Arab American University

Faculty of Graduate Studies

A Cybersecurity Framework for Micro, Small and Medium-Enterprises (MSMEs) in Palestine.

By

Rawan Jalal Ibrahim Samara

Supervisor

Dr. Majdi Owda

Co- Supervisor

Dr. Faisal Awartani

This thesis was submitted in partial fulfillment of the requirements for the Master's degree in Cybercrimes and Digital Evidence Analysis.

July / 2024

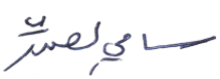
Thesis Approval

A Cybersecurity Framework for Micro, Small and Medium-Enterprises (MSMEs) in Palestine.

By

Rawan Jalal Ibrahim Samara

This thesis was defended successfully on 8/7/2024 and approved by:

Committee members	Signature
1. Dr. Majdi Owda: Supervisor	
2. Dr. Faisal Awartani: Co- Supervisor	
3. Dr. Sami Sadder: Internal examiner	
4. Dr. Mousa Faraj Allah: External examiner	

Declaration

I declare that the thesis titled "A Cybersecurity Framework for Micro, Small and Medium-Enterprises (MSMEs) in Palestine" is my work and has been composed solely by myself, does not contain work from other researchers, and has not been submitted for any other degree or scientific work except the reference is made.

The Name of The Student: Rawan Jalal Ibrahim Samara

ID: 201920283

Date: 30/9/2024

Signature: Rawan Samara

Dedication

I dedicate this thesis to my family and friends for their unconditional love and support. To my mother and my father for their support, which has not left me throughout my life. Also, to my brothers, whose support I have not always forgotten. To my dear friends for their continued support throughout my learning journey. To my teachers for their advice.

Acknowledgment

I am truly grateful to Dr. Majdi Owda and Dr. Faisal Awartani for their invaluable advice, assistance, and dedicated time spent in reviewing and refining my work. Dr. Majdi & Dr. Faisal provided helpful suggestions and advice that have had a significant effect and helped overcome many obstacles in preparing this work in the best way possible.

Abstract

This thesis presents a comprehensive Cybersecurity Framework specifically designed for Micro, Small, and Medium Enterprises (MSMEs) in Palestine, addressing the unique challenges these businesses face in an increasingly digital landscape. The rapid advancement of information technology has led to a heightened reliance on digital systems, rendering MSMEs particularly vulnerable to cyber threats. Given their critical role in the Palestinian economy, it is imperative to develop cybersecurity strategies that are not only effective but also tailored to the specific needs and constraints of these enterprises.

The proposed framework is meticulously crafted to offer flexibility and scalability, accommodating the diverse resources and operational capacities of MSMEs. It integrates both technical and non-technical components, ensuring a holistic approach to cybersecurity. Key elements of the framework include the incorporation of threat intelligence, risk assessment methodologies, and customized user awareness campaigns that are contextually relevant to the operational environment of MSMEs.

To evaluate the framework's effectiveness and practicality, this research employs a mixed-methods approach, utilizing qualitative research techniques such as case studies, surveys, and expert interviews. This methodology facilitates a thorough understanding of the current cybersecurity landscape for MSMEs in Palestine, enabling the identification of critical vulnerabilities and the development of targeted strategies to mitigate risks.

The findings of this study are anticipated to provide valuable insights into the development and implementation of cybersecurity measures that are not only relevant to Palestinian MSMEs but also applicable to similar economic and geopolitical contexts. By equipping these enterprises with the necessary tools and knowledge to navigate the

expanding cyber threat landscape, this research aims to promote the protection of their digital assets, ensure business continuity, and foster a secure environment conducive to long-term growth.

Ultimately, this thesis contributes to the broader discourse on cybersecurity in the MSME sector, highlighting the importance of tailored frameworks that consider local challenges and resources. The successful implementation of the proposed Cybersecurity Framework is expected to enhance the resilience of Palestinian MSMEs, thereby supporting job creation, poverty alleviation, and overall economic stability in the region.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

MSMEs	Micro, Small, and Medium-Enterprises.
GDP	Gross domestic product.
NIST	National Institute of Standards and Technology.
CSF	Cybersecurity Framework.
ISMS	Information Security Management Systems.
ISO	International Organization for Standardization.
IEC	The International Electrotechnical Commission.
CIS	Center for Internet Security.
COBIT	Control Objectives for Information and Related Technologies.
ISACA	The Information Systems Audit and Control Association.
C2M2	Cybersecurity Capability Maturity Model.
PMA	the Palestine Monetary Authority.
CPHC	The Council of Professors and Heads of Computing.
ISC2	International Information System Security Certification Consortium.
PCI DSS	The Payment Card Industry Data Security Standards.
HIPAA	The Health Insurance Portability and Accountability Act.
ePHI	electronic Personal Health Information.
SOX	Sarbanes Oxley Act.
InfoSec	Information Security.
PDCA	Plan-Do-Check-Act.
IEC	The International Electrotechnical Commission.

BSI	British Standards Institution.
CM	Configuration Management.
CP	Contingency Planning.
IA	Identification and Authentication.
IR	Incident Response.
MA	Maintenance Controls.
MP	Media Protection.
PS	Personnel Security.
PE	Protection of the Physical Environment.
PL	Planning Controls.
PM	Program Management.
RA	Risk Assessment.
CA	Security Assessment and Authorization.
SC	System and Communications Protection.
SI	System and Information Integrity.
SA	System and Services Acquisition.
DOS	Denial-Of-Service Attacks
ITIL	The Information Technology Infrastructure Library.
SAMA	The Saudi Arabian Monetary Authority Framework.
GCI	Global Cybersecurity Index 2020
ITU	The International Telecommunication Union
SOGP	Standard of Good Practice for Information Security
BCBS	The Basel Committee on Banking Supervision

DTI	The Department of Trade and Industry
AAA	Authentication, Authorization, and Accounting
ISA	International Society of Automation
IACS	The security of industrial automation and control systems
GL Model	The Gordon–Loeb Model
KIS	Keep It Simple
CYSEC	Cybersecurity Coach
CCB	The Centre for Cybersecurity Belgium
TLP	Traffic light protocol
CTR	Click-Through Rate

Chapter One

1. Introduction

1.1. MSME Introduction

Micro, Small, and Medium-Enterprises (MSMEs) play an essential role in the global economy, contributing considerably to job creation, economic development, and innovation. The word "MSME" refers to Micro, Small, and Medium-Enterprises, and these enterprises are distinguished by their small size of operations and staff [1]. The Palestinian Ministry of National Economy has introduced new criteria for classifying economic enterprises based on the number of employees and annual turnover. The classifications are as follows: Micro Enterprises (1-4 employees, up to $100,000 turnover), Very Small Enterprises (5-9 employees, $100,001 - $500,000 turnover), Small Enterprises (10-49 employees, $500,001 - $5,000,000 turnover), Medium Enterprises (50-249 employees, $5,000,001 - $50,000,000 turnover), and Large Enterprises (250 or more employees, over $50,000,000 turnover). These definitions aim to provide a unified reference for all institutions in Palestine, facilitating better policy development and support for these enterprises [2] [3] [4].

MSMEs are defined differently in each nation, although they are typically classed based on variables such as investment in equipment and machinery, turnover, and the number of workers. Here is the Number of establishments in the private sector, civil sector, and government companies in the rest of the West Bank and Gaza Strip by governorate and categories of labor size in 2007.

Table 1.1: The Number of establishments in the private sector, civil sector, and government companies in Palestine [5].

Governorate	Employment Size Categories						
	100+	99-50	49-20	19-10	9-5	4-1	Total
Remaining West Bank and Gaza Strip	99	157	788	2,227	7,449	98,966	109,686
Remaining West Bank	67	118	600	1,595	5,203	70,056	77,639
Jenin	1	7	45	144	445	10,491	11,133
Tubas	0	0	3	11	73	1,583	1,670
Tulkarm	2	8	47	84	325	5,684	6,150
Nablus	12	26	73	261	948	12,547	13,867
Qalqilya	2	0	24	67	217	3,569	3,879
Salfit	0	1	5	37	111	2,014	2,168
Ramallah and Al-Bireh	26	40	161	328	1,018	9,512	11,085
Jericho and the Jordan Valley	1	1	21	24	105	1,075	1,227
Jerusalem	2	5	31	97	299	3,694	4,128
Bethlehem	8	17	77	182	449	5,152	5,885
Hebron	13	13	113	360	1,213	14,735	16,447
Gaza Strip	32	39	188	632	2,246	28,910	32,047
North Gaza	2	5	25	86	292	4,367	4,777
Gaza	23	26	105	375	1,181	11,692	13,402
Deir al-Balah	4	0	24	53	239	4,121	4,441
Khan Yunis	3	4	22	65	321	5,320	5,735
Rafah	0	4	12	53	213	3,410	3,692

MSMEs are well-known for their agility, flexibility, and capacity to propel local economies. They are frequently incubators for entrepreneurship and innovation, promoting economic growth and development. These businesses operate in various industries, including manufacturing, services, commerce, and agriculture, and contribute considerably to the GDP of many countries.

Governments and politicians frequently realize the value of MSMEs and develop measures to help them thrive. These policies include financial incentives, loan access, technology assistance, and capacity-building initiatives. Furthermore, measures that promote ease of doing business, streamline regulatory processes, and establish a friendly business climate are critical for the long-term success of MSMEs.

Despite their economic importance, MSMEs confront various hurdles, including restricted access to capital, technology, markets, and trained labor. Addressing these issues is critical to releasing MSMEs' full potential and ensuring their resilience in a fast-changing global business context.

Concerning Palestine [6], Micro and small enterprises (MSMEs) in Palestine face several significant challenges, including difficulty in accessing finance due to stringent bank requirements, political instability creating an uncertain business environment, and a lack of clear regulatory and legal frameworks. Additionally, MSMEs struggle with market access and competition, inadequate infrastructure and technology, and insufficient vocational training and skills development programs. Addressing these issues requires coordinated efforts from the government, financial institutions, and international organizations to foster a more supportive environment for the growth and sustainability of MSMEs in Palestine. MSMEs are frequently supported and promoted as part of economic development efforts. This aid may include financial assistance, market access, training programs, and other tools to help small businesses succeed [7] [8] [9].

In conclusion, MSMEs constitute the backbone of many economies, contributing significantly to job creation, economic diversity, and overall growth. Recognizing and resolving MSMEs' needs and concerns is critical to maintaining a vibrant and inclusive economic climate.

1.2. Cybersecurity Framework Introduction

A cybersecurity framework is a structured collection of standards and best practices designed to help businesses effectively manage and enhance their cybersecurity stance. These frameworks provide a methodical approach to identifying, safeguarding, responding to, and rebounding from cybersecurity issues. They are required for enterprises to have a solid and robust cybersecurity foundation. Here are a few examples of well-known cybersecurity frameworks [10]:

- NIST (National Institute of Standards and Technology): The Cybersecurity Framework (CSF), developed by the National Institute of Standards and

Technology (NIST), adopts a risk-based methodology. It comprises five key functions: identification, protection, detection, response, and recovery.

- ISO/IEC 27001:2005: This standard for Information Security Management Systems (ISMS) was created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It offers a systematic approach to handling sensitive firm information while assuring its security, integrity, and availability.
- Critical Information Security Controls (CIS Controls): Critical Security Controls are a set of best practices provided by the Center for Internet Security (CIS). These measures are intended to give precise and practical methods for countering the most prevalent cybersecurity risks.
- Control Objectives for Information and Related Technologies (COBIT): COBIT, developed by the Information Systems Audit and Control Association (ISACA), offers a comprehensive governance and management strategy for business IT.
- C2M2 (Cybersecurity Capability Maturity Model): C2M2 is a model developed by the US Department of Energy that assists companies in assessing and improving their cybersecurity capabilities. It focuses on various topics, such as risk management, situational awareness, and incident response.
- Model of Zero Trust Security: While not a standard framework, the Zero Trust concept is gaining prominence. It is designed with the notion that dangers can exist within and outside a network, and tight access controls are enforced regardless of the user's location [11].

- Frameworx: Frameworx is a security framework for the telecommunications sector developed by TM Forum. It handles various information security issues, including threat intelligence and incident response [12].

Organizations should examine their unique sector, legal needs, and risk profile while creating a cybersecurity strategy. Parts from several frameworks may need to be combined to develop a tailored and effective cybersecurity strategy. A robust cybersecurity architecture requires regular upgrades and flexibility to change threats.

1.3. Objectives

The primary objective of this research is to develop a tailored Cybersecurity Framework specifically designed for Micro, Small, and Medium Enterprises (MSMEs) in Palestine. This framework aims to address the unique operational challenges, resource constraints, and cybersecurity needs that these businesses face in an increasingly digital environment.

To achieve this, the research will begin with a thorough assessment of the current cybersecurity postures within Palestinian MSMEs. This will involve conducting surveys and interviews to establish a baseline understanding of existing practices and vulnerabilities, thereby identifying areas that require improvement. Incorporating best practices and relevant international cybersecurity standards is another key objective. The framework will be designed to align with global benchmarks while remaining adaptable to the local context, ensuring that it meets the specific needs of Palestinian MSMEs. Additionally, the research aims to enhance cybersecurity awareness and training among employees of these enterprises. Targeted training programs and awareness campaigns will be developed to educate staff about cybersecurity threats, preventive measures, and the importance of maintaining robust security practices.

The effectiveness of the proposed Cybersecurity Framework will be evaluated through its implementation in selected MSMEs. This evaluation will utilize qualitative and quantitative

metrics to assess improvements in threat detection, incident response, and overall cybersecurity posture. Furthermore, the research seeks to foster collaboration among MSMEs by promoting information sharing and collective cybersecurity efforts. This collaborative approach will enable these enterprises to better defend against cyber threats and enhance their overall resilience. Ultimately, this research aims to contribute to the economic stability and growth of the Palestinian economy. By equipping MSMEs with the necessary tools and knowledge to navigate the digital landscape securely, the framework will help create an environment conducive to innovation and development, thereby supporting the broader objectives of job creation and poverty alleviation in the region.

1.4. Contribution

This research significantly contributes to the field of cybersecurity by developing a customized Cybersecurity Framework specifically for Micro, Small, and Medium Enterprises (MSMEs) in Palestine. It addresses the unique challenges faced by these enterprises, which are often overlooked in broader discussions. By integrating local economic, cultural, and political contexts, the framework offers practical solutions that are relevant and sustainable for Palestinian MSMEs. A key aspect of this research is its emphasis on capacity building through targeted training programs and awareness initiatives. By empowering employees with the necessary knowledge and skills to recognize and respond to cybersecurity threats, the study fosters a culture of cybersecurity awareness within these organizations. Additionally, the framework promotes collaboration and information sharing among MSMEs, encouraging a collective approach to cybersecurity that enhances overall resilience.

Ultimately, this research supports the broader goals of economic stability and growth in Palestine. By equipping MSMEs with effective cybersecurity strategies, it helps protect digital

assets, ensure business continuity, and create an environment conducive to innovation and development, thereby contributing to job creation and poverty alleviation in the region.

1.5. Overview

The remaining sections of this thesis are structured as follows: Chapter 2 provides a comprehensive literature review, synthesizing and critically analyzing existing publications on MSMEs, cybersecurity, key themes, and cybersecurity frameworks. This chapter aims to establish a solid theoretical foundation by examining relevant works and identifying research gaps. In Chapter 3, an exploratory data analysis is conducted, utilizing visual representations to uncover correlations within the dataset and derive significant insights. This analysis aims to provide a deeper understanding of the data collected from surveys and interviews. Chapter 4 outlines the proposed design of the Security Framework tailored for MSMEs in Palestine. This chapter details the envisioned framework, explaining its components and how it addresses the specific cybersecurity needs of Palestinian MSMEs. Chapter 5 presents the results and evaluation of the study, discussing the implementation of the proposed framework, its effectiveness, and feedback from stakeholders. The evaluation assesses the framework's impact on cybersecurity practices in MSMEs. Finally, Chapter 6 concludes the study and outlines directions for future research. This chapter summarizes the key findings, discusses the implications, and suggests areas for further investigation to continue improving cybersecurity in MSMEs.

Chapter Two

2. Literature Review

This chapter provides a thorough examination of the relevant literature on thesis topics pertaining to MSMEs, Cybersecurity, Key Themes in Cybersecurity, and Cybersecurity frameworks.

2.

2.1. Background

MSMEs are defined as establishments that maintain a certain income level or provide a certain level of service to their employees. Although small, they play a vital role in the economy and are known to stimulate various economic activities. The budget constraints and the absence of awareness of the importance of the Cybersecurity Framework for CEOs and employees often prevent the departments responsible for information technology from performing their duties. This causes them to rely on cloud services such as The Cloud, which increases their security risk. Cybercriminals are also gaining access to sensitive information about companies and their employees.

The following sections are organized: section 2.2 will talk about MSMEs, section 2.3 will explain the meaning of Cybersecurity, section 2.4 will introduce the most famous Cybersecurity frameworks, and lastly, section 2.5 will talk about some case studies about Cybersecurity.

2.2. MSMEs

Companies have various information technology requirements depending on their size, typically classified as micro, small, medium, or large based on employee and revenue characteristics. According to Gartner [13]. A midsize enterprise is defined as an organization with a yearly income of $50 million to $1 billion. But in Palestine [14], the Palestine Monetary Authority

(PMA) circular 53 defined MSMEs with less than 25 workers and yearly sales of less than 7 million USD [15]. Furthermore, MSMEs account for 99% of businesses in Palestine [16].

In addition, MSME CEOs often need more awareness of the importance of the Cybersecurity Framework in their facilities because they do not expect their company to be attacked from the outside, so they often use fewer protection strategies. Their employees have no training, and there have been no policy modifications that defend against data breaches. There is a need for security at every level in everything that MSMEs do, including how they and their workers use smart devices [17].

2.3. Cybersecurity

Cybersecurity is a set of strategies and processes for defending computers, networks, databases, and applications against assaults, illegal access, modification, or destruction. It's also known as electronic data security or data innovation security [18]. A widely accepted and important definition of cybersecurity is provided by the Cybersecurity and Infrastructure Security Agency (CISA) [19]: "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." This definition emphasizes three key principles:

- Confidentiality: Ensuring that information is accessible only to those authorized to have access.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorized users have access to information and associated assets when required.

An attack, such as a data breach, might have disastrous consequences for the company. It might harm the company's market reputation and potential business partners if information like

licenses, source files, and the protected invention is lost. Furthermore, a data breach can hurt business profits. With major data breaches becoming newsworthy, businesses must embrace and implement a robust Cybersecurity strategy.

In Palestine, several steps have been taken to enhance information security and data protection. Among these steps are:

- Regulatory Laws:
    - Cabinet Decision No. (5) of 2021 [20]: The amended information security policy was approved, aiming to regulate and protect digital data and information in Palestine.
    - Intellectual Property Laws [21]: These include the protection of digital works from piracy and electronic infringement, which enhances information security at both individual and institutional levels.
- Regulatory Standards:
    - Palestinian Monetary Authority [22]: Monitors financial institutions and ensures their compliance with information security standards. It conducts periodic audits to ensure compliance with international standards such as PCI-DSS.
    - Ministry of Telecommunications and Information Technology [23] [24]: Oversees the telecommunications and information technology sector and works on setting policies and procedures necessary to protect data.
    - International Cooperation [25]: Palestine works to keep up with international standards in the field of information security, enhancing its ability to protect digital data and information.

- Use of Advanced Technologies: Such as Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor networks and detect any abnormal activity.
- Security Audits: Conducting periodic security audits to assess vulnerabilities in systems and networks.
- Awareness Programs: Organizing awareness and training campaigns for employees and the public on the importance of information security and how to protect personal data.

Despite the efforts made, there are still significant challenges facing Palestine in the field of information security, including a lack of resources and advanced technologies. Therefore, it is essential to enhance international cooperation and develop the technical and legal infrastructure to effectively address these challenges. Fabio Cristiano's paper "Palestine: Whose Cyber Security Without Cyber Sovereignty?" [26] examines the interplay between cybersecurity and sovereignty in Palestine. It discusses the monopoly of Hadara in the Palestinian internet market, the adverse effects of Israeli occupation on telecommunications, and the limited regulatory power of the Palestinian Authority (PA). The PA's 2018 cybercrime law, intended to protect national unity, also enforces censorship and surveillance. The document highlights the conflict between security measures and digital rights, explores the concept of cyber sovereignty, and addresses Hamas's involvement in cyber operations. It concludes with recommendations for a national strategy to improve digital rights and tackle the challenges of occupation, advocating for a comprehensive approach to cybersecurity amidst political and territorial conflicts.

2.4. Cybersecurity Key Themes

The Council of Professors and Heads of Computing (CPHC) [27] and International Information System Security Certification Consortium (ISC2) [28], The world's largest not-for-profit

membership organization of trusted information and software security professionals, recently convened a diverse panel of industry and academic experts. Together, they pinpointed crucial cybersecurity concepts and themes that can be integrated as best practice [29]:

1. Risk and Information: Information is an organizational asset with utility and value and can be classified to reflect its importance to an organization or individual. It is vulnerable to threats in systems because it has attributes such as confidentiality, possession or control, integrity, authenticity, availability, and utility, all of which can make it vulnerable to attack (for example, legal and regulatory drivers, customer rights, or organization objectives), It has a lifespan – from creation to deletion – and protection may be necessary at any point throughout that time, information risk management is a word that refers to the process of recording what information is at risk, the type and amount of risk that has been realized, and the consequences of that realization.

2. Assaults and threats: Information, services, and systems are vulnerable to various threats. Understanding the technical and sociological viewpoints, how assaults operate, and the technologies and tactics employed are critical to defending against them [30].

3. Cybersecurity operations and architecture: Information, services, and systems are protected through various technical and procedural activities frequently grouped into a framework. The framework will include technological and logical controls and physical and process controls that may be deployed across an organization to decrease information and system risk, detect and mitigate vulnerability, and meet compliance requirements. Also, controls can be classified and chosen based on their classification. When technical controls are unavailable, additional controls can be selected, and technological controls (such as encryption, access management, anti-virus software, firewalls, and intrusion prevention systems) are detailed and need extensive

knowledge. The job of forensics and investigations is to figure out how an assault was carried out and how to help with inquiries [31].

4. Secure systems and products [32]: This subject analyzes incorporating security into a system (such as an individual service, application, server, network device, laptop, smartphone, or network, or combinations thereof). It examines the ideas of design, defensive programming, and testing and how to use them to create strong, resilient, and fit-for-purpose systems [33].

5. Cybersecurity management: Comprehending the personal, organizational, and legal/regulatory contexts in which information systems may be utilized, the dangers associated with such usage, and the restrictions (time, money, and people) that may impact how cybersecurity is implemented.

2.5. Cybersecurity Frameworks:

A cybersecurity framework is a collection of standards, precepts, and recommended procedures for handling risks in the online world. They often connect security measures, like requiring a login and password, with security goals, such as prohibiting unauthorized system access [34]. Cybersecurity frameworks are typically needed for businesses that want to adhere to national, industry, and international requirements for cybersecurity or are at the absolute least strongly encouraged to do so. For example, a company must pass an audit demonstrating compliance with the Payment Card Industry Data Security Standards (PCI DSS) framework to process credit card transactions.

Various variables can influence the decision to choose a specific Cybersecurity framework. If your company handles credit cards, you must comply with the PCI/DSS rules. You must comply with the Health Insurance Portability and Accountability Act (HIPAA) requirements if you take electronic Personal Health Information (ePHI). If you're working with the federal government, start with NIST 800-53. Publicly listed corporations will likely choose COBIT to comply with

Sarbanes Oxley (SOX) more easily. Even though the implementation procedure is long and complicated, and the certification process is complex, ISO 2700x is a good choice for a more mature security company since it applies to any industry.

2.5.1. National Institute of Standards and Technology (NIST):

The NIST Cybersecurity Framework (the Framework) serves as the cornerstone of the US government's strategy to enhance the security and resilience of critical infrastructure. It aims to foster a cyber environment that fosters efficiency, innovation, and economic prosperity while safeguarding safety, security, business confidentiality, privacy, and civil liberties.

Here is a summary of the controls used in NIST as follows:

- Identification and Authentication (IA): IA controls are tailored to an organization's unique identification and authentication policies. This encompasses verifying the identities of internal and external users and overseeing the administration of these systems.
- Configuration Management (CM): The configuration management policies of an organization determine the CM controls. This provides a base configuration to be the foundation for further information system builds and modifications. This also comprises security impact analysis controls and inventories of the components of information systems.
- Contingency Planning (CP): The CP control family provides controls particular to a company's backup plan in the case of a cybersecurity incident. This includes safeguards, testing, upgrading, training, backups, and system reconstitution for contingency plans.
- Incident Response (IR): IR policies and procedures are particular to an organization's incident response practices. This covers incident response planning, training, testing, monitoring, and reporting.

- Maintenance (MA): The MA controls in NIST revision five provide specific instructions for sustaining tools and organizational systems.
- Media Protection (MP): The controlling family for media protection includes measures for access, marking, storage, transit regulations, sanitization, and specified organizational media usage.
- Personnel Security (PS): PS controls refer to the methods a business uses to safeguard its employees, including access agreements, personnel screening, termination, and position risk.
- Protection of the Physical Environment (PE): To defend against physical dangers, the Physical and Environmental Protection control family is installed on systems, buildings, and relevant supporting infrastructure. Material access authorizations, surveillance, visitor logs, emergency shutoffs, electricity, lighting, fire prevention, and water damage protection are a few of these controls.
- Planning (PL): The PL controls in NIST are particular to the security planning policies of an organization and must consider the goal, scope, roles, and duties, management commitment, coordination between entities, and organizational compliance.
- Program Management (PM): The PM control family is crucial for overseeing and managing your cybersecurity program. It encompasses key components such as a critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture. These elements are essential for ensuring the security and effectiveness of your cybersecurity program.
- Risk Assessment (RA): The RA control family pertains to a company's vulnerability scanning tools and risk assessment procedures. Your NIST compliance processes may

be streamlined and automated using an integrated risk management system like Cyber Strong.

- Security Assessment and Authorization (CA): Controls that facilitate the implementation of security assessments, authorizations, continuous monitoring, plans of action and milestones, and system interconnections are encompassed within the Security Assessment and Authorization control family.
- System and Communications Protection (SC): Procedures for safeguarding systems and communications fall within the jurisdiction of the SC control family. This encompasses boundary protection, information encryption, secure collaborative computing devices, cryptographic measures, defense against denial-of-service attacks, and more.
- System and Information Integrity (SI): The family of System and Information Integrity (SI) controls is designed to protect the integrity of data and systems. One of the key members of this control family is NIST SI 7, which focuses on fault rectification, protection against malicious code, system monitoring, security warnings, software and firmware integrity, and spam protection.
- System and Services Acquisition (SA): The SA control family is related to controls safeguarding allotted resources and an organization's system development life cycle. This comprises developer security testing and assessment controls, development configuration management controls, and controls over information system documentation.
- The Framework has been adopted by almost half of all SMEs with 250 or more workers. [35]The research discovered that the most important aspects were decision-making utility, a proxy for cybersecurity efficacy, addressing liability, and consistent risk management communication [36].

The foundation of the architecture is a set of Cybersecurity functions that follow the fundamental cyber defense pattern of identifying, defending, detecting, responding, and recovering. The framework establishes a method for identifying risks and assets that must be safeguarded. It outlines how the company must protect these assets by recognizing risks, responding to threats, and recovering assets in the case of a security breach.

2.5.2. The Information Technology Infrastructure Library (ITIL):

ITIL is a set of guidelines for delivering IT services. ITIL's systematic approach to IT service management may assist organizations in managing risk, strengthening customer relationships, establishing cost-effective procedures, and creating a stable IT environment that allows for growth, scale, and change [37]. Because specific and more extensive standards are available, ITIL only describes some areas of Information Security Management. Conversely, ITIL emphasizes the most critical tasks and aids in identifying connections with other Service Management procedures [38].

The following advantages are provided by ITIL, which gives a systematic and expert approach to the administration of IT service provision [39]:

- lower IT expenses.
- better IT services utilizing tried-and-true best practices.
- increased client satisfaction due to a more skilled method of service delivery.
- Guidelines and standards.
- increased output.
- better utilization of knowledge and expertise.
- improved provision of third-party services by specifying ITIL or BS15000 as the benchmark for service delivery in service procurements.

2.5.3. The Saudi Arabian Monetary Authority (SAMA) Framework:

The SAMA Cyber Security Framework is a vital tool for financial institutions in Saudi Arabia, providing a structured approach to managing cybersecurity risks. By aligning with international standards and emphasizing governance, risk management, and continuous improvement, it helps institutions build a resilient and secure digital environment.

Global Cybersecurity Index 2020 (GCI) is a composite index developed, researched, and published by the International Telecommunication Union (ITU), a United Nations specialized agency. It assesses the 194 member nations' commitment to Cybersecurity to improve cybersecurity awareness. Saudi Arabia has been ranked second in the world, with the United Kingdom (with 99.54 points), among countries devoted to global cybersecurity (ITU), as shown in Figure 2.1, also the first among the Arab States region [40].

Country Name	Score	Rank
United States of America**	100	1
United Kingdom	99.54	2
Saudi Arabia	99.54	2
Estonia	99.48	3
Korea (Rep. of)	98.52	4
Singapore	98.52	4
Spain	98.52	4
Russian Federation	98.06	5
United Arab Emirates	98.06	5
Malaysia	98.06	5

Country Name	Score	Rank
Indonesia	94.88	24
Viet Nam	94.59	25
Sweden	94.55	26
Qatar	94.5	27
Greece	93.98	28
Austria	93.89	29
Poland	93.86	30
Kazakhstan	93.15	31
Denmark	92.6	32
China	92.53	33
Croatia	92.53	33

Figure 2.5.3: Global score and rank [40].

The Saudi Arabian Monetary Authority (SAMA) Cyber Security Framework is a comprehensive set of guidelines designed to enhance cybersecurity practices within financial institutions operating in Saudi Arabia. Here’s a detailed overview:

Objective: The framework aims to support regulated entities in establishing robust cybersecurity governance and infrastructure, along with necessary preventive and detective controls.

Scope: It applies to all financial institutions regulated by SAMA, including banks, insurance companies, and finance companies.

Flexibility: The framework is principle-based, allowing institutions to adopt a common approach while tailoring specific controls to their unique environments.

Alignment with Standards: It aligns with international standards such as NIST, ISO/IEC 27001, and PCI-DSS, ensuring a comprehensive and globally recognized approach to cybersecurity.

Core Components [41]:

- Cybersecurity Governance:
    - Board and Senior Management Involvement: Emphasizes the importance of oversight and support from the Board of Directors and senior management.
    - Policies and Procedures: Requires the establishment of comprehensive cybersecurity policies and procedures.
- Risk Management:
    - Risk Assessment: Mandates regular risk assessments to identify and mitigate cybersecurity risks.
    - Risk Treatment: Institutions must implement appropriate risk treatment plans based on the identified risks.
- Cybersecurity Controls:
    - Preventive Controls: Includes measures such as access control, encryption, and secure software development practices.
    - Detective Controls: Focuses on monitoring, logging, and incident detection capabilities.

    - Corrective Controls: Involves incident response, recovery, and business continuity planning.
- Third-Party Management:
    - Vendor Risk Management: Requires institutions to assess and manage cybersecurity risks associated with third-party service providers.
- Awareness and Training:
    - Employee Training: Mandates regular cybersecurity awareness training for all employees.
    - Awareness Programs: Encourages the development of programs to promote a culture of cybersecurity within the organization.

2.5.4. The Center for Internet Security (CIS):

The Center for Internet Security (CIS) is a nonprofit organization founded in October 2000. Its mission is to make the connected world a safer place by developing, validating, and promoting best practice solutions to help people, businesses, and governments protect themselves against pervasive cyber threats [42]. The CIS Controls are a short set of high-priority, highly effective defensive activities that serve as a "must-do, do-first" starting point for any company looking to strengthen its cybersecurity [43].

Key Components of CIS [44]:

- CIS Controls: A set of best practices for securing IT systems and data against cyber threats, developed through a global community of IT professionals, focuses on actionable steps to improve cybersecurity posture.
- CIS Benchmarks: Configuration guidelines for securing IT systems, covers over 100 configuration guidelines across more than 25 vendor product families, helps organizations implement and manage their cyber defenses effectively.

- CIS Hardened Images: Secure, on-demand, scalable computing environments in the cloud. pre-configured to meet CIS Benchmarks, providing a secure foundation for cloud deployments.
- Multi-State Information Sharing and Analysis Center (MS-ISAC): A resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, provides a collaborative environment for sharing cybersecurity information and best practices.
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC): Supports the cybersecurity needs of U.S. elections offices. focuses on protecting the integrity of election systems and processes.

2.5.5. BASEL:

The Basel Framework is a collection of rules established by the Basel Committee on Banking Supervision (BCBS), the leading global organization responsible for setting standards for bank regulation. All members of the BCBS have unanimously committed to fully adopting these standards and applying them to their globally operating banks.

The framework also has the following features [45]:

1. Cross-references that are interactive to make navigation simpler.
2. The ability to "time travel" allows you to choose a future period and view the framework as it will be implemented.
3. Frequently Asked Questions (FAQs) are addressed beneath the relevant paragraphs.
4. A place where you may see all the Basel Framework's previous and upcoming modifications.
5. A better search tool that makes locating particular text in each standard more straightforward.

The following 14 standards shown below make up the framework. Each standard is broken down into chapters, and many of these chapters have numerous iterations. For instance, a chapter can contain iterations that are current right now and those that will be applicable when Basel III changes have been put in place.

Acronym	Standard names
SCO	Scope and definitions
CAP	Definition of capital
RBC	Risk-based capital requirements
CRE	Calculation of RWA for credit risk
MAR	Calculation of RWA for market risk
OPE	Calculation of RWA for operational risk
LEV	Leverage ratio
LCR	Liquidity Coverage Ratio
NSF	Net Stable Funding Ratio
LEX	Large exposures
MGN	Margin requirements
SRP	Supervisory review process
DIS	Disclosure requirements
BCP	Core Principles for Effective Banking Supervision

Figure 2.5.5: Structure of the Basel Framework [45].

2.5.6. Control Objectives for Information and Related Technologies (COBIT):

COBIT, established by the Information Systems Audit and Control Association (ISACA), is an IT management framework that aids enterprises in formulating, coordinating, and executing information management and governance strategies.

COBIT was first announced in 1996 and was created as a collection of IT control objectives to aid the financial audit community in navigating the rise of IT systems. The ISACA issued version 2 in 1998, which broadened the framework's application outside the auditing community [46]. Later, in the 2000s, the ISACA created version 3, which included the IT management and information governance methodologies used in the framework today.

Manage risk (APO12), Manage security (APO13), and Manage security services (DSS05), three crucial COBIT processes for information security, provide a risk-based strategy to protect company resources against a variety of threats and vulnerabilities [46]. Before implementing measures to manage and control potential risks, it is important to identify and analyze them as part of an effective security strategy. This process is typically known as risk management. The next step is to create a thorough security program with specific controls designed for the most vulnerable resources and assets. These crucial steps are necessary for achieving successful security outcomes, particularly as the threat landscape becomes increasingly complex and evolving.

Within the field of information security, COBIT for Information Security functions as a further development of the basic framework, providing practical advice on information security processes in a corporate environment. It also offers a wide range of additional information, covering service capabilities, policies, principles, and organizational structures tailored to security, as well as security skills and competencies.

COBIT 2019 has been revised, according to the ISACA, to include [46]:

I. Focus areas and design aspects that help you create a governance system that meets your company's demands.

ii. To improve the framework's relevance, it should be more aligned with worldwide standards, frameworks, and best practices.

iii. An open-source paradigm that encourages faster updates and improvements by allowing feedback from the global governing community.

iv. On a rolling basis, updates are published regularly.

v. More tools and recommendations to help organizations design a "best-fit governance framework," making COBIT 2019 more prescriptive.

vi. A better tool for measuring IT performance and compliance with the CMMI.

vii. More decision-making assistance, including new online collaboration features.

2.5.7. Authentication, Authorization, and Accounting (AAA):

The AAA (Authentication, Authorization, and Accounting) concept is best described as a framework rather than a single standard [47]. It provides a structured approach to managing network security and access control, it is implemented through various protocols and standards, each serving specific purposes within network security. These protocols and standards collectively enable the implementation of the AAA framework across different systems and networks, ensuring secure and efficient access control.

Authentication [48]: This procedure checks a user's, device's, or system's identity while seeking to access a network or resource. It validates that the entity seeking access is who it says it is. Passwords, biometrics, smart cards, and multi-factor authentication are common authentication mechanisms.

Authorization [49]: specifies the level of access or permissions allowed once a user or system has been authenticated. It determines which resources or activities the authorized entity may access or accomplish. Authorization is frequently based on system-configured roles, privileges, or regulations.

Accounting [50]: entails monitoring and logging the activity of authorized individuals or systems. This procedure aids in auditing, monitoring, and analyzing network resource utilization. Accounting data can help spot security problems, track user activity, and verify policy compliance.

The AAA framework was not created by a single entity but rather evolved over time through contributions from various organizations and standards bodies in the field of network security. Key contributors include:

- Internet Engineering Task Force (IETF) [51] [47]: The IETF has developed several protocols and standards related to AAA, such as RADIUS (Remote Authentication Dial-In User Service) and Diameter [52].
- Telecommunications Industry Association (TIA) [47]: The TIA has also contributed to the development of AAA standards, particularly in the context of telecommunications.
- Various Technology Companies: Companies like Cisco [53], Microsoft, and others have implemented AAA mechanisms in their products and contributed to the development of best practices and protocols.

These contributions have collectively shaped the AAA framework into a fundamental component of network security and access control systems.

2.5.8. Comparative Analysis of Cybersecurity Frameworks:

To understand the landscape of cybersecurity frameworks and facilitating a better understanding of their unique characteristics and applications, a comparative analysis was conducted. Table 2.5.8 provides a summary of key frameworks, highlighting their definitions, historical development, organizational nature, and controls:

Table 2.5.8: Comprehensive overview of the key cybersecurity frameworks.

Framework	Brief Definition	Historical Overview	For Profit or Non-Profit	Issuing/Supervising Body	Country of Origin	Governmental or Independent	Controls
NIST	Provides guidelines for managing and reducing cybersecurity risk	Developed by the National Institute of Standards and Technology in 2014	Non-Profit	National Institute of Standards and Technology (NIST)	USA	Governmental	Identify, Protect, Detect, Respond, Recover
ITIL	Framework for IT service management	Developed by the UK government in the 1980s, now managed by Axelos	For Profit	Axelos	UK	Independent	Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement
SAMA	Cybersecurity framework for the Saudi financial sector	Developed by the Saudi Arabian Monetary Authority in 2017	Non-Profit	Saudi Arabian Monetary Authority (SAMA)	Saudi Arabia	Governmental	Cybersecurity Governance, Risk Management, Cybersecurity Operations, Third-Party Risk Management
CIS	Provides a set of best practices for securing IT systems and data	Developed by the Center for Internet Security in 2000	Non-Profit	Center for Internet Security (CIS)	USA	Independent	Basic, Foundational, Organizational Controls
Basel	Framework for banking supervision and risk management	Developed by the Basel Committee on Banking Supervision in 1988	Non-Profit	Basel Committee on Banking Supervision	Switzerland	Independent	Minimum Capital Requirements, Supervisory Review, Market Discipline
COBIT	Framework for IT governance and management	Developed by ISACA in 1996	Non-Profit	ISACA	USA	Independent	Governance, Management, Planning and Organization, Acquisition and Implementation, Delivery and Support, Monitoring and Evaluation
AAA	Framework for network security and access control	Evolved over time through contributions from various organizations	Non-Profit	Various (IETF, TIA, etc.)	Various	Independent	Authentication, Authorization, Accounting

2.6. Cybersecurity Standards:

2.6.1. International Organization for Standardization (ISO/IEC 27000 family):

The internationally recognized benchmark for Cybersecurity is ISO 27001/27002, also referred to as ISO 27K. The ISO/IEC 27000 family of standards provides a comprehensive framework for managing information security risks. Here's a detailed description and comparison of the key standards within this family, focusing on cybersecurity and security:

1. ISO/IEC 27000:2018 [54]

Description: Provides an overview and vocabulary for the ISMS family of standards.

Purpose: Establishes the fundamental concepts and definitions used throughout the ISO/IEC 27000 series.

Key Features: Definitions of terms and concepts related to information security management.

2. ISO/IEC 27001:2022 [55]

Description: Specifies requirements for establishing, implementing, maintaining, and continually improving an ISMS.

Purpose: Provides a systematic approach to managing sensitive company information so that it remains secure.

Key Features: Risk assessment, control implementation, continuous monitoring, and improvement.

Certification: Organizations can be certified to ISO/IEC 27001.

3. ISO/IEC 27002:2022 [56]

Description: Provides guidelines for organizational information security standards and information security management practices.

Purpose: Offers a reference set of generic information security controls, including implementation guidance.

Key Features: Detailed controls for information security, including access control, cryptography, physical security, and incident management.

4. ISO/IEC 27003:2017 [57]

Description: Provides guidance on the implementation of an ISMS.

Purpose: Helps organizations understand how to implement ISO/IEC 27001.

Key Features: Implementation phases, project planning, and resource allocation.

5. ISO/IEC 27004:2016 [58]

Description: Provides guidelines on monitoring, measurement, analysis, and evaluation of an ISMS.

Purpose: Helps organizations measure the effectiveness of their ISMS and improve it over time.

Key Features: Metrics, performance indicators, and measurement techniques.

6. ISO/IEC 27005:2018 [59]

Description: Provides guidelines for information security risk management.

Purpose: Supports the implementation of information security based on a risk management approach.

Key Features: Risk assessment, risk treatment, risk acceptance, and risk communication.

7. ISO/IEC 27006:2024 [60]

Description: Specifies requirements for bodies providing audit and certification of ISMS.

Purpose: Ensures that certification bodies are competent to audit and certify ISMS.

Key Features: Auditor qualifications, audit processes, and certification requirements.

8. ISO/IEC 27017:2015 [61]

Description: Provides guidelines for information security controls applicable to the provision and use of cloud services.

Purpose: Enhances the security of cloud services by providing additional controls.

Key Features: Cloud-specific security controls, shared responsibility model, and cloud service agreements.

9. ISO/IEC 27018:2019 [62]

Description: Focuses on the protection of personal data in the cloud.

Purpose: Provides guidelines for implementing measures to protect personal data in cloud environments.

Key Features: Data protection principles, data subject rights, and data breach management.

10. ISO/IEC 27019:2017 [63]

Description: Provides guidelines for information security management in the energy sector.

Purpose: Addresses specific security needs of the energy sector, including power generation, transmission, and distribution.

Key Features: Sector-specific controls, risk management, and incident response.

The Plan-Do-Check-Act (PDCA) cycle is a fundamental part of ISO/IEC 27001, providing a structured approach to implementing, maintaining, and continually improving an Information Security Management System (ISMS) as shown in the figure below:

Figure 2.6.1: PDCA Cycle [64]

Here’s a detailed outline and description of the PDCA cycle in the context of ISO/IEC 27001 [64]:

1. Plan

Objective: Establish the ISMS policy, objectives, processes, and procedures relevant to managing risk and improving information security.

Context of the Organization: Understand the internal and external issues that can affect the ISMS (Clause 4).

Leadership: Define leadership roles, responsibilities, and commitments (Clause 5).

Risk Assessment: Identify and assess information security risks (Clause 6).

Security Controls: Select appropriate security controls to mitigate identified risks (Clause 6).

Resources and Competence: Determine necessary resources and ensure personnel are competent (Clause 7).

2. Do

Objective: Implement and operate the ISMS policy, controls, processes, and procedures.

Implementation: Execute the planned processes and controls (Clause 8).

Training and Awareness: Ensure staff are trained and aware of their roles in information security (Clause 7).

Operational Controls: Implement operational controls to manage information security risks (Clause 8).

3. Check

Objective: Monitor and review the performance and effectiveness of the ISMS.

Performance Evaluation: Monitor, measure, analyze, and evaluate the ISMS performance (Clause 9).

Internal Audit: Conduct internal audits to assess the ISMS (Clause 9).

Management Review: Review the ISMS at planned intervals to ensure its continuing suitability, adequacy, and effectiveness (Clause 9).

4. Act

Objective: Take actions to continually improve the ISMS.

Corrective Actions: Address nonconformities and take corrective actions (Clause 10).

Continual Improvement: Identify opportunities for improvement and implement necessary changes (Clause 10).

2.6.2. ISO 31000 (Risk Management - Guidelines)

It establishes risk management concepts, a framework, and a procedure. Any organization can benefit from this versatile tool regardless of size, industry, or sector. Businesses can optimize their operational performance by enhancing the likelihood of achieving goals, identifying opportunities and risks, and efficiently managing resources for risk mitigation. It cannot be used for certification, but it can be used to guide internal or external auditing procedures. It allows organizations to evaluate risk management strategies to a globally recognized standard, resulting in solid management and corporate governance principles.

When applying ISO 31000 to cybersecurity, the same principles and processes can be followed, with a focus on identifying, assessing, and managing cybersecurity risks. Here's how it can be adapted [65]:

Risk Identification: Identify potential cybersecurity threats, vulnerabilities, and impacts on information assets.

Risk Analysis: Analyze the likelihood and impact of identified cybersecurity risks.

Risk Evaluation: Evaluate the risks to determine their significance and prioritize them for treatment.

Risk Treatment: Implement controls and measures to mitigate or eliminate cybersecurity risks.

Monitoring and Review: Continuously monitor the effectiveness of cybersecurity controls and update them as needed.

Communication and Consultation: Ensure all stakeholders are aware of cybersecurity risks and the measures in place to address them.

2.6.3. Standard of Good Practice for Information Security 2020 (SOGP):

The Standard of Good Practice for Information Security 2020 (SOGP 2020), developed by the Information Security Forum (ISF), is a comprehensive framework designed to assist organizations in managing and mitigating information security risks. SOGP 2020 addresses a wide range of information security topics, including both current and emerging threats, technologies, and risks. Its broad scope covers various aspects of cyber resilience, information security, and risk management, making it a versatile tool for organizations of all sizes [66].

The framework provides practical, trusted guidance for implementing security controls and managing information risks. It is designed to integrate good practices with business processes, information security programs, risk management, and compliance arrangements [67]. SOGP 2020 aligns with various external standards such as ISO/IEC 27002, NIST Cybersecurity Framework, and the CSA Cloud Control Matrix, helping organizations consolidate compliance activities into a unified approach [67]. The benefits of SOGP 2020 for organizations are significant. It helps organizations be agile in exploiting new opportunities while managing associated risks. The framework assists in identifying regulatory and compliance requirements and planning how best to meet them. It enhances the ability to respond rapidly to evolving threats, reducing the risk of costly incidents and operational impacts. Additionally, SOGP 2020 reduces the time and effort required to produce information security policies and procedures and incorporates supply chain considerations into a risk-based approach to information security.

It also raises the profile of information security across the organization, fostering a culture of security awareness [67].

Table 2.6.3 has a brief overview of each control with description, as shown below:

Table 2.6.3: controls with description [67].

Core Area	Description
Security Workforce	Focuses on building and maintaining a skilled security workforce.
Cloud Security Controls	Provides guidance on securing cloud environments.
Security Operation Centres (SOCs)	Covers the establishment and operation of SOCs to monitor and respond to security incidents.
Mobile Application Management	Addresses the security of mobile applications.
Asset Registers	Emphasizes the importance of maintaining accurate asset registers.
Security Assurance	Provides guidance on conducting security assurance activities.
Supply Chain Management	Focuses on managing information security risks within the supply chain.
Security Event Management	Covers the processes and technologies for managing security events.

In conclusion, the Standard of Good Practice for Information Security 2020 is a valuable resource for organizations looking to enhance their information security posture. By providing comprehensive, practical guidance and aligning with other major standards, it helps organizations navigate the complex landscape of information security and risk management.

2.6.4. The Payment Card Industry Data Security Standard (PCI DSS):

The PCI DSS is a global payment card industry data security standard. It was designed to guarantee that companies processing card payments were safe and to assist in preventing card fraud. This is accomplished by implementing stringent controls on firms' storage, transport, and processing of cardholder data. PCI DSS was designed by the Payment Card Industry Security Standards Council (PCI SSC). It is designed to safeguard sensitive cardholder information [68].

PCI DSS is organized into six control objectives, which are further divided into 12 requirements as shown in the table below:

Table 2.6.4: PCI DSS requirements [69].

Control Objective	Requirement
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs.
	6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know.
	8. Identify and authenticate access to system components.
	9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

Compliance with PCI DSS involves different validation methods based on the size and transaction volume of the business. Smaller merchants can use the Self-Assessment Questionnaire (SAQ), while larger organizations require an on-site assessment by a Qualified Security Assessor (QSA). Organizations with internal resources can perform assessments through an Internal Security Assessor (ISA) [70]. The benefits of PCI DSS compliance include enhanced security, which protects against data breaches and fraud, increased customer trust by demonstrating a commitment to security, and avoidance of penalties associated with non-compliance. However, implementing and maintaining compliance can be complex and resource-intensive, requiring continuous effort and vigilance.

2.6.5. British Standard 7799 (BS 7799):

The BSI Group (BSI) released the BS 7799 standard in 1995 [71]. It was written by the Department of Trade and Industry of the United Kingdom government (DTI). It laid the groundwork for what would later become the globally recognized ISO/IEC 27000 series of standards. The standard is not free, and its provisions are not open to the public. As a result, particular provisions cannot be mentioned. The standard is described in the publicly accessible BSI abstract: "If organizations want to keep their information safe and secure, they must identify, evaluate, treat, and manage information security threats" [72].

BS 7799 was initially divided into two main parts. BS 7799 Part 1: Code of Practice for Information Security Management provided a comprehensive set of controls comprising best practices in information security management [73]. It included 127 controls organized into 10 sections, each addressing specific security objectives. The controls were designed to be adaptable, allowing organizations to tailor them to their specific needs.

BS 7799 Part 2: Specification for Information Security Management Systems (ISMS), published in 1999, offered a formal specification for establishing, implementing, monitoring, and improving an ISMS [73]. It introduced the Plan-Do-Check-Act (PDCA) cycle, aligning it with quality management standards like ISO 9000.

In 2005, BS 7799 Part 3 was introduced, focusing on information security risk management. It provided guidelines for identifying, analyzing, and mitigating information security risks. This part was later adapted into ISO/IEC 27005 in 2008 [72].

The significance of BS 7799 was recognized internationally, leading to its adoption by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [73]. In 2000, BS 7799 Part 1 was adopted as ISO/IEC 17799, later renumbered to ISO/IEC 27002 in 2007. This standard provides guidelines for organizational

information security standards and information security management practices. BS 7799 Part 2 was adopted as ISO/IEC 27001 in 2005, specifying the requirements for establishing, implementing, maintaining, and continually improving an ISMS.

2.6.6. International Society of Automation (ISA/IEC 62443):

The ISA created the ISA/IEC 62443 standard series to strengthen the security of industrial automation and control systems (IACS) [74]. These standards establish a reliable base for the secure incorporation of industrial automation and control systems.

The ISA/IEC 62443 standards are organized into four main parts, each focusing on different aspects of IACS security. The first part, General, covers topics common to the entire series, including terminology, concepts, and models. The second part, Policies and Procedures, focuses on methods and processes associated with IACS security, such as establishing security programs and managing security risks. The third part, System Requirements, specifies the technical requirements for securing IACS, including system design and implementation. Finally, the fourth part, Component Requirements, addresses the security requirements for individual IACS components, such as devices and software [75].

The ISA/IEC 62443 standards are based on several key principles. One of these is Defense in Depth, which involves implementing multiple layers of security controls to protect IACS from various threats. Another principle is Risk Management, which entails identifying, assessing, and mitigating security risks to ensure the resilience of IACS. Additionally, Security by Design emphasizes integrating security considerations into the design and development of IACS components and systems [76].

2.6.7. Comparative Analysis of Cybersecurity Standards:

To gain a comprehensive understanding of the cybersecurity standards landscape and to better appreciate their unique characteristics and applications, a comparative analysis was performed. Table 2.6.7 summarizes key standards, detailing their definitions, historical development, organizational nature, and controls.

Table 2.6.7: Comparative Analysis of Cybersecurity Standards.

Standard	Brief Definition	Historical Overview	For Profit or Non-Profit	Issuing/Supervising Body	Country of Origin	Governmental or Independent	Criteria	Certification
ISO/IEC 27000 Family	A series of standards for information security management systems (ISMS)	Developed by ISO and IEC, first published in 2005	Non-Profit	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	International	Independent	Context of the Organization, Leadership, Planning, Support, Operation, Performance Evaluation, Improvement	Yes
ISO 31000	Provides guidelines for risk management	Developed by ISO, first published in 2009	Non-Profit	International Organization for Standardization (ISO)	International	Independent	Principles, Framework, Process	No
ISA/IEC 62443	Standards for industrial automation and control systems security	Developed by ISA and IEC, first published in 2007	Non-Profit	International Society of Automation (ISA) and International Electrotechnical Commission (IEC)	International	Independent	General, Policies and Procedures, System, Component	Yes
British Standard 7799	A standard for information security management	Developed by BSI, first published in 1995, later became ISO/IEC 27001	Non-Profit	British Standards Institution (BSI)	UK	Independent	Security Policy, Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Development and Maintenance, Information Security Incident Management, Business Continuity Management, Compliance	Yes (as ISO/IEC 27001)
PCI DSS	Standards for payment card industry security	Developed by PCI Security Standards Council, first published in 2004	Non-Profit	PCI Security Standards Council	USA	Independent	Build and Maintain a Secure Network and Systems, Protect Cardholder Data, Maintain a Vulnerability Management Program, Implement Strong Access Control Measures, Regularly Monitor and Test Networks, Maintain an Information Security Policy	Yes
Standard of Good Practice for Information Security 2020	A comprehensive framework for information security management	Developed by ISF, first published in 1996, updated regularly	Non-Profit	Information Security Forum (ISF)	International	Independent	Security Governance, Security Requirements, Control Framework, Security Monitoring, Security Improvement	No

2.7. Cybersecurity Tools:

2.7.1. The Gordon–Loeb (GL) Model Tool:

The GL Model is an important tool for organizations to evaluate the correct NIST Implementation Tier level and make efficient investments in cybersecurity operations. The results show that the GL Model is a useful approach for assessing the cost-effectiveness of cybersecurity spending, helping organizations make informed decisions about the most appropriate NIST Implementation Tier level. Furthermore, the cost-benefit analysis aids in identifying circumstances in which moving to a higher NIST Implementation Tier is advantageous [77].

2.7.2. The Baldrige Cybersecurity Excellence Builder Tool (Builder):

The Baldrige Cybersecurity Excellence Builder (Builder) is a hybrid Baldrige program and Framework systems methodology. It's a self-evaluation tool that helps businesses better understand and improve the efficacy of their cybersecurity risk assessment activities. The Builder improves the risk assessment process by incorporating the Organizational Context into the Framework Core through a series of questions. The organizational context is a solid basis for risk assessment; further parts of the evaluation can be added [78].

2.7.3. The CET Tool:

The CET tool and recommendation system are examples of executive methods used to assess their existing cybersecurity readiness. This technique will assist in identifying strengths and weaknesses and provide best-practice recommendations for successfully plugging security flaws. In other words, by employing an evaluation approach, IT directors may swiftly identify their most serious flaws, compare their maturity to that of their peers using a set of standard metrics, and select the most beneficial improvement initiatives [79].

Small businesses must act quickly. Every firm surveyed was considerably below the SME CET's suggested level of maturity. Every reasonable effort made to assess the condition of information security and act on recommendations is a positive step forward.

2.7.4. Keep It Simple Tool (KIS):

KIS was first explored in 2017 as part of a local cybersecurity cluster combining government agencies, research institutes, and end-user SMEs [80]. The KIS framework does not prescribe any rigid methodology or criteria as a first step in attaining control over cybersecurity threats; instead, it relies on the capabilities of a pool of cybersecurity specialists. To ensure sufficient help from self-proclaimed experts, a qualification procedure for those experts is implemented before any service is supplied to SMEs.

This restriction is effective because SMEs may only claim financing support through vouchers confined to a pool of certified specialists. These specialists must be able to recognize and handle cybersecurity threats specific to the SME business environment and offer appropriate protective solutions. The following essential abilities must be demonstrated and tested: a suitable level of cybersecurity knowledge and frameworks, the capacity to address all SME-specific cybersecurity concerns, and the ability to conduct organizational and technical audits using a straightforward approach that they may develop themselves [81].

2.7.5. Cybersecurity Coach (CYSEC):

CYSEC enables cybersecurity specialists to establish themes and controls that benefit small and medium-sized businesses. An SME may download and utilize CYSEC to identify its cybersecurity capability profile, get suggestions for improvement, and track the progress of those recommendations [82].

CYSEC invites the SME to provide feedback on the selection criteria and the experience of implementing the recommended practices according to SME-defined timelines. Aggregating

these observations and input from various SMEs will provide the cybersecurity developer and expert community with valuable information for improving the products and advice they provide [83].

2.7.6. Comparative Analysis of Cybersecurity Tools:

To provide a comprehensive understanding of various cybersecurity tools, a comparative analysis was conducted. The following table 2.7.6 summarizes key tools, highlighting their definitions, historical development, organizational nature, issuing or supervising bodies, and criteria. This comparison aims to elucidate the unique characteristics and applications of each tool, facilitating informed decision-making for cybersecurity professionals and researchers.

Table 2.7.6: Comparative Analysis of Cybersecurity Tools.

Tool	Brief Definition	Historical Overview	For Profit or Non-Profit	Issuing/Supervising Body	Country of Origin	Governmental or Independent	Criteria
The Gordon–Loeb (GL) Model Tool	A mathematical model for determining the optimal investment in cybersecurity	Developed by Lawrence A. Gordon and Martin P. Loeb, first published in 2002	Non-Profit	University of Maryland	USA	Independent	Cost-Benefit Analysis, Optimal Investment Level
The Baldrige Cybersecurity Excellence Builder (Builder)	A self-assessment tool for evaluating cybersecurity risk management	Developed by NIST, first published in 2017	Non-Profit	National Institute of Standards and Technology (NIST)	USA	Governmental	Organizational Context, Process Questions, Results Questions
The CET Tool	A tool for computer-assisted translation (CAT)	Developed by various organizations, widely used in translation industry	For Profit	Various	International	Independent	Translation Memory, Terminology Management, Quality Assurance
Keep It Simple Tool (KIS)	A principle and toolset for simplifying processes and designs	Originated from the U.S. Navy in 1960, popularized in various fields	Non-Profit	Various	USA	Independent	Simplicity, Efficiency, Effectiveness
Cybersecurity Coach (CYSEC)	An open-source platform providing expert cybersecurity advice	Developed by the University of Applied Sciences of Northwestern Switzerland, part of the SMESEC project	Non-Profit	University of Applied Sciences of Northwestern Switzerland	Switzerland	Independent	Interactive Coaching, Data Security, Customizable Advice

2.8. MSMEs Cybersecurity Frameworks:

2.8.1. SMESEC Framework:

SMESEC's primary purpose is to establish what MSME needs and transform them into requirements for a single framework, which will eventually comprise SMESEC partners' contributed products. The products may span various security market areas, and the unification is projected to boost the products' and Framework's added value.

• Simplicity [84]: The project's innovation items should reduce the customary amount of complexity in security systems, making them more appealing for MSMEs to employ. The term "complexity" relates to the tools' usability, installation, and update needs.

• Protection [84]: SMESEC solutions should provide a higher level of cybersecurity protection than currently existing solutions on the market or at least be on par with them.

• Cost-effectiveness [84]: Because financial limits are critical entry hurdles for cyber-security solutions in the MSMEs ecosystem, each incremental innovation must keep prices low.

• Training and awareness [84]: SMESEC seeks to evangelize the necessity of cybersecurity protection among MSMEs and the technical components. To achieve this non-technical goal, the production of supporting material will be considered throughout the innovation road-mapping process.

2.8.2. ENISA Framework:

ENISA carried out this project as part of its Work Program 2015 to present a collection of relevant suggestions on how to boost SMEs' adoption of information security and privacy standards [85]. These proposals are aimed at policymakers in the EU and MS, organizations that establish standards, and professional, industrial, and small business organizations. Extensive research examined the current security and privacy standards adoption among European MSMEs. The study delved into the key drivers incentivizing MSMEs to embrace

these standards and the perceived barriers hindering SMEs in this domain. The findings drawn from this analysis are crucial for understanding the landscape.

The paper's research methodology involved conducting interviews with subject matter experts and analyzing existing studies in the field. This framework also highlights current information security and privacy standards that may be utilized by European MSMEs, including a list of standards that MSMEs should consider adopting, as well as explanations of these standards.

The following essential recommendations are made in this framework to raise the degree of information security and privacy standardization in the European MSME community [86]:

1. Raising awareness and engagement: At all levels of the EU, public and private information security awareness groups should launch programs aimed at MSMEs to explain how information security and privacy regulations may help them secure their essential business assets and processes.

2. Promoting adoption and compliance: To encourage MSMEs to adopt information security and privacy standards, EU public authorities and/or industry groups should support creating certification systems aimed at them.

3. Facilitating implementation: Organizations establishing standards should consider designing security and privacy standards tailored to MSMEs and view their unique characteristics and procedures. MSMEs should be encouraged to use security by default configurations to make standard adoption easier later, and software manufacturers may help MSMEs by assuring secure default configurations in products aimed at small businesses.

4. Strengthening capacities: MSMEs should be encouraged by public governments at all levels of the EU to embrace security and privacy requirements. SMEs should be encouraged to appoint an Information Security Officer to guarantee ownership of the information security and data

protection duties. Member States should provide professional training programs for Information Security Officers as a foundation.

5. Fostering collaboration: International, European, and national SDOs, as well as industry groups, should collaborate to produce a unified strategy for SMEs' specific information security and privacy requirements.

2.8.3. The Centre for Cybersecurity Belgium Guide:

The Centre for Cybersecurity Belgium (CCB) collaborated closely with the Cybersecurity Coalition to prepare this framework. They've compiled a list of 12 cybersecurity themes and primary and sophisticated cybersecurity suggestions that MSMEs may employ to decrease exploitable gaps and vulnerabilities and guard against data breaches and cyber-attacks [87].

The fundamental suggestions in this framework assist MSMEs in gaining a security head start. They assist MSMEs in avoiding the most typical pitfalls and safeguarding their most sensitive information. Advanced best practices and recommendations help implement even better protection strategies.

Here is the list of Cybersecurity themes created by this framework [88]:

1. Involve senior management in cybersecurity projects to demonstrate the significance of security across all levels.

2. Communicate a corporate security policy and code of conduct to establish clear expectations for employee behavior and responsibilities related to cybersecurity.

3. Educate employees about cyber risks to raise awareness and foster a culture of vigilance.

4. Efficiently oversee critical ICT assets to ensure their security and resilience.

5. Regularly update all software applications to address vulnerabilities and enhance security.

6. Implement strong antivirus protection to defend against malware and other cyber threats.

7. Regularly back up all data to prevent loss in the case of a security incident.

8. Control access to computers and networks to prevent unauthorized entry and data breaches.

9. Secure workstations and mobile devices to safeguard sensitive information and prevent unauthorized access.

10. Bolster the security of servers and network components to minimize potential cyber threats.

11. Secure remote access to defend against unauthorized entry and data breaches.

12. Develop and maintain a business continuity and incident handling plan to effectively respond to security incidents and ensure operations continue without interruption.

2.8.4. SIFMA Cybersecurity Framework:

This guidance aims to help small financial services organizations use information from the Financial Services Information Sharing and Analysis Center more efficiently and effectively (FS-ISAC) [89]. Small businesses with one to two hours per week to examine and evaluate cybersecurity threat information are the target audience for this advice. Because information might come from various places (media, peer-to-peer interactions, law enforcement, trade groups, and so on), each person will have their own personal "go-to" sources.

The following are the tools and information needed in this framework [90]:

1. Cyber threat level table: The Cyber Threat Level was created to help financial institutions prioritize preventative actions that they may take to secure their company better and manage their overall readiness. Members of the Financial Services Industry Security Advisory Committee (FS-ISAC) can use this system to better integrate cyber threat intelligence with their internal asset protection policies to secure their companies and the financial services industry. Low, guarded, elevated, high, and severe are the five degrees of severity for the cyber threat level indicator, which are color-coded and include indicators of danger levels to the financial industry.

2. Email alerts: Daily email notifications from the FS-ISAC are sent out to offer timely information on new threats, vulnerabilities, events, mitigation methods, and intelligence analysis that may be utilized to advise a company. They have a consistent structure that may be utilized to prioritize incoming data quickly using email rules.

3. FS-ISAC portal: The FS-ISAC Portal is the critical tool for securely sharing and disseminating relevant, timely, and actionable alerts related to physical and cyber events, threats, vulnerabilities, and solutions affecting the sector's vital infrastructures and systems.

4. The cyber intelligence (CyberIntel) mailing list is an open discussion mailing list that allows for the quick transmission of cyber information, aiding in discovering a specific danger or event as it occurs. All FS-ISAC members have access to the CyberIntel email list, commonly used for communication.

5. Traffic light protocol (TLP classification): The FS-ISAC uses the Traffic Light Protocol to maintain tight information processing standards (TLP). The following categorization is shown in Figure 2.1 and is used to classify and handle any information supplied, processed, stored, archived, or disposed of. Unless otherwise stated, all information is classified as private (Amber) and not shared with parties outside the FS-ISAC without the originator's consent.

TLP Classification	
Classification	Target Audience
FS-ISAC Red	Restricted to a defined group (e.g., only those present in a meeting.) Information labeled RED should not be shared with anyone outside of the group.
FS-ISAC Amber	This information may be shared with FS-ISAC members only and should be considered confidential.
FS-ISAC Green	Information within this category may be shared with FS-ISAC members and partners (e.g., government agencies and ISACs.) Information in this category is not to be shared in public forums.
FS-ISAC White	This information may be shared freely and is subject to standard copyright rules.

Figure 2.8.4: TLP Classification [89].

2.8.5. ISO 44003:2021(Collaborative business relationship management Guidelines for micro, small and medium-sized enterprises on the implementation of the fundamental principles) [91]:

This standard advises micro, small, and medium-sized firms (MSMEs) on increasing their collaborative capabilities by using the twelve principles of collaborative business interactions outlined in ISO/TR 44000. It applies to MSMEs of all types, regardless of what they do, where they are located, their operational environment, culture, social capital, or goals.

2.8.6. Small Business Cybersecurity Workbook:

The Cybersecurity Workbook is a starting point for developing a Written Information Security Program for your small organization. The essence of this framework is creating a suitable program for addressing cybersecurity within the business. It may sound hard at first. It'll need to jot down certain items and evaluate them regularly, which may imply more work. Aside from that, maintaining a flexible structure should be a straightforward procedure that evolves with

the company [92]. This framework is intended to guide the MSMEs through the parts of their structure so that they may leave with a functioning program. It will have to adapt and adjust this program in the future, and it may seek to expand it based on the MSME's circumstances.

This framework is based on the five central concepts of the NIST CSF [93]:

1. Identification: Describe the current structures and methods used to detect potential cyber threats within your systems.

2. Protection: What essential practices are currently implemented to protect your systems from potential cyber threats?

3. Detection: How do you presently recognize and deal with any malicious activity or entities within your systems?

4. Response: What specific procedures and tactics are in place to handle and reduce the impact of a security breach if one occurs?

5. Recovery: What measures are currently in place to facilitate the reestablishment of normal business operations after a security breach?

2.8.7. HMG Security Policy Framework:

It emphasizes the significance of effective, meaningful participation of all employees on security issues. People always be the most valuable asset, no matter how advanced technology becomes. As a result, excellent management, judgment, and discretion remain the most effective security safeguards.

The Framework's emphasis on personal responsibility and accountability is a crucial component of the new policy, and it reflects the exact expectations that the Civil Service Code lays on all MSMEs. HMG framework uses protective security to ensure that it can function effectively, efficiently, and securely as follows [94]:

• Common Security Principles:

Risk management, attitudes, behaviors, policies, and processes.

• Security Outcomes:

1. Government agencies are the most knowledgeable about their operations and services, especially how to manage local risks to support operations and services.

2. Permanent Secretaries/Heads of Department are responsible for securing their organizations to Parliament.

3. An annual reporting mechanism (the Security Risk Management Overview) will assure compliance and a degree of commonality acceptable for all levels of government.

• Good Governance.

• Personnel Security.

• Physical Security.

• Improving Culture and Awareness.

• Efficient Risk Management.

• Strong Information Security.

• Advanced Technology and Services.

2.8.8. Comparative Analysis of MSMEs Cybersecurity Framework:

To gain a comprehensive understanding of cybersecurity frameworks specifically designed for Micro, Small, and Medium Enterprises (MSMEs), a detailed comparative analysis was conducted. The following table 2.8.8 provides a summary of key frameworks, outlining their definitions, historical development, organizational nature, issuing or supervising bodies, and criteria. This comparison aims to elucidate the distinct characteristics and applications of each framework, thereby aiding MSMEs in selecting the most suitable cybersecurity measures to enhance their security posture.

Table 2.8.8: Comparative Analysis of MSMEs Cybersecurity Frameworks.

Framework	Brief Definition	Historical Overview	For Profit or Non-Profit	Issuing/Supervising Body	Country of Origin	Governmental or Independent	Criteria
SMESEC Framework	A lightweight cybersecurity framework for SMEs	Developed by a consortium of European organizations, first introduced in 2017	Non-Profit	SMESEC Consortium	EU	Independent	Awareness & Training, Vulnerability Discovery, Threat Protection, Response Tools
ENISA Framework	Provides guidelines and best practices for cybersecurity in SMEs	Developed by the European Union Agency for Cybersecurity (ENISA), ongoing updates since 2004	Non-Profit	ENISA	EU	Governmental	Risk Management, Incident Response, Awareness, Training
The Centre for Cybersecurity Belgium (CCB)	National authority for cybersecurity in Belgium	Established in 2015 by the Belgian government	Non-Profit	Centre for Cybersecurity Belgium (CCB)	Belgium	Governmental	Cyberfundamentals, Incident Response, Coordination, Awareness
SIFMA Cybersecurity Framework	Cybersecurity guidelines for the financial services industry	Developed by the Securities Industry and Financial Markets Association (SIFMA), ongoing updates	Non-Profit	SIFMA	USA	Independent	Risk Management, Incident Response, Data Protection, Insider Threats
ISO 44003:2021	Guidelines for collaborative business relationships	Developed by ISO, first published in 2021	Non-Profit	International Organization for Standardization (ISO)	International	Independent	Collaboration, Risk Management, Governance, Performance Evaluation
Small Business Cybersecurity Workbook	A practical guide for small businesses to improve cybersecurity	Developed by various cybersecurity organizations, widely used	Non-Profit	Various	International	Independent	Risk Assessment, Security Controls, Incident Response, Training
HMG Security Policy Framework	Security policy framework for UK government departments	Developed by the UK government, first published in 2008	Non-Profit	UK Government	UK	Governmental	Governance, Risk Management, Information Assurance, Incident Management

2.9. Conclusions

This chapter reviews previous studies related to the work, beginning with an examination of works defining MSMEs and cybersecurity. It then describes various cybersecurity themes, followed by an analysis of previous studies on cybersecurity frameworks. Finally, it explores the use of customized frameworks for MSMEs. As mentioned in the objective section, no studies on cybersecurity in Palestine or cybersecurity frameworks for Palestinian MSMEs were found in the open literature.

Chapter Three

3. Exploratory Data Analysis

3.

3.1. Introduction

To make informed decisions regarding the cybersecurity levels in Palestinian Micro, Small, and Medium Enterprises (MSMEs) and to design a tailored framework suitable for these enterprises, this chapter employed a qualitative approach. Two questionnaires and structured interview were developed and distributed to each Palestinian MSME to evaluate the following:

- their understanding and awareness of cybersecurity importance.
- the practices they employ to address cybersecurity threats and attacks.
- their adoption of cybersecurity tools, protocols, and frameworks.
- the level of cybersecurity awareness among top management and employees.

The following section describe the methodology in detail. For more detailed information about the structured interview and questionnaire such as the design and questions used, please go to the appendix.

3.1.1. Methodology for Assessing Cybersecurity in Palestinian MSMEs

A qualitative approach was employed by randomly selecting fifty MSMEs from a list provided by the Palestinian Central Bureau of Statistics (PCBS) and the Federation of Palestinian Chambers of Commerce, Industry, and Agriculture (FPCCIA). The following steps were then undertaken:

- Design Questionnaires and Interviews:
  - Develop two questionnaires targeting employees, and MSME managers.
  - Design structured interview targeting key informants.

- Distribute Questionnaires
  - Questionnaires were distributed to fifty Palestinian MSMEs, with five employees from each MSME participating in the survey.
  - Collect responses on cybersecurity awareness, practices, and tool adoption.
- Conduct Interviews
  - Conduct structured interviews via Zoom with four key informants.
  - Gather qualitative insights on cybersecurity practices and awareness.
- Data Collection
  - Compile and analyze data from questionnaires and interviews.
  - Assess the cybersecurity landscape within Palestinian MSMEs.
- Analysis and Framework Design
  - Analyze the collected data to identify trends and gaps.
  - Design a customized cybersecurity framework suitable for Palestinian MSMEs.
- Conclusion
  - Summarize findings and propose recommendations for improving cybersecurity in Palestinian MSMEs.

The following flow chart figure 3.1.1 describe the methodology to visually represent, understand, analyze, and optimize processes, workflows.

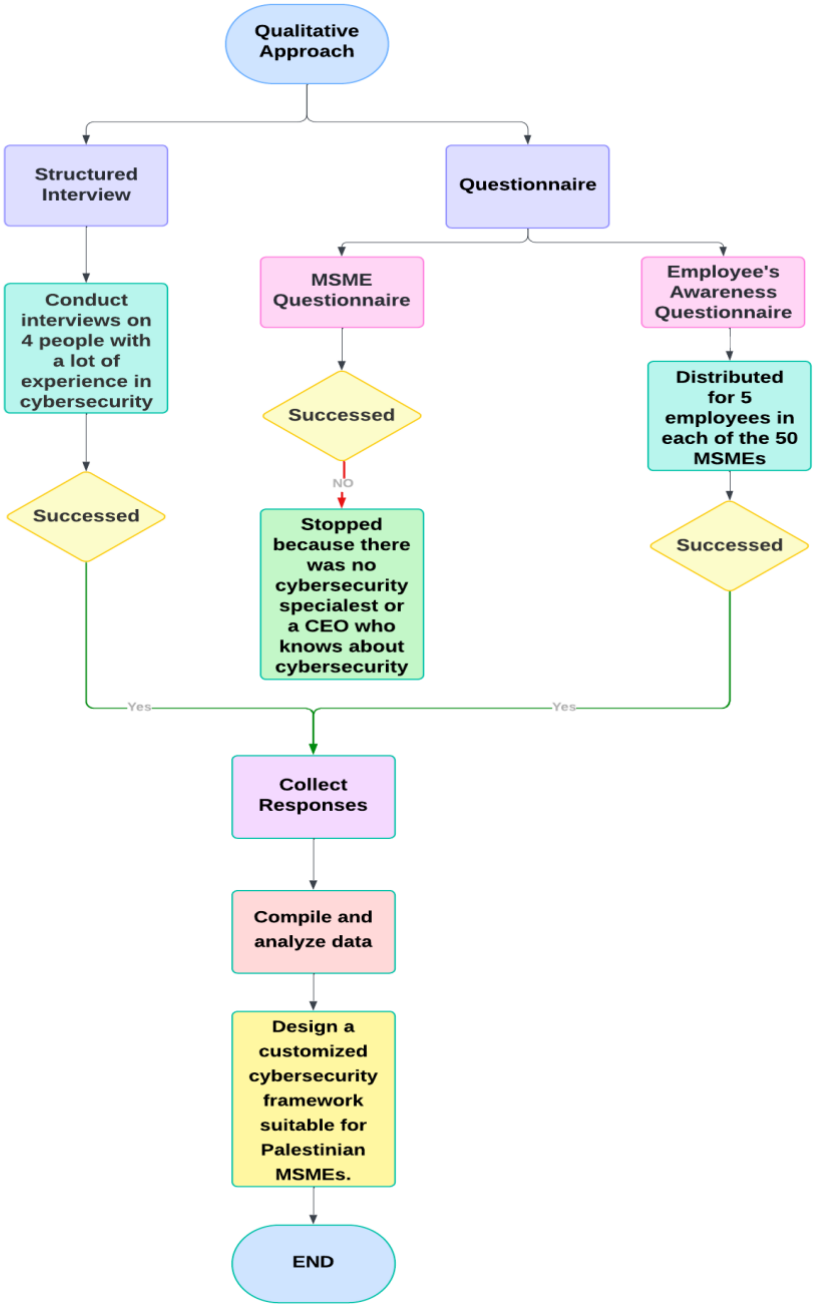


Figure 3.1.1: Methodology Flowchart.

The following sections were organized as follows: Section 3.2 covered interviews with key informants, Section 3.3 discussed the employee cybersecurity awareness questionnaire, Section 3.4 described the MSME questionnaires, Section 3.5 detailed the data collection methods, and finally, Section 3.6 provided the conclusion.

3.2. Key informants' Structured Interviews:

To detect the Cybersecurity level in Palestinian MSMEs, a structured interview was designed for the key informants to answer in an in-depth interview via Zoom. The key informants were four, they are experienced cybersecurity professionals who can offer deep insights into current trends, challenges, and best practices in the field. Cybersecurity is a rapidly evolving field. Experts can provide the latest information on emerging threats, technologies, and regulatory changes. Also Interviews with experts from different sectors (e.g., finance, healthcare, government) can provide diverse perspectives on cybersecurity issues. They can offer practical recommendations and solutions based on their experience. These insights can be particularly useful for developing actionable strategies and frameworks.

Table 3.2 presents a series of questions related to cybersecurity practices, along with responses from multiple respondents. Here's a summary and insights from the answers provided:

Table 3.2. Key informants' structured interview summary.

Question	Answer
What basic security measures have you put in place to protect your systems?	ISO controls (administrative, logical, physical), a certificate for CEO trust, firewall, patching, access control, Business Continuity Plan, training sessions for employees about essential Cybersecurity roles, backup policy, using virtual environment, encryption, email alerts, incident handling plan, penetration testing, and disaster recovery site.

How do you identify potential threats or malicious activity?	Basic security solution controls, data leakage prevention system, intrusion detecting and preventing system, file integrity solution, monitoring, email notification alerts, physical controls, firewall, antivirus, and antimalware. SIEM and firewalls are also used to detect unauthorized access attempts.
If a breach occurs, how will you handle and oversee the situation?	Incident handling plan, notifications, investigation, monitoring traffic, anti-DDoS system, and recovery system. Identify the source of threats, isolate the infected area, apply complete traffic analysis, and review all credentials controls used. ,
What is your strategy for recovering your business operations following a security breach?	Recovery system and close central server, recovery and backup plan (daily, weekly, yearly), disaster recovery (DR) site, incident handling plan, and Business Continuity Plan. Restore backups in case data is lost and ensure all software and operating systems are up to date.
What framework or protocol do you choose to use, if any, and why?	Customized framework based on the system, including risk management, assessment, registry plan, Cybersecurity policy customized ISO 27001, incident handling plan, and Business Continuity Plan. The NIST framework is effective, but a specific framework should be used only if each case requires different procedures and steps.
What are the most critical factors in determining which framework to choose?	The company needs and its work type, risk management and assessment plan, customized framework, IT audits, ease of use, flexibility, and efficiency.

What is the most important that must be in every company?	Employee awareness/training, security policy and procedure, business continuity plan, incident response plan, flexible network security controls, access management, and data center. Continuous reviews for infrastructure, policies, procedures, and users are also essential.
What are your daily procedures and processes to design a framework for MSMEs?	Risk management and assessment plan, assets and data protection and controls, daily backups, constant software updates, firewall, antivirus, antimalware, employee awareness, monitoring, and reporting.

- Risk Assessment and Management: All respondents emphasize the importance of risk assessment processes to identify threats and weaknesses in their systems. This includes customized frameworks and adherence to standards like ISO 27001.
- Security Measures: A variety of security measures are mentioned, including firewalls, intrusion detection systems, antivirus software, and data encryption. These measures are critical for protecting systems from unauthorized access and potential breaches
- Incident Handling and Recovery: Respondents highlight the need for an incident handling plan that includes monitoring traffic, notifications, and recovery systems. This indicates a proactive approach to managing potential breaches and ensuring business continuity.
- Employee Training and Awareness: There is a strong emphasis on the necessity of training employees about cybersecurity roles and responsibilities. This is seen as a fundamental aspect of maintaining security within the organization.

- Customized Frameworks: Several respondents prefer customized frameworks over generic ones, suggesting that specific organizational needs and infrastructure types dictate the best approach to cybersecurity.
- Continuous Monitoring and Updates: Regular monitoring of network traffic and keeping software up to date are recurring points. This reflects an understanding that cybersecurity is an ongoing process that requires vigilance and adaptability.
- Importance of Policies: The mention of cybersecurity policies and procedures underscores the need for formalized guidelines to govern security practices within organizations.

In conclusion, the responses collectively highlight a comprehensive understanding of cybersecurity, emphasizing the interplay between technology, policy, and human factors. Organizations are encouraged to adopt a multi-faceted approach that includes risk assessment, robust security measures, employee training, and continuous monitoring to effectively mitigate cyber threats.

To explore further, an MSMEs questionnaire was created to more accurately assess the use of cybersecurity frameworks in Palestinian MSMEs by posing in-depth questions to cybersecurity officers.

3.3. MSMEs Questionnaire:

The survey was unsuccessful due to the low level of cybersecurity in Palestinian MSMEs. The questionnaire, designed for Cybersecurity Officers, managers and CEOs, remained unanswered because no such professionals were found within these enterprises. Additionally, the managers and CEOs lack the knowledge to respond to the questions posed.

3.4. Employees' Awareness of Cybersecurity questionnaire:

The main goal of this survey is to evaluate how aware employees are of cybersecurity and how this awareness affects Palestinian MSMEs. Originally, this survey was not planned to be the primary research tool because cybersecurity practices are not widely implemented in Palestinian MSMEs. Consequently, it was challenging to gather responses for the MSMEs questionnaire.

To conduct the survey, an email was sent to the Palestinian Central Bureau of Statistics (PCBS) and the Federation of Palestinian Chambers of Commerce, Industry, and Agriculture (FPCCIA), requesting information on micro, small, and medium-sized businesses in Palestine, including their names, addresses, and contact details. In response, comprehensive lists of MSMEs in various West Bank cities were provided. The questionnaires were then distributed in Ramallah and Jenin. For more information please see appendix.

This approach allowed us to evaluate the adoption of cybersecurity frameworks and tools in Palestine, as well as the overall awareness levels regarding cybersecurity and its benefits among employees and top management.

3.5. Data Collection:

The survey was distributed in Ramallah and Jenin, consisting of fifty questionnaires divided into three parts: organization policies and regulations, practices, and knowledge. Employees completed the surveys in person, with explanations provided about the survey and answers to any questions they had.

Here are some specific challenges faced during the data collection for this survey:

1. Limited Cybersecurity Awareness: Many MSMEs in Ramallah and Jenin had limited awareness of cybersecurity practices. This lack of understanding made it difficult to engage respondents and emphasize the importance of the survey.

2. Reluctance to Participate: Some businesses were hesitant to participate due to concerns about sharing sensitive information. This reluctance was particularly pronounced among smaller enterprises that may not have formalized cybersecurity policies.
3. Logistical Issues: Distributing questionnaires in different cities posed logistical challenges. Coordinating with local businesses, ensuring timely delivery and collection of questionnaires, and managing follow-ups required significant effort and resources.
4. Language Barriers: While many business owners and employees are proficient in Arabic, the technical nature of cybersecurity terminology sometimes created misunderstandings. Ensuring that the questions were clearly understood required additional explanation and support.
5. Resource Constraints: MSMEs often operate with limited resources and staff. Finding time to complete the questionnaires amidst their daily operations was challenging for many businesses.
6. Varied Levels of Technological Adoption: The level of technological adoption varied widely among MSMEs. Some businesses had advanced IT infrastructure, while others were still relying on basic technology. This disparity affected the relevance and applicability of certain questions.
7. Data Privacy Concerns: Concerns about data privacy and the potential misuse of information were prevalent. Assuring respondents of the confidentiality and security of their responses was crucial to gaining their trust and participation.
8. Follow-Up Challenges: Ensuring a high response rate required multiple follow-ups. This was time-consuming and sometimes met with resistance from busy business owners and managers.

Despite these challenges, the data collection process provided valuable insights into the cybersecurity landscape of Palestinian MSMEs, highlighting areas for improvement and the need for tailored cybersecurity frameworks.

3.5.1. Organization policies and regulations:

This section emphasizes the regulations and restrictions each company has concerning security. The chart 3.5.1 presents responses to various questions about security practices within organizations. Here's a detailed analysis:

Password Requests:

Question: Have you been asked for your password by your supervisor or anyone else at work?

Responses: Majority answered "YES".

Incident Reporting:

Question: Do you know who to call if you've been hacked or infected with your computer?

Responses: Majority answered "NO".

Public Computer Usage:

Question: Have you used public computers, such as those at a library, cafe, or hotel lobby, to access your business accounts?

Responses: Majority answered "YES".

Risks: Public computers can be compromised with keyloggers or other malware, leading to credential theft and unauthorized access to business accounts. This practice significantly increases the risk of data breaches.

Work from Home:

Question: Do you take material from the office and work on it on your computer at home?

Responses: Majority answered "NO".

Risks: This practice can lead to data breaches if home networks are not secure or if sensitive information is accessed by unauthorized individuals. It also increases the risk of data loss if proper backup procedures are not followed.

Software Installation:

Question: Have you recently downloaded and installed software on your office computer?

Responses: Majority answered “YES”.

Risks: Unauthorized software installations can introduce malware or create vulnerabilities in the organization’s network. It can also lead to software conflicts and system instability.

Device Usage for Confidential Information:

Question: Can you use your devices, such as your mobile phone, to store or transfer confidential company information?

Responses: Majority answered “YES”.

Risks: Personal devices may not have the same level of security as company-provided devices. This can lead to unauthorized access, data leakage, and potential malware infections. Additionally, lost or stolen devices pose a significant risk to data security.

Instant Messaging:

Question: Is instant messaging allowed in your organization?

Responses: Majority answered “YES”.

Risks: Instant messaging platforms may not be secure and can be used to share sensitive information without proper encryption. This can lead to data leakage and unauthorized access to confidential information.

Email Policy Awareness:

Question: Does the company you work in have policies on what you can and cannot use email for?

Responses: Majority answered “NO”.

Website Policy Awareness:

Question: Does the company you work in have policies on which websites you can visit?

Responses: Majority answered “NO”.

Security Team:

Question: Does your company have a security team?

Responses: Majority answered “NO”.

In conclusion, the significant number of employees taking work home and using personal devices presents notable security risks. Additionally, the use of public computers and instant messaging highlights areas where organizational policies may need reinforcement to ensure better cybersecurity practices.

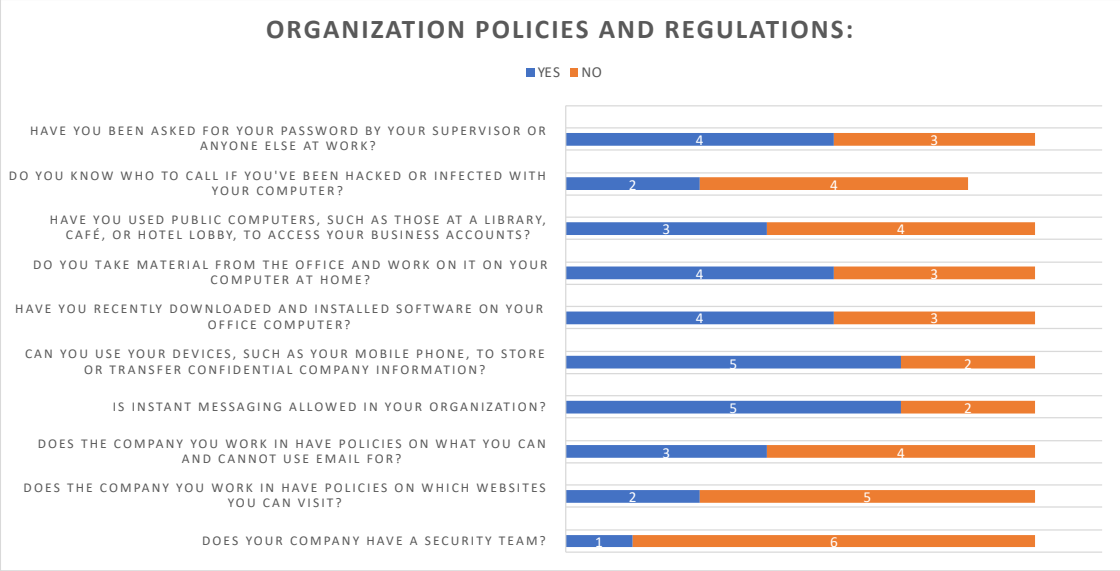


Figure 3.5.1: Organization policies and regulations chart.

As shown in Figure 3.5.1, more than half of the companies lack protection. The figure 3.5.2 below demonstrates that each question corresponds to a specific cybersecurity framework used to formulate these questions. In conclusion, ISO, NIST, CIS, and SOGP are the frameworks that encompass all the questions with their controls. This chart effectively connects common

cybersecurity concerns with recognized standards, guiding organizations in creating robust policies and procedures.

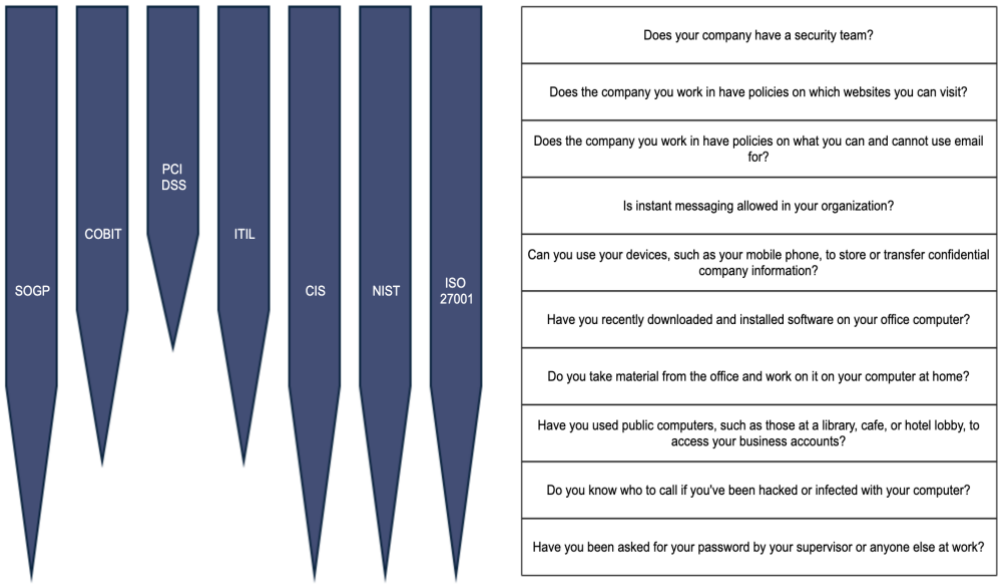


Figure 3.5.2: Questions originating from Cybersecurity frameworks.

3.5.2. Practices:

The chart figure 3.5.3 presents responses to six questions about individuals' cybersecurity practices. Here's a detailed analysis:

Use of Unpaid Software:

Question: I would use a copy of commercially available software made by a friend.

Majority Response: Yes (Blue). The majority of respondents indicated they would use a copy of commercially available software made by a friend, suggesting a general adherence to legal software usage practices.

Password Reuse

Question: Do you use the same password for your work and personal accounts, such as Facebook, Twitter, and email?

Majority Response: Yes (Blue). The majority of respondents indicated they reuse passwords across multiple platforms, which is a risky cybersecurity practice as it increases vulnerability to attacks.

Discovery of Malware or Trojan

Question: Have you ever discovered malware or Trojan on your work computer?

Majority Response: No (Orange). The majority of respondents indicated they have not discovered malware or Trojans on their work computers, suggesting either good cybersecurity practices or a lack of awareness/detection.

Antivirus Updates

Question: Is your antivirus software up to date, installed, and enabled on your computer?

Majority Response: No (Orange). The number indicates that most respondents do not have their antivirus software configured for automatic updates, which is a bad practice as it leaves systems vulnerable to new threats.

Automatic Updates

Question: Is your computer set up to get updates automatically?

Majority Response: No (Orange). The number shows that most respondents do not regularly check if their firewall is enabled, which increases the risk of unauthorized access and cyber threats.

Sharing Work Passwords

Question: Have you ever shared your work password with someone else?

Majority Response: Yes (Blue). The number shows that a significant portion of respondents reuse passwords across multiple platforms, which is a security risk.

In conclusion, most respondents demonstrate good cybersecurity practices, such as avoiding unauthorized software, keeping antivirus software updated, enabling automatic updates, and not

sharing work passwords. However, password reuse remains a significant security risk, and the lack of malware detection could either reflect effective security measures or a gap in awareness and detection capabilities. These insights highlight the need for further education and policy reinforcement to enhance cybersecurity practices.

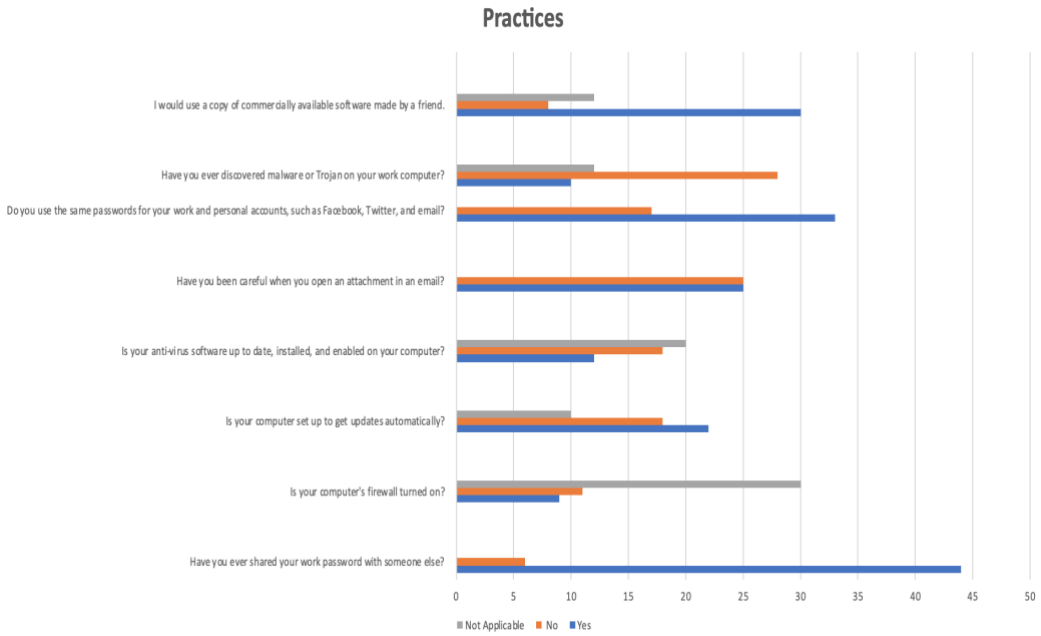


Figure 3.5.3: Practices.

The source of each survey question is detailed, as illustrated in Figure 3.5.4 below.

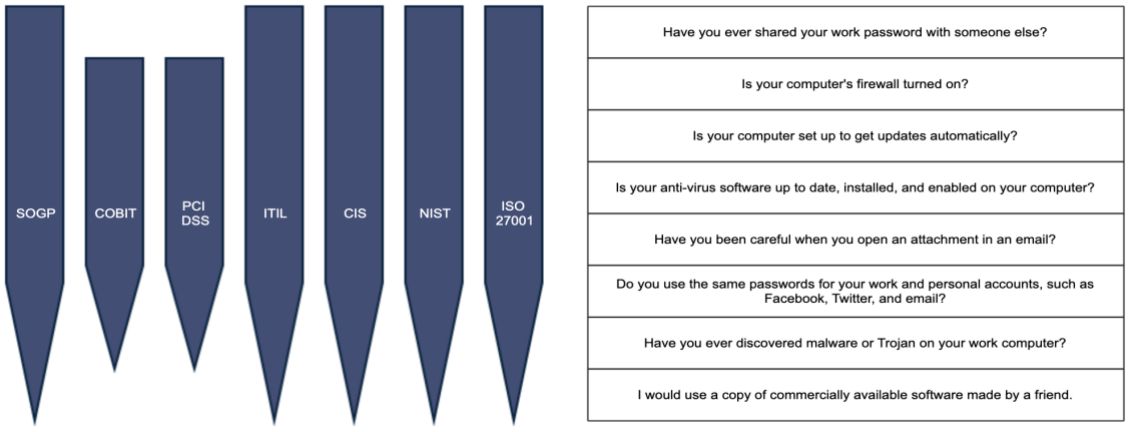


Figure 3.5.4: Questions sourced from cybersecurity frameworks.

3.5.3. Knowledge:

There are two parts designed to provide employees with basic cybersecurity knowledge. Part A figure 3.5.5 covers the fundamentals of cybersecurity, as illustrated:

Feeling of Computer Security

Question: Do you feel your computer is secure?

Responses:

Yes (Blue): A significant number of employees feel their computer is secure.

No (Orange): A smaller number of employees do not feel their computer is secure.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

Perception of Company's Data Security

Question: What do you think? Your company has no need to hide data; they do not target us.

Responses:

Yes (Blue): A moderate number of employees believe their company has no need to hide data.

No (Orange): A significant number of employees disagree, indicating they believe their company does need to hide data.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

Data Loss Perception

Question: What do you think? If your best friend stole or erased the files on it, all the information is (permanently lost)?

Responses:

Yes (Blue): A moderate number of employees believe that if files are stolen or erased, the information is permanently lost.

No (Orange): A significant number of employees disagree, indicating they believe the information can be recovered.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

Data Recovery Awareness

Question: Does data from your computer (USB stick) have to be recovered after theft?

Responses:

Yes (Blue): A significant number of employees believe data needs to be recovered after theft.

No (Orange): A smaller number of employees do not believe data needs to be recovered.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

Understanding of Phishing Scams

Question: Do you understand what a phishing scam is?

Responses:

Yes (Blue): A significant number of employees understand what a phishing scam is.

No (Orange): A smaller number of employees do not understand phishing scams.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

Awareness of Email Scams

Question: Are you aware of an email scam and how to report one?

Responses:

Yes (Blue): A significant number of employees are aware of email scams and know how to report them.

No (Orange): A smaller number of employees are not aware of email scams.

Not Applicable (Gray): A few employees indicated this question is not applicable to them.

In conclusion, many employees demonstrate a solid understanding of cybersecurity by feeling confident in their computer security, recognizing phishing scams, and knowing how to report email scams. However, there are areas of concern, such as the belief that their company does not need to hide data and the misconception that data is permanently lost if stolen or erased.

These misunderstandings could lead to vulnerabilities and highlight the need for improved data protection measures and further education.

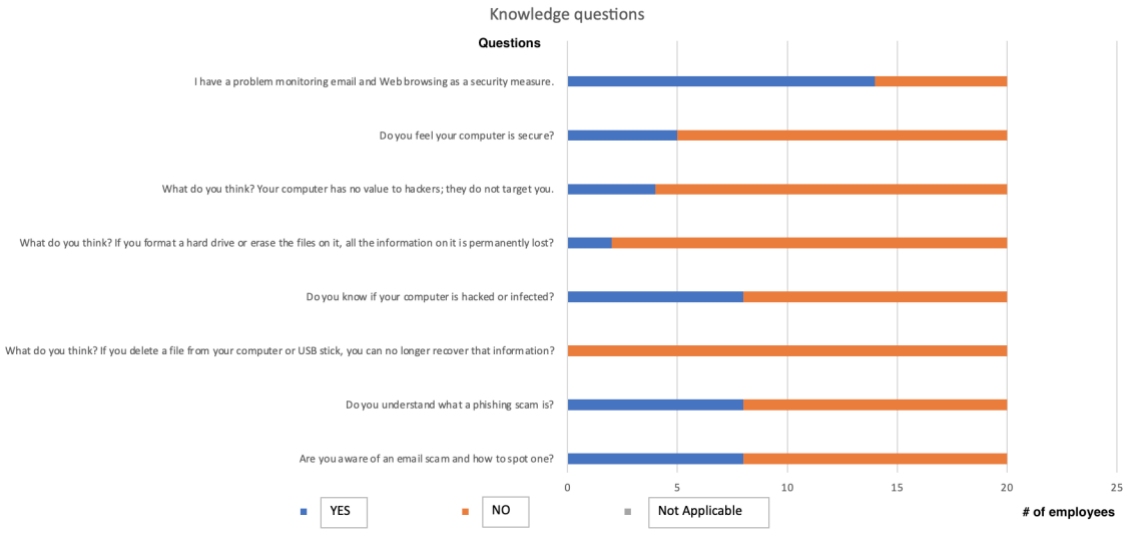
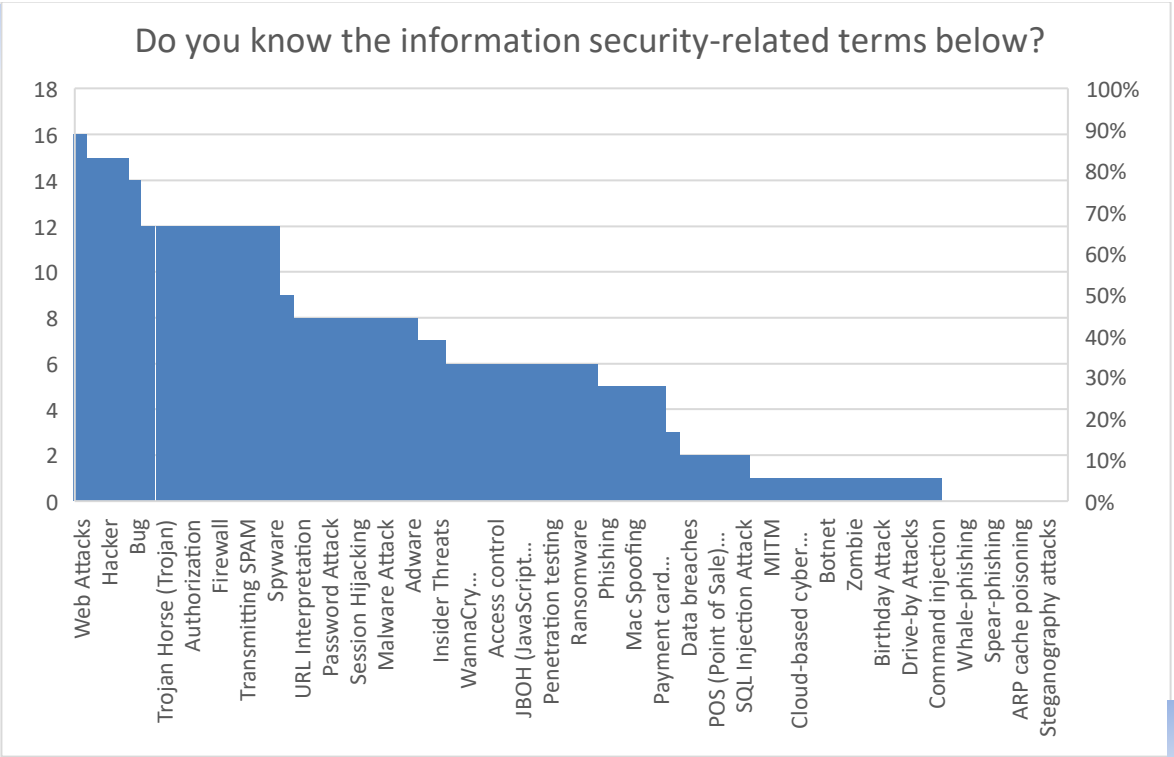


Figure 3.5.5: knowledge chart a.

Part B figure 3.5.6 includes the most well-known cybersecurity-related terms, as identified from various papers and websites, with the answers provided below.

People



Questions

Figure 3.5.6: knowledge chart b.

Terms and Responses

Wi-Fi Attack

Number of Respondents: Approximately 18 respondents are familiar with this term.

Percentage: Close to 100% of respondents.

Web Hardening

Number of Respondents: Approximately 16 respondents are familiar with this term.

Percentage: Around 90% of respondents.

Crypto-jacking

Number of Respondents: Approximately 14 respondents are familiar with this term.

Percentage: Around 80% of respondents.

Zero-Day Attack

Number of Respondents: Approximately 12 respondents are familiar with this term.

Percentage: Around 70% of respondents.

Tailgating/Piggybacking

Number of Respondents: Approximately 10 respondents are familiar with this term.

Percentage: Around 60% of respondents.

Man-in-the-Middle (MITM) Attack

Number of Respondents: Approximately 8 respondents are familiar with this term.

Percentage: Around 50% of respondents.

URL Hijacking/Typo Squatting

Number of Respondents: Approximately 6 respondents are familiar with this term.

Percentage: Around 40% of respondents.

Phishing/SpearPhishing/Vishing/Whaling/Pretexting/FraudulentEmailsorCalls/Payment Redirection Fraud/Card Not Present Fraud/Business Email Compromise (BEC)

Number of Respondents: Approximately 4 respondents are familiar with these terms.

Percentage: Around 30% of respondents.

Ransomware/Malware/Spyware/Virus/Worm/TrojanHorse/Rootkit/Keylogger/Botnet/DDoS Attack/RATs (Remote Access Trojans)

Number of Respondents: Approximately 2 respondents are familiar with these terms.

Percentage: Around 20% of respondents.

Drive-By Download Attacks/Pay-Per-Click Fraud/Cookie Stuffing/Affiliate Fraud/Ad Injection/Fake Reviews or Ratings/Bill Stuffing/Organic Search Poisoning/Cross-Site Scripting (XSS)/SQL Injection/Form-jacking/Digital Skimming/Page Hijacking/Search Engine Optimization (SEO) Poisoning/Cross-Site Request Forgery (CSRF)/Session Hijacking/Eavesdropping Attacks/Side-jacking/Wardriving/Evil Twin Attacks/Rogue Hotspots/AP Phishing/Wi-Fi Pineapple Attacks/Wi-Fi Jamming/Wireless Spoofing/Bluejacking/Blue-snarfing/Air-Gap Jumping

Number of Respondents: Approximately 1 respondent is familiar with these terms.

Percentage: Around 10% of respondents.

The results reveal that terms like "Wi-Fi Attack" and "Web Hardening" are well-known among respondents, with nearly all being familiar with these concepts. Terms such as "Crypto-jacking" and "Zero-Day Attack" have moderate recognition, with around 70-80% of respondents familiar with them. However, more complex or less commonly discussed terms, such as "Drive-By Download Attacks" and "Ransomware/Malware/Spyware," have low recognition, with only 10-20% of respondents familiar with them. These findings suggest that while basic cybersecurity terms are well understood, there is a need for increased awareness and education on more complex or less commonly discussed cybersecurity threats. Enhancing knowledge in these areas can help improve overall cybersecurity preparedness within the organization.

3.6. Conclusion

This chapter presents an exploratory data analysis, which helped focus on the collected data and determine how to design a customized framework for Palestinian MSMEs. The data visualization revealed that 90% of Palestinian MSMEs do not use any protection tools in their facilities, not even basic ones like firewalls or antivirus software. Additionally, there is a noticeable lack of awareness about the importance of cybersecurity in protecting their organizations and information.

Chapter Four

4. The Proposed Design of Cybersecurity Framework for MSMEs in Palestine

4.

4.1. Introduction

This chapter presents the proposed design of a Cybersecurity Framework tailored for MSMEs in Palestine. The objective is to develop a customized framework by categorizing the essential controls for each type of enterprise, leveraging the frameworks, standards, and tools reviewed in Chapter Two, alongside data obtained from the relevant company and insights gathered from questionnaires.

The chapter begins by inputting preliminary information into the utilized software. It then elaborates on the specific frameworks deployed for each company type. For micro enterprises, the focus is on implementing the minimum necessary controls to ensure basic security. Small enterprises, on the other hand, incorporate more comprehensive controls to enhance protection. Medium enterprises adopt a distinct set of controls tailored to their specific requirements.

This structured approach ensures that each enterprise type receives an appropriate level of cybersecurity measures, aligned with their unique needs and operational scale.

4.2. Customized Cybersecurity Framework for MSMEs:

Considering their limitations, this customized cybersecurity framework has been created to cater to Micro, Small, and Medium-sized Enterprises (MSMEs) requirements. It offers a flexible roadmap that enables MSMEs to enhance their cybersecurity defenses. The primary goal of this framework is to empower MSMEs in protecting their assets, ensuring business operations, and cultivating a secure environment that fosters long-term growth.

Here are the controls created for Micro, small, and Medium-Enterprises.

4.2.1. A Customized Cybersecurity Framework for Micro Enterprises:

In Palestine, like in other areas, there is a wide variety of small-scale businesses known as microenterprises. These businesses are primarily local. Play a role in the economy. Here are some examples of microenterprises found in Palestine:

1. Small Retail Stores: These include convenience stores, grocery shops, or specialty stores that sell items like clothing, electronics, or household goods.

2. Food and Beverage Establishments: You can find eateries, cafes, or street food vendors offering Palestinian cuisine or snacks.

3. Craftsmanship and Handicrafts: Skilled artisans produce goods such as pottery, traditional embroidery, or woodworking.

4. Agricultural Ventures: Some farms and family-owned agricultural businesses focus on growing crops, vegetables, or fruits.

5. Service-Oriented Businesses: Individuals provide services like hairdressing, tailoring, plumbing repairs, electrical repairs, and other local services.

6. Tourism-Related Enterprises: Accommodation options such as bed and breakfasts and small guesthouses cater to tourists who want to explore the cultural sites of Palestine with the help of tour guides.

7. Tech startups have grown in years with a rise in microenterprises engaged in software development, mobile app creation, and other technology-related services.

8. In markets, known as souks, you can find microentrepreneurs operating stalls or small shops offering a range of goods. These goods span from spices to handmade crafts.

9. Local communities benefit from small-scale transportation services, like taxi or delivery businesses, that cater to their needs.

10. Small beauty salons, spas, or wellness centers provide beauty and wellness services such as haircuts, massages, or skincare treatments.

It's worth mentioning that the specific types of micro-enterprises in Palestine can differ depending on the region and often mirror the economic characteristics of each area. Moreover, these establishments boost employment, foster economic growth, and strengthen community resilience. Additionally, it is evident that micro enterprises do not rely heavily on computers and electronics for data storage, which means these devices do not play a significant role in their operations. Therefore, managing this type of enterprise requires basic and simple controls to assist with security and management.

Here’s a detailed table outlining the controls for a Customized Cybersecurity Framework specifically designed for Micro Enterprises:

Table 4.2.1: The controls for a Customized Cybersecurity Framework specifically for Micro Enterprises.

Control Category	Control Description	Purpose/Objective
Information Security Policy	- Establish a basic information security policy.	- To provide a foundation for security practices and guidelines.
Code of Conduct	- Publish a simple code of conduct outlining acceptable behaviors regarding security.	- To set clear expectations for employee behavior related to information security.
Communication	- Maintain basic communication channels between management and employees.	- To ensure that security policies and updates are effectively communicated.

User Access Control	- Implement basic user access controls (e.g., unique user IDs).	- To restrict access to sensitive information and systems.
Password Management	- Enforce simple password policies (e.g., minimum length, regular changes).	- To enhance security by ensuring strong passwords are used.
Data Backup	- Establish a basic data backup procedure (e.g., weekly backups).	- To ensure data can be restored in case of loss or corruption.
Physical Security	- Implement basic physical security measures (e.g., locked doors, visitor logs).	- To protect physical assets and sensitive information from unauthorized access.
Employee Training	- Provide basic cybersecurity awareness training for employees.	- To educate employees on security best practices and potential threats.
Incident Reporting	- Establish a simple process for reporting security incidents.	- To ensure timely reporting and response to security breaches.
Software Updates	- Regularly update software and systems to patch vulnerabilities.	- To protect against known security threats and vulnerabilities.
Data Handling Procedures	- Define basic procedures for handling sensitive data (e.g., encryption for storage).	- To ensure that sensitive data is protected during storage and transmission.

Network Security	- Implement basic network security measures (e.g., firewalls, secure Wi-Fi).	- To protect the network from unauthorized access and attacks.
Access to Resources	- Limit access to resources based on job roles and responsibilities.	- To minimize the risk of unauthorized access to sensitive information.
Incident Response Plan	- Develop a simple incident response plan outlining steps to take in case of a breach.	- To ensure a structured response to security incidents to minimize impact.
Compliance Awareness	- Educate employees on basic compliance requirements relevant to the business.	- To ensure that the enterprise adheres to applicable laws and regulations.
Monitoring and Logging	- Implement basic logging of user activities and access to sensitive information.	- To provide a record of actions taken within the system for auditing and investigation.

This table provides a comprehensive overview of the specific controls that can be implemented in a Customized Cybersecurity Framework for Micro Enterprises, focusing on essential practices to enhance their cybersecurity posture.

4.2.2. A Customized Cybersecurity Framework for Small Enterprises:

Like in other areas, small businesses play a crucial role in the local economy in Palestine. There is a variety of enterprises found in Palestine, such as:

1. Local Grocery Stores: These independent grocery stores cater to the community's needs by offering a range of food and household products.

2. Bakeries: Small-scale bakeries specialize in producing and selling baked bread, pastries, and other delightful treats.

3. Restaurants and Cafes: Family-owned restaurants and cafes provide an array of international cuisine options for locals and visitors.

4. Clothing Boutiques: Charming retail shops offer clothing, accessories, and fashionable items to cater to customers' tastes.

5. Craftsmanship and Artisans: Artisans or small workshops passionately create crafts, pottery, or traditional Palestinian embroidery.

6. Pharmacies: Local pharmacies serve the community by providing healthcare products and medications.

7. Tech Repair Shops: Small businesses expertly handle repair services for devices like smartphones and computers.

8. Landscaping and Gardening Services: Enterprises specializing in landscaping, gardening upkeep, and maintenance services are available for homes and businesses.

9. Tourism Services: Tour operators or guesthouses tourists who want to explore Palestine’s rich historical sites and cultural wonders.

10. Translation & Language Services: Freelancers or small agencies offer professional translation services tailored to business clients and individuals seeking language assistance.

11. Fitness and wellness centers are gyms or wellness studios that offer fitness classes, personal training sessions, and spa services.

12. Educational services encompass tutors or small educational centers that provide tutoring or after-school programs for students.

13. Graphic design and printing services are typically offered by freelancers or small businesses who specialize in design, printing, and branding services.

14. Web development and IT services involve professionals who offer website development and various IT-related solutions.

15. Catering Services: Some small-scale catering companies excel at offering specialized services for events like weddings and special occasions.

16. Agriculture: Palestine has family-owned farms that cultivate crops, fruits, or vegetables to cater to the community's needs.

17. Transportation Services: taxi services or delivery companies that offer transportation solutions.

18. Photography Studios: Photography services for events, portraits, or commercial needs. There are freelance photographers and small studios to meet your requirements.

19. Beauty Salons: There are beauty salons where you can get hair styling, skincare treatments, and other beauty services.

20. Art Galleries: Art galleries showcase artists' creations in the community while contributing to the vibrant cultural scene.

These examples illustrate the diversity of enterprises contributing to Palestine's local economy. Here are the controls suitable for Palestinian micro-enterprises, here’s a detailed table 4.2.2 outlining the controls for a Customized Cybersecurity Framework specifically designed for Small Enterprises:

Table 4.2.2: The controls for a Customized Cybersecurity Framework specifically for Small Enterprises.

Control Category	Control Description	Purpose/Objective
Information Security Policy	- Develop a comprehensive information security policy that includes roles and responsibilities.	- To provide a clear framework for security practices and accountability.

Code of Conduct	- Publish a detailed code of conduct that outlines acceptable and unacceptable behaviors regarding security.	- To establish clear expectations for employee behavior related to information security.
Communication	- Maintain effective communication channels for security updates and policy changes.	- To ensure that all employees are informed about security practices and changes.
User Access Control	- Implement role-based access control (RBAC) to restrict access to sensitive information based on job roles.	- To minimize the risk of unauthorized access to critical systems and data.
Password Management	- Enforce strong password policies, including complexity requirements and regular changes.	- To enhance security by ensuring that passwords are robust and regularly updated.
Data Backup	- Establish a regular data backup schedule with secure storage solutions (e.g., offsite backups).	- To ensure data can be restored in case of loss, corruption, or ransomware attacks.
Physical Security	- Implement enhanced physical security measures, such as access controls, surveillance cameras, and secure areas for sensitive information.	- To protect physical assets and sensitive information from unauthorized access.
Employee Training	- Provide regular cybersecurity training sessions for employees, covering topics like phishing, social	- To educate employees on security best practices and potential threats.

	engineering, and safe internet practices.	
Incident Reporting	- Establish a formal process for reporting security incidents, including a designated point of contact.	- To ensure timely reporting and response to security breaches.
Software Updates	- Implement a policy for regular software updates and patch management to address vulnerabilities.	- To protect against known security threats and vulnerabilities.
Data Handling Procedures	- Define clear procedures for handling sensitive data, including encryption for storage and transmission.	- To ensure that sensitive data is protected throughout its lifecycle.
Network Security	- Implement advanced network security measures, such as firewalls, intrusion detection systems (IDS), and secure Wi-Fi configurations.	- To protect the network from unauthorized access and cyber threats.
Access to Resources	- Regularly review and update access permissions to ensure they align with current job roles and responsibilities.	- To minimize the risk of unauthorized access to sensitive information.
Incident Response Plan	- Develop a detailed incident response plan that outlines steps to take in case of a security breach, including communication protocols.	- To ensure a structured and effective response to security incidents to minimize impact.

Compliance Awareness	- Educate employees on relevant compliance requirements (e.g., GDPR, HIPAA) and the importance of adherence.	- To ensure that the enterprise meets legal and regulatory obligations.
Monitoring and Logging	- Implement comprehensive logging of user activities, access to sensitive information, and system events for auditing purposes.	- To provide a record of actions taken within the system for auditing and investigation.
Third-Party Risk Management	- Assess and manage risks associated with third-party vendors and service providers, including security requirements in contracts.	- To mitigate risks posed by external partners and ensure they adhere to security standards.
Business Continuity Plan	- Develop a Business Continuity Plan (BCP) that outlines how the organization will sustain its functions, operations, and services during a disruptive incident.	- To minimize downtime and uphold business operations despite disruptions.
Cyber Threat Level Table	- Create a Cyber Threat Level Table to classify and convey existing cybersecurity threats or risks the organization may face.	- To help stakeholders comprehend the gravity of threats and facilitate informed decision-making.

This table provides a comprehensive overview of the specific controls that can be implemented in a Customized Cybersecurity Framework for Small Enterprises, focusing on essential practices to enhance their cybersecurity posture and protect against evolving threats.

4.2.3. A Customized Cybersecurity Framework for Medium-Enterprises:

Sized businesses play a role in Palestine's local economy, just like in many other regions. They contribute by offering a range of products and services. Let me provide you with some examples of enterprises that you can find in Palestine:

1. Manufacturing Companies: These manufacturers produce textiles, furniture, or food products specifically for the local and regional markets.

2. Technology and Software Development Firms: These companies specialize in software development IT services or technology solutions catered to businesses.

3. Construction and Engineering Companies: Medium construction firms are actively engaged in commercial construction projects.

4. Tourism and Hospitality Businesses: You'll find sized hotels, travel agencies, or tour operators that cater to tourists exploring the historical and cultural sites of Palestine.

5. Educational Institutions and Training Centers: Schools, colleges, or training centers that offer education programs and skill development opportunities.

6. Retail Chains: Retail chains operate multiple outlets where you can find various products ranging from electronics to clothing or household items.

7. Healthcare. Services: Sized healthcare facilities provide medical services, including clinics specialized in various healthcare domains.

8. Food and drink chains: These establishments, like restaurants, cafes, or catering services, have branches and offer a variety of cuisines.

9. Companies in the logistics and transportation industry: These companies specialize in shipping, freight, or delivery services.

10. Enterprises in the energy sector: These companies specialize in creating innovative energy solutions, strongly emphasizing solar and wind energy projects.

11. Financial Service Providers: Banks, credit unions, or financial services companies cater to businesses and individuals by offering a range of banking and financial products.

12. Telecommunications Companies: These telecommunications companies provide internet, phone, and communication services to customers.

13. Environmental Consulting Firms: These enterprises specialize in consulting, sustainability practices, and eco solutions for various industries.

14. Marketing and Advertising Agencies: Sized marketing and advertising agencies that offer their expertise to businesses and organizations in promoting their products or services.

15. Real Estate Development: This refers to the process of developing properties and land for commercial purposes.

16. Textile and clothing manufacturing: These are companies of size that are involved in the production of textiles and garments

17. Automotive dealerships and services: These car dealerships sell and provide services for cars, trucks, and other vehicles.

18. Pharmaceutical and biotech companies: These are firms that specialize in developing and producing pharmaceuticals or biotechnological products.

19. Waste management and recycling: These companies focus on managing waste, promoting recycling, and ensuring sustainability.

20. Consulting services: small law firms or consulting services offer clients legal advice and business guidance.

Here’s a detailed table for a Customized Cybersecurity Framework for Medium Enterprises, outlining various controls, their descriptions, purposes, and implementation strategies:

Table 4.2.3: The controls for a Customized Cybersecurity Framework specifically for Medium Enterprises.

Control Category	Control Description	Purpose/Objective	Implementation Strategy
Information Security Policy	Develop a comprehensive information security policy that includes roles, responsibilities, and compliance requirements.	To provide a clear framework for security practices and accountability across the organization.	Draft policy documents, involve stakeholders, and ensure regular reviews and updates.
Risk Assessment	Conduct regular risk assessments to identify vulnerabilities and threats to the organization's assets.	To proactively identify and mitigate risks that could impact business operations.	Use risk assessment frameworks and tools to evaluate risks periodically.
Access Control Management	Implement role-based access control (RBAC) and the principle of least privilege to restrict access to sensitive information.	To minimize the risk of unauthorized access to critical systems and data.	Use access management tools to assign and review permissions regularly.
Password Management	Enforce strong password policies, including complexity requirements, expiration, and multi-	To enhance security by ensuring that passwords are robust and access is secured.	Implement password management software and MFA solutions.

	factor authentication (MFA).		
Data Encryption	Utilize encryption for sensitive data at rest and in transit to protect against unauthorized access.	To ensure that sensitive information remains confidential and secure.	Implement encryption protocols and regularly review encryption practices.
Data Backup and Recovery	Establish a comprehensive data backup and recovery plan, including regular backups and secure storage solutions.	To ensure data can be restored in case of loss, corruption, or ransomware attacks.	Schedule automated backups and test restoration processes periodically.
Physical Security	Implement enhanced physical security measures, such as access controls, surveillance cameras, and secure areas for sensitive information.	To protect physical assets and sensitive information from unauthorized access.	Install security systems and conduct regular security assessments.
Employee Training and Awareness	Provide regular cybersecurity training sessions for employees, covering topics like phishing, social	To educate employees on security best practices and potential threats.	Organize workshops, online courses, and simulations to reinforce learning.

	engineering, and safe internet practices.		
Incident Response Plan	Develop a detailed incident response plan that outlines steps to take in case of a security breach, including communication protocols.	To ensure a structured and effective response to security incidents to minimize impact.	Create a response team, define roles, and conduct regular drills to test the plan.
Network Security	Implement advanced network security measures, such as firewalls, intrusion detection systems (IDS), and secure Wi-Fi configurations.	To protect the network from unauthorized access and cyber threats.	Configure firewalls and IDS, and regularly review network configurations.
Software Update Management	Establish a policy for regular software updates and patch management to address vulnerabilities.	To protect against known security threats and vulnerabilities.	Use automated update tools and maintain an inventory of software.
Monitoring and Logging	Implement comprehensive logging of user activities, access	To provide a record of actions taken within the	Use logging tools and regularly review logs for anomalies

	to sensitive information, and system events for auditing purposes.	system for auditing and investigation.	and suspicious activities.
Third-Party Risk Management	Assess and manage risks associated with third-party vendors and service providers, including security requirements in contracts.	To mitigate risks posed by external partners and ensure they adhere to security standards.	Conduct risk assessments and require security certifications from vendors.
Business Continuity Plan	Develop a Business Continuity Plan (BCP) that outlines how the organization will sustain its functions, operations, and services during a disruptive incident.	To minimize downtime and uphold business operations despite disruptions.	Identify critical functions, develop recovery strategies, and conduct drills.
Compliance Management	Ensure adherence to relevant legal and regulatory requirements (e.g., GDPR, HIPAA) and industry standards.	To mitigate legal risks and ensure the organization meets compliance obligations.	Conduct regular compliance audits and provide training on relevant regulations.
Vulnerability Management	Implement a vulnerability management program to	To proactively address security weaknesses	Conduct regular vulnerability scans

	identify, assess, and remediate vulnerabilities in systems and applications.	before they can be exploited.	and penetration testing.
Secure Development Practices	Integrate security into the software development lifecycle (SDLC) to ensure that applications are developed securely.	To reduce the risk of vulnerabilities in applications and systems.	Provide training for developers on secure coding practices and conduct code reviews.
Cyber Threat Intelligence	Utilize threat intelligence to stay informed about emerging threats and vulnerabilities relevant to the organization.	To enhance the organization's ability to anticipate and respond to cyber threats.	Subscribe to threat intelligence services and integrate findings into security practices.

This detailed table provides a comprehensive overview of the controls necessary for a Customized Cybersecurity Framework for Medium Enterprises, including their descriptions, purposes, and strategies for implementation.

4.2.4. Comparative Analysis for the Customized Cybersecurity frameworks:

Here's a comparison table summarizing the cybersecurity frameworks for Micro, Small, and Medium Enterprises (MSMEs):

Table 4.2.4: Comparison table for the cybersecurity frameworks for Micro, Small, and Medium Enterprises (MSMEs)

Aspect	Micro Enterprises	Small Enterprises	Medium Enterprises
Number of Controls	- Minimum number of controls to achieve basic security	- More detailed controls to protect against threats	- Comprehensive set of controls tailored to larger operations
Focus Areas	- Basic security measures	- Enhanced security protocols	- Advanced security measures
Examples of Controls	- Basic information security policy - Simple code of conduct - Basic communication with management	- Regular security training for employees - Defined duties and responsibilities - Regular review of security policies	- Formal user registration and access control - Background verification checks for employees - Business continuity and incident handling plans

Risk Management	- Basic risk awareness - Informal identification of risks	- Structured risk assessment processes - Regular risk assessments and updates	- Comprehensive risk management plan - Detailed risk identification, assessment, and mitigation strategies
Technical Measures	- Basic protection against unauthorized access - Simple password policies	- Implementation of firewalls and anti-malware - Regular updates and patch management	- Strong detection, prevention, and recovery controls - Advanced intrusion detection systems
Data Protection	- Simple data backup procedures	- Regular data backups and secure disposal of media	- Advanced encryption and secure data transfer protocols
	- Basic data access controls	- Defined data classification and handling procedures	- Comprehensive data loss prevention strategies
Incident Response	- Informal incident handling	- Defined incident response procedures	- Formal incident response plan with clear protocols
	- Basic reporting of incidents	- Regular incident response drills	- Continuous improvement of

			incident response capabilities
Compliance	- Basic compliance with local regulations	- Compliance with industry standards	- Adherence to international standards (e.g., ISO 27001)
	- Limited awareness of compliance requirements	- Regular compliance audits	- Comprehensive compliance management system
User Access Control	- Basic user access management	- Defined user roles and access levels	- Formal user registration and re-registration processes
	- Simple password management	- Regular password changes and complexity requirements	- Multi-factor authentication for sensitive systems
Physical Security	- Basic physical security measures	- Enhanced physical security protocols	- Comprehensive physical and environmental security measures
	- Simple access controls for physical locations	- Surveillance and monitoring systems	- Advanced access control systems and monitoring

Training and Awareness	- Basic cybersecurity awareness for employees	- Regular security training sessions	- Comprehensive training programs and awareness campaigns
	- Informal training on security practices	- Defined training schedules and materials	- Continuous education on emerging threats and best practices

This table provides a clear overview of how the cybersecurity frameworks differ across micro, small, and medium enterprises, highlighting the increasing complexity and comprehensiveness of controls as the size of the enterprise grows.

4.3. Software Development of a CCSF Prototype

In this section, we detail the development of a prototype for the Customized Cybersecurity Framework (CCSF), aimed at enhancing the usability and transparency of cybersecurity measures for Micro, Small, and Medium Enterprises (MSMEs). The prototype was developed using Python, a versatile programming language known for its simplicity and effectiveness in rapid application development.

4.3.1. Objectives of the Prototype

The primary objective of the CCSF prototype is to provide MSMEs with a tailored cybersecurity solution that aligns with their specific operational needs and resource constraints. By allowing users to input relevant company information, the prototype generates a customized cybersecurity framework that addresses the unique challenges faced by these enterprises.

4.3.2. User Input and Interaction

The prototype interface is designed to be user-friendly, enabling users to easily navigate through the application. Upon launching the software, users are prompted to enter key details about their organization as shown in figure 4.3.2 below, including:

- Company Name: The official name of the enterprise.
- Type of Company: The sector or industry in which the company operates (e.g., retail, manufacturing, services).
- Number of Employees: A count of the workforce, which helps in assessing the scale of cybersecurity measures required.

This information is crucial as it allows the prototype to tailor recommendations based on the size and nature of the business.

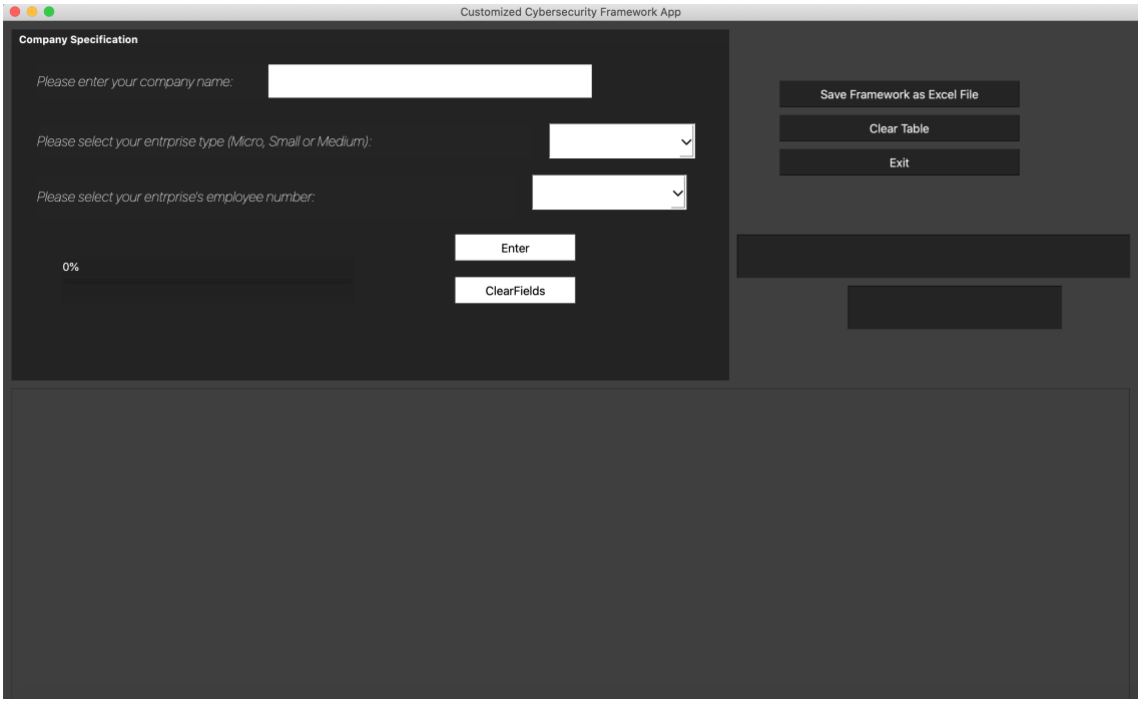


Figure 4.3.2: Software first window.

4.3.3. Framework Generation

Once the user inputs the necessary information, the prototype processes this data to identify the most suitable cybersecurity framework for the organization as shown in figure 4.3.3.

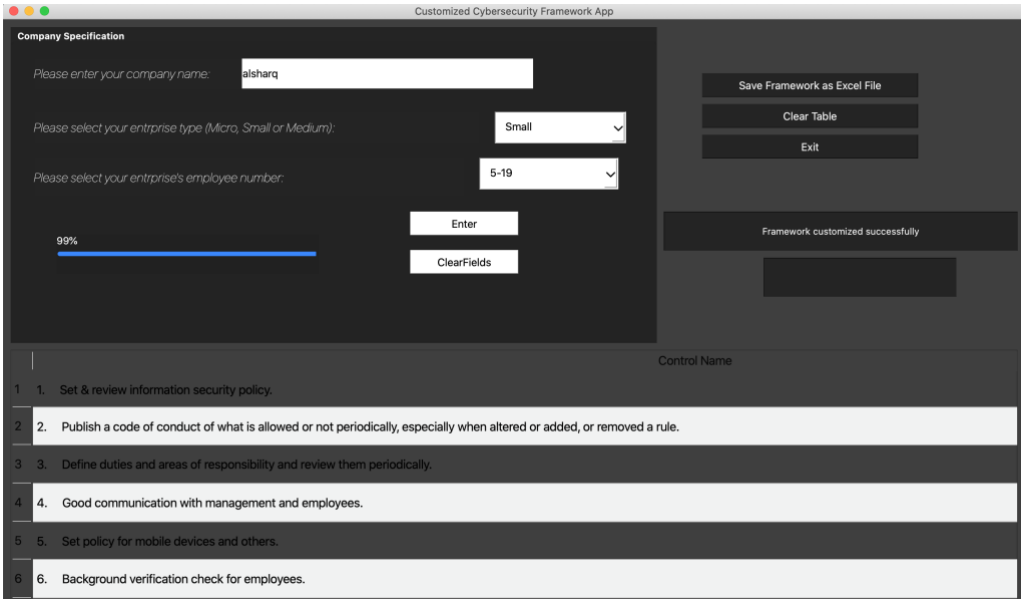


Figure 4.3.3: Software works successfully.

The framework generation involves several key components:

Risk Assessment: The prototype incorporates risk assessment techniques to evaluate potential vulnerabilities and threats specific to the user's business context.

Threat Intelligence Integration: By leveraging existing threat intelligence, the prototype can provide insights into prevalent cyber threats that may impact the user's industry.

Customized Recommendations: Based on the input data and risk assessment, the prototype generates a set of tailored cybersecurity strategies and best practices. These recommendations are designed to be practical and scalable, ensuring that even small enterprises can implement them effectively.

User Awareness Campaigns: In addition to framework generation, the prototype emphasizes the importance of user awareness. It includes features that suggest customized user awareness campaigns, which are essential for educating employees about cybersecurity risks and safe practices. These campaigns are tailored to the operational context of the MSMEs, ensuring relevance and effectiveness.

Interactive Dashboard: The prototype features an intuitive dashboard that provides users with a visual overview of their cybersecurity posture. This includes key metrics, risk levels, and compliance status, allowing users to quickly assess their security standing.

Guided Framework Selection: The prototype offers a step-by-step guide to help users select the most appropriate cybersecurity controls based on their specific business type and size. This feature simplifies the decision-making process and ensures that users are aware of the necessary controls.

Automated Reporting: Users can generate automated reports summarizing their cybersecurity framework, risk assessments, and recommended actions. These reports can be useful for internal reviews and compliance purposes.

Incident Response Planning: The prototype includes a feature for developing incident response plans tailored to the specific needs of the organization. This feature guides users through the process of creating a structured response plan to address potential cybersecurity incidents.

Resource Library: A built-in resource library provides users with access to best practices, guidelines, and tools related to cybersecurity. This library is continuously updated to reflect the latest trends and threats in the cybersecurity landscape.

Feedback Mechanism: The prototype incorporates a feedback mechanism that allows users to provide input on their experience and suggest improvements. This feature is essential for the continuous enhancement of the prototype based on user needs.

The development of the CCSF prototype represents a significant step towards empowering Palestinian MSMEs to enhance their cybersecurity posture. By providing a flexible and scalable solution, the prototype aims to facilitate informed decision-making and promote a culture of cybersecurity awareness within these organizations. Future iterations of the prototype will focus on incorporating feedback from users and integrating advanced features to further enhance its functionality and effectiveness.

4.3.4. Additional Functional Buttons

The CCSF prototype includes four additional functional buttons that enhance user interaction and streamline the overall experience as shown in the figure 4.3.4:

- Clear Fields Button: This button allows users to quickly erase all the information entered in the input fields. It is particularly useful for users who may want to start over or correct any mistakes without having to manually delete each entry. This feature promotes efficiency and reduces user frustration.
- Save Framework as Excel File Button: This functionality enables users to save the generated cybersecurity framework and recommendations as an Excel file. This feature

is beneficial for documentation purposes, allowing users to easily share the framework with stakeholders or keep a record for future reference. The saved file includes all relevant details, making it easy to review and implement the recommended controls.

- Clear Table Button: This button clears the table that displays the recommended cybersecurity controls and strategies. It allows users to refresh the view, especially after making changes to the input data or when they wish to generate a new set of recommendations. This feature ensures that users can maintain an organized and clear interface.
- Exit Button: The exit button provides a straightforward way for users to close the application. This feature ensures that users can easily terminate their session when they have completed their tasks, promoting a user-friendly experience.

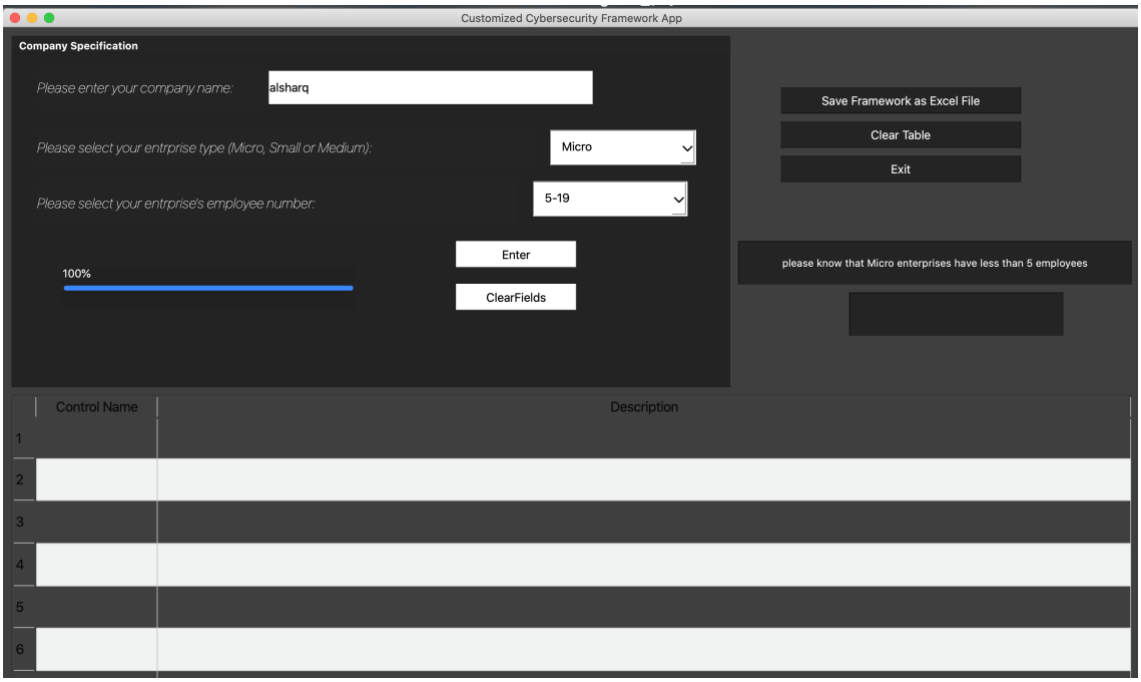


Figure 4.3.4: Prototype buttons and error messages.

4.4. Conclusion

In conclusion, this chapter has successfully outlined the proposed design of a Cybersecurity Framework specifically tailored for Micro, Small, and Medium Enterprises (MSMEs) in Palestine. The primary objective of this framework is to provide a customized approach that categorizes essential cybersecurity controls for each type of enterprise, ensuring that the unique needs and operational scales of these businesses are adequately addressed.

By leveraging the frameworks, standards, and tools reviewed in Chapter Two, along with data obtained from relevant companies and insights gathered from questionnaires, the chapter has established a structured methodology for implementing cybersecurity measures. The initial step involves inputting preliminary information into the designated software, which serves as a foundation for the subsequent deployment of tailored frameworks for each enterprise type.

For micro enterprises, the framework emphasizes the implementation of the minimum necessary controls to establish basic security, recognizing their limited resources and operational capacities. In contrast, small enterprises benefit from more comprehensive controls that enhance their protection against cyber threats. Medium enterprises are provided with a distinct set of controls that cater to their specific requirements, ensuring a robust cybersecurity posture.

This structured and tiered approach not only facilitates the effective implementation of cybersecurity measures across different enterprise types but also promotes a culture of security awareness and responsibility within the MSME sector. As these businesses navigate the complexities of the digital landscape, the proposed Cybersecurity Framework stands as a vital tool in safeguarding their assets and ensuring business continuity.

Moving forward, it is essential to continuously evaluate the effectiveness of this framework, adapt it to emerging threats, and engage with cybersecurity professionals to support MSMEs in their ongoing efforts to enhance their cybersecurity resilience. The successful implementation

of this framework will ultimately contribute to the long-term growth and sustainability of Palestinian MSMEs in an increasingly digital world.

Furthermore, the development of the CCSF prototype serves as a practical tool to facilitate the implementation of the framework. By allowing users to input relevant company information and receive customized recommendations, the prototype simplifies the process of adopting cybersecurity measures. The inclusion of interactive features, such as automated reporting and user awareness campaigns, underscores the commitment to empowering MSMEs in their cybersecurity journey.

As digitalization continues to permeate various sectors, the importance of robust cybersecurity measures cannot be overstated. The proposed framework and its accompanying prototype represent a significant advancement in safeguarding the interests of Palestinian MSMEs, ultimately contributing to their long-term growth and sustainability. Moving forward, it is essential to monitor the effectiveness of the framework, adapt it to emerging threats, and engage with cybersecurity professionals to ensure that these enterprises remain well-equipped to navigate the complexities of the digital landscape.

Chapter Five

5. Evaluation

5.

5.1. Introduction

There are two sets of measures in the evaluation process. The first is founded on quantitative measurements, such as job success. The second category is based on various qualitative factors, including prototype ease of use, the naturalness of system answers, appearance, text on screen, information structure, and error message clarity.

A questionnaire has been created to evaluate the programmed prototype. The user-friendly scales in the table make it straightforward to gather and analyze data after the examination.

5.2. Qualitative and Quantitative Measures

During this research, several qualitative and quantitative measures were taken to evaluate the developed prototype and measure user acceptance of the system produced.

5.2.1. Qualitative Measures

This study employed a qualitative methodology to assess the prototype's efficiency, user-friendliness, and overall user satisfaction, incorporating opinions and qualitative data analysis. Additionally, 15 participants were chosen randomly and asked to perform tasks in the prototype under different scenarios and to express their satisfaction or dissatisfaction with specific aspects of the prototype.

Capturing these measures is done through a user questionnaire. That was distributed to 15 people to answer.

- The system is easy to use: Measures user satisfaction with the prototype system’s simplicity, friendliness, flexibility, and effortlessness.

- Naturalness of system responses: user satisfaction with the language used.
- Good appearance: Measures user satisfaction with the language used.
- Good text type and size: measures user satisfaction with the text type and size.
- The organization of information: measures user satisfaction with the distribution of information in the interface.
- Meeting Expectations: This measure concerns user expectations and whether the system met these expectations.
- User understands error messages.

5.2.2. Quantitative Measures

Using data and metrics, this research used a quantitative approach to measure prototypes' effectiveness, usability, and performance. By calculating the following measures:

Task Success Rate: This refers to the percentage of tasks that users complete. To calculate it, divide the number of completed tasks by the number of tasks and multiply by 100. This metric measures the percentage of tasks that users successfully complete. A high task success rate suggests that users can effectively achieve their goals using the system. This is a crucial indicator of usability and overall system effectiveness.

Task Completion Time: Task completion time measures the duration it takes for users to finish tasks. You can calculate this by finding each task's mean or median completion time.

Error Rate: Error rate signifies the percentage of errors made by users during task execution. You can compute it by dividing the number of errors by the number of actions and multiplying by 100. This metric represents the frequency of errors made by users while interacting with the system. A low error rate indicates that the system is user-friendly and that users can navigate it with minimal mistakes. Reducing the error rate is essential for improving user satisfaction and efficiency.

Conversion Rate: The conversion rate is the percentage of users who take a desired action, like signing up or purchasing. This metric is calculated by dividing the number of conversions by the total number of users and multiplying the result by 100. This metric measures the percentage of users who complete a desired action, such as making a purchase or signing up for a newsletter. A conversion rate of approximately 0.2 suggests that a certain proportion of users are taking the desired actions. This metric is particularly important in evaluating the effectiveness of marketing strategies and user engagement.

Click-Through Rate (CTR): The proportion of users who click on an element, link, or feature by calculating the number of clicks on the element/number of users) multiplied by 100. This metric indicates the percentage of users who click on a specific link or call-to-action. A CTR of approximately 0.2 shows how well the system or content is capturing user interest and prompting them to take action. High CTRs are often associated with effective design and compelling content.

Each of these metrics provides valuable insights into different aspects of system performance and user interaction. By analyzing these metrics, you can identify strengths and areas for improvement, ultimately enhancing the overall user experience.

5.3. Results

Here are the results in the figure 5.3.1 below from the questionnaire distributed to 15 participants, indicating that the programmed prototype system is good, easy to use, and understandable

System is easy to use:

Result: The green bar reaches up to 18, while the blue bar reaches up to approximately 16. This indicates that both groups find the system relatively easy to use, with the green group rating it slightly higher.

Natural feel of system interaction:

Result: The green bar is at about 12, and the blue bar is around 6. The green group feels that the system interaction is more natural compared to the blue group, which has a significantly lower rating.

Good appearance:

Result: Both bars are equal, reaching up to about 16. Both groups agree that the system has a good appearance, with equal ratings for this category.

Organization of information:

Result: Both bars are equal, reaching up to approximately 17. Both groups find the organization of information to be well done, with high and equal ratings.

Meeting expectations:

Result: Both bars are around 15. Both groups feel that the system meets their expectations, with similar ratings.

User understanding of error message:

Result: Both bars reach up to about 14. Both groups have a similar understanding of error messages, with equal ratings in this category.

These results provide a comparative view of user feedback on various aspects of the system's usability and satisfaction levels.

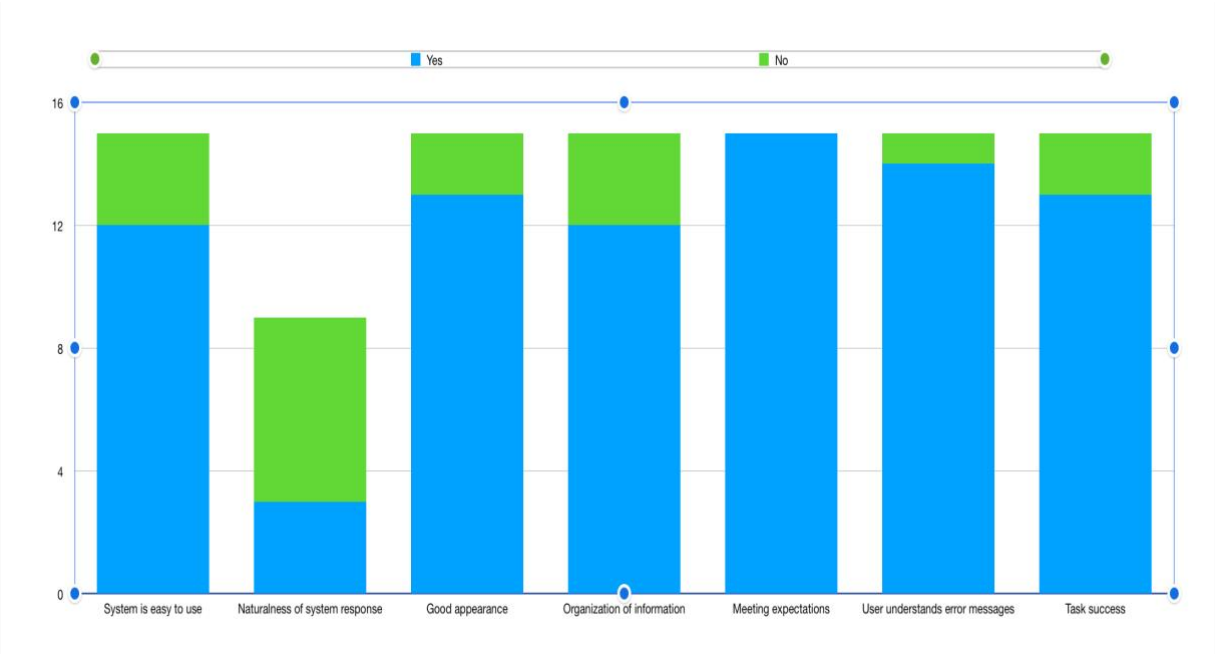


Figure 5.3.1: questionnaire results.

Figure 5.3.2 below displays the calculated percentages for the quantitative measures taken for 15 participants, as shown in the chart.

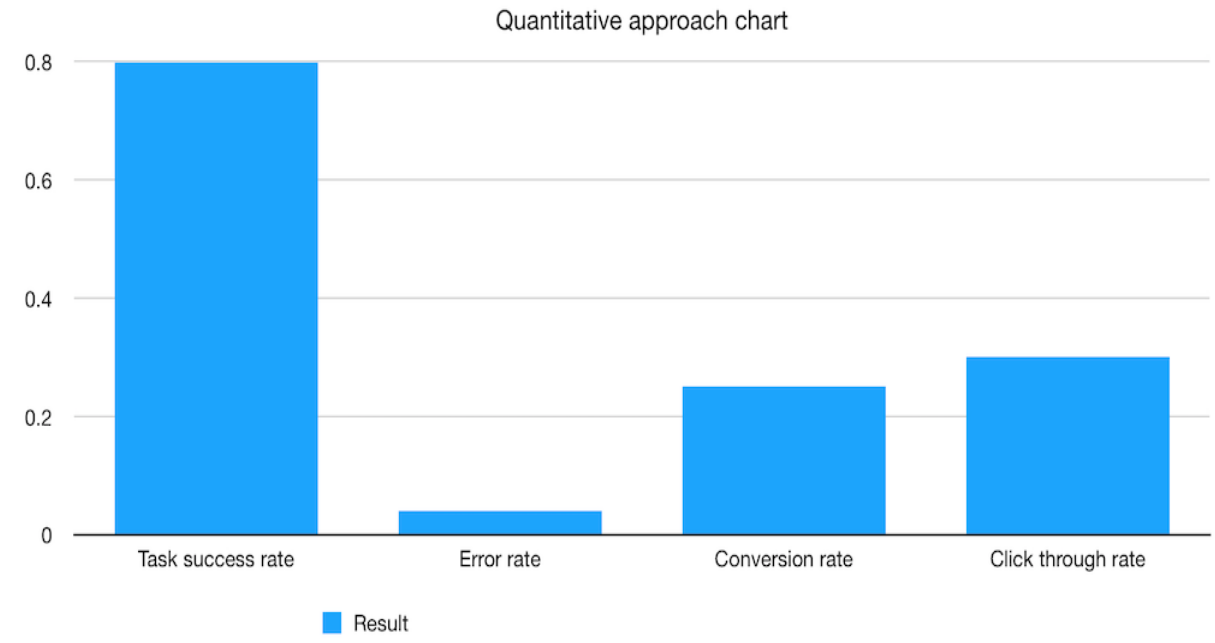


Figure 5.3.2: quantitative measures.

Here are the results from the graph in figure 5.3.2 along with their descriptions:

Task Success Rate:

Result: The bar reaches up to approximately 0.8 on the vertical axis. This indicates a high task success rate, meaning that users are successfully completing their tasks most of the time. This is a positive indicator of the system's usability and effectiveness.

Error Rate:

Result: The bar stands at roughly 0.1 on the vertical axis. This low error rate suggests that users are making few mistakes while interacting with the system. A low error rate is crucial for a smooth and efficient user experience.

Conversion Rate:

Result: The bar reaches up to approximately 0.1 on the vertical axis. This indicates a relatively low conversion rate, meaning that a smaller percentage of users are completing desired actions, such as making a purchase or signing up for a service. Improving this metric could be a focus area for enhancing user engagement and achieving business goals.

Click Through Rate (CTR):

Result: The bar reaches up to approximately 0.2 on the vertical axis. This suggests a moderate click-through rate, indicating that a certain percentage of users are clicking on links or call-to-action buttons. A higher CTR can be associated with effective content and design that captures user interest.

Task success rate = 12/15 *100% = 80%

Error rate = 2/50 *100% = 4%

Conversion rate = 3\15 *100% = 20%

Click through rate = 4/15 *100% = 26.6

Chapter Six

6. Conclusion and Future Work

6.

6.1. Conclusion

In conclusion, the development of a tailored Cybersecurity Framework for Micro, Small, and Medium Enterprises (MSMEs) in Palestine represents a significant advancement in addressing the unique cybersecurity challenges faced by these businesses. This research has highlighted the critical importance of a customized approach that aligns with the specific needs, resources, and operational contexts of MSMEs, which are often characterized by limited budgets and varying levels of cybersecurity awareness.

The proposed framework is designed to categorize essential cybersecurity controls based on the size and type of enterprise, ensuring that each business receives an appropriate level of protection. For micro enterprises, the focus is on implementing fundamental security measures that establish a baseline of protection, such as basic firewalls and antivirus software. Small enterprises benefit from a more comprehensive set of controls that enhance their security posture, while medium enterprises are equipped with tailored solutions that address their specific operational requirements and risk profiles.

Throughout this research, the integration of data obtained from relevant companies and insights gathered from questionnaires has been instrumental in shaping the framework. This evidence-based approach ensures that the framework is not only theoretically sound but also practically applicable in the real-world context of Palestinian MSMEs. The development of a user-friendly prototype software further facilitates the implementation process, allowing businesses to input

their specific information and receive customized recommendations for their cybersecurity strategies.

The implementation of this Cybersecurity Framework is expected to yield several positive outcomes, including improved threat detection capabilities, enhanced incident response strategies, and a heightened awareness of cybersecurity best practices among employees. By fostering a culture of cybersecurity within these organizations, the framework aims to empower MSMEs to take proactive measures in safeguarding their digital assets and ensuring business continuity in the face of increasing cyber threats.

Moreover, the framework serves as a foundational tool for promoting collaboration and information sharing among MSMEs, which can collectively strengthen their cybersecurity strategies. As these enterprises navigate the complexities of the digital landscape, the framework not only provides a roadmap for enhancing their defenses but also contributes to the overall economic stability and growth of the Palestinian business community.

In summary, the tailored Cybersecurity Framework represents a crucial step toward equipping Palestinian MSMEs with the necessary tools and knowledge to effectively combat cyber threats. As the digital landscape continues to evolve, ongoing efforts to refine and adapt this framework will be essential in ensuring that these enterprises remain resilient and competitive in an increasingly interconnected world.

6.2. Future Work

Looking ahead, there are several avenues for future work that can further enhance the effectiveness of the Cybersecurity Framework for MSMEs in Palestine. Key areas for development include:

- Integration of Crisis Management Strategies: Incorporating robust crisis management and resilience strategies into the framework will enable MSMEs to maintain operations during cyber incidents and recover more effectively.
- Regulatory Compliance: Staying abreast of evolving international cybersecurity regulations and integrating compliance measures into the framework will help MSMEs navigate legal requirements and enhance their credibility.
- Cloud Security Guidelines: Developing specific guidelines and best practices for MSMEs utilizing cloud services will address the unique security challenges associated with cloud technology adoption.
- Capacity Building and Training: Implementing capacity-building programs and training sessions for employees will enhance their understanding of cybersecurity threats and preventive measures, thereby strengthening the overall security posture of the organization.
- Simulation Exercises: Conducting simulation exercises to test and refine incident response plans will help identify areas for improvement and ensure that MSMEs are well-prepared to respond to real-world cyber incidents.
- Technological Applications: Exploring innovative technological solutions for securing financial transactions and sensitive data will further bolster the cybersecurity defenses of MSMEs.

By focusing on these areas, the Cybersecurity Framework can be continuously improved and adapted to meet the dynamic challenges posed by the digital landscape. Collaboration with international cybersecurity experts and ongoing engagement with the MSME community will be essential in achieving these goals and ensuring the long-term sustainability of Palestinian MSMEs in an increasingly interconnected world.

References

European Digital SME Alliance, "The EU Cybersecurity Act and the Role of Standards for SMEs," European Digital SME Alliance, 2020.

Wafa - The Palestinian News and Information Agency., "The Ministry of Economy Sets the Unified National Standards for the Definition and Classification of Economic Enterprises.," [Online]. Available: https://wafa.ps/Pages/Details/27197. [Accessed 5 September 2024].

United Nations Conference On Trade And Development, "Palestinian Small And Medium-Sized Enterprises: Dynamics And Contribution To Development," 2004. [Online]. Available: https://unctad.org/system/files/official-document/gdsapp20041_en.pdf. [Accessed 5 September 2024].

Palestine Economic Policy Research Institute MAS, "Problems of Micro, Small and Medium Enterprises in Palestine," 2009. [Online]. Available: https://library.palestineeconomy.ps/public/files/server/20152501091632-1.pdf. [Accessed 5 September 2024].

The Palestinian Central Bureau of Statistics pcbs , "The Number of establishments in the private sector, civil sector, and government companies in the rest of the West Bank and Gaza Strip by governorate and categories of labor size, 2007.," 2007. [Online]. Available: https://www.pcbs.gov.ps/Portals/_Rainbow/Documents/est_07a.htm. [Accessed 6 September 2024].

The European Union Agency For Cybersecurity, "MSME development policies and programmes in Palestine," EUROPEAN UNION, [Online]. Available: https://medmsmes.eu/palestine. [Accessed 8 September 2024].

M. Bayyoud, "Challenges in Financing Small and Medium Enterprises in Palestine," 2016. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=2844895. [Accessed 5 September 2024].

Mai Al Saifi, "Challenges Facing Micro, Small and Medium-Sized Enterprise (MSMEs) When Accessing Funds from Financial Institutions in the West Bank," 2021. [Online]. Available: https://www.ashwinanokha.com/resources/v20-4%20-%2021-104-mai.pdf. [Accessed 5 September 2024].

Nidal Sabri , " MSMEs in Palestine; challenges and potential," 2010. [Online]. Available: https://fada.birzeit.edu/bitstream/20.500.11889/4812/1/msmes%20in%20Palestine.pdf. [Accessed 5 September 2024].

Cybersecurity and Infrastructure Security Agency, "Cybersecurity Framework," [Online]. Available: https://us-cert.cisa.gov/resources/cybersecurity-framework. [Accessed 14 September 2024].

SSL Team, "Understanding the Zero Trust Security Model," [Online]. Available: https://www.ssl.com/article/understanding-the-zero-trust-security-model/. [Accessed 5 September 2024].

Wikipedia, "Frameworx," [Online]. Available: https://en.wikipedia.org/wiki/Frameworx. [Accessed 5 Septemeber 2024].

Gartner, "Midsize Enterprise (MSE)," [Online]. Available: https://www.gartner.com/en/information-technology/glossary/midsize-enterprise-mse#:~:text=Gartner%20defines%20midsize%20enterprise%20%28MSE%29%20as%20those%20organizations,by%20revenues%20or%20number%20of%20employees%20is%20arbitrary..

Hashem Ismail Ramadan and Saari bin Ahmad, "Issues and challenges of SMEs in Palestine," 2017. [Online]. Available: https://www.academia.edu/82229237/Issues_and_challenges_of_smes_in_Palestine. [Accessed 6 September 2024].

Nasr Atayni and Sara Al Haj Ali, "Problems of Micro, Small and Medium Enterprises in Palestine," 2009. [Online]. Available: https://library.palestineeconomy.ps/public/files/server/20152501091632-1.pdf. [Accessed 6 September 2024].

Nidal Rashid Sabri, Ahmed Jalad, Firas Melhem, Mohammad Khalifa, Nasr Atayni, Anton Sabella, Ibrahim Hantash, Muhannad Hamed, Fathi Srouji, Issam Abdeen, Nasr Abdelkarim, Obaida Salah and Sara Al Haj Ali, "International Experiences in Supporting MSMEs: Lessons for Palestine," 2010. [Online]. Available: https://library.palestineeconomy.ps/public/files/server/20152501091333-1.pdf. [Accessed 6 September 2024].

DCAF In Palestine, "Law by Decree No. 10 of 2018 on Cybercrime," 2018, [Online]. Available: https://security-legislation.ps/latest-laws/law-by-decree-no-10-of-2018-on-cybercrime/. [Accessed 6 September 2024].

IBM, "What is data security?," [Online]. Available: https://www.ibm.com/topics/data-security. [Accessed 14 September 2024].

The Cybersecurity and Infrastructure Security Agency (CISA), "What is Cybersecurity?," 2021. [Online]. Available: https://www.cisa.gov/news-events/news/what-cybersecurity. [Accessed 6 September 2024].

Dr. Mohammad Shtayyeh, "Cabinet Decision No. (5) of 2021 approving the Information Security Policy.," 2021. [Online]. Available: http://muqtafi.birzeit.edu/pg/getleg.asp?Id=17520. [Accessed 6 September 2024].

Hadeel Barham, "Cybersecurity and its Challenges in Light of Intellectual Property Rights.," 2021. [Online]. Available: https://repository.najah.edu/items/21675795-d8a3-4373-87de-69d56454a1c3. [Accessed 6 September 2024].

Palestine Monetary Authority PMA, "The Palestine Monetary Authority Obtains PCI-DSS Compliance Certification for Payment Card Data Security Standards.," 2018. [Online]. Available:

Https://www.pma.ps/ar/%D8%A7%D9%84%D8%A5%D8%B9%D9%84%D8%A7%D9%85/%D8%A8%D9%8A%D8%A7%D9%86%D8%A7%D8%AA-%D8%B5%D8%AD%D9%81%D9%8A%D8%A9/pci-

dss%D8%B3%D9%84%D8%B7%D8%A9-
%D8%A7%D9%84%D9%86%D9%82%D8%AF-%D8%AA%D8%AD%D8%B5%D9%84-
%D8%B9%D9%84%D9%89-%D8%B4%D9%87%D8. [Accessed 6 September 2024].

Samy S Abu Naser, "The Impact of Applying the Dimensions of IT Governance in Improving E-training - Case Study of the Ministry of Telecommunications and Information Technology in Gaza Governorates," 2017. [Online]. Available: https://www.academia.edu/96012095/The_Impact_of_Applying_the_Dimensions_of_IT_Governance_in_Improving_E_training_Case_Study_of_the_Ministry_of_Telecommunications_and_Information_Technology_in_Gaza_Governorates. [Accessed 6 September 2024].

Dr. Fady Draidi, "Information Security Management in Palestinian Banking," 2017. [Online]. Available: https://repository.najah.edu/items/3edfd240-9635-4d87-93e8-fa90b0f951db/full. [Accessed 6 September 2024].

UN, "Occupation, discrimination driving Israel-Palestine conflict, recurring violence," 2022. [Online]. Available: https://news.un.org/en/story/2022/06/1119912. [Accessed 6 September 2024].

Fabio Cristiano, "Palestine: Whose Cyber Security without Cyber Sovereignty?," 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?Abstract_id=3700850. [Accessed 14 September 2024].

UK Cyber Security Council, "Council of Professors and Heads of Computing (CPHC)," [Online]. Available: https://cphc.ac.uk/tag/cybersecurity/. [Accessed 10 September 2024].

The International Information System Security Certification Consortium, "The World’s Leading Cybersecurity Professional Organization," [Online]. Available: https://www.isc2.org/About#. [Accessed 10 September 2024].

Kaspersky, "What is Cyber Security?," [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed 10 September 2024].

Carole Theriault, "What is an information security framework and why do I need one?," TEG Security, [Online]. Available: https://tbgsecurity.com/what-is-an-information-security-framework-and-why-do-i-need-one/. [Accessed 14 September 2024].

European Commission, "Supporting specialised skills development: big data, Internet of Things and cybersecurity for SMEs.," European Commission, 2019.

Eduardo B. Fernandez, Nobukazu Yoshioka, Hironori Washizaki & Joseph Yoder, "Abstract security patterns and the design of secure systems," springeropen, 2022.

The security policy framework, "Security policy framework: protecting government assets," [Online]. Available: https://www.gov.uk/government/publications/security-policy-framework. [Accessed 10 September 2024].

Vishnu Venkatesh, "Design of Cybersecurity Risk Assessment Tool for Small and Medium Sized Businesses using the NIST Cybersecurity Framework".

National Institute of Standards and Technology, "NIST Cybersecurity Framework," [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 10 September 2024].

National Institute of Standards and Technology, "NIST," [Online]. Available: https://www.nist.gov/. [Accessed 10 September 2024].

The Information Technology Infrastructure Library (ITIL), "ITIL Library," [Online]. Available: https://www.itlibrary.org/. [Accessed 10 September 2024].

Lynn Greiner, Sarah K White., "What is ITIL? Your guide to the IT Infrastructure Library," 2019. [Online]. Available: https://www.cio.com/article/2439501/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html. [Accessed 10 September 2024].

CIO, "What is ITIL? Your guide to the IT Infrastructure Library," [Online]. Available: https://www.cio.com/article/272361/infrastructure-it-infrastructure-library-itil-definition-and-solutions.html. [Accessed 14 September 2024].

The Saudi Arabian Monetary Authority (Sama), "SAMA," 2017. [Online]. Available: https://www.niiconsulting.com/whitepapers/SAMA-Framework.pdf. [Accessed 7 September 2024].

Saudi Arabian Monetary Authority, "Cyber Security Framework SAMA," 2017. [Online]. Available: https://www.sama.gov.sa/en-US/Laws/bankingrules/SAMA%20Cyber%20Security%20Framework.pdf. [Accessed 7 September 2024].

The Center for Internet Security, Inc. (CIS), "About us," [Online]. Available: https://www.cisecurity.org/about-us. [Accessed 7 September 2024].

SANS Institute American security company, "CIS Controls v8," [Online]. Available: https://www.sans.org/blog/cis-controls-v8/. [Accessed 7 September 2024].

Wikipedia, "Center for Internet Security," [Online]. Available: https://en.wikipedia.org/wiki/Center_for_Internet_Security. [Accessed 7 September 2024].

BIS, "Structure of the consolidated Basel Framework," 2021. [Online]. Available: https://www.bis.org/baselframework/bcbs_framework_structure_211108.pdf. [Accessed 14 September 2024].

The Information Systems Audit and Control Association, "Selected COBIT 5 Processes for Essential Enterprise Security," [Online]. Available: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2015/volume-2/selected-cobit-5-processes-for-essential-enterprise-security_joa_eng_0315#:~:text=The%20three%20essential%20COBIT%205,range%20of%20threats%20and%20vulnerabilities.. [Accessed 10 September 2024].

Wekipedia, "Authentication, authorization, and accounting," [Online]. Available: https://en.wikipedia.org/wiki/Authentication,_authorization,_and_accounting. [Accessed 7 September 2024].

Identity Management Institute, "AAA Identity and Access Management Framework Model," [Online]. Available: https://identitymanagementinstitute.org/identity-and-access-management-model/. [Accessed 7 September 2024].

FORTINET, "AAA," [Online]. Available: https://www.fortinet.com/resources/cyberglossary/aaa-security. [Accessed 7 September 2024].

Geeks For Geeks, "What is AAA (Authentication, Authorization, and Accounting)?," 2020. [Online]. Available: https://www.geeksforgeeks.org/what-is-aaa-authentication-authorization-and-accounting/. [Accessed 7 September 2024].

IETF Organization, "Introduction to the IETF," [Online]. Available: https://www.ietf.org/about/introduction/. [Accessed 7 September 2024].

Hannes Tschofenig, Sebastien Decugis, Jean Mahoney, Jouni Korhonen, "Diameter: New Generation Aaa Protocol - Design, Practice, And Applications," in Diameter: New Generation Aaa Protocol - Design, Practice, And Applications, Vols. 1-7, Wiley Telecom, 2019.

Cisco, "Information About AAA," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/general/asa-general-cli/aaa-overview.pdf. [Accessed 7 September 2024].

International Organization for Standardization, "ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and

vocabulary," 2018. [Online]. Available: https://www.iso.org/standard/73906.html. [Accessed 6 September 2024].

International Organization for Standardization , "ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements," 2022. [Online]. Available: https://www.iso.org/standard/54534.html. [Accessed 6 September 2024].

International Organization for Standardization , "ISO/IEC 27002:2022 Information technology Security techniques Code of practice for information security controls," [Online]. Available: https://www.iso.org/standard/54533.html. [Accessed 6 September 2024].

International Organization for Standardization , "ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance," 2017. [Online]. Available: https://www.iso.org/standard/63417.html. [Accessed 6 September 2024].

International Organization for Standardization, "ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation," 2016. [Online]. Available: https://www.iso.org/standard/64120.html. [Accessed 6 September 2024].

International Organization for Standardization, "ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management," 2018. [Online]. Available: https://www.iso.org/standard/56742.html. [Accessed 6 September 2024].

International Organization for Standardization , "ISO/IEC 27006-1:2024," 2024. [Online]. Available: https://www.iso.org/standard/82908.html. [Accessed 6 September 2024].

International Organization for Standardization, "ISO/IEC 27017:2015," 2015. [Online]. Available: https://www.iso.org/standard/43757.html. [Accessed 6 September 2024].

International Organization for Standardization, "ISO/IEC 27018:2019," 2019. [Online]. Available: https://www.iso.org/standard/76559.html. [Accessed 6 September 2024].

International Organization for Standardization, "ISO/IEC 27019:2017," 2017. [Online]. Available: https://www.iso.org/standard/68091.html. [Accessed 6 September 2024].

ASQ.org, "What is the Plan-Do-Check-Act (PDCA) Cycle?," [Online]. Available: https://asq.org/quality-resources/pdca-cycle. [Accessed 6 September 2024].

International Organization for Standardization, "ISO 31000 Risk management," 2018. [Online]. Available: https://www.iso.org/iso-31000-risk-management.html/. [Accessed 6 September 2024].

Information Security Forum Organization (ISF) in the United Kingdom, "Standard Of Good Practice For Information Security 2020," 2020. [Online]. Available: https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/. [Accessed 6 September 2024].

Wikipedia, "Standard of Good Practice for Information Security," [Online]. Available: https://en.wikipedia.org/wiki/Standard_of_Good_Practice_for_Information_Security. [Accessed 7 September 2024].

Payment Card Industry (PCI), "Payment Card Industry (PCI) Payment Application Data Security Standard," [Online]. Available:

https://listings.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf. [Accessed 10 September 2024].

Wikipedia, "Payment Card Industry Data Security Standard," [Online]. Available: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard. [Accessed 7 September 2024].

Talend , "PCI DSS: Definition, 12 Requirements, and Compliance," [Online]. Available: https://www.talend.com/resources/pci-dss/. [Accessed 7 September 2024].

UK Goverment, "BS-7799," [Online]. Available: https://shop.bsigroup.com/. [Accessed 7 September 2024].

ENISA, "BS-7799 3," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/laws-regulation/rm-ra-standards/bs-7799-3. [Accessed 7 September 2024].

Wekipedia, "BS-7799," [Online]. Available: https://en.wikipedia.org/wiki/BS_7799. [Accessed 7 September 2024].

The International Society of Automation (ISA), "The International Society of Automation (ISA)," [Online]. Available: https://www.isa.org/. [Accessed 10 September 2024].

Wikipedia, "IEC 62443," [Online]. Available: https://en.wikipedia.org/wiki/IEC_62443. [Accessed 7 September 2024].

Cisco, "Securing industrial networks: What is ISA/IEC 62443?," [Online]. Available: https://www.cisco.com/c/en/us/td/docs/solutions/Verticals/iot_Security_Lab/IEC62443_WP.pdf. [Accessed 7 September 2024].

Lawrence Gordon ,Martin Loeb , Lei Zhou, "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model," Journal of Cybersecurity, p. 1–8, 2020.

NIST’s Information Technology Laboratory, Applied Cybersecurity Division, and the Baldrige Excellence Framework, "Baldrige Cybersecurity Excellence Builder Key Questions For Improving Your Organization’s Cybersecurity Performance," [Online]. Available: https://www.nist.gov/system/files/documents/2019/03/24/baldrige-cybersecurity-excellence-builder-v1.1.pdf. [Accessed 10 September 2024].

Michael Benz, Dave Chatterjee, "Calculated risk? A cybersecurity evaluation tool for SMEs," Business Horizons, vol. 63, no. 4, pp. 531-540, 2020.

Kis Keep It Simple, "Cybersecurity is more than just implementing a hardware or software solution—it's a process.," [Online]. Available: https://www.kiscc.com/cybersecurity/. [Accessed 7 september 2024].

Namirial Focus, "The K.I.S.S. principle for cyber security," [Online]. Available: https://focus.namirial.global/kiss-principle-cyber-security/. [Accessed 10 September 2024].

Cyseccoach, "Staying Ahead in 2024: The Latest Cybersecurity Trends You Need to Know," [Online]. Available: https://cyseccoach.com/cybersecurity-trends-for-the-year-ahead/. [Accessed 14 September 2024].

Alireza Shojaifar, Samuel A. Fricker, Martin Gwerder, "Elicitation of SME Requirements for Cybersecurity Solutions by Studying Adherence to Recommendations".

Cybersecurity for SMEs - SMESEC, "SMESEC Framework," [Online]. Available: https://www.smesec.eu/framework.html. [Accessed 7 September 2024].

The European Union Agency For Cybersecurity (Enisa), "Information security and privacy standards for SMEs/ ENISA," [Online]. Available: https://www.enisa.europa.eu/publications/standardisation-for-smes. [Accessed 7 September 2024].

The European Union Agency For Cybersecurity (Enisa), "Information security and privacy standards for SMEs Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises," 2015. [Online]. Available: https://www.enisa.europa.eu/. [Accessed 10 September 2024].

The Centre For Cyber Security Belgium (Ccb) In Partnership With The Cyber Security Coalition Belgium For Small And Medium-Sized Enterprises (SME)., "Cyber Security Guide For SME / Belgium," [Online]. Available: https://ccb.belgium.be/en/document/guide-sme. [Accessed 10 September 2024].

Christophe Ponsard, Philippe Massonet, Jeremy Grandclaudon, Nicolas Point, "From Lightweight Cybersecurity Assessment to SME Certification Scheme," in Ieee European Symposium On Security And Privacy Workshops (Euros&Pw)., Belgium, 2020.

The U.S. Department Of Labor, "Cybersecurity Small Firms Guide - SIFMA," [Online]. Available: https://www.sifma.org. [Accessed 7 September 2024].

Securities Industry and Financial Markets Association United States industry trade group, "Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Business," SIFMA, [Online]. Available: https://www.sifma.org/resources/general/small-firms-cybersecurity-guidance-how-small-firms-can-better-protect-their-business/. [Accessed 10 September 2024].

International Organization for Standardization , "ISO 44003," 2021. [Online]. Available: https://www.iso.org/standard/72801.html. [Accessed 6 September 2024].

California Building Industry Association, "Small Business Cybersecurity Workbook," CBIA; the Connecticut Small Business Development Center, [Online]. Available: https://www.cbia.com/resources/small-business/cybersecurity/small-business-cybersecurity-workbook/. [Accessed 7 September 2024].

Christophe Ponsard, Jeremy Grandclaudon and Sebastien Ba, "Survey and lessons learned on raising SME awareness about cybersecurity," in 5th Int. Conf. On Information Systems Security and Privacy, Prague, 2019.

Cabinet Office, National security and intelligence and Government Security Profession, "Policy paper Security policy framework: protecting government assets," [Online]. Available: https://www.gov.uk/government/publications/security-policy-framework. [Accessed 14 September 2024].

Global Knowledge, A Skillsoft Company, "Cybersecurity Glossary of Terms | Global Knowledge," 05 April 2022. [Online]. Available: https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/. [Accessed 14 September 2024].

International Telecommunication Union, "Global Cyber Security Index 2020," [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx. [Accessed 14 September 2024].

Norton, "115 cybersecurity statistics and trends you need to know in 2021," Norton, 05 April 2022. [Online]. Available: https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html. [Accessed 10 September 2024].

Varonis, "134 Cybersecurity Statistics and Trends for 2021.," 05 April 2022. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics. [Accessed 10 September 2024].

Fortinet, "Top 20 Most Common Types Of Cyber Attacks | Fortinet.," 05 April 2022. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks. [Accessed 14 September 2024].

Yusuf Perwej, "A Systematic Literature Review on the Cyber Security," 2022.

Internet Security Alliance (ISA), "Internet Security Alliance," [Online]. Available: https://isalliance.org/. [Accessed 7 September 2024].

Nicolas Poggi, "Cybersecurity Frameworks 101 – The Complete Guide," [Online]. Available: https://preyproject.com/blog/en/cybersecurity-frameworks-101/. [Accessed 10 September 2024].

Appendices

This section contains many sections like questionnaires, code, etc.

Appendix (1): Key informants' questionnaire

Participant Consent Form:

CONFIDENTIAL

The research title is A Cybersecurity Framework for Micro, Small, and Medium-Enterprises (MSMEs) in Palestine.

Please tick the following boxes:

1.	I verify that I have diligently examined the information sheet for the study mentioned above and have had all of my inquiries answered to my satisfaction.	☐
2.	By taking part in this research, I recognize that my participation is optional. I have the right to stop the experimental session at any time, without having to give a justification, and without it impacting any care or service.	☐
3.	I agree that any data collected may be used in journal and conference papers.	☐

_____

4.	I agree that any collected data may be passed as anonymous to other researchers via a publicly accessible database (e.g., http://www.physionet.org/).	
5.	I agree to take part in the above study.	

Participant Details:

CONFIDENTIAL

1. Age.

2. Gender.

3. Educational Qualifications.

4. Practical experiences.

5. Workplace.

Name of participant	Date	Signature
Name of person taking consent.	Date	Signature

Name of the researcher to contact if there are any problems: _____

One form for participant: 1 to be kept as part of the study documentation.

Key Informants Questions:

CONFIDENTIAL

Question 1	
What cyber-threat detection systems and processes do you have in place?	
Answer / Discussion	
Participant	

Question 2	
What basic measures do you put in place to protect your systems?	
Answer / Discussion	
Participant	

Question 3	
What factors do you use to determine whether or not someone or something is malicious?	
Answer / Discussion	
Participant	

Question 4	
How will you respond if and when a breach occurs?	
Answer / Discussion	
Participant	

Question 5

After a cyber-attack, how will you restore your business to normal?	
Answer / Discussion	
Participant	

Question 6	
What is the framework or protocol you choose to use, if there is any, and why?	
Answer / Discussion	
Participant	

Question 7	
Do you prefer using a specific framework or a customized framework for MSMEs?	
Answer / Discussion	
Participant	

Question 8	
In your opinion, what are the most critical factors in determining which framework to choose?	
Answer / Discussion	
Participant	

Question 9	
What are the most critical controls that must be in every company?	
Answer / Discussion	
Participant	

Question 10	
What are your daily procedures and processes to design a framework for MSMEs?	
Answer / Discussion	
Participant	

Signature:

I confirm that the answers and discussions for the scenarios are an accurate representation of what occurred during the meeting that took place on _____

Name: _____

Date: _____

Signature: _____

Appendix (2): MSMEs questionnaire

Participant Consent Form:

CONFIDENTIAL

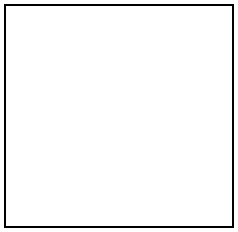
The research title is A Cybersecurity Framework for Micro, Small, and Medium-Enterprises (MSMEs) in Palestine.

Please tick the following boxes:

1.	I verify that I have diligently examined the information sheet for the study mentioned above, and have had all of my inquiries answered to my satisfaction.	☐
2.	By taking part in this research, I recognize that my participation is optional. I have the right to stop the experimental session at any time, without having to give a justification, and without it impacting any care or service.	☐
3.	I agree that any data collected may be used in journal and conference papers.	☐
4.	I agree that any collected data may be passed as anonymous to other researchers via a publicly accessible database (e.g., http://www.physionet.org/).	☐

_____

5. I agree to take part in the above study.



Participant Details:

CONFIDENTIAL

Participant detail

1. Age.

2. Gender.

3. Educational Qualifications.

4. Practical experiences.

5. Workplace.

Name of participant	Date	Signature
Name of person taking consent.	Date	Signature

Name of the researcher to contact if there are any problems: _____

One form for participant: 1 to be kept as part of the study documentation.

MSMEs Questions:

CONFIDENTIAL

Question 1	
What practices do you have in place to raise staff awareness about security, cyber risks, and privacy? If there is any if not, why?	
Answer / Discussion	
Participant	

Question 2	
Have your company Adopted any information security and privacy standards? If not, why?	
Answer / Discussion	
Participant	

Question 3	
Does your company design security and privacy standards tailored to MSMEs and consider their unique characteristics and procedures? If not, why?	
Answer / Discussion	
Participant	

Question 4
Has your company appointed an Information Security Officer? If not, why?

Answer / Discussion	
Participant	

Question 5
Does your company Provide professional training programs for Information Security Officers? If not, why?
Answer / Discussion
Participant

Question 6
Does top management get Involved in Cybersecurity decisions and practices? If not, why?
Answer / Discussion
Participant

Question 7
Does your company update all programs and apply patches in frequent phases? If not, why?
Answer / Discussion
Participant

Question 8	
Does your company have an antivirus protection software? If not, why?	
Answer / Discussion	
Participant	

Question 9	
Do you back up all information periodically? If not, why?	
Answer / Discussion	
Participant	

Question 10	
Do you manage the access to your computers and networks? If not, why?	
Answer / Discussion	
Participant	

Question 11	
Do you have processes to secure workstations and mobile devices? If not, why?	
Answer / Discussion	
Participant	

Question 12

Do you have any practices to secure servers and network components? If yes, what are they? If not, why?	
Answer / Discussion	
Participant	

Question 13	
Do you implement any practices to secure remote access? If yes, what are they? If not, why?	
Answer / Discussion	
Participant	

Question 14	
Does your system Have an incident handling plan? If not, why?	
Answer / Discussion	
Participant	

Question 15	
Does your company Publish the security policy and the code of conduct? If not, why?	
Answer / Discussion	
Participant	

Question 16

Do you prefer having a cyber threat level table to analyze the threat's danger and how to deal with every threat according to its level of risk?	
Answer / Discussion	
Participant	

Question 17	
Do you send Email alerts about threats? If not, why? And what do you use instead?	
Answer / Discussion	
Participant	

Question 18	
Do you have risk management? If not, why?	
Answer / Discussion	
Participant	

Question 19	
Do you analyze attitudes and behavior responses?	
Answer / Discussion	
Participant	

Question 20

Does your company have physical and environmental security? If not, why?	
Answer / Discussion	
Participant	

Question 21	
Does your company try to adopt the latest technology and services? If yes, what are they?	
Answer / Discussion	
Participant	

Question 22	
Does your company do human resources security before, during, and at the end of employment?	
Answer / Discussion	
Participant	

Question 23	
Does your company have an assets management like ownership… etc? If not, why?	
Answer / Discussion	
Participant	

Question 24	
Does your company do any information classification? If not, why?	
Answer / Discussion	
Participant	

Question 25	
Does your company have user responsibility management and user access management? If not, why?	
Answer / Discussion	
Participant	

Question 26	
Do you have system and application access control? If not, why?	
Answer / Discussion	
Participant	

Question 27
Do you have equipment security? If not, why?
Answer / Discussion

Participant	

Question 28	
Do you do the reporting and documentation stage? If not, why?	
Answer / Discussion	
Participant	

Question 29	
Do you have a logging and monitoring system? If not, why?	
Answer / Discussion	
Participant	

Question 30	
Do you have information system audits? If not, why?	
Answer / Discussion	
Participant	

Question 31	
Do you have network security management and communication security? If not, why?	
Answer / Discussion	
Participant	

Question 32	
Do you have any practices to secure information transfer? If not, why?	
Answer / Discussion	
Participant	

Question 33	
Do you implement any practices to do Information security reviews? If not, why?	
Answer / Discussion	
Participant	

Question 34	
Does your system have security in development and support processes? If not, why?	
Answer / Discussion	
Participant	

Question 35
Does your company comply with legal and contractual requirements to avoid breaches of legal, statutory, regulatory, or contractual obligations related to information security and any security requirements?
Answer / Discussion

Participant	

Question 36	
Does your company use cryptography to protect information?	
Answer / Discussion	
Participant	

Question 37	
Does your company use System acquisition, development, and maintenance security processes?	
Answer / Discussion	
Participant	

Question 38	
Do you test data protection? Test data shall be selected carefully, protected, and controlled.	
Answer / Discussion	
Participant	

Question 39
Do you have the protection of the organization's assets accessible by suppliers?
Answer / Discussion

Participant	

Question 40	
Does your information processing facilities have implemented redundancy sufficient to meet availability requirements?	
Answer / Discussion	
Participant	

Question 41	
Does your company handle media security to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media? If not, why?	
Answer / Discussion	
Participant	

Question 42	
Is your company equipped with robust recovery processes and procedures to swiftly restore systems or assets impacted by cybersecurity incidents? If so, could you elaborate on these protocols?	
Answer / Discussion	
Participant	

Question 43	
Does the organization comprehensively understand cybersecurity vulnerabilities affecting its operational functions, mission, reputation, corporate assets, and individuals? [2]	
Answer / Discussion	
Participant	

Question 44	
Are the organization's priorities, constraints, risk tolerances, and assumptions established and used to support risk decisions associated with managing supply chain risk?	
Answer / Discussion	
Participant	

Question 45	
Does your company use any extra processes or procedures for security that should be mentioned above? If yes, what are they?	
Answer / Discussion	
Participant	

Signature

I confirm that the answers and discussions for the scenarios are an accurate representation of what occurred during the meeting that took place on _____

Name: _____

Date: _____

Signature: _____

Appendix (3): Cybersecurity terms table

Q: To what degree would you rank your knowledge of the information security-related terms below? [95] [96] [97] [98] [99]			
Ransomware	1. Low	2. Average	3. High
Phishing	1. Low	2. Average	3. High
DoS and DDoS	1. Low	2. Average	3. High
MITM	1. Low	2. Average	3. High
Whale-phishing	1. Low	2. Average	3. High
Spear-phishing	1. Low	2. Average	3. High
Password Attack	1. Low	2. Average	3. High
SQL Injection Attack	1. Low	2. Average	3. High
URL Interpretation	1. Low	2. Average	3. High
DNS Spoofing	1. Low	2. Average	3. High
Session Hijacking	1. Low	2. Average	3. High
Brute force attack	1. Low	2. Average	3. High
Web Attacks	1. Low	2. Average	3. High
Insider Threats	1. Low	2. Average	3. High
Trojan Horses	1. Low	2. Average	3. High
Drive-by Attacks	1. Low	2. Average	3. High
XSS Attacks	1. Low	2. Average	3. High
Eavesdropping Attacks	1. Low	2. Average	3. High
Birthday Attack	1. Low	2. Average	3. High

Malware Attack	1. Low	2. Average	3. High
Transmitting SPAM	1. Low	2. Average	3. High
Clickjacking	1. Low	2. Average	3. High
Link jacking	1. Low	2. Average	3. High
JBOH (JavaScript-Binding-Over-HTTP)	1. Low	2. Average	3. High
Keylogger	1. Low	2. Average	3. High
Packet sniffing	1. Low	2. Average	3. High
Payment card skimmers	1. Low	2. Average	3. High
Penetration testing	1. Low	2. Average	3. High
Social engineering	1. Low	2. Average	3. High
Physical attacks	1. Low	2. Average	3. High
POS (Point of Sale) intrusions	1. Low	2. Average	3. High
Sniffing	1. Low	2. Average	3. High
Mac Spoofing	1. Low	2. Average	3. High
Spear phishing	1. Low	2. Average	3. High
Trojan Horse (Trojan)	1. Low	2. Average	3. High
Virus	1. Low	2. Average	3. High
Worm	1. Low	2. Average	3. High
Vishing	1. Low	2. Average	3. High
Spyware	1. Low	2. Average	3. High
Deepfake	1. Low	2. Average	3. High
Rootkit	1. Low	2. Average	3. High
Remote code execution attacks	1. Low	2. Average	3. High

WannaCry ransomware attack	1. Low	2. Average	3. High
Data breaches	1. Low	2. Average	3. High
Cloud-based cyber-attacks	1. Low	2. Average	3. High
Event-bot Trojan	1. Low	2. Average	3. High
Spam email	1. Low	2. Average	3. High
Fraudulent emails	1. Low	2. Average	3. High
Cryptocurrency ransomware payments	1. Low	2. Average	3. High
Stalker-ware	1. Low	2. Average	3. High
Adware	1. Low	2. Average	3. High
Crypto jacking	1. Low	2. Average	3. High
Malicious third-party apps	1. Low	2. Average	3. High
Botnet	1. Low	2. Average	3. High
Telnet	1. Low	2. Average	3. High
Zombie	1. Low	2. Average	3. High
Hacktivism	1. Low	2. Average	3. High
Encryption	1. Low	2. Average	3. High
DMZ	1. Low	2. Average	3. High
Hacker	1. Low	2. Average	3. High
Firewall	1. Low	2. Average	3. High
Identity theft	1. Low	2. Average	3. High
Access control	1. Low	2. Average	3. High
Authentication	1. Low	2. Average	3. High
Authorization	1. Low	2. Average	3. High

Bug	1. Low	2. Average	3. High
Cracker	1. Low	2. Average	3. High
Honeypot	1. Low	2. Average	3. High
ARP cache poisoning	1. Low	2. Average	3. High
Command injection	1. Low	2. Average	3. High
Steganography attacks	1. Low	2. Average	3. High
Backdoor attacks	1. Low	2. Average	3. High

Appendix (4): Employee awareness questionnaire

The research title is A Cybersecurity Framework for Micro, Small, and Medium-Enterprises (MSMEs) in Palestine

Participant Consent Form

[CONFIDENTIAL]:

Please tick the following boxes:

1.	I verify that I have diligently examined the information sheet for the study mentioned above and have had all of my inquiries answered to my satisfaction.	☐
2.	By taking part in this research, I recognize that my participation is optional. I have the right to stop the experimental session at any time, without having to give a justification, and without it impacting any care or service.	☐
3.	I agree that any data collected may be used in journal and conference papers.	☐
4.	I agree that any collected data may be passed as anonymous to other researchers via a publicly accessible database (e.g., http://www.physionet.org/).	☐

5. I agree to take part in the above study.

Employees' Questions

[CONFIDENTIAL]:

Part One. Organization policies and regulations:				
	Does your company employ a dedicated security team?	1. Yes	2. No	3. Not Applicable
	Are there specific guidelines in place at your company regarding which websites are allowed to be visited?	1. Yes	2. No	3. Not Applicable
	Are there specific company policies that outline the acceptable and unacceptable uses of email?	1. Yes	2. No	3. Not Applicable
	Are employees allowed to use instant messaging within the company?	1. Yes	2. No	3. Not Applicable
	Are you using your mobile phone or other devices to securely store or transfer sensitive company data?	1. Yes	2. No	3. Not Applicable
	Have you recently downloaded and installed software on your office computer?	1. Yes	2. No	3. Not Applicable
	Do you take material from the office and work it on your home computer?	1. Yes	2. No	3. Not Applicable
	Have you used public computers, such as those at a library, café, or hotel lobby, to access your business accounts?	1. Yes	2. No	3. Not Applicable
	Do you know who to call if you've been hacked or infected with your computer?	1. Yes	2. No	3. Not Applicable
	Have your supervisor or anyone else at work asked you for your password?	1. Yes	2. No	3. Not Applicable

Part Two: a. Which of the following do you/ your company use?				
1.	Anti-Virus	1. Used	2. Not Used	3. I don't know
2.	Firewall	1. Used	2. Not Used	3. I don't know
3.	Web filter	1. Used	2. Not Used	3. I don't know
4.	Spam filter	1. Used	2. Not Used	3. I don't know
5.	Thin client	1. Used	2. Not Used	3. I don't know
6.	Encryption	1. Used	2. Not Used	3. I don't know
7.	Cloud computing	1. Used	2. Not Used	3. I don't know

Part Two. b. Practices:				
	Have you ever shared your work password with someone else?	1. Yes	2. No	3. Not Applicable
	Is your computer's firewall turned on?	1. Yes	2. No	3. Not Applicable
	Is your computer set up to get updates automatically?	1. Yes	2. No	3. Not Applicable
	Is your anti-virus software up to date, installed, and enabled on your computer?	1. Yes	2. No	3. Not Applicable
	Have you been careful when you open an attachment in an email?	1. Yes	2. No	3. Not Applicable
	Do you use the same passwords for your work and personal accounts, such as Facebook, Twitter, and email?	1. Yes	2. No	3. Not Applicable
	Have you ever discovered malware or Trojan on your work computer?	1. Yes	2. No	3. Not Applicable
	I would use a copy of commercially available software made by a friend.	1. Yes	2. No	3. Not Applicable

Part Three. a. Knowledge questions:				
	Are you aware of an email scam, and how do you spot one?	1. Yes	2. No	3. Not Applicable
	Do you understand what a phishing scam is?	1. Yes	2. No	3. Not Applicable
	What do you think? If you delete a file from your computer or USB stick, you can no longer recover that information.	1. Yes	2. No	3. Not Applicable
	Do you know if your computer is hacked or infected?	1. Yes	2. No	3. Not Applicable
	What do you think? If you format a hard drive or erase its files, is all its information permanently lost?	1. Yes	2. No	3. Not Applicable
	What do you think? Your computer has no value to hackers: they do not target you.	1. Yes	2. No	3. Not Applicable
	Do you feel your computer is secure?	1. Yes	2. No	3. Not Applicable
	I have a problem monitoring email and Web browsing as a security measure.	1. Yes	2. No	3. Not Applicable

Part Three: b. Do you know the information security-related terms below?				
	Ransomware	1. Yes	2. No	3. Not Applicable
	Phishing	1. Yes	2. No	3. Not Applicable
	DoS and DDoS	1. Yes	2. No	3. Not Applicable
	MITM	1. Yes	2. No	3. Not Applicable
	Whale-phishing	1. Yes	2. No	3. Not Applicable
	Spear-phishing	1. Yes	2. No	3. Not Applicable
	Password Attack	1. Yes	2. No	3. Not Applicable
	SQL Injection Attack	1. Yes	2. No	3. Not Applicable
	URL Interpretation	1. Yes	2. No	3. Not Applicable
	DNS Spoofing	1. Yes	2. No	3. Not Applicable
	Session Hijacking	1. Yes	2. No	3. Not Applicable
	Brute force attack	1. Yes	2. No	3. Not Applicable
	Web Attacks	1. Yes	2. No	3. Not Applicable
	Insider Threats	1. Yes	2. No	3. Not Applicable
	Trojan Horses	1. Yes	2. No	3. Not Applicable
	Drive-by Attacks	1. Yes	2. No	3. Not Applicable
	XSS Attacks	1. Yes	2. No	3. Not Applicable
	Eavesdropping Attacks	1. Yes	2. No	3. Not Applicable
	Birthday Attack	1. Yes	2. No	3. Not Applicable
	Malware Attack	1. Yes	2. No	3. Not Applicable

Part Four. Background questions:					
	Gender:	1. Male			2. Female
	Company name:	_ _			
	Position within the company:	1. Full time	2. Part-time	3. Trainee	
	Age:	_ _			
	Marital status:	1. Single	2. Married	3. Divorced	4. Widowed
	Education level:	1. High school or less	2. Bachelor	3. Master	3. PhD
	Governorate:	_ _			
	The interview ends at (in hours and minutes):	_ _ _ /_ _ _			

Appendix (5): Evaluation questionnaire

Participant Consent Form:

CONFIDENTIAL

The research title is A Cybersecurity Framework for Micro, Small, and Medium-Enterprises (MSMEs) in Palestine.

Please tick the following boxes:

1.	I verify that I have diligently examined the information sheet for the study mentioned above, and have had all of my inquiries answered to my satisfaction.	☐
2.	By taking part in this research, I recognize that my participation is optional. I have the right to stop the experimental session at any time, without having to give a justification, and without it impacting any care or service.	☐
3.	I agree that any data collected may be used in journal and conference papers.	☐
4.	I agree that any collected data may be passed as anonymous to other researchers via a publicly accessible database (e.g., http://www.physionet.org/).	☐

5. I agree to take part in the above study.

Participant Details:

CONFIDENTIAL

1. Age.

2. Gender.

3. Educational Qualifications.

4. Practical experiences.

5. Workplace.	

Name of participant	Date	Signature
Name of person taking consent.	Date	Signature

Appendix (6): Evaluation Questions

CONFIDENTIAL

Evaluation questionnaire			
The system is easy to use	1. YES	2.NO	N/A
The naturalness of system responses	1. YES	2.NO	N/A
Good appearance	1. YES	2.NO	N/A
Good text type and size	1. YES	2.NO	N/A
Organization of information	1. YES	2.NO	N/A
Meeting Expectations	1. YES	2.NO	N/A
The user understands error messages	1. YES	2.NO	N/A
Task success	1. YES	2.NO	N/A

Appendix (7): Code

```
import sys
import json
import folium
import webbrowser
import re
import pandas as pd
import openpyxl
from PyQt6 import QtWidgets, uic , QtCore , QtGui
from PyQt6.QtWidgets import QApplication, QWidget,  QProgressBar
from PyQt6.QtWidgets import QTableWidget, QTableWidgetItem, QHeaderView, QSizePolicy
from PyQt6.QtCore import QBasicTimer,Qt, QSortFilterProxyModel
from PyQt6.QtGui import QStandardItemModel, QStandardItem
from PyQt6.uic import *



class AppDemo(QtWidgets.QMainWindow):
 def __init__(self):
  super(AppDemo, self).__init__()
  QtWidgets.QMainWindow.__init__(self)
  uic.loadUi('Main menu copy.ui', self)
  self.setWindowTitle("Customized Cybersecurity Framework App")
  """self.table.setRowCount(20)
```

```
 self.table.setColumnCount(2)
 self.table.setStyleSheet('font-size: 16px : height: 30px')
 self.table.setHorizontalHeaderLabels(["Control Name","Description"])"""
 self.buttonexit.clicked.connect(self.exitProgram)
 self.buttonsave.clicked.connect(self.saveProgram)
 self.buttonclear.clicked.connect(self.clearTable)
 self.buttonclear2.clicked.connect(self.clearFields)
 self.buttonsearch.clicked.connect(self.selectType)
 #self.table.setFixedWidth(self.table.columnWidth(0) + self.table.columnWidth(1))

 self.table.resizeColumnsToContents()
 self.table.resizeRowsToContents()

 self.timer = QBasicTimer()
 self.step = 0



def progressBar(self):


 if self.timer.isActive():
self.timer.stop()
 if self.step > 100:
self.timer.stop()
return
```

```
 self.step +=99
 self.progressbar.setValue(self.step)

def exitProgram(self):
 try:
demo.close()
sys.exit()
 except SystemExit:
print("Closing window...")

def saveProgram(self):
 df_json.to_excel('DATAFILE.xlsx')
 self.label2.clear()
 self.label2.setText("Export to Excel-File completed")

def clearTable(self):
 self.label2.clear()
 self.table.clear()
 self.table.setHorizontalHeaderLabels(["Control Name","Description"])

def clearFields(self):
 self.label1.clear()
 self.label2.clear()
```

```
 self.lineEdit.clear()
 self.combobox.clear()
 self.combobox2.clear()


def selectType(self):
 self.label2.clear()
 self.table.setRowCount(20)
 self.table.setColumnCount(2)
 self.table.setStyleSheet('font-size: 16px : height: 30px')
 self.table.setHorizontalHeaderLabels(["Control Name","Description"])
 self.table.clear()
 self.table.setHorizontalHeaderLabels(["Control Name","Description"])
 count = 0
 count2 = 0
 value = self.combobox.currentIndex()
 value2 = self.combobox2.currentIndex()

 if value == 0 and value2 == 0:
c1 = 0
c2 = 0
self.table.setRowCount(20)
wb = openpyxl.load_workbook("Customized Cybersecurity Framework.xlsx")
ws = wb["Micro"]
```

```
for col in ws.iter_cols(1, ws.max_column):
 for row in range(1, ws.max_row):
  self.table.setItem( c2, c1 , QTableWidgetItem(str(col[row].value)))
  self.table.resizeColumnsToContents()
  self.table.resizeRowsToContents()
  c2= c2 +1
  self.step = c2
  self.progressBar()
 c2 = 0
 c1= c1 +1
 count= count +1


  elif value == 1 and value2 == 1:
c1 = 0
c2 = 0
self.table.setRowCount(26)
wb = openpyxl.load_workbook("Customized Cybersecurity Framework.xlsx")
ws = wb["Small"]
for col in ws.iter_cols(1, ws.max_column):
 for row in range(1, ws.max_row):
  self.table.setItem( c2, c1 , QTableWidgetItem(str(col[row].value)))
  self.table.resizeColumnsToContents()
  self.table.resizeRowsToContents()
  c2= c2 +1
```

```
 c2 = 0
 c1= c1 +1
 count= count +1
 self.step = c2
 self.progressBar()
  elif value == 2 and value2 == 2:
c1 = 0
c2 = 0
self.table.setRowCount(28)
wb = openpyxl.load_workbook("Customized Cybersecurity Framework.xlsx")
ws = wb["Medium"]
for col in ws.iter_cols(1, ws.max_column):
 for row in range(1, ws.max_row):
  self.table.setItem( c2, c1 , QTableWidgetItem(str(col[row].value)))
  self.table.resizeColumnsToContents()
  self.table.resizeRowsToContents()
  c2= c2 +1
 c2 = 0
 c1= c1 +1
 count= count +1
 self.step = c2
 self.progressBar()

  elif value == 0 and value2 == 1:
```

```
self.label2.clear()
self.label2.setText("please know that Micro enterprises have less than 5 employees")
count2= count2 +1

 elif value == 0 and value2 == 2:
self.label2.clear()
self.label2.setText("please know that Micro enterprises have less than 5 employees")
count2= count2 +1

 elif value == 1 and value2 == 0:
self.label2.clear()
self.label2.setText("please know that Small enterprises have employees between 5-19")
count2= count2 +1

 elif value == 1 and value2 == 2:
self.label2.clear()
self.label2.setText("please know that Small enterprises have employees between 5-19")
count2= count2 +1

 elif value == 2 and value2 == 0:
self.label2.clear()
self.label2.setText("please know that Medium-Enterprises have employees between 20-49")
count2= count2 +1
```

```
 elif value == 2 and value2 == 1:
 self.label2.clear()
 self.label2.setText("please know that Medium-Enterprises have employees between 20-49")
 count2= count2 +1

 if count > 0 and count2 == 0:
self.label2.clear()
self.label2.setText("Framework customized successfully")
 elif count2 == 0:
self.label2.clear()
self.label2.setText("No option found")

 searchkeyword =str(self.lineEdit.text())
 if searchkeyword == "":
self.label1.clear()
self.label1.setText("Please enter your company name")
 else:
self.label1.clear()

 self.table.resizeColumnsToContents()
 self.table.resizeRowsToContents()

if __name__ == '__main__':
app = QApplication(sys.argv)
```

```
demo = AppDemo()

demo.show()


try:

sys.exit(app.exec())

except SystemExit:

print("Closing window...")
```

الملخص

تقدم هذه الرسالة إطار عمل شامل للأمن السيبراني مصمم خصيصًا للمؤسسات الصغيرة والمتوسطة في فلسطين، حيث يتناول التحديات الفريدة التي تواجهها هذه الأعمال في بيئة رقمية متزايدة. لقد أدت التطورات السريعة في تكنولوجيا المعلومات إلى زيادة الاعتماد على الأنظمة الرقمية، مما جعل المؤسسات الصغيرة والمتوسطة عرضة بشكل خاص للتهديدات السيبرانية. نظرًا لدورها الحيوي في الاقتصاد الفلسطيني، من الضروري تطوير استراتيجيات للأمن السيبراني تكون فعالة ومصممة خصيصًا لتلبية الاحتياجات والقيود الخاصة بهذه المؤسسات.

تم تصميم الإطار المقترح بعناية ليقدم مرونة وقابلية للتوسع، مما يتناسب مع الموارد المتنوعة والقدرات التشغيلية للمؤسسات الصغيرة والمتوسطة. ويجمع بين المكونات التقنية وغير التقنية، مما يضمن نهجًا شاملاً للأمن السيبراني. تشمل العناصر الرئيسية للإطار دمج معلومات التهديدات، ومنهجيات تقييم المخاطر، وحملات توعية مخصصة للمستخدمين تكون ذات صلة بالسياق البيئي التشغيلي للمؤسسات الصغيرة والمتوسطة .لتقييم فعالية الإطار وملاءمته، تستخدم هذه الدراسة منهجية مختلطة، تعتمد على تقنيات البحث النوعي مثل دراسات الحالة، والاستطلاعات، ومقابلات الخبراء. تسهل هذه المنهجية فهمًا شاملاً للمشهد الحالي للأمن السيبراني للمؤسسات الصغيرة والمتوسطة في فلسطين، مما يمكّن من تحديد الثغرات الحرجة وتطوير استراتيجيات مستهدفة للتخفيف من المخاطر. من المتوقع أن توفر نتائج هذه الدراسة رؤى قيمة حول تطوير وتنفيذ تدابير الأمن السيبراني التي لا تقتصر على المؤسسات الصغيرة والمتوسطة الفلسطينية فحسب، بل يمكن تطبيقها أيضًا في سياقات اقتصادية وجيوسياسية مماثلة. من خلال تزويد هذه المؤسسات بالأدوات والمعرفة اللازمة للتنقل في مشهد التهديدات السيبرانية المتزايد، تهدف هذه الدراسة إلى تعزيز حماية أصولها الرقمية، وضمان استمرارية الأعمال، وتعزيز بيئة آمنة تعزز النمو على المدى الطويل.

في النهاية، تسهم هذه الرسالة في النقاش الأوسع حول الأمن السيبراني في قطاع المؤسسات الصغيرة والمتوسطة، مما يبرز أهمية الأطر المصممة خصيصًا التي تأخذ في الاعتبار التحديات والموارد المحلية. من المتوقع أن يؤدي التنفيذ الناجح لإطار عمل الأمن السيبراني المقترح إلى تعزيز مرونة المؤسسات الصغيرة والمتوسطة الفلسطينية، وبالتالي دعم خلق فرص العمل، وتخفيف الفقر، والاستقرار الاقتصادي العام في المنطقة.