced Employees as Sources of Information System Security Threats.” Financial Cryptography and Data Security, 2020, pp. 8–10, 10.1007/978-3-030-54455-3_10.

P, Yevseiev S., et al. Construction Methodology of Information Security System of Banking. Repository.hneu.edu.ua, Premier Publishing s. r. o., 2018, pp. 41–46, 80–90, 200–206, 213–216, repository.hneu.edu.ua/handle/123456789/21043.

Paloma, Jay. “Windows Server 2008 in an Organization’s Defense in Depth Strategy.” Docs.microsoft.com, Microsoft, 20 May 2008, docs.microsoft.com/en-us/previous-versions/tn-archive/cc512681(v=technet.10).

Parker, D. "Toward a New Framework for Information Security," in The Computer Security Handbook,4th ed., New York, John Wiley & sons, 2002.

Patel, Sandip C., et al. “Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements.” International Journal of Information Management, vol. 28, no. 6, 1 Dec. 2008, pp. 483–491, www.sciencedirect.com/science/article/abs/pii/S0268401208000054, 10.1016/j.ijinfomgt.2008.01.009.

Perfilieva, I. "Fuzzy Function: Theoretical and Practical Point of View," in EUSFLAT, Aix-les-Bains, France, 2011.

PETKOVSKA, T. (2015). Original scientific paper Tatjana PETKOVSKA 1 ) THE ROLE AND IMPORTANCE OF INNOVATION IN BUSINESS OF SMALL AND MEDIUM ENTERPRISES. Retrieved from https://www.ek-inst.ukim.edu.mk/wp-content/uploads/2018/07/4-ROLE-AND-IMPORTANCE-OF-INNOVATION-IN-BUSINESS-OF-SMALL-AND-MEDIUM-ENTERPRISES.pdf

Ponsard, Christophe, et al. “Survey and Lessons Learned on Raising SME Awareness about Cybersecurity.” Proceedings of the 5th International Conference on Information Systems Security and Privacy, 2019, www.scitepress.org/Papers/2019/75743/75743.pdf, 10.5220/0007574305580563.

Popescul, Daniela. The Confidentiality -Integrity - Accessibility Triad into the Knowledge Security: A Reassessment from the Point of View of the Knowledge Contribution to Innovation. 2011.

Rae, Andrew, and Asma Patel. Defining a New Composite Cybersecurity Rating Scheme for SMEs in the U.K. 2019.

Ramakrishnan, R. “BFSI: Best Practices in Financial Inclusion.” 22nd SKOCH Summit 2010 the India Decide, 19 Mar. 2010, www.researchgate.net/profile/Ramakrishnan-Ramachandran-2/publication/228119633_BFSI_Best_Practices_in_Financial_Inclusion/links/02e7e516e971a368df000000/BFSI-Best-Practices-in-Financial-Inclusion.pdf.

Ramukumba, Takalani. “Overcoming SMEs Challenges through Critical Success Factors: A Case of SMEs in the Western Cape Province, South Africa.” Economic and Business Review, vol. 16, no. 1, 1 Aug. 2014, 10.15458/2335-4216.1178.

Riahi, Arbia, et al. “A Systemic and Cognitive Approach for IoT Security.” IEEE Xplore, 1 Feb. 2014, ieeexplore.ieee.org/abstract/document/6785328.

Kapodistria, Helen, et al. “An Advanced Web Attack Detection and Prevention Tool.” Researchgate, July 2011, www.researchgate.net/profile/Sarandis-Mitropoulos/publication/220208181_An_Advanced_Web_Attack_Detection_and_Prevention_Tool/links/60abe72c92851ca9dce1cc6c/An-Advanced-Web-Attack-Detection-and-Prevention-Tool.pdf.

Keller, Nicole. “Cybersecurity Framework.” NIST, 8 July 2019, www.nist.gov/cyberframework.

Kim, Sangkyun. “Classification of ISO27002 Controls.”, 10 Nov. 2011.

Liao, Qinyu. RANSOMWARE: A GROWING THREAT to SMEs. 2008.

Meszaros, Jan, and Alena Buchalcevova. “Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management.” Computers & Security, vol. 65, Mar. 2017, pp. 300–313, 10.1016/j.cose.2016.12.008.

Ministry of Micro, Small and Medium Enterprises, Government of India. “What’s MSME | Ministry of Micro, Small and Medium Enterprises.” Msme.gov.in, 2019, msme.gov.in/know-about-msme.

Naseer, Ayesha, et al. “Real-Time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-Based Analysis.” International Journal of Information Management, vol. 59, Aug. 2021, p. 102334, 10.1016/j.ijinfomgt.2021.102334.

Nazir, Sajid, et al. “Assessing and Augmenting SCADA Cyber Security: A Survey of Techniques.” Computers & Security, vol. 70, Sept. 2017, pp. 436–454, 10.1016/j.cose.2017.06.010.

NIST – Cyber Risk - Definition, CSRC Content. “Cyber Risk - Glossary | CSRC.” Csrc.nist.gov, 2018, csrc.nist.gov/glossary/term/cyber_risk.

NIST – Cyber Threat - Definition, CSRC Content. “Cyber Threat - Glossary | CSRC.” Csrc.nist.gov, 2018, csrc.nist.gov/glossary/term/Cyber_Threat.

Papa, Stephen, et al. Availability Based Risk Analysis for SCADA Embedded Computer Systems. 2011.

Pawar, S. and Palivela, Dr.H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, [online] 2(1), p.100080. doi:10.1016/j.jjimei.2022.100080.

PETKOVSKA, Tatjana. Original Scientific Paper Tatjana PETKOVSKA 1) the ROLE and IMPORTANCE of INNOVATION in BUSINESS of SMALL and MEDIUM ENTERPRISES. 2015.

PhishMe. “Cofense.” Cofense, PhishMe, Inc., 2018, cofense.com/whitepaper/enterprise-phishing-susceptibility-report/.

Pratt, Mary K. “What Is Zero Trust? A Model for More Effective Security.” CSO Online, 16 Jan. 2018, www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html.

Ozier, Will. "Risk Assessment," in Information Security Management Handbook, CRC Press, 2002.

Ralston, P.A.S., et al. “Cyber Security Risk Assessment for SCADA and DCS Networks.” ISA Transactions, vol. 46, no. 4, Oct. 2007, pp. 583–594, 10.1016/j.isatra.2007.04.003.

Saleem, Jibran, et al. “A State of the Art Survey - Impact of Cyber Attacks on SME’s.” Proceedings of the International Conference on Future Networks and Distributed Systems, 19 July 2017, 10.1145/3102304.3109812.

Samarati, Pierangela, and Sabrina De Capitani Di Vimercati. Cloud Security: Issues and Concerns. 2016.

Samonas, Spyridon, and David Coss. “THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY, and AVAILABILITY in SECURITY.”, 2014.

SENSEON. "The State of Cyber Security SME Report 2019." Senseon.io, 2019, [ebook] p. 4. https://www.cbronline.com/wp-content/uploads/dlm_uploads/2019/06/Senseon-SME-Report-2019-Web.pdf

Shepherd, Maddie. "30 Surprising Small Business Cyber Security Statistics (2021)." Fundera, Fundera, 30 Aug. 2019, www.fundera.com/resources/small-business-cyber-security-statistics.

Siewert, Sam, et al. "Fail-Safe, Fail-Secure Experiments for Small UAS and UAM Traffic in Urban Airspace." IEEE Xplore, 1 Sept. 2019, ieeexplore.ieee.org/abstract/document/9081710.

Shaurette, K. M. (2004). "The Building Blocks of Information Security," in Information Security Management Handbook (5th ed.). Boca Raton, London, New York, Washington D.C.: Auerbach Publishers.

Shojaie, Bahareh, and Hannes Federrath. "Evaluating the Effectiveness of ISO 27001:2013 Based on Annex A." 11 Sept. 2014.

Stajano, F., and R. Anderson. "The Resurrecting Duckling: Security Issues for Ubiquitous Computing." Computer, vol. 35, no. 4, Apr. 2002, pp. supl22–supl26, 10.1109/mc.2002.1012427.

Sukmaji, Muhammad, et al. "INFORMATION SECURITY POLICY and SOP as the ACCESS CONTROL DOCUMENT of PT. JUI SHIN INDONESIA USING ISO/IEC 27002:2013." Pilar Nusa Mandiri: Journal of Computing and Information System, vol. 17, no. 2, 6 Sept. 2021, pp. 115–112, ejournal.nusamandiri.ac.id/index.php/pilar/article/view/2282/865, 10.33480/pilar.v17i2.2282.

Sutton, Steve, et al. "Risk Analysis in Extended Enterprise Environments: Identification of Critical Risk Factors in B2B E-Commerce Relationships." Journal of the Association for Information Systems, vol. 9, no. 4, Apr. 2008, pp. 160–174, 10.17705/1jais.00155.

Swenson. "New NIST Guide Helps Small Businesses Improve Cybersecurity." NIST, 10 Nov. 2016, www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity.

Tan, K.S., Chong, S.C., Lin, B., Eze, U.: Internet-based ICT adoption: evidence from Malaysian SMEs. Industrial Management & Data Systems, 224–244 (2009).

Tandon, Aditya, and Anand Nayyar. “A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat.” Researchgate, 2019, www.researchgate.net/profile/Anand-Nayyar/publication/327536189_A_Comprehensive_Survey_on_Ransomware_Attack_A_Growing_Havoc_Cyberthreat_Proceedings_of_ICDMAI_2018_Volume_2/links/5b9b62a7a6fdccd3cb533ccb/A-Comprehensive-Survey-on-Ransomware-Attack-A-Growing-Havoc-Cyberthreat-Proceedings-of-ICDMAI-2018-Volume-2.pdf.

Tatar, Ünal, and Bilge Karabacak. “An Hierarchical Asset Valuation Method for Information Security Risk Analysis.” IEEE Xplore, 1 June 2012, ieeexplore.ieee.org/abstract/document/6284977/.

Thinyane, Mamello, and Debora Christine. “CYBERRESILIENCE in ASIA-PACIFIC.” United Nations University, 2020, pp. 12–13, 20–21, 15–17, 79, collections.unu.edu/eserv/UNU:7760/n2020_Cyber_Resilience_in_Asia-Pacific.pdf.

Trentesaux, D. and Karnouskos, S. (2021). Engineering ethical behaviors in autonomous industrial cyber-physical human systems. Cognition, Technology & Work.

Vidalis, Dr. Stilianos, and Dr. Andrew Jones. “Analyzing Threat Agents & Their Attributes.” ECIW, June 2005, pp. 369–380, www.researchgate.net/profile/Andy-Jones-6/publication/220947230_Analyzing_Threat_Agents_and_Their_Attributes/links/00b49539bff10d7f49000000/Analyzing-Threat-Agents-and-Their-Attributes.pdf.

Vegh, L. and Miclea, L. (2015). Authenticity, integrity and secure communication in cyber-physical systems. Journal of Computer Science and Control Systems, 8(1).

Walker, J. "Internet Security," in Computer & Information Security Handbook, Morgan-Kaufmann, Inc., 2009, pp. 93-117.

Wall, K. The Kaplan and Garrick Definition of Risk and Its Application to Managerial Decision Problems. 2011.

Whitman, Michael E, and Herbert J Mattord. Principles of Information Security. 6th ed., Boston, Mass., Cengage Learning, 2018.

Wichers, Dave. “OWASP Top-10 2017.” OWASP, 2017, upload.wikimedia.org/wikipedia/mediawiki/archive/e/e9/20180111214627%21OWASP_Top-10_2017_-_Presentation.pdf.

WTO. “WTO | World Trade Report 2016 | Levelling the Trading Field for SMEs.” Www.wto.org, World Trade Organization, 2016, www.wto.org/english/res_e/publications_e/wtr16_e.htm.

Yee, Chai Kar, and Mohamad Fadli Zolkipli. “Review on Confidentiality, Integrity and Availability in Information Security.” Journal of ICT in Education, vol. 8, no. 2, 13 July 2021, pp. 34–42, ojs.upsi.edu.my/index.php/JICTIE/article/view/5203, 10.37134/jictie.vol8.2.4.2021.

Zadeh, L. "The Concept of a Liinguistic Variable and Its Application to Approximate Reasoning," Information Sciences, vol. 8, pp. 199-257, 1975.

Zimmerman, P. The Official PGP User's Guide, MIT Press, 1995.

Zolkipli, Mohamad Fadli, and A. Jantan. “An Approach for Malware Behavior Identification and Classification.” IEEE Xplore, 1 Mar. 2011, ieeexplore.ieee.org/abstract/document/5764001.