International Journal of Cybersecurity Intelligence & Cybercrime

Volume 8 | Issue 1 Article 4

4-2025

# NEED OF PARADIGM SHIFT IN CYBERSECURITY IMPLEMENTATION FOR SMALL AND MEDIUM ENTERPRISES (SMES)

cybersecurity, BDSLCCI, SME, SMB, MSME, Framework



## Recommended Citation

Pawar, S. & Palivela, H. (2025). Pawar, Shekhar . *International Journal of Cybersecurity Intelligence & Cybercrime, 8(1)*, - . DOI: https://doi.org/10.52306/2578-3289.1184
Available at: https://vc.bridgew.edu/ijcic/vol8/iss1/4

Pawar & Palivela. (2025). *International Journal of Cybersecurity Intelligence and Cybercrime, 8*(1), 39-75.

# Need of Paradigm Shift in Cybersecurity Implementation for Small and Medium Enterprises (SMES)

Shekhar Pawar*, Ph.D., Swiss School of Business and Management Geneva, Switzerland.
Hemant Palivela, Ph.D., Swiss School of Business and Management Geneva, Switzerland.

*Keywords: SME; MSME; SMB; cybersecurity; BDSLCCI; framework.*

**Abstract:**
The increasing digitization of small and medium enterprises (SMEs) has significantly expanded their attack surface, creating opportunities for various cyber threats. Despite the availability of numerous cybersecurity standards and frameworks in the global market, there are still many reports of sophisticated cyberattacks targeting organizations worldwide. Recent studies indicate that one out of five cyberattacks targets SMEs. Although SMEs are relatively smaller individually, they contribute significantly to the global economy, including playing a major role in GDP and providing numerous employment opportunities. Compared to large-sized organizations, SMEs generally have limited resources and funds and prioritize specific business domains. Existing cybersecurity standards and frameworks are often generic and not aligned with the business goals of SMEs. Additionally, these standards require SMEs to implement hundreds of cybersecurity controls to achieve a certain level of global cybersecurity maturity. This paper, based on an international research study, will assess the current cybersecurity posture of SMEs and the challenges they face in implementing cybersecurity measures. The authors will also propose a new cybersecurity framework to address these challenges, considering the prioritization of the CIA Triad and Defense in Depth concepts.

## Introduction

With the Industry 4.0 revolution and the ongoing transition to Industry 5.0, small and medium enterprises (SMEs) worldwide have faced increasing internal and external pressure to adapt (Madhavan, 2024; Hein-Pensel, 2023). The COVID-19 pandemic has also negatively impacted SMEs' key activities, with lockdown rules and interventions affecting them differently across various locations. Many SMEs were forced to change their ways of working and adopt cloud technologies and other methods to sustain their operations (Erdiaw- Kwasie, 2023).

To thrive in a competitive market and embrace the digital era, SMEs now incorporate various components from the shop floor to the top floor, encompassing a wide range of technologies from IoT devices to cloud computing (Müller, 2018). While these advancements bring benefits, they also increase the cyber-attack surface for these organizations. Recent studies indicate that half of SMEs have a significant chance of experiencing a cyber breach, with more than 50% of them being targeted by cyberattacks (SENSEON, 2019; Osborn, 2015; Aguilar, 2015).

The definition of an SME varies by country, with some referring to them as small and medium businesses (SMBs) or micro, small, and medium enterprises (MSMEs). This categorization typically depends on the number of employees and/or a specific range of annual turnover (Pawar, 2023). Globally, more than 400 million SMEs constitute 90% of the business population, contributing 55% to the Gross Domestic Product (GDP) of developed economies and supporting 70% of global employment (WTO, 2016).

*Corresponding author
Shekhar Pawar*, Doctor of Business Administrator, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland.
Email: shekharpawarmgm@gmail.com

It is important to distinguish between cybersecurity and information security, as they are often mistakenly considered the same. According to ISO definitions, cyberspace is formed by internet connectivity or connectivity without the internet among physical entities. Cybersecurity refers to the measures that ensure the confidentiality, integrity, and availability of information within cyberspace (Bay, 2016).

Given the recent statistics on SMEs under cyber threats, there is a pressing need for research studies to understand the detailed problems faced by SMEs, who are prime victims in these cases. This paper presents a detailed research survey conducted among various SMEs worldwide to gather valuable insights. Many top management executives voluntarily participated in this survey, despite the sensitive nature of cybersecurity information within their organizations. The findings from 115 SMEs, followed by an analysis of the results, will be presented. Based on these inputs, the authors will recommend resolutions for SMEs. In the following sections, the authors will explain the need for a paradigm shift in the implementation of cybersecurity controls for SMEs, moving away from traditional cybersecurity standards or frameworks.

**Related Work**

Most enterprises use ISO 27001 as the primary information security standard or framework, as it provides a formal set of specifications for controls to mitigate information security risks. It also offers formal Information Security Management System (ISMS) certification for qualifying organizations (Mohamed, 2012). ISO 27001:2013 includes 114 controls mapped to 14 different objectives, while ISO/IEC 27002:2013 provides guidelines for implementing these controls (Shojaie, 2014; Sukmaji, 2021). The recently launched ISO 27001:2022 includes 93 controls divided into four categories: 37 organizational controls, 8 people control, 14 physical controls, and 34 technological controls (Surya, 2024; Suorsa, 2023; McIntosh, 2024). It is important to note that ISO 27001 underwent significant changes in 2022, the first update since 2013.

In addition to ISMS, the National Institute for Standards and Technology (NIST) framework for cybersecurity is widely accepted. It is based on five core functions: Identify, Protect, Detect, Respond, and Recover. This framework focuses on the cybersecurity of critical infrastructure, regardless of an organization's size. Unlike industry-specific standards, the NIST framework can be applied globally across all segments. It emphasizes risk management at the organizational level for delivering critical services and continuously improving Information Technology (IT) and Industrial Control Systems (ICS) environments (NIST, 2014). NIST Special Publication 800-53 Revision 4 includes around 900 unique security controls from 18 control families (Bodeau, 2013). The NIST Cybersecurity Framework (CSF) has evolved through several versions. CSF 1.0, launched in 2014, targeted critical infrastructure sectors and provided a structured approach to managing cybersecurity risks. CSF 1.1, introduced in 2018, enhanced supply chain risk management, self-assessment processes, and alignment with other standards. The latest version, CSF 2.0, launched in 2024, expands the framework's applicability to all organizations, regardless of size or sector. It includes new guidance on cybersecurity governance, continuous improvement practices, and a broader focus on managing cybersecurity as a major enterprise risk (Dimakopoulou, 2024; Toussaint, 2024; Wang, 2024; Parmar, 2024).

Key cost factors for ISO 27001 and NIST include assessment and gap analysis, implementation, training and awareness, and ongoing annual maintenance. For SMEs, the cost of such certifications can amount to thousands of US dollars per phase, depending on the number of employees and other factors (Leszczyna, 2024; El-Hajj, 2024).

Another popular framework is the Security System Engineering Capability Maturity Model (SSE-CMM), which consists of System Security Engineering (SSE) and Capability Maturity Model (CMM). SSE-CMM includes 11 process areas mapped to five maturity levels: initial, repeatable, defined, managed, and optimized. The Common Criteria (CC) framework focuses on the security objectives of IT products or system operational environments (Bialas, 2011). Additionally, the Zero Trust Concept, which adheres to the practice of "no trust" for any access request, is gaining popularity (Lee, 2017).

While CC is effective for evaluating IT product security, it is time-consuming and costly. SSE-CMM provides guidelines but does not define specific processes. ISO/IEC 27001 helps develop ISMS but can be challenging for organizations lacking security knowledge. The NIST framework requires significant resources for successful implementation and has some gaps. Smaller organizations may be hesitant to adopt the framework due to perceived low risk (GAO, 2018). Although the Zero Trust concept is beneficial, it requires substantial resources and may not meet all domain-specific requirements (Alsinawi, 2018).

Recent research highlights emerging cybersecurity threats such as ransomware attacks, advanced persistent threats (APTs), Internet of Things (IoT) vulnerabilities, deepfakes, and social engineering exploits. Cybercriminals are leveraging new vulnerabilities, technologies, and methodologies, making it clear that new cybersecurity threats pose serious risks to individuals and organizations. Consequently, cybersecurity strategies must evolve more frequently and adopt a multi-layered approach, including strong security measures, thorough employee training, and regular security audits (Dave, 2023; Gulyas, 2023).

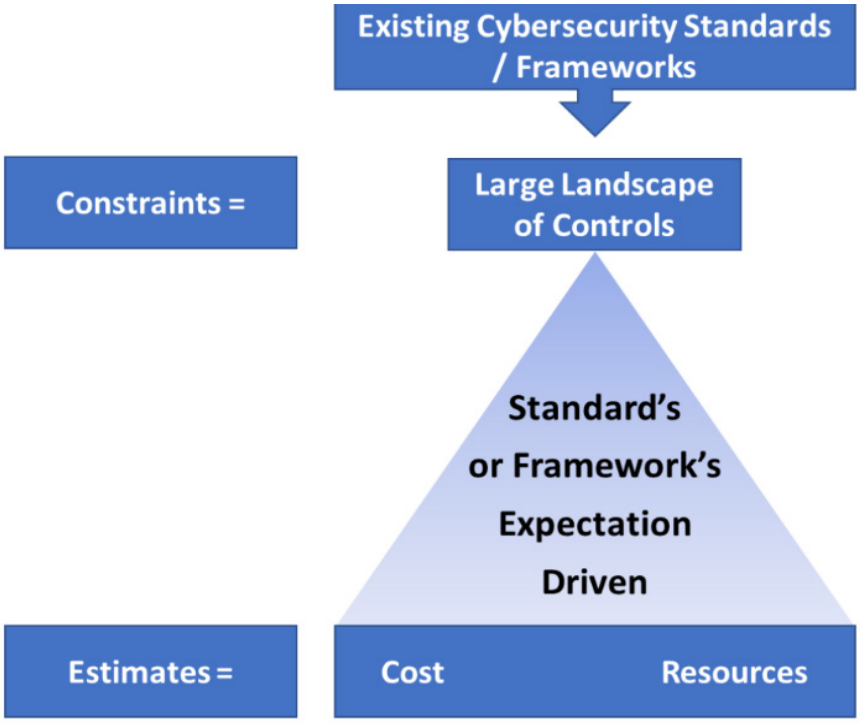


*Figure 1*: Current Paradigm of Cybersecurity

Various studies conducted in recent years indicate that SMEs worldwide face common challenges such as financial constraints, a lack of skilled workforce and/or skilled top management, and limited resources. For any enterprise to sustain and grow, strategic planning is essential, starting with defining the business environment and strategic objectives. Top management then establishes programs to achieve these goals. However, SMEs often struggle to invest in areas like cybersecurity due to financial constraints and limited resources, making it difficult to align these investments with their strategic objectives (Arroyabe, 2024; Ayyagari, 2017; Junior, 2023; Erdogan, 2023; PETKOVSKA, 2015; Prasanna, 2020; Duan, 2002; Emine, 2012; Farsi, 2014; Moeuf, 2017; Muriithi, 2017; Ramukumba, 2014; Siti, 2009; Khalique, 2011; Maritan, 2009).

In summary, existing research highlights several key challenges faced by SMEs in adopting cybersecurity standards and frameworks. These include the high number of controls required, significant financial investment for consulting and implementation, long implementation periods, a lack of alignment with the latest cyber threats, and insufficient focus on the business goals of the organization.

As illustrated in Figure 1, SMEs need substantial funds and resources to implement the extensive list of controls required by existing cybersecurity standards or frameworks. Consequently, if an SME's top management decides to adopt a cybersecurity standard or framework, they must be prepared for the considerable financial and resource commitments involved.

**Research Survey and Analysis of Results**

In addition to the points identified in the related work section, the authors took further steps to understand the current cybersecurity posture and real ground-level issues faced by SMEs regarding cybersecurity implementation. In the third quarter of 2021, the authors approached the top management of hundreds of SMEs to gather insights within their enterprises. Given the critical nature of cybersecurity for any organization, only 115 SMEs voluntarily participated in this research survey. The valuable direct information from these SMEs is analyzed and discussed in this section.

The survey participants included top management such as directors, owners, C-level executives, and business unit heads. As shown in Figure 2, SMEs from various countries participated, including India, the United States, Australia, the United Arab Emirates, Russia, Sweden, South Africa, Indonesia, Norway, Israel, Singapore, Sri Lanka, Ireland, Bangladesh, the United Kingdom, Ghana, Cyprus, Kenya, and Nigeria. Additionally, there was diverse participation from different business domains, including the IT industry, E- commerce, Telecommunication, Banking, Manufacturing, Marketing, Education, Maritime, Travel Technology, Oil Industry, Online Services, Exports, Financial Services, Fast-Moving Consumer Goods (FMCG), Fintech, Financial Services and Insurance (BFSI), Consulting, Education Technology, Executive Coaching, Healthcare, Hospitality, Insurance, Logistics and Supply Chain Management, Human Resources, Pharmaceutical, and Renewable Energy sectors.

As shown in Figure 3, when the authors asked "How old is your SME?" to the top management of the participating SMEs, the survey results were quite interesting. The responses revealed that 40% of the SME participants were from enterprises with more than 10 years of business history, followed by 18% of SMEs that had been in existence for between 5 and 10 years. This indicates that around 58% of the participating SMEs were mature in their business domains, having sustained their operations for several years. These m-

ature SMEs likely recognize the growing importance of cybersecurity as their businesses expand.

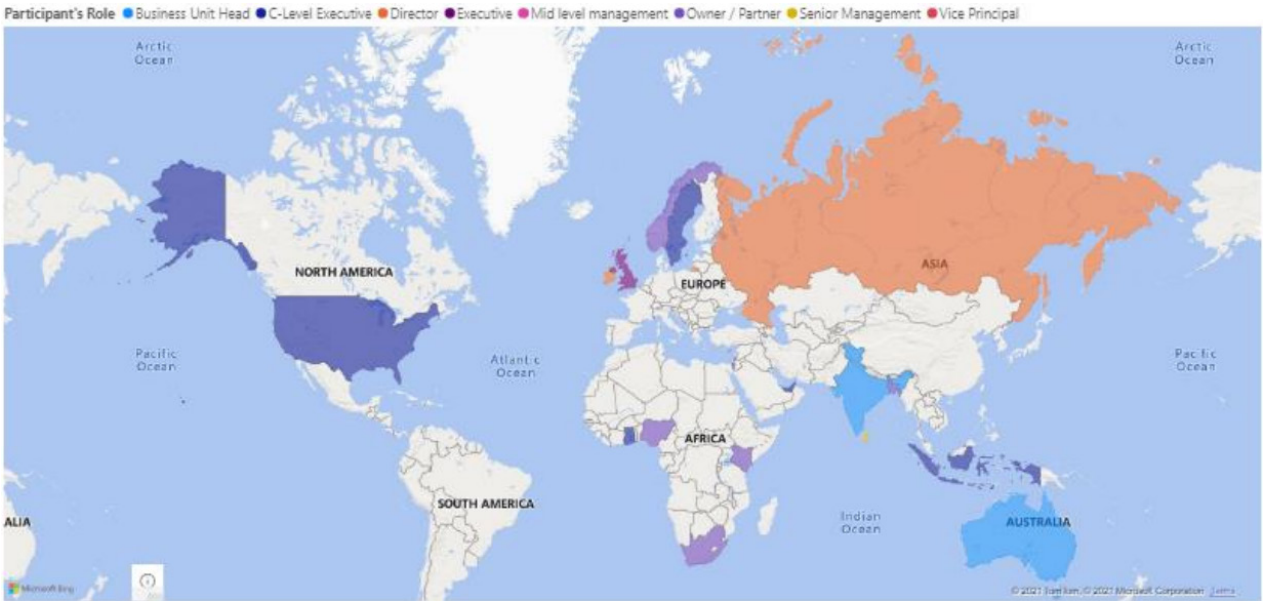


*Figure 2*: SME Participation

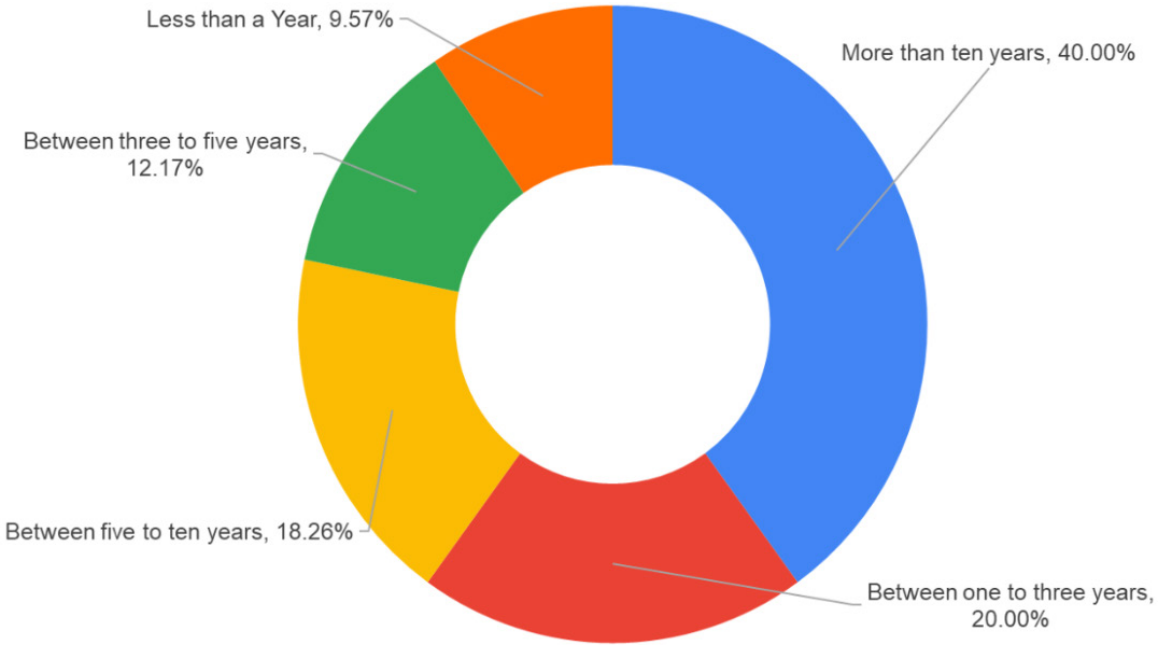


*Figure 3*: Age of SME participated in Survey

Further, when asked, "Does your organization have any of the below standards or frameworks implemented?" as shown in Figure 4, it was evident that more than half of SMEs do not have any cybersecurity standards or frameworks in place. Looking at cumulative percentage, ISO 27001, widely known as ISMS, is implemented by about 23% of SMEs, followed by the popular GDPR, also adopted by around 23% of SMEs.

While standards like the Payment Card Industry Data Security Standard (PCI-DSS), EU General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Financial Industry Regulatory Authority (FINRA), Food Safety and Standards Authority of India (FSSAI), and Singapore Personal Data Protection Act (PDPA) fulfill specific compliance requirements, they are not comprehensive cybersecurity standards or frameworks that can protect all critical assets of an SME. NIST's CSF has been implemented by about 8% of SMEs.

Interestingly, around 1% of SMEs are attempting to implement their own standards or frameworks to protect against cyber threats. However, half of the SMEs are completely exposed to cyber threats, which poses a significant risk. Many SMEs that adopt only compliance-related or best practices controls without firm protection at different levels are at high risk of cyber-attacks. More than two-thirds of SMEs are highly exposed to cyber threats, even if ISO 27001 and NIST are properly implemented within a few.

The vast scope of cyberspace has become an integral part of our daily lives in today's rapidly evolving digital landscape, underscoring the increasing importance and demand for robust cybersecurity measures for any organization. Rather than randomly selecting cybersecurity controls, it is crucial for SMEs to adopt a systematic cybersecurity standard or framework (Wang, 2024).

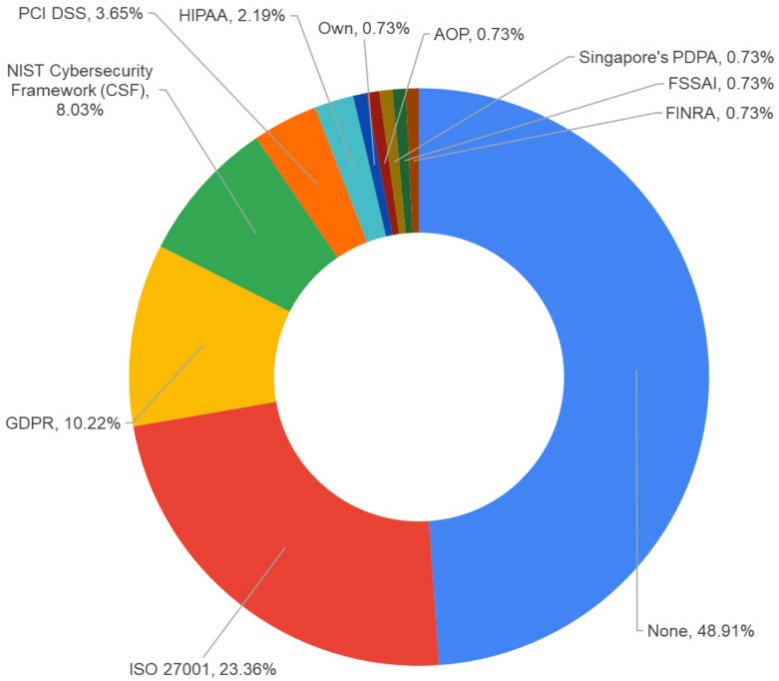


*Figure 4*: Security Standards / Frameworks Implemented in SMEs

As shown in Figure 5, in response to the question "Does your organization have security controls in place?" it was found that approximately 28% of SMEs do not have any cybersecurity controls implemented. This means they have "NO" or "ZERO" cybersecurity controls in place. Additionally, almost 16% of SMEs are unsure if they have any cybersecurity controls, indicating a lack of awareness or confusion among some organizations. This uncertainty suggests that some SMEs might mistakenly believe they are cyber secure, while others are uncertain about their cybersecurity status. This lack of awareness among top management about cybersecurity implementation is concerning.

According to the World Economic Forum's Global Risk Report, cybersecurity is one of the risks that has worsened significantly due to the COVID-19 pandemic. SMEs without sufficient cybersecurity controls are more likely to experience successful cyberattacks (Neri, 2024; Al-Somali, 2024). Around 57% of SMEs reported having cybersecurity controls in place. These SMEs might be those that have adopted cybersecurity standards like ISO 27001 or NIST, while others might have implemented self-identified controls, giving them a sense of security.

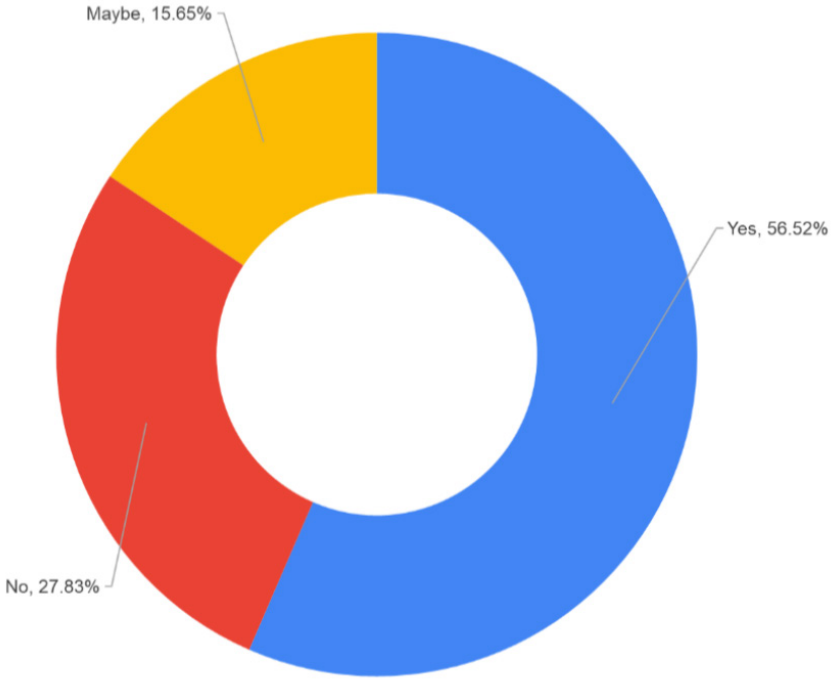


*Figure 5*: Any Security Controls Implementation for SME

Any cybersecurity posture includes three main categories of controls: physical controls, logical or technical controls, and administrative controls. Physical controls are tangible measures visible to all individuals associated with SMEs. Technical controls involve technology implementations to achieve specific cybersecurity goals. Administrative controls focus on processes, guidelines, and procedures that everyone in the organization must follow to meet cybersecurity objectives. The authors investigated the implementation of these three types of controls among SMEs.

Physical controls, aimed at enhancing cybersecurity posture, primarily focus on monitoring and contribute to all three areas: people, process, and technology. These controls are crucial for protecting critical assets or facilities against theft, sabotage, or similar threats (Xie, 2019).

As shown in Figure 6, when asked, "If you have security controls in place, please share the 'physical security' controls already in place," considering cumulative percentage, it was found that around 8% of SMEs do not have any physical cybersecurity controls. The most popular physical controls were CCTV (16%), physical gates (12%), and access cards (10%).

Physical controls are essential in cybersecurity. For example, SMEs should enforce strict policies regarding the handling of tangible documents and removable storage devices, as well as maintaining clear screens in information processing areas. Organizations should create and implement clean desk and screen policies, ensuring all relevant staff members are aware of these guidelines. This approach reduces the risk of physical social engineering attacks and minimizes unauthorized access (Papathanasiou, 2024). However, motion controls, security lighting, and environmental controls were among the least implemented physical controls, indicating that many SMEs lack adequate physical security measures.

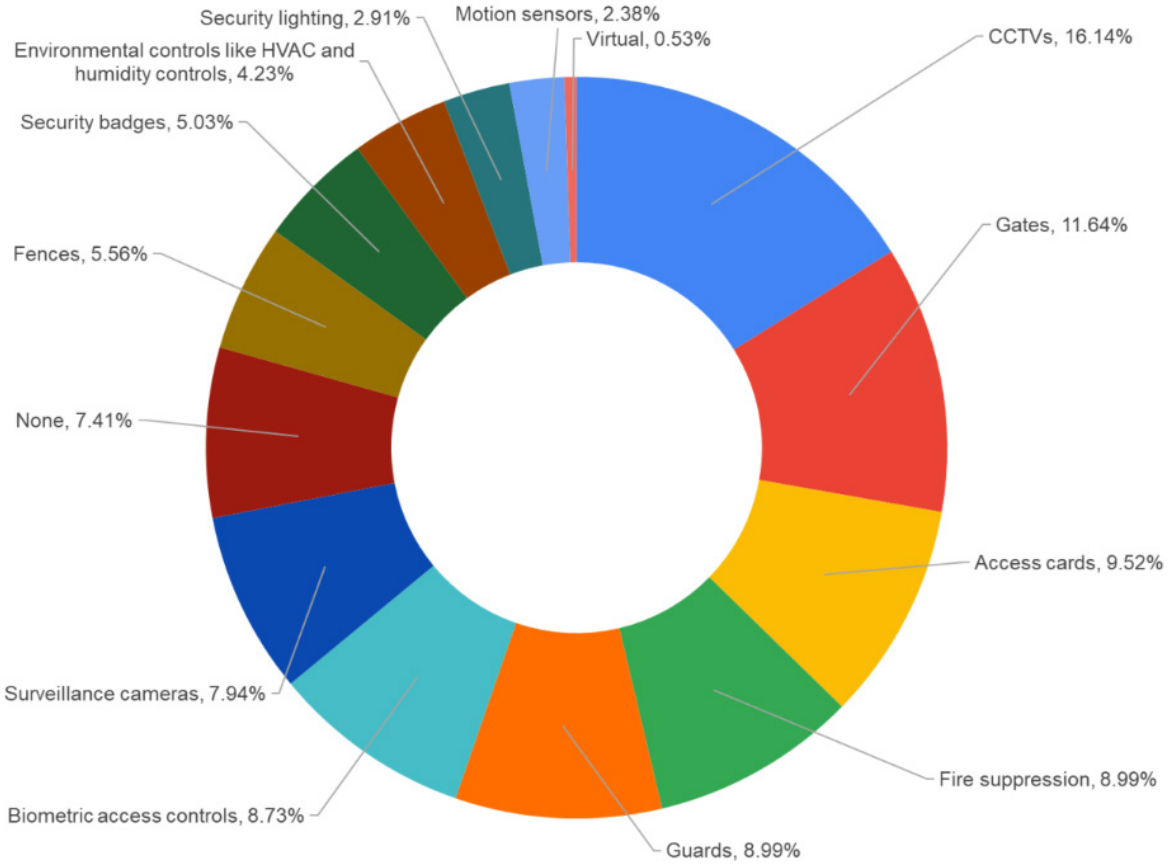


*Figure 6*: Types of Physical Security Controls Implementation among SMEs which have those implemented

For critical cybersecurity functions to operate effectively, technical controls are essential in any organization. These controls play crucial roles in areas such as monitoring, logging, encryption, access control, and alert mechanisms (SONG, 2013). As shown in Figure 7, when asked, "If you have security controls in place, please share the 'technical security' controls already in place," it was found that around 8% of SMEs do not have any technical controls implemented.

Cybersecurity involves complex interactions between social and technical elements. According to the Canadian Centre for Cybersecurity, cybersecurity is "the protection of digital information as well as the integrity of the infrastructure housing and transmitting digital information." More precisely, cybersecurity encompasses tools, procedures, practices, and response and mitigation strategies designed to protect computers, networks, software, and data from harm, attack, and unauthorized access, ensuring availability, confidentiality, and integrity. While networks, hardware, and software are fundamental components of cybersecurity, they require support from physical and administrative controls to manage its complexity (Hoong, 2024).

According to inputs from SMEs, the most popular technical controls are antivirus software, as the cumulative percentage, implemented by around 25% of SMEs, followed by firewalls, which are in place in about 20% of SMEs. Given the widespread use of computers, where most SMEs likely have at least a few machines, it is concerning that only about one-fourth of SMEs have antivirus software. This indicates that many SMEs are lagging in implementing basic technical controls, which is crucial as they advance in the digital era.

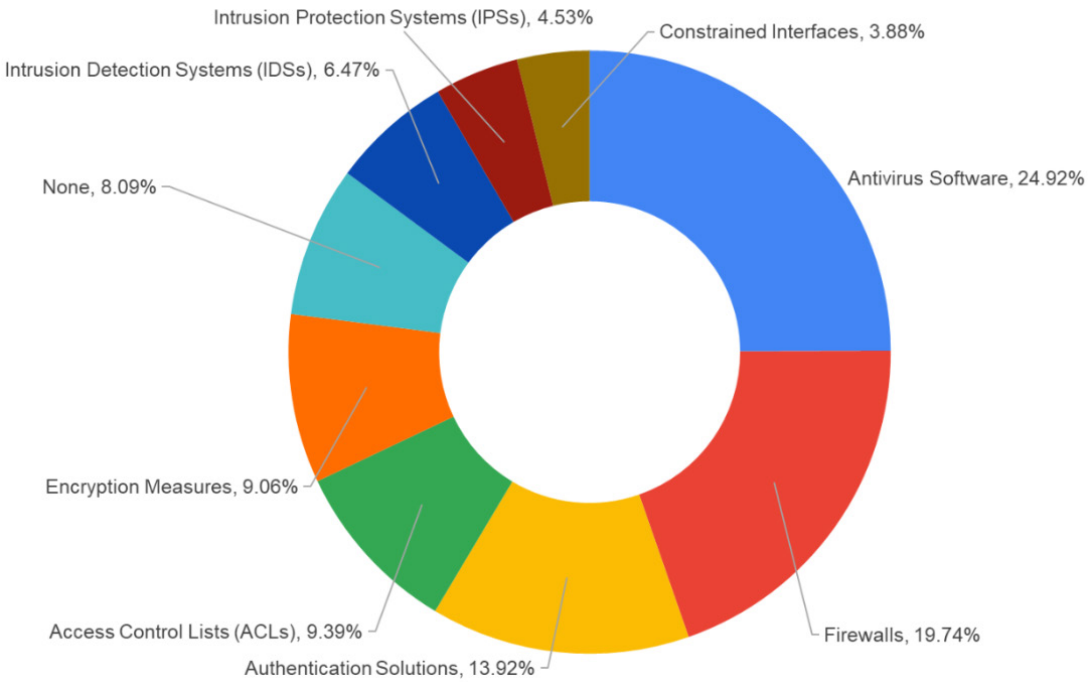


*Figure 7*: Types of Technical Security Controls Implementation among SMEs which have those implemented

As shown in Figure 8, displaying the cumulative percentage, when asked, "If you have security controls in place, please share the 'administrative security' controls already in place," it was found that more than 20% of SMEs do not have any policies, guidelines, or procedures supporting cybersecurity. Around one-third of SMEs have a security policy in place, which should provide clear, comprehensive approaches and well-defined best practices for the SMEs. However, more than 73% of SMEs do not have security guidelines, and around 80% lack any procedures to help stakeholders within the organization.

Many employees working for SMEs do not have guidelines or procedures to help them adhere to cybersecurity practices while working in different environments or performing operations that could negatively impact the organization if not properly executed. It is crucial for any enterprise to document and execute cybersecurity processes, supported by fair guidelines and procedures. These controls should be regularly updated to reflect changes in the technology landscape, external parameters, and business directions. Administrative controls are important as they influence human factors within the enterprise (Cebula, 2010).

Numerous SMEs fall prey to cyberattacks that exploit human weaknesses. The main issue that administrative controls attempt to address is the necessity for ongoing, dynamic risk assessment and management in the face of expanding and evolving cyber threats. Administrative controls encompass knowledge of and adherence to documented security policies, guidelines, and procedures that support various operations (Neri, 2024; Olagbemide, 2024; Kwong, 2024).

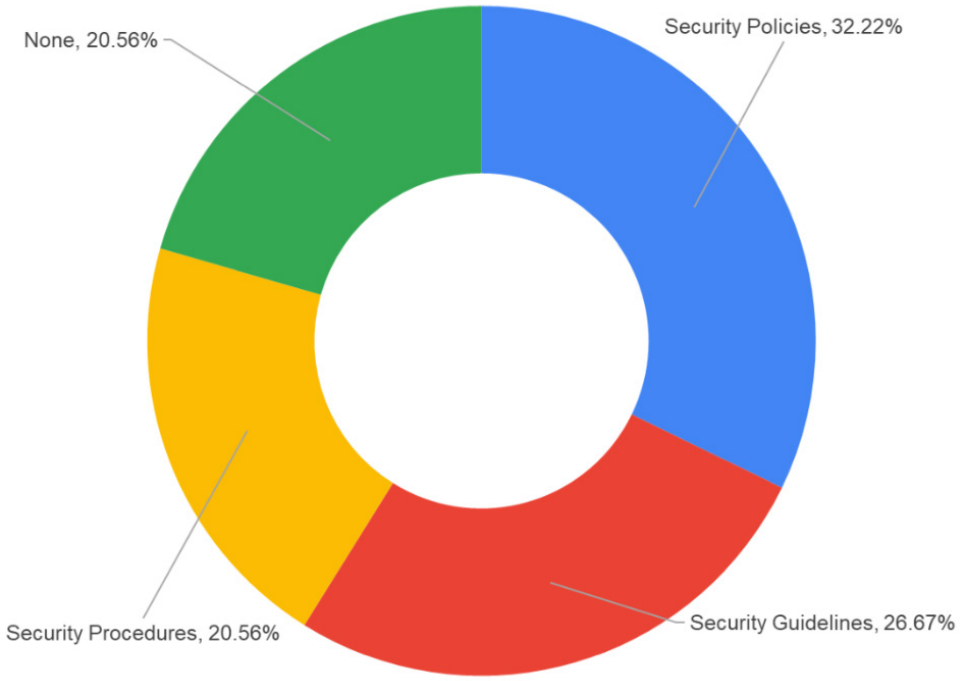


*Figure 8*: Types of Administrative Security Controls Implementation among SMEs which have those implemented

When asked, "How frequently is security awareness training conducted for employees?" as shown in Figure 9, it was found that around 34% of enterprises have never conducted any cybersecurity training for their employees. Human beings, including employees, vendor teams, partners, and visitors, are often the weakest link in cybersecurity, making them prime targets for successful cyber-attacks.

It is crucial to improve cybersecurity awareness among all these groups through frequent training sessions. Without regular cybersecurity awareness training, the effectiveness of other cybersecurity controls is significantly diminished. Such training should be designed to effectively communicate the importance of information security, identify who should deliver the information, discourage shortcuts that bypass processes, and emphasize commitments, norms, salience, affect, and even ego (Bada, 2019).

Enhancing cybersecurity awareness through regular training helps ensure that everyone associated with the organization understands their role in maintaining security and can recognize and respond to potential threats appropriately.

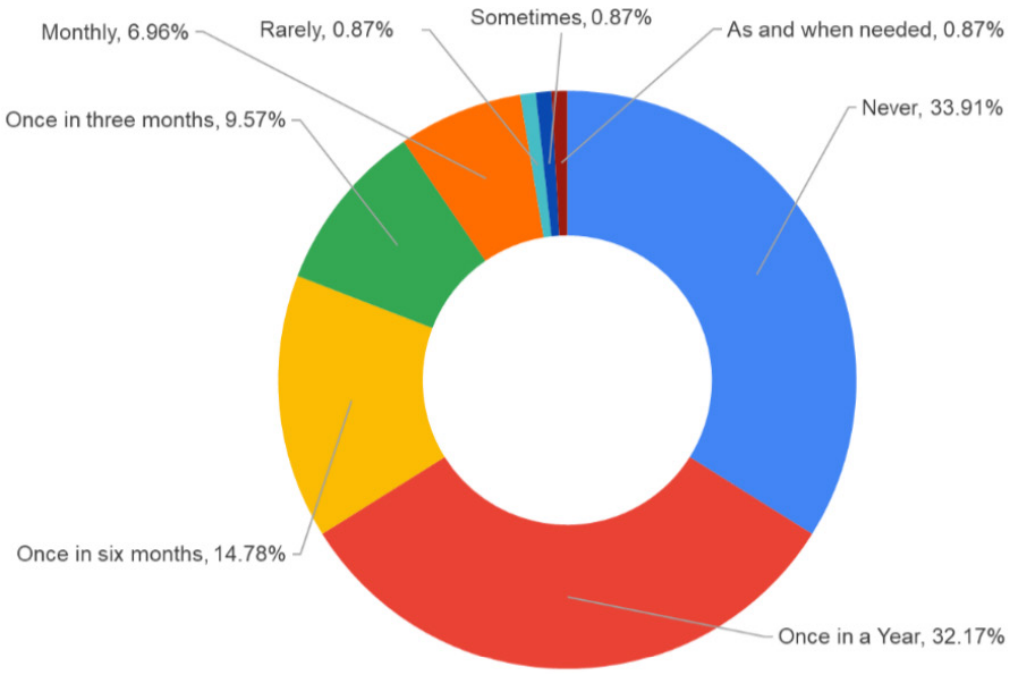


*Figure 9*: Frequency Security Awareness Training for Employees in SME

When the authors sought to identify the cyber threats most commonly faced by SMEs, they found that around 48% of SMEs were confident they had not experienced any cyber- attacks to date. However, malware attacks, phishing attacks, insider threats, web attacks, ransomware, Denial-of-Service (DoS) attacks, and Man-in-the-Middle (MITM) attacks were among the threats that many SMEs had encountered in the past.

As shown in Figure 10, showing the cumulative percentage, in response to the question "Has your organization undergone any cyberattack?" it was observed that malware attacks (around 14%), phishing attacks (more than 10%), and insider threats (around 10%) were the most common cyber threats experienced by SMEs.

Malware, a combination of malicious intent and software, is designed by cybercriminals to attack victims' systems. These malicious software programs often reach victims through spam email attachments, trojan horses, etc. (Kong, 2013). Phishing involves sending emails that appear urgent, prompting the recipient to click on a link that leads to a malicious website designed to capture sensitive information (Tamal, 2024).

Insider threat arises from individuals within the organization, such as employees, vendors, partners, or visitors, who misuse their access to harm the organization (Bishop, 2008). In case of web attacks, cybercriminals exploit vulnerabilities in web applications to gain unauthorized access or disrupt services (Luo, 2021).

Ransomware attacks involve encrypting the victim's data and demanding a ransom for the decryption key, often with the intent of financial gain or data theft (Mohurle, 2017). Using DoS attacks, cybercriminals flood a network with traffic to disrupt services and deny access to legitimate users (Uddin, 2024). In case of MITM attacks, cybercriminals intercept and potentially alter communication between two parties without their knowledge (KARMOUS, 2024). These cyber threats can be mitigated or significantly reduced through the implementation of various physical, logical, and administrative controls.

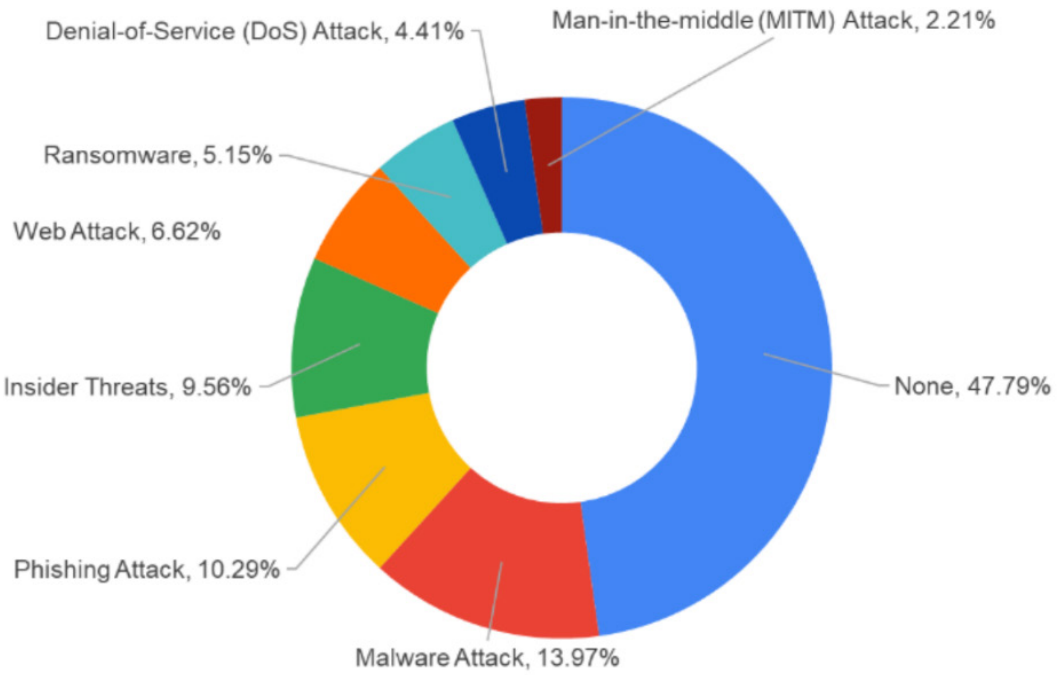


*Figure 10*: Cyber-Threats faced by SMEs

The most important insight from SMEs is shown in Figure 11, which is displaying the cumulative percentage, where the authors received answers to the question, "What are the biggest problems you face while implementing or planning to implement cybersecurity controls for your organization?" This helps to understand the fundamental issues preventing SMEs from implementing cybersecurity controls.

Around 25% of SMEs face issues related to financial investment or budget allocation for cybersecurity. About 8% of SMEs feel that existing cybersecurity standards and frameworks require heavy investments to adopt. Approximately 20% of SMEs are unsure which cybersecurity controls would be beneficial for them. Around 18% of SMEs report a shortage of resources to implement and maintain cybersecurity controls. More than 17% of SMEs prioritize other business goals over implementing cybersecurity controls. Over 11% of SMEs do not receive proper directions or step-by-step guidelines for implementing cybersecurity controls.

These points highlight that SMEs struggle to see a clear return on investment (ROI) in improving their cybersecurity posture. Many cybersecurity standards and frameworks focus on a list of controls without considering the specific domain or business goals of the enterprises. For decades, SMEs have not been fully convinced that cybersecurity contributes to their business sustenance and growth. They often view the implementation of cybersecurity standards or frameworks as merely fulfilling a set of controls rather than aligning with their business objectives.

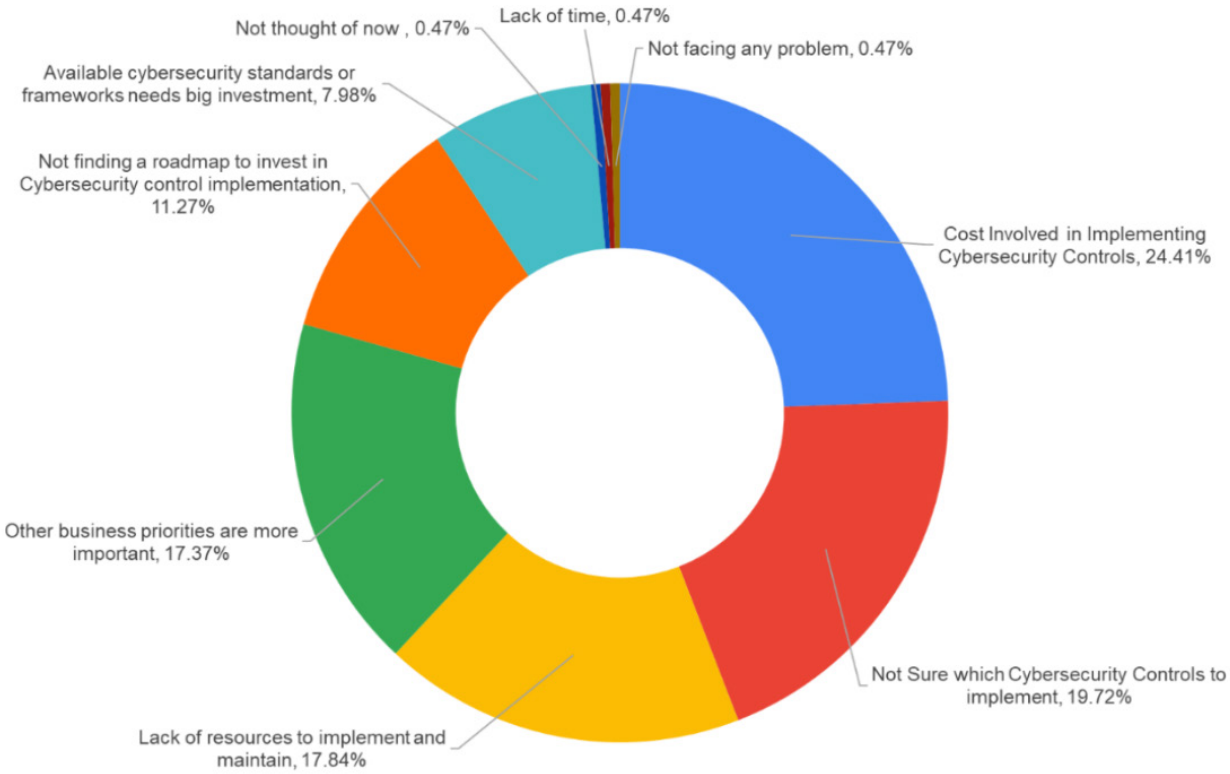


*Figure 11*: List of issues faced by SMEs while forming Cybersecurity Posture

There is a need to address these issues by providing a cybersecurity framework that aligns with business goals. This framework should offer detailed, step-by-step guidance to help SMEs implement at least the minimum required cybersecurity controls.

**Core Cybersecurity Concepts Helping Prioritization**

For the past few decades, the Confidentiality, Integrity, and Availability (CIA) Triad, along with Defense in Depth (DiD), have been the foundation of all cybersecurity frameworks and standards. Confidentiality can be maintained in a cybersecurity posture by avoiding disclosure, integrity can be enhanced in cyberspace by preventing unauthorized alterations or modifications, and optimal availability can be achieved by preventing any destruction within an enterprise's cybersecurity infrastructure (Samonas, 2014). Each of these three areas is unique and serves different purposes, yet there is always some overlap among them.

Confidentiality can be mapped to specific cybersecurity controls, which may be physical, logical, or administrative, in alignment with the people, processes, and technology of an enterprise. The same applies to integrity and availability, which will touch upon different cybersecurity controls.

Each business has its domain with specific objectives to achieve, and thus each domain has different critical assets on which they depend for sustenance and growth. As each business domain of an SME is different, so too are the specific priorities for their critical assets, and even deeper, the different priorities for each area of the CIA triad.

Considering the example provided in Table 1, an example is given for an SME's Business-Critical Asset (BCA), which is further mapped with the CIA triad. For SMEs in the Banking, Financial Services, and Insurance (BFSI) sector, the confidentiality of financial transactions performed through its web portal is of the highest priority. If this web portal is non-functional for a few hours, it is more tolerable than losing the confidentiality of transactions. Hence, in BFSI, confidentiality is a priority for this web portal as a critical asset, followed by integrity and availability (AL-ALAWI, 2020).

If an SME's core business domain is e-commerce, where the critical business asset is the e-commerce website, the biggest risk for the business is when the website is non-functional for hours or days. This means availability is most critical, followed by integrity and confidentiality (Sutton, 2008; Guynes, 2011). For a pharmaceutical, drug-manufacturing SME, the system crucial for the drug formula is a critical asset. Any minor changes in the mixture of ingredients can result in harmful products such as medicines or pills, which can be dangerous to the consumer's life. This shows the highest priority for this asset is integrity, ensuring no unauthorized alterations occur to the correct formula. Availability and confidentiality are considered after integrity (Arden, 2021).

It is important to take inputs from SME's top management, who are the driving force of the business, to decide on the BCA and the prioritization of the CIA triad. They have a better understanding of their business priorities and can identify hidden areas within SMEs. For example, if an SME has an e-commerce business and is also listed on the stock market, top management will likely prioritize confidentiality and integrity, or all three areas of the CIA triad, for implementing cybersecurity controls for its e-commerce pla-

tform. This is because if SMEs fail to maintain confidentiality or integrity due to information security breaches, they will lose their market reputation and face legal suits. Hence, the choice of prioritization needs to be business-focused, with cybersecurity aspects in mind for top management (Das, 2012).

Table 1. *Prioritization in CIA Triad for Specific BDCA of Particular Domain*

| The domain of SME Business | SME's Business Critical Asset (BCA) | Prioritization in CIA Triad in Ascending Order of Highest to Lowest |
|---|---|---|
| Banking, Financial Services, and Insurance (BSFI) | Web Portal for Financial Transaction | Confidentiality, followed by Integrity, and Availability |
| E-commerce | Online Shopping Web Portal | Availability, followed by Integrity, and Confidentiality |
| Pharmaceutical Medicine Manufacturing | Drug Formula Software System | Integrity, followed by Availability, and Confidentiality |

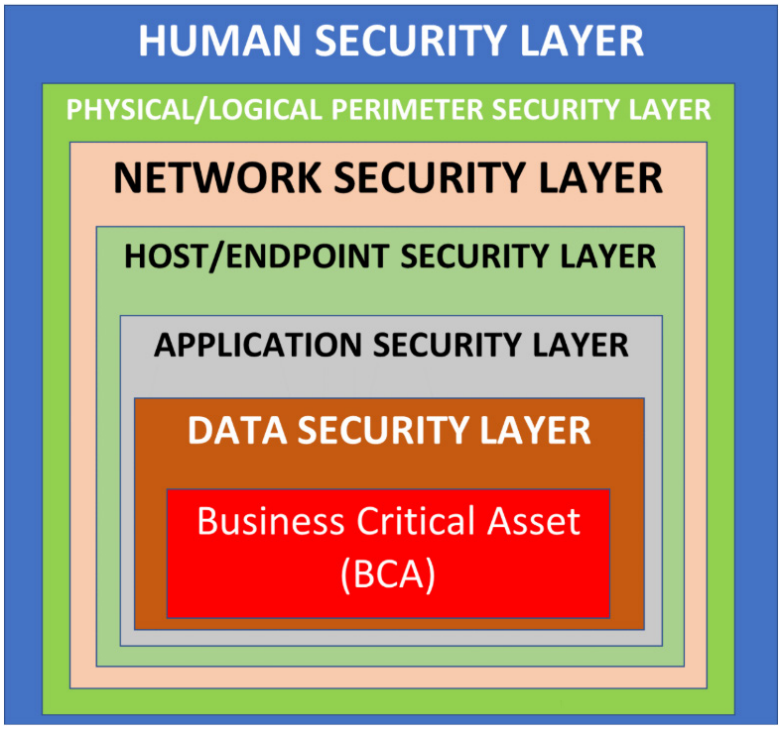


*Figure 12*: Defense in Depth (DiD) Layered Concept

Just as a castle has multiple layers of security to increase the difficulty for an external attacker to reach a critical central location, the Defense in Depth (DiD) model, also known as the "Castle" model, has been adopted in cybersecurity innovations for a long time. This model was initiated by the US National Security Agency (NSA). As shown in Figure 12, the Business-Critical Asset (BCA) is situated at the innermost layer of the DiD, protected by various controls at each layer. These conceptual layers, from the innermost to the outermost, include the data layer, application layer, host or endpoint layer, network layer, logical or physical perimeter layer, and human layer. Enterprises should implement a mission-centric approach, which means safeguarding themselves to protect the BCA from each layer's objectives during the implementation of DiD (Jajodia, 2011). As discussed in an earlier section, the human layer remains the weakest link in performing successful cyber-attacks, as it influences all controls of the other layers within the enterprise.

**Three Stages of Recommended Solution**

Based on the issues identified through research results, literature review, and core cybersecurity concepts, the authors propose a recommended solution in three stages, as illustrated in Figure 13. The first stage involves identifying business-critical assets (BCA) from the list of assets that SMEs possess. This stage includes a list of tailored cybersecurity controls designed to meet the cybersecurity requirements of specific BCAs, considering the CIA triad. For more information, refer to Appendix A. Additionally, in this stage, the top management identifies the CIA triad priorities for the identified BCAs. SMEs need to implement these controls to protect BCAs that impact business goals.

In the second stage, SMEs must implement the minimum cybersecurity controls for the prioritized layers of the overall organization. This involves a list of tailored cybersecurity controls to fulfill the requirements of Defense in Depth (DiD). Tailored cybersecurity can be achieved first by identifying BCAs and then by creating an overall tailored list of DiD controls. Finally, in the third stage, the SME's maturity level in cybersecurity implementation will be assessed based on the previous two stages. All controls implemented according to the recommended framework must adhere to Governance, Risk Management, and Compliance (GRC) (Brandis, 2019; Devos, 2015; Feltus, 2012; Meszaros, 2017; P, 2018; Caralli, 2007; Ralston, 2007; Haastrecht, 2021; Hubbard, 2012; Harris, 2019; Freitas, 2018; Asnar, 2011). Additionally, each cybersecurity control should prioritize human safety as an essential consideration (Siewert, 2019; Riahi, 2014; Thinyane, 2020).


*Figure 13*: Three Stages of Recommended Solution

***BCA and CIA Priotized Controls Implementation***

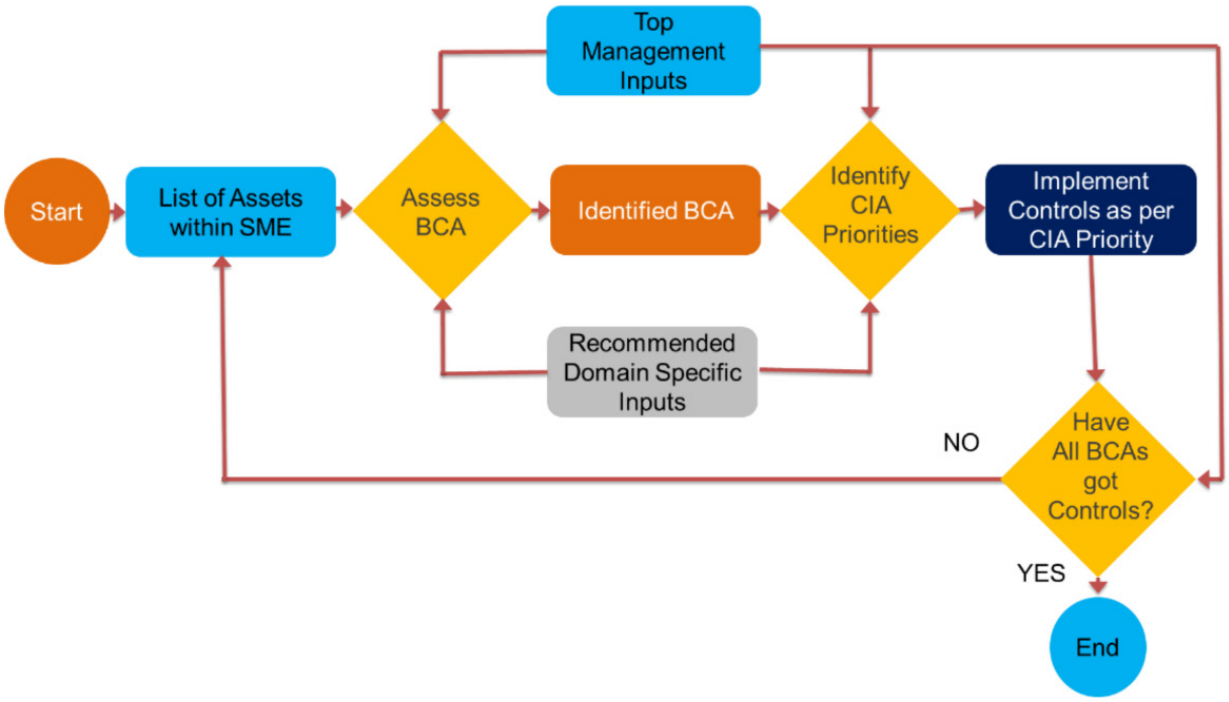


*Figure 14*: Stage 1 - Identify BCA And Implement CIA Prioritized Controls for SME

As shown in Figure 14, SMEs need to analyze their list of assets and Business-Critical Assets (BCA). The BCA can change depending on multiple factors such as the SME's business domain, business goals set by top management, and various external parameters. An SME can have multiple BCAs, but top management must decide which one or multiple BCAs should have CIA-prioritized controls. While top management is free to choose multiple areas of the CIA triad for implementation, the recommended solution provides a stepwise approach to implementing CIA triad-related cybersecurity controls.

To address the challenge of a lack of cybersecurity knowledge when choosing BCAs, the framework can be enhanced with the knowledge of potential BCAs and their controls, with input from top management. This can be achieved using an AI-ML-based software platform.

As shown in Table 2, different domains may have different business-critical assets. For some SMEs, financial transactions are crucial, while for others, 24/7 presence or production might be important. It is also important to understand that even within the same domain, two different SMEs can have different BCAs, and thus different cybersecurity needs. Depending on whether one, two, or all three areas of the CIA triad are considered for a BCA, the level of protection from cyber threats can vary. Implementing all areas of the CIA triad for a BCA will provide maximum cybersecurity.

Table 2. *Calculating CIA Implementation Level for Particular SME*

| Implementation of Cybersecurity Controls for BDCA with Prioritization in CIA Triad | CIA Triad Implementation Level |
|---|---|
| Either of Confidentiality, Integrity or Availability | 1 - Low |
| Either of Confidentiality and Integrity, Integrity and Availability or Confidentiality and Availability | 2 - Medium |
| All Confidentiality, Integrity & Availability | 3 - High |

This recommended solution will not consider all available cybersecurity controls but will be tailored to only the necessary controls that fulfill the requirements of the Business-Critical Assets (BCA), focusing on protecting the business objectives of the particular SME. For example, in the tools manufacturing business domain, the BCA might be a computer numerical control (CNC) machine on the shop floor. If CNC machines are subjected to a cyber-attack, such as ransomware, the entire production of the SME will halt, causing significant business losses. Therefore, the availability aspect of the CIA triad will be prioritized when implementing cybersecurity controls to protect CNC machines. This ensures that protection is prioritized to keep the CNC machines operational and prevent business losses. Refer to Table 3 for the sample recommended controls for the CNC machine.

Table 3. *Tailored Controls List for CIA Implementation of CNC Machine*

| Cybersecurity Controls to be Implemented | CIA Triad Consideration | Priority Sequence |
|---|---|---|
| • Network segmentation and segregation | Availability | 1 |
| • Keeping systems up to date | | |
| • Network Firewall | | |
| • Regular Maintenance | | |
| • Skilled manpower | | |
| • Power backup | | |
| • Role Based Access | Integrity | 2 |
| • Access control | Confidentiality | 3 |

As evident in Appendix A, Figure 15 illustrates different Business-Domain Critical Assets (BDCA) with varying priorities of the CIA triad for the manufacturing domain of SMEs.


*Figure 15:* CIA prioritization for different BDCAs for Manufacturing domain SMEs

### *Implement Overall Cybersecurity Controls for Enterprise*

As explained in earlier sections, any cybersecurity framework is incomplete without considering DiD. It increases obstacles to sophisticated cyber-attacks.

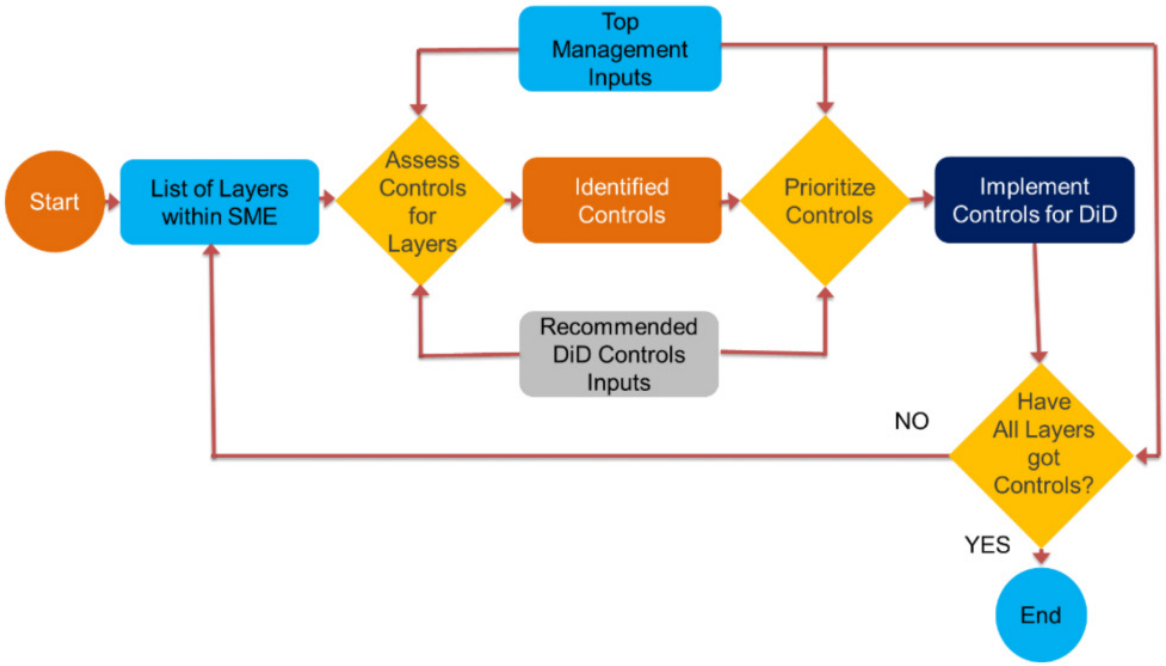


*Figure 16*: Stage 2 - Implement DiD Prioritized Controls for SME

As explained in Table 4, based on the analysis of research results and literature review, the authors recommend that SMEs strengthen the security of the human layer, the perimeter layer (both physical and digital), and the host or endpoint layer. Additionally, if SMEs have networks, applications, or data layers that are publicly accessible outside the physical boundaries of the enterprise, these should not be ignored due to increasing exposure factors. This level of Defense in Depth (DiD) implementation will be considered as level 1.

The authors recommend implementing internal network and application layer security, which will elevate the enterprise to level 2 in DiD implementation. To achieve level 3, SMEs need to also implement data layer security. To address the challenge of a lack of cybersecurity knowledge when choosing DiD controls, the framework can be enhanced with the knowledge of these controls, with input from top management. This can be achieved using an AI-ML-based software platform.

Furthermore, the authors recommend that top management can consider starting with any layer and effectively implementing controls to protect it. This means that, parallel to the BCA's CIA triad-focused tailored cybersecurity controls implementation, DiD controls will contribute to the overall organization's cybersecurity posture, reducing the attack surface. As shown in Figure 16, SMEs need to implement defense for all layers.

Table 4. *Calculating DiD Implementation Level for Particular SME*

| Implementation of Overall Cybersecurity Controls | DiD Implementation Level |
|---|---|
| Human Layer Security + 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 | 1 - Low |
| All in Level 1 + Internal Network Layer Security<br>+ Internal Application Layer Security | 2 - Medium |
| All in Level 2 + Internal Data Layer Security | 3 - High |

***Calculate SME's Cybersecurity Controls Maturity Level***

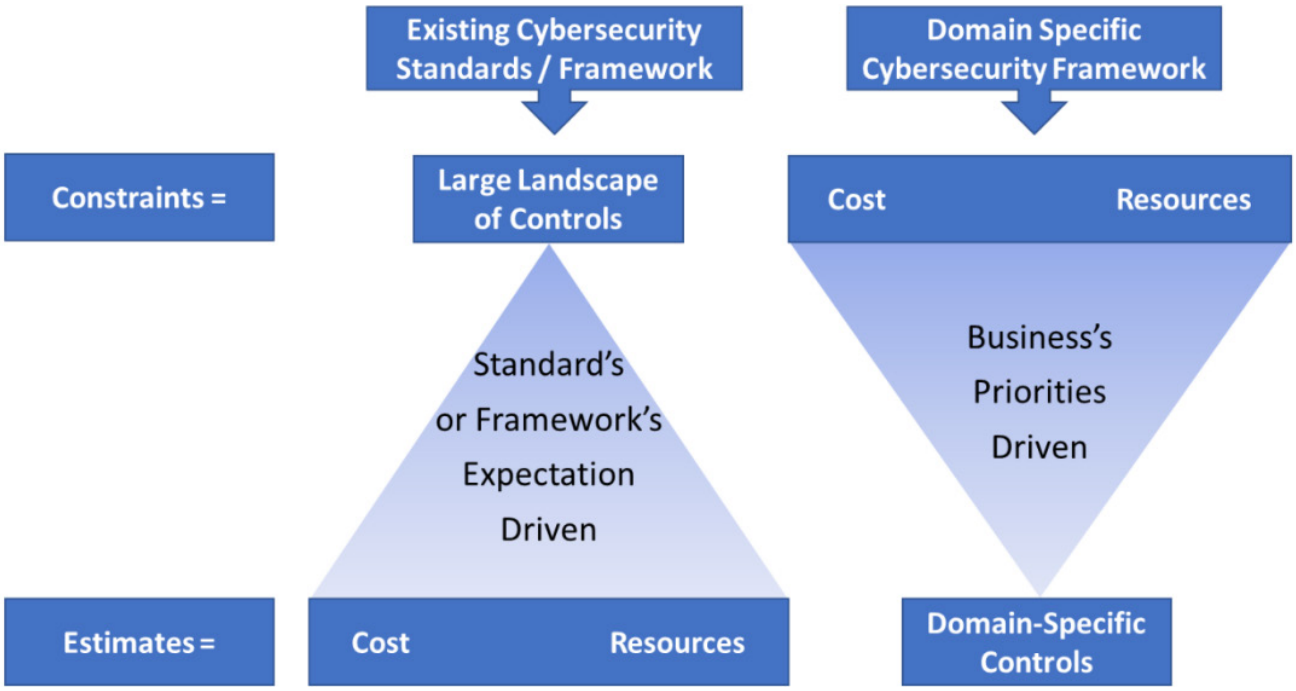


*Figure 17*: Paradigm Shift in New Framework

As explained in the earlier two stages, SMEs can implement cybersecurity controls incrementally to safeguard their main business-critical assets and ensure minimum cybersecurity controls in each organizational layer. The proposed steps allow top management to decide which controls to choose to satisfy business goals or protect critical areas. Top management of any SME understands their business better and is in a better position to assess the impact of changes in any parameter linked to their business objectives.

Considering business priorities set by top management should be a valuable input for implementing cybersecurity controls. As shown in Figure 17, this approach represents a paradigm shift in improving the cybersecurity posture for SMEs. This new framework provides a domain-specific security posture, helping to protect key asset areas of the organization. By considering a tailored list of cybersecurity controls for each business domain of the SME, it reduces costs and other resources required for implementation.

Most cybersecurity standards and frameworks include a list of controls that should be implemented within any organization, regardless of employee strength, business domain considerations, and other resources. Often, some controls are not suitable for SMEs with specific business domains, which might discourage them from implementing such standards or frameworks. Many SMEs have not yet taken their first step towards cybersecurity, leaving them unprotected against growing cyber threats. Some SMEs may not even be aware if they have been cyber-attacked. They need support and motivation to adopt appropriate cybersecurity controls. Top management should recognize the link between their investment in cybersecurity implementation and the maximum protection for their business goals, preventing damage from cyber threats.

Table 5. *Calculating Cybersecurity Maturity Level for Particular SME*

| CIA Implementation Level for Particular SME | Implementation of DiD Prioritized Controls for SME | SME's Maturity Level |
|---|---|---|
| Either of Confidentiality, Integrity or Availability | Human Layer Security + 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 | 1 - Low |
| Either of Confidentiality and Integrity,<br>Integrity and Availability or Confidentiality and Availability | All in Level 1 + Internal Network Layer Security<br>+ Internal Application Layer Security | 2 - Medium |
| All Confidentiality, Integrity & Availability | All in Level 2 + Internal Data Layer Security | 3 - High |

As explained in Table 5, the maturity level of any SME's cybersecurity posture can be calculated based on the implementation of BCA-focused cybersecurity controls along with DiD-focused cybersecurity controls. When an SME fulfills both areas to cover all specified aspects, it will be considered as having the minimum necessary cybersecurity controls in place to protect itself. This is far better for any organization than having "NO" or "RANDOM" cybersecurity controls.

This framework is named "Business Domain Specific Least Cybersecurity Controls Implementation (BDSLCCI)" (Pawar, 2022; Pawar, 2023; Pawar, 2024; Pawar, S. and Pawar, P., 2024). Since January 2024, BDSLCCI 2.0 has been available for SMEs, incorporating modified Defense in Depth controls as shown in Table 6.

Table 6. *Prioritization in CIA Triad for Specific BDCA of Particular Domain*

| Priority Sequence | Layer Name | Maturity Level | BDSLCCI Controls |
|---|---|---|---|
| 1 | Host/Endpoint Security Layer | **BDSLCCI Level 1** | 1.1 - Host/Endpoint - Less Permission to Use<br>1.2 - Host/Endpoint - Endpoint Protection - Anti-Virus<br>1.3 - Host/Endpoint - Licensed Operating System (OS)<br>1.4 - Host/Endpoint - Block File Transfers |
| 2 | Data Security Layer | | 1.5 - Data - Encryption<br>1.6 - Data - Access control<br>1.7 - Data - Backup<br>1.8 - Data - Data Loss Prevention<br>1.9 - Data - Secure Deletion |
| 3 | Human Security Layer | | 1.10 - Human - Cybersecurity Awareness Training<br>1.11 - Human - Separation of Duties<br>1.12 - Human - Service Level Agreement (SLA)<br>1.13 - Human - Employee Background Check<br>1.14 - Human - Review Access Rights<br>1.15 - Human - Cyber Threat Alert Notifications<br>1.16 - Human - Cybersecurity Banners / Posters<br>1.17 - Human - Non-Disclosure Agreement (NDA) |
| 4 | | **BDSLCCI Level 2** | 2.1 - Network - Network Firewall<br>2.2 - Network - Network Access Control<br>2.3 - Network - Remote Access VPN<br>2.4 - Network - Instruction Detection & Prevention Systems (IDPS) |
| 5 | | | 2.5 - Application - OWASP Coding Practices<br>2.6 - Application - Application Hardening |
| 6 | Physical Perimeter Security Layer | **BDSLCCI Level 3** | 3.1 - Physical Perimeter - Locked and Dead-Bolted Steel Doors<br>3.2 - Physical Perimeter - Closed-Circuit Surveillance Cameras (CCTV)<br>3.3 - Physical Perimeter - Picture IDs<br>3.4 - Physical Perimeter - Security Guards / Proper Lighting / Biometrics / Environmental Control |
| 7 | Governance Security Layer | | 3.5 - Governance - Incident Response Process<br>3.6 - Governance - Business Continuity Plan (BCP)<br>3.7 - Governance - Periodic Audit |

The BDSLCCI framework is assisting many small and medium-sized enterprises (SMEs), small and medium-sized businesses (SMBs), micro, small, and medium enterprises (MSMEs), and even startup companies in their initial stages. To facilitate deployment for many SMEs, this framework is available as an AI-ML-powered web portal known as BDSLCCI.com, which offers the following features and services:

- Registration to the BDSLCCI Web Portal as an SMB or SME (each company can register for their own business domain)
- Online Security Gap Analysis (for BDSLCCI baseline)
- List of Recommended Cybersecurity Controls (in ascending order of BDSLCCI- recommended implemen tation)
- Access for other teammates to the portal
- Crawler Tool to scan and identify vulnerabilities in endpoints (such as laptops, desktops, and servers)
- Key cybersecurity policies, matrices, guidelines, and forms as documentation
- Online cybersecurity awareness training, followed by a test and training certificate for employees
- Cybersecurity awareness posters and banners for employees
- Daily cyber threat alert email notifications (the company receives an email with the latest cyber-attack title, description, possible impact, and recommended precautions and solutions)
- BDSLCCI online/physical audit and assessment • BDSLCCI Achieved Level Certificate and Transcript (an outcome of the audit and assessment)
- Web analytics report showing various graphs and details on the coverage and effectiveness of the BDSLCCI controls implemented (an outcome of the audit and assessment)
- Option to download various status reports in PDF format • Additional consulting and/or assistance for the implementation of BDSLCCI- recommended controls

**Conclusion and Future Work**

It is evident that many SMEs are already facing various challenges in their journey and are not prioritizing investments in cybersecurity. If SMEs can see the benefits aligned with their business objectives, along with the step-by-step implementation of cybersecurity controls, it will attract decision-makers within the enterprise.

To conclude the discussion, below are a couple of points:

i. SMEs are encountering many problems when considering the implementation of cybersecurity controls. There is also a need to help them understand the importance of an improved cybersecurity posture for their business sustenance and growth.

ii. The recommended new cybersecurity framework is designed to solve many key problems for SMEs and will be more attractive to the top management of enterprises due to its paradigm shift.

In the future, such a framework, with some enhancements, could even assist enterprises that are not SMEs.

## References

Aguilar, L. A. (2015, October 19). *The need for greater focus on the cybersecurity challenges facing small and mid-dsize businesses*. SEC.gov. https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-mid-size-businesses.html

AL-ALAWI, A. I., & AL-BASSAM, S. A. (2020). The significance of cybersecurity system in helping managing risk in banking and financial sector. *Journal of Xidian University, 14*. https://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

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational cybersecurity systems and sustainable business performance of small and medium enterprises (SMEs) in Saudi Arabia: The mediating and moderating role of cybersecurity resilience and organizational culture. *Sustainability, 16*(5), 1880.

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*. https://doi.org/10.5121/csit.2017.70305

Alqatawna, J. (2014). The challenge of implementing information security standards in small and medium e-business enterprises. *Journal of Software Engineering and Applications, 7*(10), 883–890. https://doi.org/10.4236/jsea.2014.710079

Alsinawi, B. (2018, June 14). Is the NIST cybersecurity framework enough to protect your organization? *ISACA*. https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/is-the-nist-cybersecurity-framework-enough-to-protect-your-organization

Arden, N. S., et al. (2021). Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future. *International Journal of Pharmaceutics, 602*, 120554. https://doi.org/10.1016/j.ijpharm.2021.120554

Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society, 78*, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

Asnar, Y., & Massacci, F. (2011). A method for security governance, risk, and compliance (GRC): A goal-process approach. *In Springer* (pp. 152–184). Berlin/Heidelberg, Germany.

Ayyagari, M., et al. (2017). Policy research working paper: SME finance. World Bank Group, *Development Research Group*.

Bada, M., et al. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? *International Conference on Cyber Security for Sustainable Society*.

Bay, M. (2016). What is cybersecurity? In search of an encompassing definition for the post-Snowden era. French *Journal for Media Research*.

Bialas, A. (2011). Common criteria related security design patterns for intelligent sensors—Knowledge engineering-based implementation. *Sensors, 11*(8), 8085–8114. https://doi.org/10.3390/s110808085

Bishop, M., & Gates, C. (2008). Defining the insider threat.

Bodeau, D., et al. (2013). Cyber resiliency and NIST special publication 800-53 Rev.4 controls. NIST.

Brandis, K., et al. (2019). Governance, risk, and compliance in cloud scenarios. *Applied Sciences, 9*(2), 320. https://doi.org/10.3390/app9020320

Caralli, R., et al. (2007). Introducing OCTAVE Allegro: Improving the information security risk assessment process.

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Apps.dtic.mil. https://apps.dtic.mil/sti/citations/ADA537111

Das, S., et al. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy & Security, 8*(14), 33–36. https://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

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023, November). *The new frontier of cybersecurity: Emerging threats and innovations.* In 2023 29th International Conference on Telecommunications (ICT) (pp. 1-6). IEEE.

Devos, J., & Van De Ginste, K. (2015). Towards a theoretical foundation of IT governance - the COBIT 5 case.

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *Journal of Marine Science and Engineering, 12*(6), 919.

Duan, Y., et al. (2002). Addressing ICTs skill challenges in SMEs: Insights from three country investigations. *Journal of European Industrial Training*. https://d1wqtxts1xzle7.cloudfront.net/43951112/Addressing_ICTs_skill_challenges_in_SMEs20160321-13038-1tw6wyv-with-cover-page-v2.pdf

El-Hajj, M., & Mirza, Z. A. (2024). Protecting small and medium enterprises: A specialized cybersecurity risk assessment framework and tool.

Emine, D. (2012). Financial challenges that impede increasing the productivity of SMEs in Arab region. *Journal of Contemporary Management.* https://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

Erdiaw-Kwasie, M. O., Abunyewah, M., Yusif, S., & Arhin, P. (2023). Small and medium enterprises (SMEs) in a pandemic: A systematic review of pandemic risk impacts, coping strategies and resilience. *Heliyon*.

Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity awareness and capacities of SMEs.

Farsi, J. Y., & Toghraee, M. (2014). Identification of the main challenges of small and medium-sized enterprises in exploiting innovative opportunities (Case study: Iran SMEs). *Journal of Global Entrepreneurship Research, 2*(1), 4. https://doi.org/10.1186/2251-7316-2-4

Feltus, C. (2012). *Introducing ISO/IEC 38500: Corporate governance in ICT*. ITSMF Jaarcongres 2008, 27–28. https://www.academia.edu/download/45983421/Introducing_ISO_IEC_38500_Corporate_Governance_in_ICT.pdf

Freitas, M. da C., & Mira da Silva, M. (2018). GDPR compliance in SMEs: There is much to be done. *Journal of Information Systems Engineering & Management, 3*(4). https://doi.org/10.20897/jisem/3941

GAO, The Government Accountability Office's. (2018, March 5). *GAO reports challenges and successes in cybersecurity framework adoption*. VNF.com. https://www.vnf.com/gao-reports-challenges-and-successes-in-cybersecurity-framework

Gulyas, O., & Kiss, G. (2023). Impact of cyber-attacks on financial institutions. *Procedia Computer Science*, 219, 84-90.

Guynes, C. S., et al. (2011). E-commerce/network security considerations. *International Journal of Management & Information Systems, 15*(2). https://clutejournals.com/index.php/IJMIS/article/download/4147/4202

Haastrecht, M. van, et al. (2021). *A threat-based cybersecurity risk assessment approach addressing SME needs*. The 16th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3465481.3469199

Hein-Pensel, F., Winkler, H., Brückner, A., Wölke, M., Jabs, I., Mayan, I. J., Kirschenbaum, A., Friedrich, J., & Zinke-Wehlmann, C. (2023). Maturity assessment for Industry 5.0: A review of existing maturity models. *Journal of Manufacturing Systems, 66*, 200-210.

Harris, M. A., & Martin, R. (2019). Promoting cybersecurity compliance. In Cybersecurity Education for Awareness and Compliance (pp. 54–71). *IGI Global*. https://www.researchgate.net/profile/Mark-Harris-10/publication/332028771_Published_Chapter/links/5c9b88c6299bf111694bae16/Published-Chapter.pdf

Hoong, Y. (2024). Governance and socio-technical change in Canadian SMEs: Securing cybersecurity (Doc toral dissertation, University of Guelph).

Hubbard, D., & Seiersen, R. (2012). How to measure anything in cybersecurity risk.

Irawan, H., Muhammad, A. H., & Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS Controls v8. *Jurnal Inovtek Polbeng Seri Informatika, 9*(1).

Jajodia, S., et al. (2011). Cauldron mission-centric cyber situational awareness with defense in depth. IEEE Xplore. https://doi.org/10.1109/CSF.2011.6127490

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, unfunded and uneducated: A systematic review of SME cybersecurity. arXiv preprint arXiv:2309.17186.

Karmous, N., Hizem, M., Dhiab, Y. B., Aoueileyine, M. O. E., Bouallegue, R., & Youssef, N. (2024). Hybrid cryptographic end-to-end encryption method for protecting IoT devices against MitM attacks. *Radioengineering, 33*(4), 583.

Khalique, M. (2011). Challenges for Pakistani SMEs in a knowledge-based economy. *Indus Journal of Management & Social Sciences, 5*(2), 74–80. https://d1wqtxts1xzle7.cloudfront.net/6314806/7-2-Khalique-Malasia-Challenges_for_Pakistani_SMEs_in_a_Knowledge_-Based_Economy-0-with-cover-page-v2.pdf

Kong, D., & Yan, G. (2013). Discriminant malware distance learning on structural information for automated malware classification. *Citeseerx*. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.704.1958&rep=rep1&type=pdf

Kurniawan, E., & Riadi, I. (2018). 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), 16*(1). https://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

Kwong, J., & Pearlson, K. (2024). Supply chain cybersecurity and small and medium-sized enterprises (SMEs): Exploring shortcomings in third party risk management of SMEs.

Lee, B., et al. (2017). *Situational awareness based risk-adaptable access control in enterprise networks*. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security. https://doi.org/10.5220/0006363404000405

Leszczyna, R. (2024). ISO/IEC 27001-based estimation of cybersecurity costs with Caspea. In B. Marcinkowski, A. Przybylek, A. Jarzębowicz, N. Iivari, E. Insfran, M. Lang, H. Linger, & C. Schneider (Eds.), Harnessing opportunities: Reshaping ISD in the post-COVID-19 and generative AI era (ISD2024 Proceedings). *University of Gdańsk*. https://doi.org/10.62036/ISD.2024.71

Luo, C., et al. (2021). A novel web attack detection system for Internet of Things via ensemble classification. *IEEE Transactions on Industrial Informatics, 17*(8), 5810–5818. https://doi.org/10.1109/TII.2020.3038761

Madhavan, M., Sharafuddin, M. A., & Wangtueai, S. (2024). Measuring the Industry 5.0-readiness level of SMEs using Industry 1.0–5.0 practices: The case of the seafood processing industry. *Sustainability, 16*(5), 2205.

Mappings, P. C. (2024). Mapping relationships between documentary standards, regulations, frameworks, and guidelines.

Maritan, D., & Panizzolo, R. (2009). Identifying business priorities through quality function deployment: Insights from a case study. *Marketing Intelligence & Planning, 27*, 714–728. https://doi.org/10.1108/02634500910977917

McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., & Halgamuge, M. N. (2024). From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. *Computers & Security, 144*, 103964.

Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cybersecurity risk management. *Computers & Security, 65*, 300–313. https://doi.org/10.1016/j.cose.2016.12.008

Moeuf, A., et al. (2017). The industrial management of SMEs in the era of Industry 4.0. *International Journal of Production Research*. https://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

Mohamed, N., & Singh, J. K. G. (2012). A conceptual framework for information technology governance effectiveness in private organizations. *Information Management & Computer Security, 20*(2), 88–106. https://doi.org/10.1108/09685221211235616

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science, 8*(5). https://sbgsmedia.in/2018/05/10/2261f190e292ad93d6887198d7050dec.pdf

Müller, J. M., et al. (2018). Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. *Technological Forecasting and Social Change, 132*, 2–17. https://doi.org/10.1016/j.techfore.2017.12.019

Muriithi, S. (2017). *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.

Neri, M., Niccolini, F., & Martino, L. (2024). Organizational cybersecurity readiness in the ICT sector: A quanti-qualitative assessment. *Information & Computer Security, 32*(1), 38-52.

NIST. (2014). Framework for improving critical infrastructure cybersecurity. *National Institute for Standards and Technology (NIST)*. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Olagbemide, V. A. (2024). Developing an effective framework for information security compliance management in small and medium-sized enterprises (SMEs). *University of Derby*. https://www.researchgate.net/profile/Vincent-Olagbemide/publication/384256107_Developing_an_Effective_Framework_for_Information_Security_Compliance_Management_in_Small_and_Medium-sized_Enterprises_SMEs_Developing_an_Effective_Framework_for_Information_Security_Compliance_Manage/links/66f160d9c0570c21feb6c206/Developing-an-Effective-Framework-for-Information-Security-Compliance-Management-in-Small-and-Medium-sized-Enterprises-SMEs-Developing-an-Effective-Framework-for-Information-Security-Compliance-Manage.pdf

Osborn, E. (2015). Business versus technology: Sources of the perceived lack of cyber security in SMEs. *Ora.ox.ac.uk*. https://ora.ox.ac.uk/objects/uuid:4363144b-5667-4fdd-8cd3-b8e35436107e

P, Y. S., et al. (2018). Construction methodology of information security system of banking. Repository.hneu.edu.ua, *Premier Publishing* s. r. o., 41–46, 80–90, 200–206, 213–216. https://repository.hneu.edu.ua/handle/123456789/21043

Papathanasiou, A., Liontos, G., Liagkou, V., & Glavas, E. (2024). Enhancing information security for businesses and organizations: Practical controls and systems frameworks. *SCIREA Journal of Information Science and Systems Science, 8*(5), 154-173.

Parmar, M., & Miles, A. (2024, May). Cyber security frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards. In 2024 Security for Space Systems (3S) (pp. 1-7). *IEEE*.

Pawar, S., & Palivela, 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, 2*(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

Pawar, S. A., & Palivela, H. (2023). Importance of least cybersecurity controls for small and medium enterprises (SMEs) for better global digitalised economy. *Contemporary Studies in Economic and Financial Analysis, 110B*, 21–53. https://ideas.repec.org/h/eme/csefzz/s1569-37592023000110b002.html

Pawar, S., & Palivela, H. (2024). Need of stepwise cybersecurity controls implementation framework for small and medium enterprises (SMEs). *Journal of Business Management and Economics Statistics, 2*(1). https://scientificeminencegroup.com/articles/JBME/Need-of-Stepwise-Cybersecurity-Controls-Implementation-Framework.pdf

Pawar, S., & Pawar, P. (2023). BDSLCCI. Notionpress.com. https://notionpress.com/read/bdslcci

PETKOVSKA, T. (2015). The role and importance of innovation in business of small and medium enterprises.

Prasanna, R. P. I. R., et al. (2019). Sustainability of SMEs in the competition: A systemic review on technological challenges and SME performance. *Journal of Open Innovation: Technology, Market, and Complexity, 5*(4), 100. https://doi.org/10.3390/joitmc5040100

Ralston, P. A. S., et al. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions, 46*(4), 583–594. https://doi.org/10.1016/j.isatra.2007.04.003

Ramukumba, T. (2014). Overcoming SMEs challenges through critical success factors: A case of SMEs in the Western Cape Province, South Africa. *Economic and Business Review, 16*(1). https://doi.org/10.15458/2335-4216.1178

Riahi, A., et al. (2014). A systemic and cognitive approach for IoT security. *IEEE Xplore*. https://doi.org/10.1109/ICCS.2014.6785328

Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security.

SENSEON. (2019). The state of cyber security SME report 2019. Senseon.io.

Shojaie, B., & Federrath, H. (2014). Evaluating the effectiveness of ISO 27001:2013 based on Annex A.

Siewert, S., et al. (2019). Fail-safe, fail-secure experiments for small UAS and UAM traffic in urban airspace. *IEEE Xplore*. https://doi.org/10.1109/AERO.2019.9081710

Siti, S., et al. (2009). The background and challenges faced by the small medium enterprises: A human resource development perspective.

Song, J. G., et al. (2013). An analysis of technical security control requirements for digital I&C systems in nuclear power plants. *Nuclear Engineering and Technology, 45*(5), 637–652. https://doi.org/10.5516/NET.04.2012.091

Sukmaji, M., et al. (2021). 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, 17*(2), 115–112. https://doi.org/10.33480/pilar.v17i2.2282

Suorsa, M., & Helo, P. (2023, November). Information security failures measured and ISO/IEC 27001:2022 controls ranked by General Data Protection Regulation penalty analysis. In 2023 11th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-5). IEEE.

Surya, I. C., Mulyana, R., & Nugraha, R. A. (2024). BPRDCo SME digital transformation by designing information security using ISO 27001:2022. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), 8*(4), 1242-1253.

Sutton, S., et al. (2008). Risk analysis in extended enterprise environments: Identification of critical risk factors in B2B e-commerce relationships. *Journal of the Association for Information Systems, 9*(4), 160–174. https://doi.org/10.17705/1jais.00155

Tamal, M. A., Islam, M. K., Bhuiyan, T., Sattar, A., & Prince, N. U. (2024). Unveiling suspicious phishing attacks: Enhancing detection with an optimal feature vectorization algorithm and supervised machine learning. *Frontiers in Computer Science, 6*, 1428013.

Thinyane, M., & Christine, D. (2020). Cyberresilience in Asia-Pacific. *United Nations University*.

Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, 100604.

Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. *Ad Hoc Networks, 152*, 103322.

Wang, W., Sadjadi, S. M., & Rishe, N. (2024, May). A survey of major cybersecurity compliance frameworks. In 2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity) (pp. 23-34). *IEEE*.

WTO. (2016). WTO | World Trade Report 2016 | Levelling the trading field for SMEs. *World Trade Organization*. https://www.wto.org/english/res_e/publications_e/wtr16_e.htm

Xie, J., et al. (2016). Physical and cyber security in a smart grid environment. Wiley Interdisciplinary Reviews: *Energy and Environment, 5*(5), 519–542. https://doi.org/10.1002/wene.202.

**Appendix A**

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. As an outcome of interviews with these top managements of SMEs, authors tried to understand the priority of a few BDCAs with reference to the CIA triad. The below table indicates the inputs received.

| Number of Participants | Business Domain | BDCA | Prioritization on a scale of 1 to 10 | | |
|---|---|---|---|---|---|
| | | | 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 Soft-ware 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 | 1- | 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 | 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 |