SCIENTIFIC EMINENCE GROUP

Research Article

Open Access

Journal of Business Management and Economics Statistics

JBME@scientificeminencegroup.com

Need of Stepwise Cybersecurity Controls Implementation Framework for Small and Medium Enterprises (SMEs)

Shekhar Pawar[1,*] **and Hemant Palivela**[2]

[1]*DBA, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland*

[2]*Visiting Professor, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland*

*Corresponding Author

Shekhar Pawar, DBA, Swiss School of Business and Management School Geneva, Geneva Business Center, Avenue des Morgines 12, Genève, 1213, Switzerland, E--mail: shekharpawarmgm@gmail.com

Citation

Shekhar Pawar, Hemant Palivela (2024) Need of Stepwise Cybersecurity Controls Implementation Framework for Small and Medium Enterprises (SMEs) J Bus Manage Econ Stat 2: 1-31

Publication Dates

Received date: February 15, 2024
Accepted date: March 15, 2024
Published date: March 18, 2024

Abstract

Small and medium enterprises (SME companies) are the major contributors to overall employment, the GDP of most countries, and the global economy. Recent cyberattack statistics show that SMEs are always a target for cybercriminals, posing a direct threat to the global economy if they are not protected. To understand the current scenarios in the SME segment, the authors conducted a research survey to get insights into the current cybersecurity posture of each participant SME as well as the problems faced by enterprises in adopting cybersecurity controls. The input from more than a hundred SMEs in different domains and from different countries helped the authors understand the gaps that are helping cybercriminals be successful attackers. The top three issues identified during research were a lack of required financial investment, a lack of skilled resources, and other business priorities deemed more important than cybersecurity by top management. To attract SMEs to implement cybersecurity controls, there is a need to divide the large landscape of cybersecurity controls and provide a stepwise implementation path in a prioritized manner where core cybersecurity concepts can play a crucial role. For the solution design, the authors conducted research interviews with the top management of more than 100 SMEs to map their business priorities relevant to it. To bridge the gaps identified, the authors will attempt to recommend a solution by considering confidentiality, integrity, and availability (the CIA triad), as well as defense in depth (DiD) concepts.

Keywords: Cybersecurity; Small and Medium Enterprises; Cyberattack; Cybercriminals; Cyber Breach

List of Abbreviations

AI: Artificial Intelligence; **BDCA**: Business Domain Critical Asset; **BFSI**: Banking, Financial Services, and Insurance; **CIA triad**: Confidentiality, Integrity, and Availabili-

ty triad; **CNI**: Critical National Infrastructure; **DiD**: Defense in Depth; **DDoS attack**: Distributed-denial-of-service attack; **DoS attack**: Denial-of-service attack; **GDPR**: General Data Protection Regulation; **HR**: Human Resources; **ICT**: Information and Communications Technology; **IoT**: Internet of Things; **ISO**: The International Organization for Standardization; **NCSC**: National Cyber Security Centre; **NIST**: The National Institute of Standards and Technology; **SAAS**: Software Development in areas of business process automation for SMB and SME; **SAS Services**: A Software As A Service Platform; **SME**: Small and Medium Enterprise

Introduction

Small and Medium Enterprises (SMEs) are often defined by a particular range of yearly turnover and employee numbers in various nations. Around 400 million SMEs cover 90% of the businesses along with almost 70% of global employment and 55% of the GDP of the developed economies [1]. Growing digitization starting from IoT sensors to Cloud is changing an entire industry, SME is not an apart [2]. Big data, cyber-physical systems, and interoperability are examples of Industry 4.0 technologies that have a substantial positive impact on SMEs' business success. The digital transformation of SMEs enhances operational efficiency by cutting costs [3]. It has increased the cyber-attack surface for organizations. Interesting studies by the NCSC say that one in two SMEs has a fair chance of experiencing a cyber breach [4]. Given that SMEs are the target of more than half of assaults, they are at a significant risk [5,6]. As per the latest cybercrime statistics, around 43% of businesses that are getting targeted by cybercriminals are small businesses. Also, those who become the victim of successful cyber-attacks, are not able to sustain their business for more than 6 months [7]. Since the 2022 year start, according to the latest cyber news, again there is a sharp rise in cyber-attacks by Russia-backed cybercriminals which are primarily targeting Small and Medium Businesses (SMBs) [8-12].

It is important to study the current cybersecurity posture and real problems SMEs are undergoing. Here authors are touching on two parts, one is research to state the problem, and the other is the recommendation for the resolution of the problem.

To achieve the first part, the authors conducted a research survey in the second half of the year 2021 with well-designed key questions which will give various insights about participant SMEs, such as the number of years of existence of the enterprise, knowledge about if they have adopted cybersecurity standards/frameworks, types of security controls present, frequency of employee training for cybersecurity awareness within the organization, obstacles for implementing cybersecurity and what kind of cyber-attacks faced by SMEs. This survey tries to understand the currently implemented cybersecurity controls within SMEs, which is very crucial information about knowing what is helping cybercriminals. Even though the authors approached hundreds of SMEs, looking at the criticality of their cybersecurity implementation-related inputs only the top management of 115 SMEs volunteered with their valuable participation. The valuable inputs received from directors, owners, C-level executives, and other top management personnel will be discussed in upcoming sections.

In the coming sections, after highlighting the latest gaps identified and learning from the research survey participated by various SMEs, in the second part, the authors will elaborate few key cybersecurity concepts to plot a recommended stepwise solution. To provide a high-level solution for SMEs, the authors will explain how the least implementation of cybersecurity controls can be achieved after prioritization of critical assets and mapping it with the CIA triad. Also, the authors will throw light on how DiD will benefit SMEs to have additional layers of security in place. The authors will also share how responsible AI will contribute to the recommended solution [13].

Related Work

Leading cybersecurity frameworks and standards at the moment include ISO/IES 27001, NIST, System Security Engineering Capability and Maturity Model (SSE-CMM), Common Criteria (CC), and Zero Trust Concept. Each of these offers the universal cybersecurity safeguards that every firm needs. Zero Trust is a concept where enterprises should design access controls where they should never trust any access request to their systems. It takes into account the level of trust for people and devices in relation to contextual information such location, hour of the day, kind of task, etc. [14]. Additionally, the user's immediate environment is currently under a level of security threat, meaning anything attempting to connect to

their system must first pass security verification [15]. Yet it requires many resources for successful implementation and even not mapping to each requirement of a specific domain [16]. The NIST, which also provides a framework for Small and Medium Businesses, has identified five main tasks that it believes are essential for defending against cyber threats, identifying them, responding to them, and recovering from cyber-attacks (SMBs). CC is of excellent use while evaluating the security of IT products, but on other hand, it is very time--consuming to prepare for it. Also, it is costly to use the same. SSE-CMM shares guidelines but does not define specific processes. ISO/IEC 27001 standard helps enterprises to develop information security management systems (ISMS) required for them. It is quite difficult for many organizations due to lagging security knowledge as well as the disability to develop the same due to various reasons [17]. Recent study for examination of the impact of COVID-19 on SMEs is indicating a significant rise in failure rates across all sectors of SMEs in addition to gaps in current standards and frameworks [18]. Also, as shown in figure 1, coverage of various components of the leading standards and frameworks of cybersecurity differs which is not always promising comprehensive cybersecurity controls implementation [19,20]. In order to meet the needs of any enterprises, a standard need to be feasible, affordable, and take into consideration the constraints of available resources and technology. It must also satisfy the standard's verification requirements, since enterprises anticipate being able to evaluate security quality on their own - even when combining framework strength testing with other security testing tasks. Furthermore, an issue in determining the starting point when protection will begin arises from a lack of understanding of the cybersecurity areas required by the standard [19].

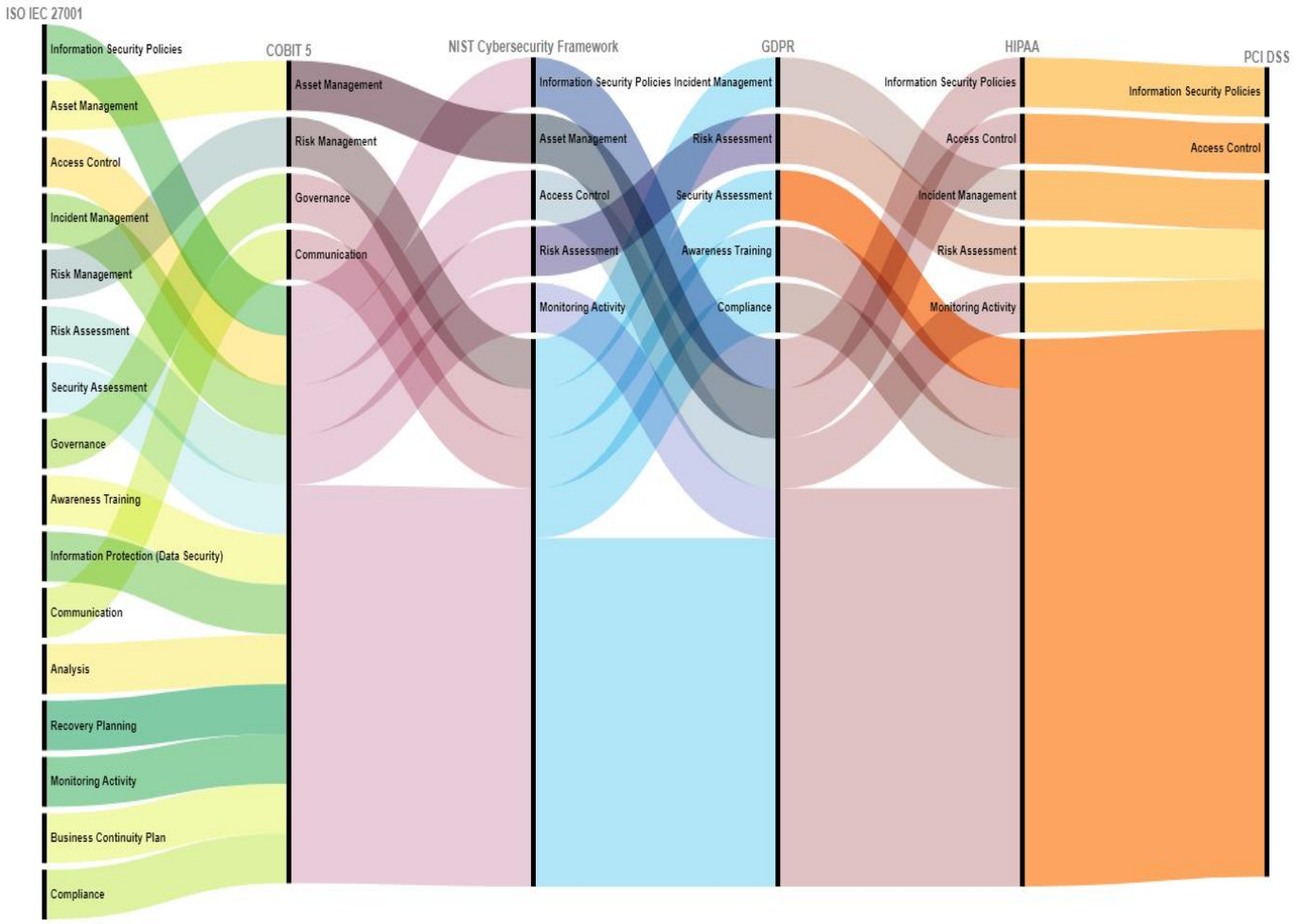

Figure 1: Analysis of leading cybersecurity standards and frameworks components

Recent COVID-19 pandemic caused many holes to cybersecurity posture of organizations. Around 2,215 IT and IT security professionals in the US, UK, DACH, Benelux, Scandinavia, and ANZ were polled by the Ponemon Institute (Australia and New Zealand). All of the respondents to this study work for companies who have given their staff furloughs or told

them to telework as a result of COVID-19. The research found that, on average, 58 percent of these firms' workers now work remotely, up from an earlier average of 22 percent before COVID-19. On average, 33% of workers were placed on leave. The effectiveness of the organization's security posture has been considerably decreased by the remote workforce. BYOD has reduced the security posture of enterprises. Sixty-seven percent of respondents claim that the security posture of their firms has weakened as a result of remote workers using their personal mobile devices, such as tablets and smartphones, to access mission-critical IT infrastructure and applications. The most vulnerable endpoints or access points to enterprises' networks and enterprise systems are smartphones, laptops, and mobile devices [21]. Flow control attack, injection attack, information leakage attack, and denial of service (DoS) attack were the most observed cyber-threats during pandemic [22].

Earlier studies show that more than half of SMEs shut down their business within the first five years of their operations [23,24]. There are many existing problems SMEs are undergoing for many years. In-country like Ghana, SMEs are facing financial challenges where there are gaps in accessing credits [25]. In the USA, Spain, Portugal, Netherlands, and several countries, SMEs are facing finance-related problems and constraints related to the same [26]. For every business to succeed, effective brand management is necessary. SMEs are lagging behind in brand management due to a lack of resources and knowledge [27]. The successful cyber-attacks can even damage the brand reputation build by an enterprise which can cause negative consequences on an organization’s business [28]. Reference to various problems faced by SMEs in terms of cybersecurity implementation, as a summary of issues most of those are facing is pointing to problems like less finance with related support, skilled human resources, and other business priorities ignoring sufficient investment in cybersecurity posture by top management [29-39].

Apart from the SMEs’ definitions present globally which are mainly focused on the number of employees, revenues, and capital, SMEs are characterized by uncertain revenues in developing countries which are having an economy based on fluctuating currencies. It has an impact on SMEs dependent on the same. Also, SMEs need to undergo re-classification of assets after a certain period, as their asset values keep on changing as it is dependent on business dynamics such as changing goals, focus, etc. In previous studies, it was evident that most SMEs in developing countries are facing issues related to confidentiality, integrity, and availability [40]. These enterprises are undergoing cyber-threats such as various social engineering attacks, phishing emails with malicious attachments, spamming, spyware, natural disasters, lack of inadequate authentication methodologies, viruses, hacking, power outages, and/or failure, missing backups, etc. Identification of SME's critical assets is a very crucial stage, where inputs from SME's top management must be involved as they knew changing business directions [40].

Summarizing the inputs from different research studies, available cybersecurity standards or frameworks are less attractive to SMEs which are undergoing problems such as those being costly to implement, requiring a long-time investment, demand to have in-depth knowledge, and missing helpful guidelines to start till finishing implementation. Also, one big observation is none of the existing standards or frameworks can provide Enterprise with a solution in line with its business domain. The common problems which overall SMEs are facing while considering strategy and implementation of cybersecurity controls will have a significant impact on the way forward towards new recommendations.

Seven Stages of Research

Even though it is evident that there are a few existing problems that SMEs are facing as explained in the above section, the authors decided to reach SMEs and collect fresh insights. The entire research has seven stages as illustrated in Figure 2. The first stage is about studying the results of a research survey. This first stage will conclude the problems faced by SMEs. Moving ahead to the second stage, the authors will move towards a recommended solution for the gaps identified in the first stage. The authors will revisit the primary concepts of cybersecurity in the second stage. In the third stage, readers will understand how SMEs’ domain-specific needs of confidentiality, integrity, and availability change based on their priorities of the core business. Here authors will also share valuable inputs from the top management of SMEs via research interviews. In the fourth stage, the authors will explain how SMEs can identify business domain critical assets (BDCA) for themselves. The fifth stage will discuss how SMEs can implement prioritized CIA triad areas for BDCA. After which SMEs need to implement the least cybersecurity

controls with prioritized layers of the overall organization as explained in stage six. Finally, SMEs need to calculate the maturity progress based on the earlier two stages.

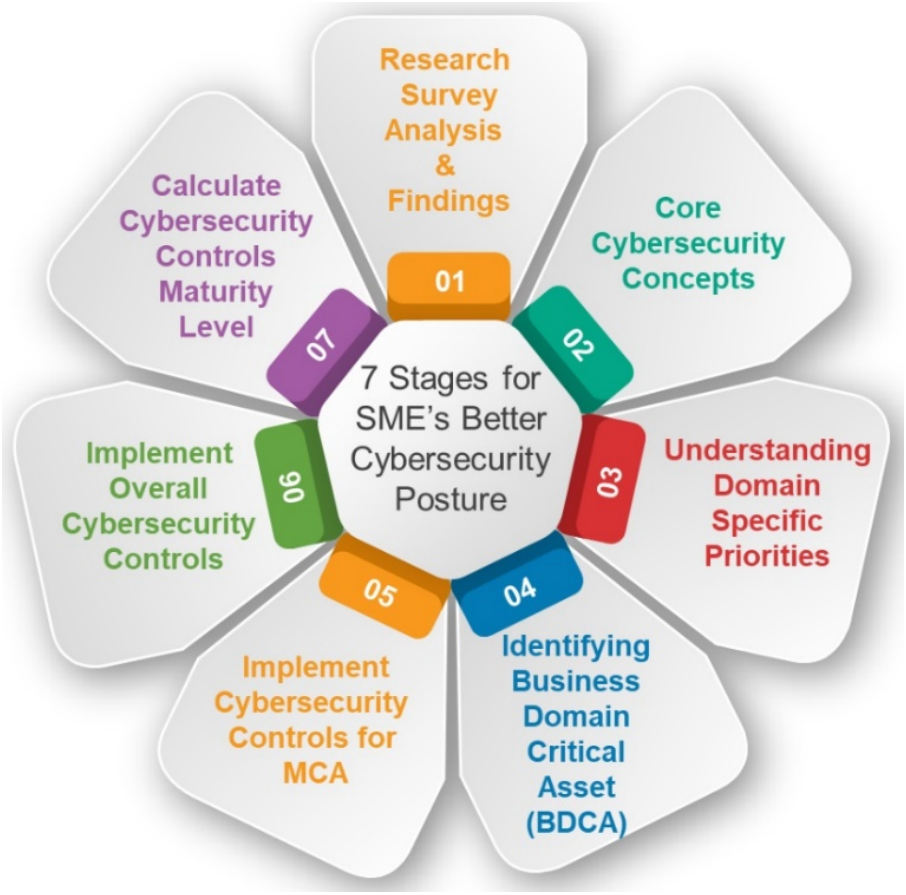

Figure 2: Seven Stages of Research

Research Survey Analysis and Findings

As pointed out in the related work section, there are already known issues that are faced by the SME segment. Apart from that from July to September 2021, the authors approached a few hundred SMEs. Out of those only 115 SMEs shared valuable inputs in this survey as cybersecurity has been a very sensitive and crucial area of any enterprise.

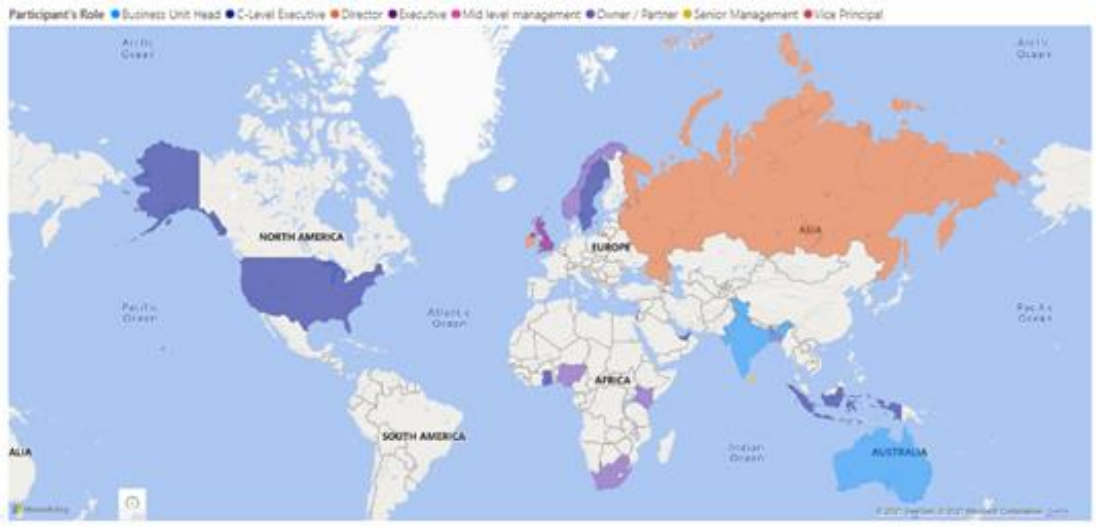

Figure 3: SME Participation from Various Countries

As shown in Figure 3, this survey participants were top management of SMEs across various countries and from domains like B2C SaaS Hyper Mobility and Fintech consumer services, BSFI, Cold Storage & Warehousing, Consulting, Distribution of primary packaging material, E-commerce, Education, Education Technology, Executive Coaching, Exports, Finance Services, FMCG, Healthcare, Hospitality, Insurance, International Humanitarian Charity, IT industry, Legal and Accounting Services, Legal Services, Logistics, Manpower supply (HR), Manufacturing, Maritime, Logistics, and Supply Chain Management, Marketing Consultant, Oil Industry, Online Services, and marketing, Pharmaceutical, Renewable Energy, SAAS, SAS services (for Insurance Brokers Services), Media, Telecommunication, Travel Technology, etc. According to a research survey conducted by authors among various domains of SMEs, they found interesting insights into the current implementations of cybersecurity controls and real problems faced by SMEs. 40% of SMEs who had participated survey were having existed for more than 10 years following around 18% of SMEs working for more than 5 years.

Referring to Figure 4, it is evident that around two-thirds of participant enterprises were having more than or equal to 5 years of existence. The 40% of SMEs in this survey who participated voluntarily had been in business for more than ten years. More than 18% of participating SMEs were aged between 5 to 10. Around 20% of SMEs were having execution between one to three years. Around 12% of SMEs have between three to five years of existence. Less than 10% of participant SMEs were just stated in the last twelve months.

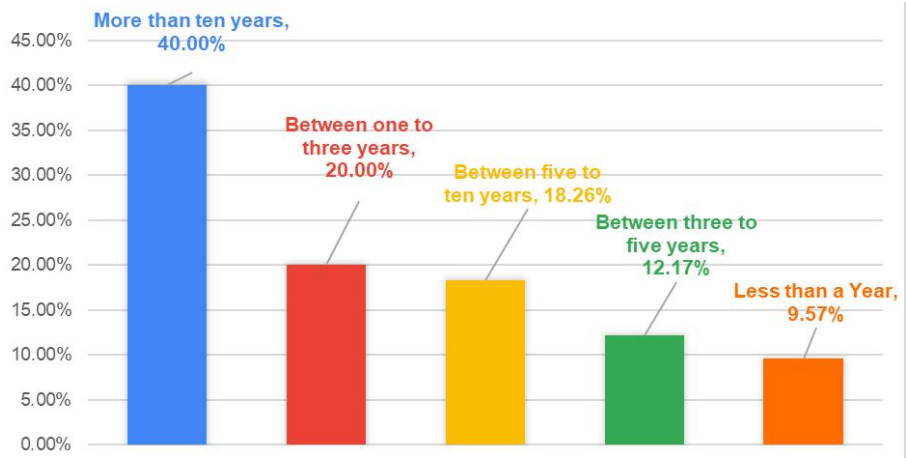

Figure 4: SME Participation from Various Countries

The purpose of cybersecurity controls is to safeguard people, processes, and technology areas of the enterprise. Implementation of the collection of cybersecurity best practices to protect enterprises against cyber threats can be achieved through cybersecurity standards or frameworks. As shown in Figure 5, popular ISO 27001 has been implemented by around 28.3% of SMEs, out of which around 9% of SMEs have GDPR, PCI DSS, NIST Cybersecurity Framework (CSF), HIPAA and Singapore's PDPA as a combination while implementation. Overall GDPR is in place for around 10.12% of SMEs. These SMEs were from countries like Sweden, United Arab Emirates, the United States, Australia, Sri Lanka, Nigeria, and India. Even though SMEs are not located in Europe, they must have clients from Europe which is making them adopt GDPR compliance. NIST's CSF is adopted as only one framework by around 6.8% of SMEs. As is clear from the data, more than 57% of SMEs lack cybersecurity standards or guidelines. In other words, vulnerability to cyber dangers is not clearly under control. Additionally, there may be a few reasons preventing SMEs from moving forward with them. If enterprises do not have proper implementation of cybersecurity standards or frameworks, it is more likely that there would be many open weaknesses that cybercriminals will penetrate to fulfill malicious intentions. Even if that enterprise has some sort of random or own way of implementing cybersecurity controls, which are not adopted from existing well-known standards or frameworks, there are fair chances that top management or any stakeholders will not come to know the cyber threat risk.

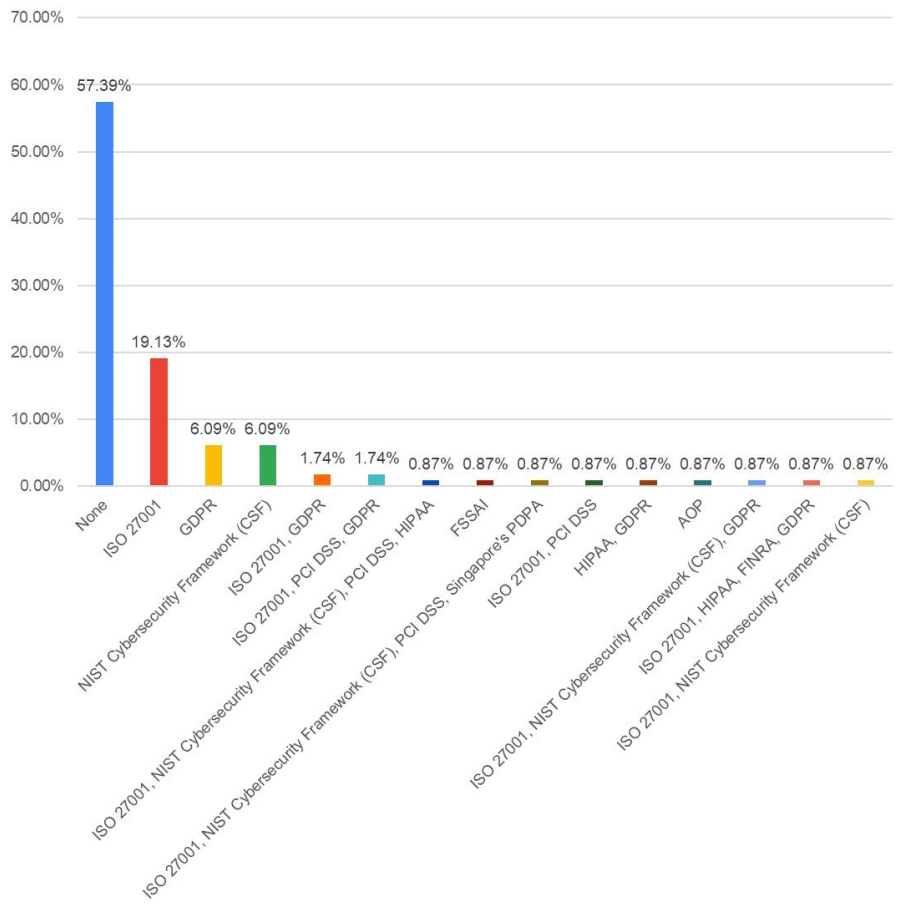

Figure 5: Security Standards / Frameworks Implemented in SMEs

As shown in Figure 6, around 57% of SMEs have either existing popular standards to implement as cybersecurity controls or they might have created their assumptions to get some sort of cybersecurity controls implemented. Around 28% of SMEs acknowledged that they have no cybersecurity measures in place, while another 16% are unsure. Taking these three factors into account, roughly 72% of SMEs have some form of cybersecurity control in place, with only about 28% having none. It illustrates that many SMEs lag in the implementation of measures, despite the broad acceptance of current cybersecurity standards or frameworks.

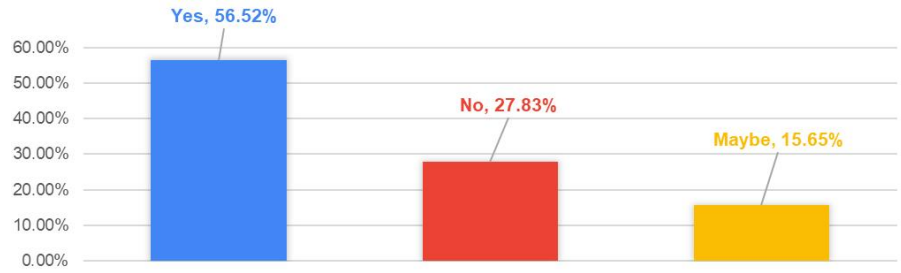

Figure 6: Any implementation of security controls for SMEs

As per the enterprise's asset needs, physical cybersecurity controls are helpful for monitoring, helping in three areas which are people, process, and technology; for protection of critical assets or facilities against sabotage, theft, or any similar human attack threats as well [41]. Among the enterprises that have some physical cybersecurity controls implemented, CCTV, physical gates, guards, and access cards are the most popular physical controls as shown as a part of research survey data in Figure 7. Motion controls, security lighting, and environment controls appeared as the least implemented physical controls.

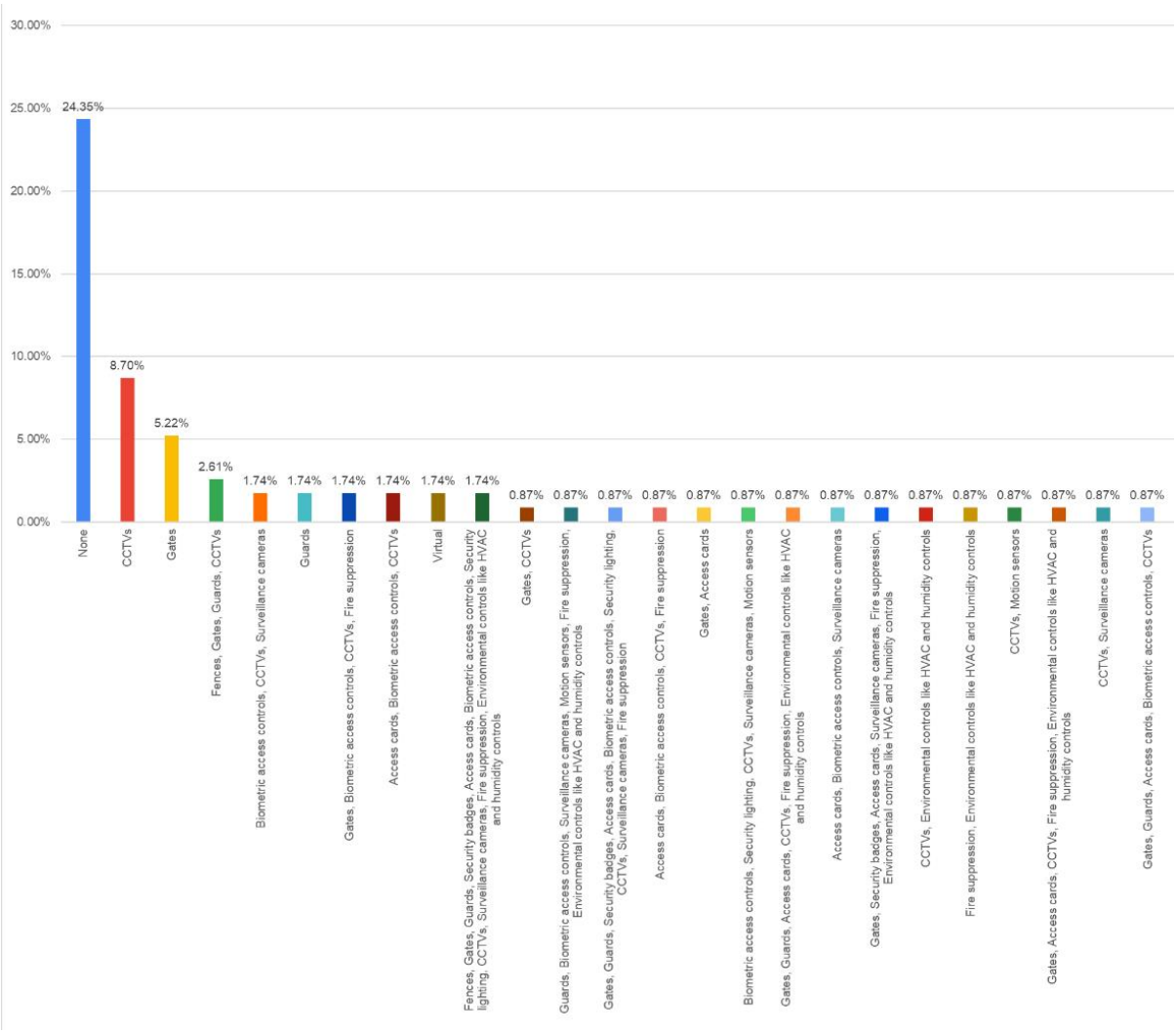

Figure 7: Physical Security Controls Implementation for SMEs

Many times, information security and cybersecurity are considered as same terms. It is not true, but these terms have some overlap. In the case of definition by ISO, preserving the CIA Triad requirement of information in cyberspace is "cybersecurity". It also makes clear that physical objects connected to each other or connected to the internet form the foundation of cyberspace. In short, information security is the protection of the information as an asset from cyber threats and vulnerabilities; cybersecurity on other hand has broader coverage where protection of cyberspace and all the assets present in that cyberspace [42]. It is important to note that, cyberspace is not limited to entities connected to the internet, but also entities that are communicating with each other without even connecting to the internet. Internet is one of the subsets of it. Cyber assets or ICT assets can be distinguished as tangible and intangible. Intangible assets include information, data, intellectual property, goodwill, reputation, an image in the market, service, software programs, and applications. Tangible assets include hardware, storage media, equipment, machines, printouts, and end-users [43]. Cyberspaces may experience security issues due to viruses, unauthorised access, theft of the organization's confidential information, DoS attacks, insider threats, laptop theft, financial fraud, abuse of a web application with a public interface, system penetration by unauthorised entities, misuse of wireless networks, sabotage, telecommunication fraud, website defacement, etc. [44]. Furthermore, cyberspace is formed by relationships present between high-level layers of physical devices, systems, applications, people, and processes. In short, cyberspace is incomplete without consideration of people, process, and technology and their linkage with each other in both cases of connected to or not connected to the internet [45].

Technical controls must be up to mark to perform critical cybersecurity functions such as access control, monitoring, logging, encryption, alert generation, and many such tasks [46]. As shown in Figure 8, 64% of SMEs had considered antivirus software and 52% had considered firewalls as technical con-

trols among a combination of different technical cybersecurity controls. More than a quarter of SMEs had no technical cybersecurity procedures in place. It means that hackers can use enormous attack surfaces in cyberspace for harmful purposes, progressing to more sophisticated cyber-attacks.

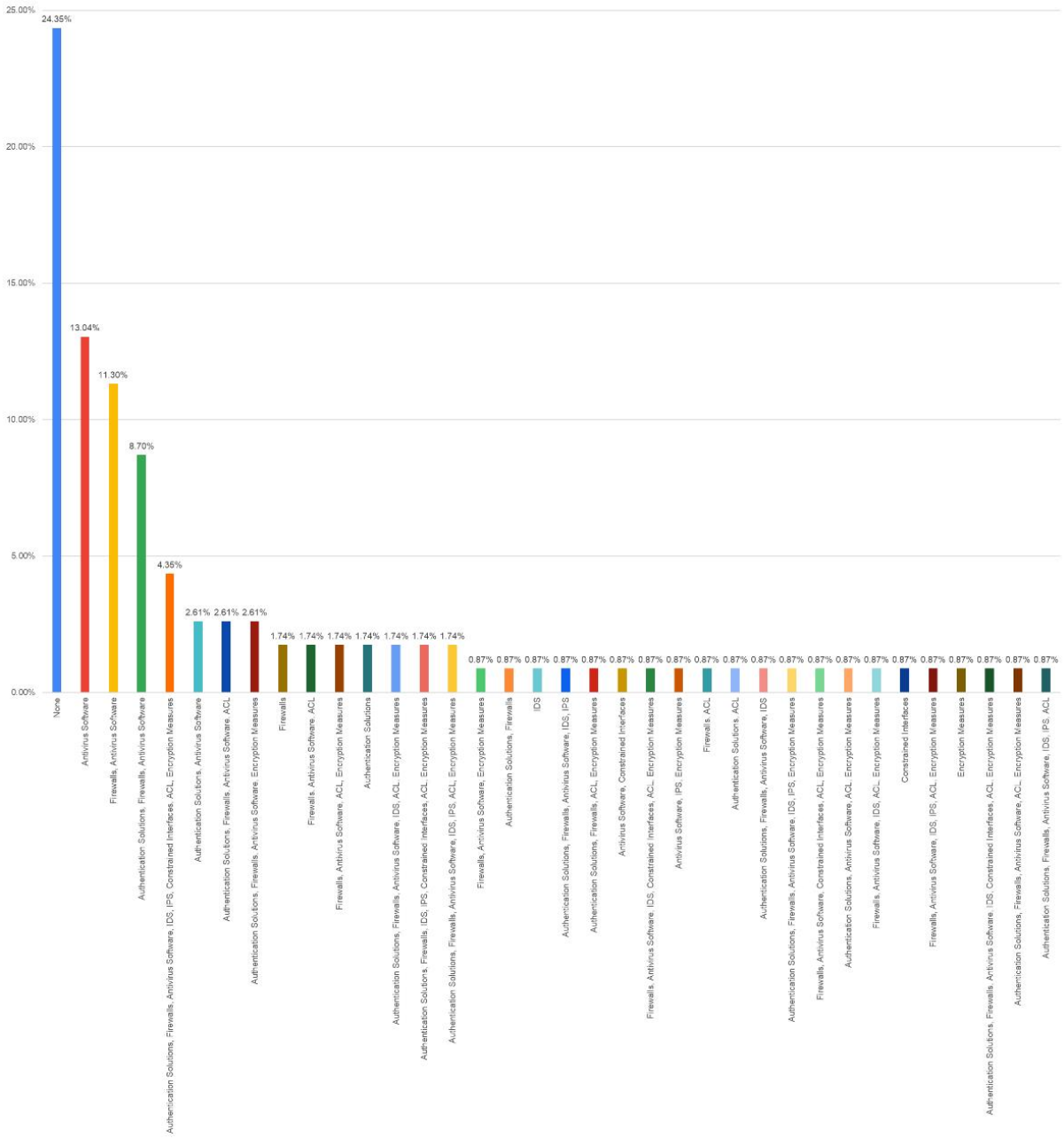

Figure 8: Technical Security Control Types Implemented for SMEs

While standards are used to provide the bare minimum criteria for attaining the objective, security policies help the firm define a set of broad ideas. Locking down the operating system of a worker's laptop or desktop while he or she is not there is the most basic requirement for assessing eligibility for security clearance. Guidelines are recommended best practises that aren't mandated but can help staff members or other stakeholders in the company follow the law in certain situations. In order to build policies that will be followed inside the business, procedures are actions that are clearly stated in a logical manner while taking legal requirements into consideration. This makes it simpler for participants or staff members to do the work securely. Administrative controls are security controls that outline clearly defined processes, methods, and necessary guidelines for directing all organisation stakeholders, and the implementation of comprehensive cybersecurity for any business depends on people's involvement. This sort of control covers many different areas, such as catastrophe

planning, disaster recovery plans, staff recruitment via resignation, and position separation. Training and awareness are two of the most crucial administrative controls. Additionally, administrative controls provide vital strategies that support firms. Any company that wants to respond to a cyber threat and prevent the consequences of a successful attack must have an incident response (IR) plan in place [47]. Such occurrences must be recorded by SME in an appropriate format, followed by an issue report including the precise root cause diagnosis and a strategy for problem solving.

As shown in Figure 9, among the SMEs who had some kind of administrative controls in place, more than 50% of SMEs do not have any policies, approximately 58% of SMEs do not have guidelines, and around 68% of SMEs do not have procedures as administrative cybersecurity controls. Around 17% of SMEs were only having security policies, but no security guidelines or procedures to support those. About 14% of enterprises, were only having security guidelines but no security policies or procedures. Also, less than 4% of enterprises were having some sort of security procedures, but no security policies or guidelines.

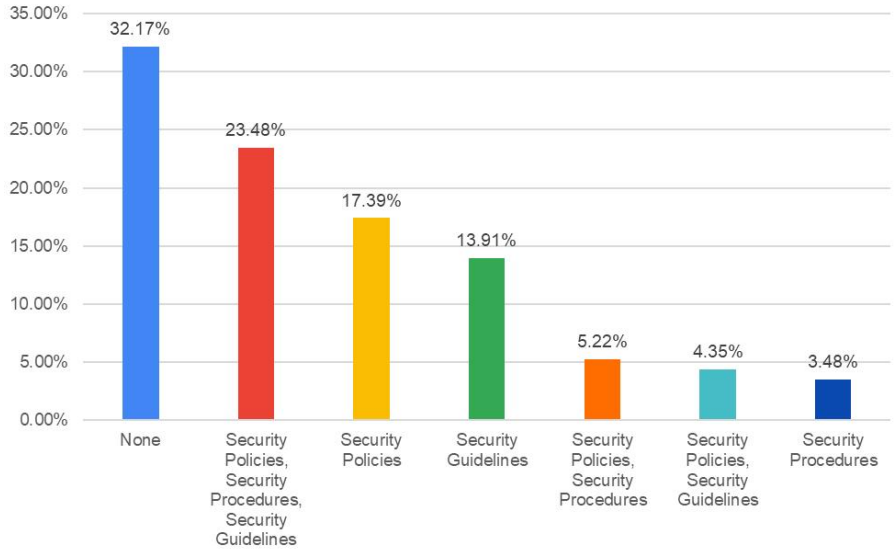

Figure 9: Administrative Security Controls Implemented for SMEs

Enterprises must have cybersecurity processes where every person working in it should get a series of steps or actions to perform certain tasks. Also, procedures are required to be very helpful for executing policies, followed by guidelines that recommend best practices. Most importantly all these should get regular updates as with its dependent areas such as actions of people, required changes in systems or technology, failure in the existing process, or even external events which are not in control of the enterprise [48]. As it is evident in Figure 10, around 34% of enterprises never conducted any cybersecurity training for employees. Human beings working for any organization are the weakest link for cybercriminals. Hence cybersecurity awareness pieces of training must be more frequent where it should consider the effectiveness of the message delivered which can contain critical factors such as "who" communicates information, "avoiding" shortcuts, norms, defaults, salience, priming, affect, commitments, and ego [49].

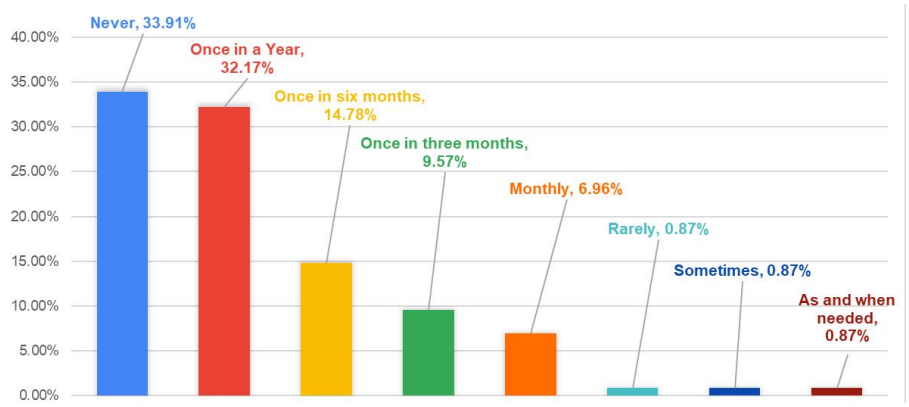

Figure 10: Frequency Security Awareness Training for Employees in SME

Also as shown in Figure 11, when authors collected inputs to understand problems that SMEs are facing while implementing cybersecurity controls, finance for implementing cybersecurity, the shortage of resources appeared, and other business priorities are more important for them found as the biggest problems for them. These top 3 problems indicate that SMEs are not able to find any link between their business goals and the cybersecurity controls to get the motivation to implement those further. SMEs don't take cybersecurity posture as important as other business priorities. Cybersecurity controls implementation should be in alignment with business priorities to be accepted by SMEs, it is an important finding among the three top findings. Apart from these, SMEs are struggling with knowledge, a roadmap to invest for cybersecurity controls, and existing standards or frameworks need big investments – these are key issues identified by the authors.

Figure 11: The biggest obstacles faced by SMEs

Malware and Phishing attacks along with Insider attacks are the most faced cyber threats by SMEs as per Figure 12. Malware is a malicious software program that is prepared by cybercriminals for cyber-attacks. These are mounted to the target system through various techniques such as using trojan horse, spam email attachments, etc [50]. Phishing is performed by fooling the email recipient by showing urgency to act where the receiver helps in performing malicious activity. Using the link in such emails, the victim is generally navigated to mimicked legitimate websites prepared by cybercriminals where the user's sensitive information is captured for performing a cyber-attack [51]. Nowadays many enterprises are exposed to insider threats as their employees, partners, vendors or even any stakeholder can access critical business assets due to the lack of or lagging effectiveness of the cybersecurity controls. Insider threat can be considered as either or both of two approaches which are - either by determining what an unauthorized person can do with access or by determining the access control mechanism [52]. Presently as almost all enterprises are using the cloud for storing or processing data, a web interface interacts with this database. Starting from IoT till any AI-related software systems have access developed in web format, hence to mitigate web attacks is the ultimate need of any SME [53]. Depending on the name of the

cybercriminal gang and type of infection process, different ransomware attack types are named uniquely. These ransomware attacks are generally performed in a very sophisticated manner where the victim's system gets encrypted and to get its decryption key hacker demands a certain ransom amount. Nowadays it's even becoming worse where many hackers get a backup of the database before encrypting the system where they increase the chances of getting more and more financial gain by more threatening the victim [54]. DoS attacks or even DDoS attacks are performed by cyber-criminals to deny access to legitimate users or subsystems to targeted network services. Such attacks are performed using open vulnerabilities in software where hackers keep consuming maximum or all resources required for those services. Those services can be related to the server's CPU processing power, memory used for operations, network link, or similar. The difference between DoS and DDoS is only that in DDoS cybercriminals use multiple devices to attack the targeted system which increases difficulties in blocking the source from where the attack is performed [55]. A volumetric DDoS assault aims to overwhelm the target's computing capacity or nearby network links by coordinating the coordinated delivery of a massive number of meaningless materials. On the one hand, the main Internet routers commonly use the FIFO (First-In--First-Out) and DROP-TAIL queuing disciplines, which do not differentiate between types of traffic, imposing equivalent loss rates for attacks and genuine data. This results in high success rates for this sort of attack. Attack traffic lacks this commitment; therefore, the links are surpassed even while legitimate traffic tends to retire to avoid further congestion. As a result, regular traffic is also impeded. The attackers, on the other hand, are using more sophisticated techniques to amplify their attacks and harm the target, including DDoS-for-hire, IoT-based DDoS attacks, and reflection DDoS attacks. They are doing this by taking advantage of the computational power and geographic distribution made possible by the large number of devices and the diverse mobility patterns they support, which are typically built into IoT and mobile IoT scenarios [56]. When communication between individuals or systems may be monitored or tampered with, a man-in-the-middle assault occurs. The most recent data in transit encryption solutions can aid in preventing these assaults [57].

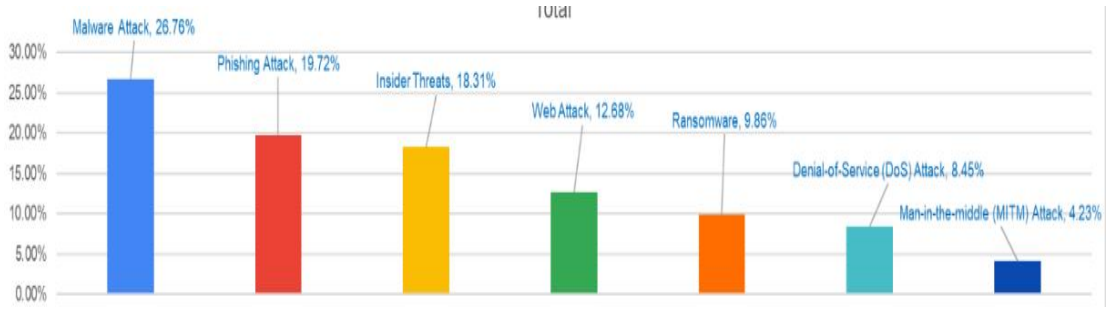

Figure 12: The biggest obstacles faced by SMEs

Readers must have benefited from the sharing by SMEs to understand the need to design a new cybersecurity framework for them.

Revisiting Core Cybersecurity Concepts

Any cybersecurity framework or standard cannot complete without considering CIA Triad which is nothing but confidentiality, integrity, and availability.

To avoid "Disclosure", implementation of controls supporting "Confidentiality" are important. "Modification" or "Alteration" should be avoided by implementing "Integrity" in cybersecurity posture. To prevent "Destruction", "Availability" should be considered in the design itself [58]. As shown in Figure 13, showing the Venn diagram of the CIA Triad, there is always overlap among the three of those.

Figure 13: CIA Triad

As illustrated in Figure 14, the CIA Triad can be mapped to additional tenets of cybersecurity such as authenticity, correct specifications, ethicality, identity management, people's integrity, non-repudiation, responsibility, and trust. Even more, such tenets can be mapped to this cybersecurity core concept [58]. Authenticity is the process of verifying the integrity of the user is genuine and legitimate [59]. For measuring the effectiveness of accountability, it must be defined clearly - it is related to responsibility in depth. For example, in the case of supply chain governance, accountability is defined as component responsibility, solution responsibility, whole system responsibility, sector responsibility, and CNI responsibility [60]. When a certain user can deny the involvement in acting without other intended users having any way to prove otherwise, it is known as a repudiation threat. For example, in a system that cannot trace forbidden actions, such a user might undertake an illegal or malicious operation. The ability of a system to protect against repudiation threats is known as non-repudiation [61]. Such quite a few terms of the cybersecurity posture are taken care of by CIA Triad.

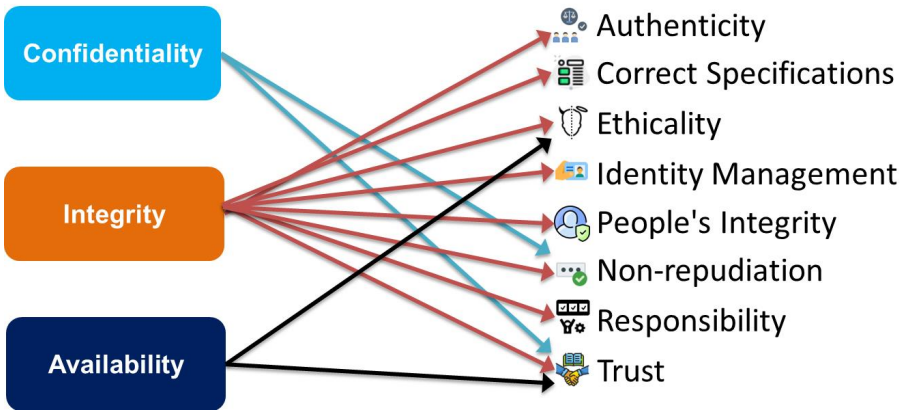

Figure 14: CIA Triad Mapping with Additional Tenets

Defense in Depth (DiD), also known as the "Castle" model, is a very old conceptual model innovated by US National Security Agency (NSA). In cybersecurity, as shown in Figure 15, there are generally a few to seven layers that are considered to protect the BDCA of an organization. SMEs should identify the high impact and high likelihood of risk by analyzing the list of assets, to find BDCA [62]. In cybersecurity, most of the time BDCA is a piece of information. In such case, security of

sensitive information should be taken into account in building information modelling (BIM). Encryption or the use of secure file exchange servers during transmission are required to guarantee data security. Enterprise's fears about security can be allayed by limiting password protection and evaluating authority regulations, which can guarantee security and privacy [63]. This is further protected by multiple layers such as the data layer, application layer, host/endpoint layer, network layer, logical/physical layer, and human layer. Any organization should beware of the mission-centric approach for each layer while implementing DiD [64].

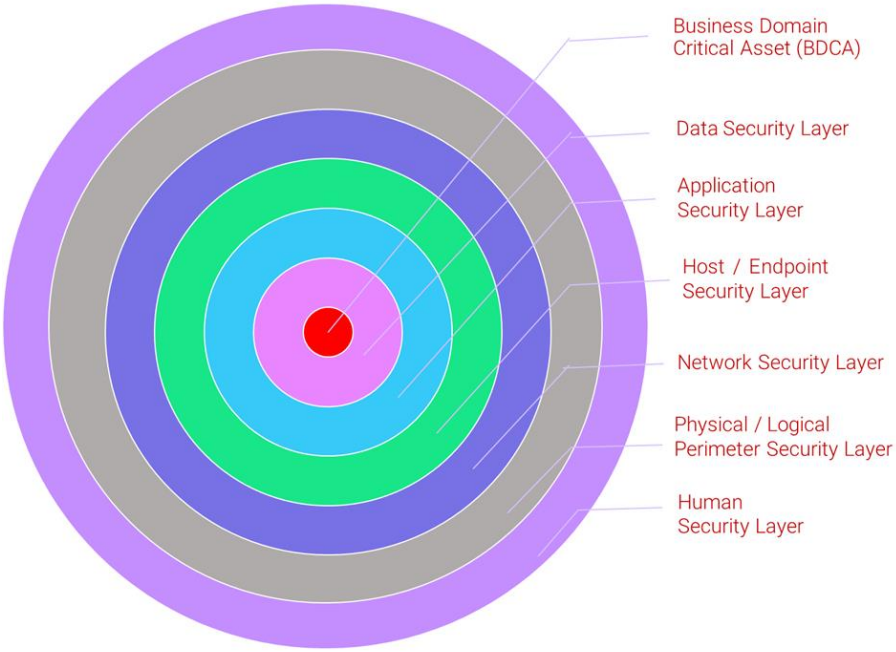

Figure 15: Seven Layers of Defense in Depth Concept

Each of these layers will have many different controls helping the cybersecurity of the respective layer. The human layer is the weakest link for performing successful cyber-attacks as those are responsible for the successful execution of the rest of the layers.

Understanding Prioritization of Domain-Specific CIA

Each domain will have different priorities based on the demand and importance of a particular aspect. This aspect can be mapped either or all from people, processes, and 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 A, where the authors had interviewed top management of SMEs from the different business domains, to understand their business prioritized BDCA and prioritization of CIA. Figure 16 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 senior management, confidentiality is more important than honesty or availability for these BDCAs. Similar to the Robot algorithm, medicine formulae, software technology servers, and supply chain network algorithms, integrity is prioritised by top management over confidentiality and availability in these BDCAs. In a few production fields, SME's senior management, automated equipment, and tools were all BDCA. Additionally, it was determined that BDCA accessibility was the most crucial element, followed by confidentiality and honesty. The top management of this area additionally identified quality control, line operation, and software of detector tolerance range as BDCAs. Additionally, integrity was given the top priority for the same, followed by accessibility and secrecy.

Figure 16: BDCA & CIA Prioritization in Manufacturing Domain

As shown in Table 1, it is giving an example of a particular SME domain mapped with its BDCA. Based on that BDCA, ascending order of prioritized areas of the CIA triad can be calculated. A BSFI domain enterprise might have a web application through which its clients are doing financial transactions as a BDCA. In that domain, confidentiality will be most important compared to integrity or availability. Consider two scenarios for the elaboration of this. Consider scenario-I, in which this web application's financial transaction data leaked – it is a confidentiality issue. Consider another scenario-II, in which this web application is not available for its users for a few hours due to maintenance hours or any other reason. If readers will closely analyze the high impact risk, scenario-II is tolerable as compared to scenario-I, meaning confidentially is the number one importance for this domain [65]. Similarly, for medicine or drug manufacturing pharmaceutical enterprise, the actual digital system which has formulae of the different compositions of ingredients for saving human lives can be considered as BDCA. If these formulae got altered by any unauthorized entities, it can harm the lives of patients. Here integrity of this system must be considered the highest priority, compared to rest two areas of the CIA triad [66]. Similarly, for e-commerce domain enterprises, the online shopping web portal might be their BDCA. For this web portal, availability will be most important to run the business than anything else. If this shopping web portal is not reachable to customers for a

few hours or during peak business hours, it will be the biggest threat to business [67,68].

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

The domain of SME Business	Business Domain Critical Asset (BDCA)	Prioritization in CIA Triad in Ascending Order of Highest to Lowest
BSFI	Web Portal for Financial Transaction	(1) Confidentiality (2) Integrity (3) Availability
E-commerce	Online Shopping Web Portal	(1) Availability (2) Integrity (3) Confidentiality
Pharmaceutical Drug Manufacturing	Medicine or Drug Formula Software System	(1) Integrity (2) Availability (3) Confidentiality

For example, if e-commerce products are visible to the public without authentication it won't be that serious to their business that the web or mobile platform is not working for a couple of days. It means the highest priority is availability for the BDCA which is an e-commerce platform in this example. Similarly, being financial transactions as the core business of BSFI domain SMEs, confidentiality is a must for them. To avoid alteration in human life-related crucial information, pharmaceutical enterprises will have integrity as the highest prioritized area [69,70].

Understanding Business Domain Critical Asset Needs

BDCA is a dynamic entity across industries. It keeps on changing depending on the business domain and even business goals for a particular enterprise. Each business domain may have different business domain key assets, as indicated in Table 1. For a few SMEs financial transactions are crucial, for a few 24X7 presence or production might be important, and so on.

It's also critical to realise that, even within the same industry, two distinct SMEs may have disparate BDCAs and, as a result, differing requirements for the implementation of cybersecurity.

Implementation of Cybersecurity Controls for BDCA

As discussed in the fourth stage, BDCA is very important for the existence and growth of any enterprise. Also, for a particular domain's demand and business purpose, this BDCA will differ.

As explained in Table 2, depending on the consideration of either only one area or two areas, or three areas of the CIA triad for BDCA, the protection from cyber threats can change.

If all areas of the CIA triad are implemented for BDCA, will provide maximum cybersecurity for it.

Table 2: Prioritization in CIA Triad for Specific BDCA of Particular Domain

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

Implementation of Defense in Depth Controls

As explained in stage 2, no cybersecurity framework will be complete without DiD in consideration. It helps in the holistic defense against cyber threats.

As illustrated in Table 3, every SME should first concentrate on enhancing the security of the host or endpoint layer, physical and digital perimeter layer, and human layer. If there are any public-facing networks, applications, or data layers those should be prioritized as well. As readers can see, it will be considered as DiD Implementation Level 1. Further, if the enterprise implements internal network and application layer security, it can be considered DiD Implementation Level 2. With additional steps to even implement data layer security within an enterprise, DiD Implementation Level 3 can be achieved.

The results and comments can be provided separately or in one part, and they can be divided into heading subsections if desired.

Table 3: Calculating DiD Implementation Level for Particular SME

Overall Cybersecurity Controls Implementation with Layered Approach of DiD	DiD Implementation Level
Human Layer Security+ Perimeter Security (both Physical & Digital)+ Host/Endpoint Security + Public-Facing Network Security + Public-Facing Application Layer Security + Public-Facing Data Layer Security	1 - Low
All in Level 1 + Internal Network Layer Security + Internal Application Layer Security	2 - Medium
All in Level 2 + Internal Data Layer Security	3 - High

Calculating Cybersecurity Controls Maturity Level

As earlier stages have certain implementations of cybersecurity controls, in this stage SMEs can be assessed to find the level of maturity they have achieved to safeguard their business in a particular domain. For which the two inputs are considered which are the outcome from stage 5 and stage 6.

As shown in Table 4, enterprises can start implementing overall cybersecurity controls along with a prioritized approach for BDCA. With the step-wise approach, they can start with a lower budget and resource investment, and can plan for better protection against cyber threats.

Table 4: Calculating Cybersecurity Maturity Level for Particular SME

BDCA Implementation with Prioritized CIA	Overall Cybersecurity Controls Implementation with Layered Approach of DiD	Maturity Level
Either of Confidentiality, Integrity, or Availability	Human Layer Security+ Perimeter Security (both Physical & Digital)+ Host/Endpoint Security + Public-Facing Network Security + Public-Facing Application Layer Security + Public-Facing Data Layer Security	1 - Low
Either of Confidentiality and Integrity, Integrity and Availability or Confidentiality and Availability	All in Level 1 + Internal Network Layer Security + Internal Application Layer Security	2 - Medium
All Confidentiality, Integrity & Availability	All in Level 2 + Internal Data Layer Security	3 - High

As explained in Table 4, Maturity Level 1, covers either of the areas in the CIA triad and considers the cybersecurity of the three most vulnerable layers of DiD. With increasing levels, it keeps on growing towards holistic implementation. Maturity Level 1 has fewer cybersecurity controls implemented as compared to Maturity Level 3. SMEs need to move towards Maturity Level 3 with the time.

AI-Driven Cybersecurity Controls Mapping for SME

BDCA implementation with prioritized CIA triad and overall cybersecurity controls implementation with a layered ap-

proach of DiD can be mapped with the particular SME having a specific business domain. Artificial Intelligence (AI) can aid in the identification of appropriate controls for a given SME business domain and mission-critical asset.

Responsible AI for Mapping Cybersecurity Controls for SME

AI should help with the ethical standards while selecting the appropriate controls for cybersecurity implementation. Therefore, this is translated to responsible AI principles that are a component of the methodology for using Artificial Intelligence techniques in real-world settings while retaining model responsibility and explainability [71]. Figure 17 illustrates how the installation of cybersecurity controls may be matched to ten fundamental principles of responsible AI [13].

Understanding the purpose of each vital asset in the particular business sector that a SME operates in is essential when it comes to the first responsible AI concept, "Assess positive and negative consequences and implications." 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 doing 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 unlocking doors to prevent human deaths or injuries. In this case, organizations must assess whether another solution for database security is required.

The envisaged AI supporting framework will make sure that human rights law is not ignored when implementing cybersecurity rules, which is the fifth principle. This principle ensures conformity with human values and human rights. 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 are 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, appeals, damag-

ing errors, and so on during the implementation of the framework.

In order to ensure that processes inside SMEs handle any cyber-attack incident, complaint, appeals, damaging errors, and other cybersecurity controls more effectively, it is crucial to ensure that the processes adhere to the tenth responsible AI principle, "Enforce, and accept the enforcement of, liabilities and sanctions." It should also ensure that SMEs are well-positioned to meet the demands of external stakeholders in their eco-system or specific region/country.

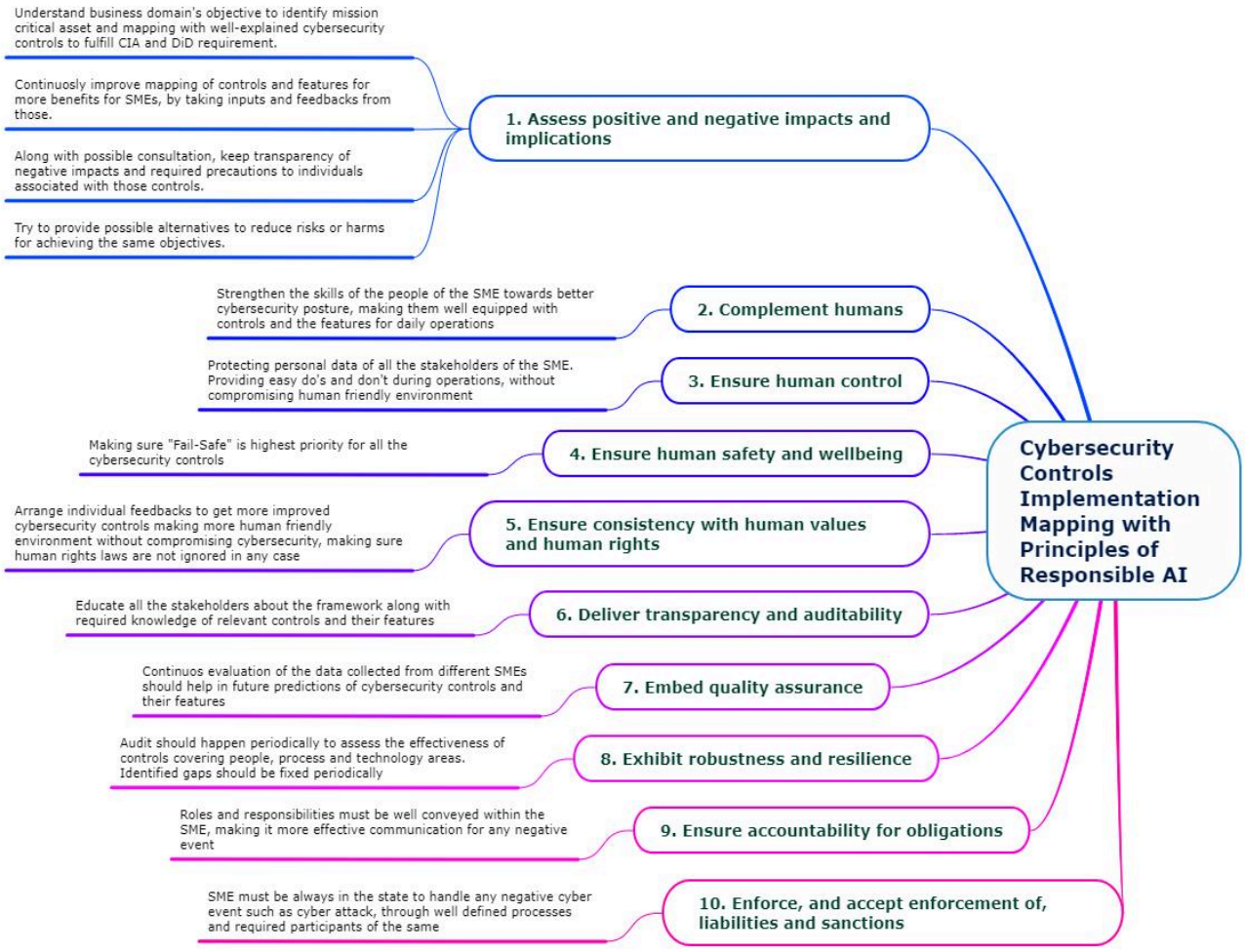

Figure 17: Cybersecurity Controls Implementation Mapping with Principles of Responsible AI

Software for Step-wise Cybersecurity Controls Mapping for SME

The authors are 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 itself adding key information such as business domain and its specific mission-critical asset. Taking it as input software predicts the prioritization in the CIA triad, relevant cybersecurity controls, and their specific features.

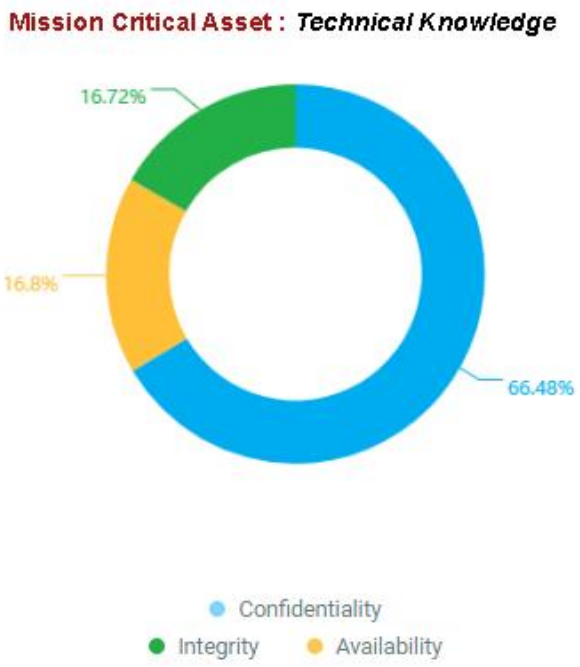

Figure 18: Web Application Flow Screenshot showing priority of components in CIA Triad

The research data that was gathered is utilised as the first input for the CIA triad's business domain, BDCA, and prioritising components. A multiclass classification technique is being used in this section of the ML programme. The class of a piece of data—in this example, the three elements of the CIA triad of secrecy, integrity, and availability—is predicted using supervised machine learning. This method requires a set of labelled samples as input. They all start out as text data. After that, it is transformed into the Key (numeric) type via the Term Transform. A classifier is the result of a classification method, and it is used to forecast the class of fresh unlabeled examples [72,73]. Firstly, with helps in predicting prioritized components in the CIA triad based on particular BDCA. Further, this algorithm predicts the CIA triad prioritization and its cybersecurity controls mapping, categorizing those controls as per their relevance in either 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 19: Web Application Screenshot showing Recommended Cybersecurity Controls for Particular BDCA and Confidentiality as priority

For example, refer the Figure 18 which is highlighting one of SMEs' BDCA it is showing Confidentiality is the highest priority. Further as shown in Figure 19, the software can pull required cybersecurity controls to fulfill the security requirement for the same. Similarly, it will help SMEs to implement cybersecurity controls for Integrity and Availability in further steps. In an also similar way, this software also giving recommended 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.

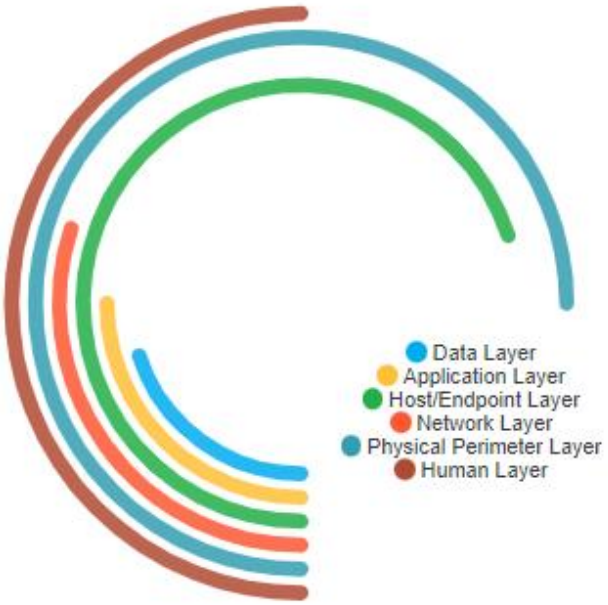

Figure 20: Cybersecurity Controls Implementation for DiD Levels

As shown in Figure 20, even software can show the achieved fulfilling minimum level of cybersecurity controls implementation for DiD layers.

BDSLCCI 2.0, which has been available since January 1, 2024, refers to the below sequence of controls in different DiD layers where data layer security has been prioritized based on various digital data privacy compliances that are more prioritized in various countries [70]. Refer to Appendix B for the list of control areas for BDSLCCI 2.0. It is important to note that the BDSLCCI security governance layer focuses on preparedness to overcome any unseen security event as well as continuous improvement in cybersecurity posture via periodic cybersecurity audits and fixation of the vulnerabilities identified in those audits.

Also, through BDSLCCI web platform, small and medium enterprises gains below benefits.

- 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 implementation)
- Access for other Teammates to the Portal
- SecureClaw Crawler Tool to Scan and Identify Vulnerabilities in EndPoints (such as Laptops, Desktops, and Servers)
- Key Cybersecurity Policy, Matrix, Guidelines, and Forms as Documentation
- Online Cybersecurity Awareness Trainings, followed by a Test and Training Certificate for Employees
- Cybersecurity Awareness Posters and Banners for Employees
- Daily Cyber Threat Alert Email Notification (The company received 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 (It is one of the outcomes of the audit and assessment)

- Web Analytics Report Showing various graphs and details showing coverage and effectiveness of the BDSLCCI controls implemented (It is one of the outcomes 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 & Future Work

Small and medium enterprises (SMEs) are playing a crucial role in the global economy, and any threat to their growth or existence will negatively impact the economy. It is critical to protect SMEs in order to maintain employment opportunities and boost GDP in developed economies. With the growing need for digitization in Industry 4.0, every organization, including SMEs, is seeing an increase in the surface of cyberattacks. If organizations do not implement proper controls to protect themselves, cybercriminals can perform malicious activities and cause harm to the business. It has been discovered that nearly half of these enterprises are vulnerable to various cyberthreats. From the inputs received from the top management of various SMEs, there are four high-level problems. Existing cybersecurity standards or frameworks demand many generic controls to be implemented, which is expensive. Secondly, SME companies do not have the skilled resources to implement or maintain such cybersecurity controls. Thirdly, SME top management cannot relate cybersecurity to one of their top business priorities. It might be because the existing cybersecurity standards or frameworks do not directly specify their business domain. Finally, SMEs are not receiving systematic guidance on where to begin the journey of implementing cybersecurity controls. To address these problems, it is important to have a different approach.

Hence, there are two areas where SMEs need to focus. The first is that SMEs need to identify and protect their business domain critical assets (BDCA), without which they could not execute their business. Also, the confidentiality, integrity, and availability (CIA Triad) prioritization needs of any such BDCA differ based on the enterprise's business domain. There should be the implementation of BDCA-focused cybersecurity controls as per the priority. The second area for any SME is to implement defense mechanisms in each layer of the organization, which can start by implementing the least amount of cybersecurity controls to safeguard each layer. It is widely known as the "defense in depth" (DiD) technique. It can provide comprehensive protection, lowering the overall risk of a cyberattack. With the gradual installation of the simplest cybersecurity controls, an SME's maturity level can be raised while putting less strain on other aspects of the business. Many SMEs are lagging in matching the rising needs of cybersecurity implementation for themselves. It would be better if they would get a structured, step-by-step approach to a new cybersecurity framework to begin with and mature over time. The recommended method of stepwise implementation of cybersecurity controls can help SMEs, rather than "no" or "random" cybersecurity control implementation.

In the future, SMEs need to maintain a level of maturity in cybersecurity along with fixing and improving open vulnerabilities in regular assessments to avoid any implementation gaps in their cybersecurity posture. Even additional controls can be implemented with time. The framework can be more useful by using responsible AI or similar advanced technology while compiling various inputs from different SMEs, different domains, and different BDCAs to assist in providing recommended cybersecurity controls. SMEs can choose a different asset that is crucial to their goal and continue to develop controls for each one. These new recommended solutions as part of the research can be further enhanced for large enterprises or other segments as well.

Author Contributions

Conceptualization, S.P., and H.P.; methodology, S.P.; software, S.P.; validation, S.P., and H.P.; formal analysis, S.P., and H.P; investigation, S.P.; resources, S.P.; data curation, S.P.; writing—original draft preparation, S.P.; writing—review and editing, H.P.; visualization, S.P.; supervision, H.P.; project administration, H.P.

Funding

This research received no external funding

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The data presented in this study are available on request from the corresponding author.

Acknowledgments

This project received no external finance. The authors like to thank participants from SMEs who shared their valuable inputs.

Conflicts of Interest

The authors declare no conflict of interest.

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

Number of Participants	**Business Domain**	Business Domain Critical Asset (BDCA)	**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 Labaur	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 of 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 of 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 modelling 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	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 Softwares	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 Laboure	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

Appendix B: The following are the enhanced DiD Layers in BDSLCCI 2.0 version which is available since January 2024

PrioritySequence	Layer Name	Maturity Level	BDSLCCI Controls
1	Host/Endpoint Security Layer	BDSLCCI Level 1	1.1 - Host/Endpoint - Less Permission to Use 1.2 - Host/Endpoint - Endpoint Protection - Anti-Virus 1.3 - Host/Endpoint - Licensed Operating System (OS) 1.4 - Host/Endpoint - Block File Transfers 1.5 - Data - Encryption 1.6 - Data - Access control 1.7 - Data - Backup 1.8 - Data - Data Loss Prevention 1.9 - Data - Secure Deletion 1.10 - Human - Cybersecurity Awareness Training 1.11 - Human - Separation of Duties 1.12 - Human - Service Level Agreement (SLA) 1.13 - Human - Employee Background Check 1.14 - Human - Review Access Rights 1.15 - Human - Cyber Threat Alert Notifications 1.16 - Human - Cybersecurity Banners / Posters 1.17 - Human - Non-Disclosure Agreement (NDA)
2	Data Security Layer		
3	Human Security Layer		
4	Network Security Layer	BDSLCCI Level 2	2.1 - Network - Network Firewall 2.2 - Network - Network Access Control 2.3 - Network - Remote Access VPN 2.4 - Network - Instruction Detection & Prevention Systems (IDPS) 2.5 - Application - OWASP Coding Practices 2.6 - Application - Application Hardening
5	Application Security Layer		

6	Physical Perimeter Security Layer	BDSLCCI Level 3	3.1 - Physical Perimeter - Locked and Dead-Bolted Steel Doors 3.2 - Physical Perimeter - Closed-Circuit Surveillance Cameras (CCTV) 3.3 - Physical Perimeter - Picture IDs 3.4 - Physical Perimeter - Security Guards / Proper Lighting / Biometrics / Environmental Control 3.5 - Governance - Incident Response Process 3.6 - Governance - Business Continuity Plan (BCP) 3.7 - Governance - Periodic Audit
7	Governance Security Layer		

References

1. WTO (2016) WTO | World Trade Report 2016 | Levelling the trading field for SMEs. Www.wto.org; World Trade Organization.

2. Müller JM, Buliga O, Voigt K-I (2018) Fortune favors the prepared: How SMEs approach business model innovations in Industry 4.0. Technological Forecasting and Social Change, 132, 2–17.

3. Teng X, Wu Z, Yang F (2022) Impact of the Digital Transformation of Small-and Medium-Sized Listed Companies on Performance: Based on a Cost-Benefit Analysis Framework. Journal of Mathematics. 2022: 14.

4. SENSEON (2019) The State of Cyber Security SME Report 2019. In senseon.io (p. 4). Senseon.io.

5. Aguilar CLA (2015) SEC.gov | The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses.

6. Osborn E (2015) Business versus Technology: Sources of the Perceived Lack of Cyber Security in SMEs. Ora.ox.ac.uk.

7. Shepherd M (2023) 30 Surprising Small Business Cyber Security Statistics. Fundera; Fundera.

8. Paul K, Milmo D (2022) Russia-backed hackers behind powerful new malware, UK and US say. The Guardian.

9. Madnick S (2022) What Russia's Ongoing Cyberattacks in Ukraine Suggest About the Future of Cyber Warfare. Harvard Business Review.

10. Help Net Security (2022) Sharp rise in SMB cyberattacks by Russia and China. Help Net Security.

11. Guta M (2022) Small Business Cybersecurity Concerns Amid Russia-Ukraine Crisis. Small Business Trends.

12. Guynn J (2022) "Ticking time bomb": Russian ransomware attacks are coming. What small businesses should do right now. USA TODAY.

13. Clarke R (2019) Principles and business processes for responsible AI. Computer Law & Security Review, 35: 410-22.

14. Lee B, Vanickis R, Rogelio F, Jacob P (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.

15. Pratt MK (2018) What is Zero Trust? A model for more effective security. CSO Online.

16. Alsinawi B (2018) Is the NIST Cybersecurity Framework Enough to Protect Your Organization?

17. Alqatawna J (2014) The Challenge of Implementing Information Security Standards in Small and Medium e-Business Enterprises. Journal of Software Engineering and Applications, 07: 883–90.

18. Gourinchas P-O, Kalemli-Özcan Ş, Penciakova V, Sander N (2020) COVID-19 AND SME FAILURES.

19. Syafrizal M, Selamat SR, Zakaria NA (2020) Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12: 417-32.

20. Hamdani SWA, Abbas H, Janjua AR, Shahid WB, Amjad MF et al. (2021) Cybersecurity standards in the context of operating system: practical aspects, analysis, and comparisons. ACM Computing Surveys (CSUR), 54: 1-36.

21. Keeper Security, Inc. (2020). Cybersecurity in the Remote Work Era: A Global Risk Report. Ponemon Institute.

22. Rabie A Ramadan, Bassam W Aboshosha, Jalawi Sulaiman Alshudukhi, Abdullah J Alzahrani, Ayman El-Sayed et al. (2021) "Cybersecurity and Countermeasures at the Time of Pandemic", Journal of Advanced Transportation, 2021: 19.

23. Ahmad NH, Seet P-S (2009) Understanding business success through the lens of SME founder-owners in Australia and Malaysia. International Journal of Entrepreneurial Venturing, 1: 72–87.

24. Reiss F (2016) Article: Why Small Businesses Fail.

25. Ackah J, Vuvor S (2011) The Challenges faced by Small & Medium Enterprises (SMEs) in Obtaining Credit in Ghana.

26. Sannajust A (2014) Impact of the World Financial Cri-

sis to SMEs: The determinants of bank loan rejection in Europe and USA.

27. Plessis AJD, Indavong S, Marriott J (2015) SME brand management: a lack of business skills, financial support and human resources. Unitec.ac.nz.

28. Piggin R (2016) Cyber security trends: What should keep CEOs awake at night. International Journal of Critical Infrastructure Protection. 13: 36-38.

29. Ayyagari M, Demirgüç-Kunt A, Maksimovic V (2017) Policy Research Working Paper : SME Finance. In worldbank.org. World Bank Group, Development Research Group.

30. Duan Y, Mullins R, Hamblin D, Stanek S, Sroka H et al. (2002) Addressing ICTs skill challenges in SMEs: insights from three country investigations. Journal of European Industrial Training, 430–41.

31. Emine D (2012) Financial Challenges That Impede Increasing the Productivity of SMEs in Arab Region. Journal of Contemporary Management.

32. Farsi JY, Toghraee M (2014) Identification the main challenges of small and medium sized enterprises in exploiting of innovative opportunities (Case study: Iran SMEs). Journal of Global Entrepreneurship Research, 4: 1-15.

33. Khalique M (2011) Challenges for Pakistani SMEs in a Knowledge-Based Economy. Indus Journal of Management & Social Sciences, 5: 74-80.

34. Moeuf A, Pellerin R, Lamouri S, Tamayo-Giraldo S, Barbaray R (2017) The industrial management of SMEs in the era of Industry 4.0. International Journal of Production Research. 56: 1-19.

35. 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. 5: 1-13.

36. PETKOVSKA T (2015) Original scientific paper Tatjana PETKOVSKA 1) THE ROLE AND IMPORTANCE OF INNOVATION IN BUSINESS OF SMALL AND MEDIUM ENTERPRISES. 1-20.

37. Prasanna R, Jayasundara J, Naradda Gamage SK, Ekanayake E, Rajapakshe P 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: 100.

38. 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. 1-21.

39. Siti S, Omar Arokiasamy L, Ismail M (2009) The Background and Challenges Faced by the Small Medium Enterprises. A Human Resource Development Perspective. In International Journal of Business. 4: 1-8.

40. Osei, E., & Yeboah-Boateng. (2013). Aalborg Universitet Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA) 155-8.

41. Xie J, Stefanov A, Liu CC (2016) Physical and cyber security in a smart grid environment. Wiley Interdisciplinary Reviews: Energy and Environment 5: 519-42.

42. Bay M (2016) What is Cybersecurity? In search of an encompassing definition for the post-Snowden era. In French Journal For Media Research 15-6.

43. Ozier W (2002) "Risk Assessment," in Information Security Management Handbook. CRC Press.

44. Fenz S (2005) Cyberspace Security: A definition and a description of remaining problems. In univie.ac.at.

45. Daras N (2018) On the Mathematical Definition of Cyberspace. Theoretical Mathematics & Applications, 8: 1792-9709.

46. Song JG, Lee JW, Park GY, Kwon KC, Lee DY, Lee CK (2013) An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants. Nuclear Engineering and Technology, 45: 637-52.

47. Naseer A, Naseer H, Ahmad A, Maynard SB. Masood Siddiqui A (2021) Real-time analytics, incident response process

agility and enterprise cybersecurity performance: A contingent resource-based analysis. International Journal of Information Management, 59: 102334.

48. Cebula JL, Young LR (2010) A Taxonomy of Operational Cyber Security Risks.

49. Bada M, Sasse A, Nurse J (2019) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? In arxiv.org. International Conference on Cyber Security for Sustainable Society.

50. Kong D, Yan G (2013) Discriminant Malware Distance Learning on Structural Information for Automated Malware Classification.

51. Bhasin Dr M (2007) Mitigating Cyber Threats To Banking Industry.

52. Bishop M, Gates C (2008) Title Defining the Insider Threat Publication Date Defining the Insider Threat. In escholarship.org.

53. Luo C, Tan Z, Min G, Gan J, Shi W, Tian Z (2021) A Novel Web Attack Detection System for Internet of Things via Ensemble Classification. IEEE Transactions on Industrial Informatics, 17: 5810-8.

54. Mohurle S, Patil M (2017) A brief study of Wannacry Threat: Ransomware Attack 2017. International Journal of Advanced Research in Computer Science, 8.

55. Cheng CM, Kung HT, Tan KS (2002) Use of Spectral Analysis in Defense Against DoS Attacks. Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE. Harvard University.

56. Francisco Sales de Lima Filho, Frederico A. F. Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, Luiz F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning", Security and Communication Networks, 2019: 1574749.

57. Huang X, Shah PG, Sharma D (2010) Protecting from Attacking the Man-in-Middle in Wireless Sensor Networks with Elliptic Curve Cryptography Key Exchange. 2010 Fourth International Conference on Network and System Security.

58. Samonas, S., & Coss, D. (2014). The Cia Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. In proso.com 29-38.

59. Mahrouqi A, Tobin P, Abdalla S, Kechadi T (2016) Simulating SQL-Injection Cyber-Attacks Using GNS3. International Journal of Computer Theory and Engineering, 8: 213-7.

60. Wallis T, Johnson C (2020) Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. IEEE Xplore.

61. Moniz PMS (2011) Confidentiality, integrity and non-repudiation in smartgrids. Repositorio.ul.pt.

62. Sosin A (2017) How to Secure Information Assurance in an Information Age.

63. Pengfei Li, Shengqin Zheng, Hongyun Si, Ke Xu (2019) "Critical Challenges for BIM Adoption in Small and Medium--Sized Enterprises: Evidence from China", Advances in Civil Engineering, 2019: 9482350.

64. Jajodia S, Noel S, Kalapa P, Albanese M, Williams J (2011) Cauldron mission-centric cyber situational awareness with defense in depth. IEEE Xplore.

65. AL-ALAWI, Prof. AI, AL-BASSAM Ms. SA (2020) The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. Journal of Xidian University, 14.

66. Arden NS, Fisher AC, Tyner K, Yu LX, Lee SL, Kopcha M (2021) Industry 4.0 for pharmaceutical manufacturing: Preparing for the smart factories of the future. International Journal of Pharmaceutics, 602: 120554.

67. Guynes CS, Wu YA, Windsor J (2011) E-Commerce/Network Security Considerations. International Journal of Management & Information Systems – Second Quarter 2011, 15.

68. Sutton S, Hampton C, Khazanchi D, Arnold V (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: 160-74.

69. Pawar S, 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, 2: 100080.

70. Pawar, Shekhar, Poonam Pawar (2024) “BDSLCCI.” Notionpress.com, 27 July 2023, notionpress.com/read/bdslcci.

71. Wahidul Hasan Abir, Md. Fahim Uddin, Faria Rahman Khanam, Tahia Tazin, Mohammad Monirujjaman Khan, Mehedi Masud, Sultan Aljahdali, "Explainable AI in Diagnosing and Anticipating Leukemia Using Transfer Learning Method", Computational Intelligence and Neuroscience, 2023: 5140148.

72. Hector Alaiz-Moreton, Jose Aveleira-Mata, Jorge Ondicol-Garcia, Angel Luis Muñoz-Castañeda, Isaías García, Carmen Benavides (2019) "Multiclass Classification Procedure for Detecting Attacks on MQTT-IoT Protocol", Complexity, 2019: 6516253.

73. Anam Mustaqeem, Syed Muhammad Anwar, Muahammad Majid (2018) "Multiclass Classification of Cardiac Arrhythmia Using Improved Feature Selection and SVM Invariants", Comput Math Methods Med, 2018: 7310496.