

INSTITUTE *of*
TECHNOLOGY

CARLOW

Institiúid Teicneolaíochta Cheatharlach

**“INVESTIGATING THE CURRENT INFORMATION
SECURITY PRACTICES OF THE SMEs: THREATS TO
INFORMATION SECURITY AND BARRIERS TO
IMPLEMENT PREREQUISITE INFORMATION SECURITY
MEASURES FOR THE SMEs.”**

Student Name: Srikanth Chundu

Student ID: C00246158

CW_KRITM_M_Y5

Masters of Science

in

Information Technology Management

Supervisor: Mr. Martin McNamara

Institute of Technology Carlow

LIFELONG LEARNING CENTRE

**Work submitted for assessment which does not include this declaration
will not be assessed.**

Declaration

- I declare that all materials in this submission are entirely my work was duly acknowledged.
- I have cited the sources of all paraphrases, summaries, quotations of information, tables, diagrams, or other material; including software and electronic media in which intellectual property rights may reside.
- I have provided a complete bibliography of all my works and sources used in the preparation of this submission.
- I understand that failure to comply with the institute regulations governing plagiarism constitutes a serious offense.

Student Name:	Srikanth Chundu
Student Number:	C00246158
Programme Title & Yr:	MSc.IT Management & Y5 (2019-20)
Module :	Dissertation
Signature:	ch.srikanth
Date:	29 th June 2020

Acknowledgments

I would like to sincerely thank a few important individuals who supported, assisted, and inspired me to complete this dissertation.

Professor Martin McNamara, supervisor of my dissertation.

This research would not have been possible without the participants who gave their precious time to participate in surveys.

I would like to finish by thanking my family and friends who have always been there to encourage me.

Abstract

Small and medium-sized IT organizations mostly rely on their IT systems to achieve the organization's goals. Technological innovations develop new opportunities to enhance organizational effectiveness and operations. They also create numerous security threats to the data in SMEs. The recognition of such information security threats, information security practices following by the SMEs to prevent threats and barriers to implement information security practices, is important in the growth and sustainability of the SMEs. This research aims to investigate the current information security practices of the SMEs, threats to information security, and barriers to implementing information security practices for SMEs in Ireland.

Several theories and studies by various researchers, referring to journals, textbooks, articles, and annual conference reports are discussed in the literature review which examined the information security practices, threats, and barriers for the SMEs. Gaps observed in the literature review are further investigated by conducting the surveys in two phases where 16 responses were recorded. The findings from the survey results on information security are represented in the form of charts and diagrams. Analysis of these results further demonstrated how it applies to the literature review and research questions by putting forward an argument to support the endpoint.

This research will highlight the relationship between employees, policies and procedures, and different managements such as network security management, risk management, and business continuity management of the organizations where one affects the other. This research will also highlight major threats that are inflicting more damage to the organizations and major barriers to implement prerequisite information security measures by the SMEs.

Table of Contents:

Chapter 1: Introduction.....	1
1.1 Problem Statement.....	1
1.2 Research Background.....	1
1.3 Research Aim.....	2
1.4 Research Objectives.....	2
1.5 Proposed Title of Dissertation.....	2
1.6 Research Questions.....	3
1.7 Client Organization.....	3
1.8 Rationale for the Study.....	3
1.9 Structure of the Dissertation.....	4
1.9.1 Literature Review	4
1.9.2 Methodology.....	4
1.9.3 Results.....	5
1.9.4 Discussion.....	5
1.9.5 Conclusion:.....	5
Chapter 2: Literature Review.....	6
2.1. Section 1: Introduction.....	6
2.2. Section 2: Information Security Definitions.....	6
2.2.1 Principals of Information Security.....	7
2.3. Section 3: Information Security Practices.....	7
2.3.1 Employees.....	8
2.3.2 Policies and Procedures.....	9
2.3.3 Network Security and Associated Infrastructure.....	10
2.3.4 Risk Management.....	11
2.3.5 Business Continuity Management.....	11
2.4. Section 4: Threats to Information Security.....	12
2.4.1 Insider Threats.....	13
2.4.2 Technical Threats (System-specific).....	13
2.4.3 Environmental and Physical Threats.....	16
2.5. Section 5: Barriers for the SMEs to Implement the Prerequisite Information Security Practices.....	16
2.5.1 Lack of Expertise and Knowledge.....	17

2.5.2 Implementation Costs.....	17
2.5.3 Lack of Resources and Capital.....	18
2.6. Section 6 : Conclusion.....	18
Chapter 3: Methodology.....	20
3.1 Introduction.....	20
3.2 Research Questions.....	20
3.3 Research Philosophy.....	20
3.4 Research Design.....	21
3.5 Quantitative Methodology, Descriptive Method, and Research Survey.....	22
3.5.1 Quantitative Methodology.....	22
3.5.2 Descriptive Method.....	23
3.5.3 Survey Research.....	23
3.5.4 Cross-Sectional Survey.....	24
3.6 Approach.....	24
3.7 Data Collection Methodology.....	25
3.7.1 Primary Research Data Collection.....	27
3.7.2 Secondary Research Data Collection.....	27
3.8 Research Data Analysis.....	27
3.9 Reliability and Validity.....	28
3.10 Triangulation.....	29
3.11 Research Ethical Issues.....	29
3.12 Limitations.....	29
3.13 Conclusion.....	30
Chapter 4: Results.....	31
4.1 Introduction.....	31
4.2 Quantitative Findings.....	31
4.3 Demographic Findings.....	33
4.4 Current Information Security Practices.....	36
4.4.1 Employees.....	36
4.4.2 Policies and Procedures.....	44
4.4.3 Network Security and Associated Infrastructure.....	46
4.4.4 Risk Management.....	47
4.4.5 Business Continuity Management.....	50
4.4.6 Correlation coefficient test.....	52

4.5 Threats to Information Security.....	57
4.5.1 Insider threats, Technical Threats (System-specific), and Environmental and Physical threats.....	59
4.6 Barriers to Implement Prerequisite Information Security Measures....	62
4.6.1 Lack of Expertise and Knowledge, Implementation Costs, and Lack of Resources and Capital.....	62
4.7 Conclusion.....	64
Chapter 5: Discussion.....	65
5.1 Introduction.....	65
5.2 Profile of the Participants.....	65
5.3 Data Triangulation.....	65
5.4 Current Information Security Practices.....	71
5.5 Threats to Information Security.....	75
5.6 Barriers to Implement Prerequisite Information Security Measures....	76
5.7 Conclusion.....	77
Chapter 6: Conclusion.....	79
6.1 Introduction.....	79
6.2 Current Information Security Practices.....	79
6.3 Threats to Information Security.....	80
6.4 Barriers to Implement Prerequisite Information Security Measures....	81
6.5 Recommendations.....	82
6.6 Future Research:.....	83
7.References.....	84
8.Appendices.....	93
8.1 Questionnaire:.....	100

List of Figures:

Figure 1: Represents the percentages of the magnitude of the organizations (survey 1).....	33
Figure 2: Represents the percentages of the magnitude of the organizations (survey 2).....	34
Figure 3: Represents the no.of organizations belongs to individual IT sectors (survey 1).	35
Figure 4: Represents the no.of organizations belongs to individual IT sectors (survey 2).	35
Figure 5: Represents the percentages of employment roles of the participants in the organizations (survey 1).	37
Figure 6: Represents the percentages of employment roles of the participants in the organizations (survey 2).....	38
Figure 7: Represents the percentages of the importance of information security in organizations (survey 1).....	39
Figure 8: Represents the percentages of the importance of information security in organizations (survey 2).....	39
Figure 9: Represents the percentages of confidence of the organizations in their information security framework (survey 1).....	40
Figure 10: Represents the percentages of confidence of the organizations in their information security framework (survey 2).....	41
Figure 11: Represents the percentages of the type of awareness briefings and training methods in the organizations (survey 1).....	42
Figure 12: Represents the percentages of the type of awareness briefings and training methods in the organizations (survey 2).....	42
Figure 13: Represents the percentages of how often the training programs are conducting by your organizations (survey 1).....	43
Figure 14: Represents the percentages of how often the training programs are conducting by your organizations (survey 2).....	44
Figure 15: Represents the percentages of confidence of the organizations on information security policies and procedures (survey 1).....	45
Figure 16: Represents the percentages of confidence of the organizations on information security policies and procedures (survey 2).....	45

Figure 17: Represents the percentages of information security measures implemented in the organizations. (survey 1).....	46
Figure 18: Represents the percentages of information security measures implemented in the organizations. (survey 2).....	47
Figure 19: Represents the percentages of confidence of the organizations on information security risk management (survey 1).....	48
Figure 20: Represents the percentages of confidence of the organizations on information security risk management (survey 2).....	48
Figure 21: Shows the percentage of the organizations that implemented a business continuity plan (survey 1).....	49
Figure 22: Shows the percentage of the organizations that implemented a business continuity plan (survey 2).....	50
Figure 23: Represents the percentages of confidence of the organizations on their business continuity management (survey 1).....	51
Figure 24: Represents the percentages of confidence of the organizations on their business continuity management (survey 2).....	51
Figure 25: Shows the percentages of organizations experienced an information security breach and when (survey 1).....	58
Figure 26: Shows the percentages of organizations experienced an information security breach and when (survey 2).....	58
Figure 27: Shows the individual ratings of the information security threats posed within the organizations (survey 1).....	59
Figure 28: Shows the individual ratings of the information security threats posed within the organizations (survey 2).....	60
Figure 29: Shows the percentages of insider threats the most likely to happen in the organizations (survey 1).....	61
Figure 30: Shows the percentages of insider threats the most likely to happen in the organizations (survey 2).....	61
Figure 31: Represents the percentages of barriers that prevent organizations to implement prerequisite information security measures (survey 1).....	63
Figure 32: Represents the percentages of barriers that prevent organizations to implement prerequisite information security measures (survey 2).....	64

List of Tables:

Table 1: Shows the topics and questions related to them.....	32
Table 2: Correlation coefficient test values for survey 1 results.	54
Table 3: Correlation coefficient test values for survey 2 results.....	56
Table 4: Data triangulation.....	71
Table 5: Frequency table for the type of awareness & training methods...	95
Table 6: Shows the no.of participants rated individual threats (survey 1).	96
Table 7: Shows the no.of participants rated individual threats (survey 2).	97
Table 8: Frequency table for information security measures implemented in the organizations.	98
Table 9: Frequency table for information security barriers in the organizations.....	99

Chapter 1: Introduction

1.1 Problem Statement

Small and medium-sized IT organizations mostly rely on their data systems to achieve the organization's goals (Freeman A, Doyle L, 2010). Technological innovations develop new opportunities to enhance organizational effectiveness and operations. They also create numerous security threats to the data in SMEs. The recognition of such information security threats performs a crucial role in the growth and sustainability of SMEs (Freeman A, Doyle L, 2010). Such security threats can ultimately threaten the continuity of business and cause financial losses, as well as other types of losses, such as reputation to SMEs. And also information security metrics are critical to handle (Alex Campanelli, 2018).

1.2 Research Background

Small and medium IT firms are the organizations with less than 250 employees, with annual revenue of not more than EUR 50 million and an estimated annual income statement of not more than EUR 43 million (Central Statistical Office(CSO), 2015). Over 99% of organizations in Ireland are SMEs (Central Statistical Office(CSO), 2015). Over the past 5 years, they also generate about 85% of job opportunities, generating two-thirds of higher growth in employment (Central Statistical Office(CSO), 2015).

Currently, all SME's rely on IT systems. Some researches did not view information security as a significant aspect of the behavioral intention on the implementation of IT systems. Throughout the deployment and implementation of IT systems, particularly in SMEs, information security is becoming extremely important nowadays. The new information security procedures are being developed and implemented to support organizations by integrating best practices and reducing threats into their processes. Towards this purpose, a thorough and effective implementation of data security

practices by SME's could be a beneficial variable in focusing on business development, continuity, and competitiveness.

1.3 Research Aim

To investigate the current information security practices of the SME's, threats for information security, and barriers to implement prerequisite information security practices for small and medium-sized IT organizations in Ireland.

1.4 Research Objectives

The research objectives are to:

- Investigate the current information security practices following in small and medium-sized IT organizations.
- Analyze the major threats to information security in small and medium-sized IT organizations.
- Examine the major barriers to implement prerequisite information security practices for small and medium-sized IT organizations.

1.5 Proposed Title of Dissertation

“Investigating the current information security practices following by the SME's: Threats to information security and barriers to implementing prerequisite information security practices for small and medium-sized IT organizations”.

1.6 Research Questions

- What are the current information security practices following in small and medium-sized IT organizations?
- What are the threats to information security in small and medium-sized IT organizations?
- What are the barriers to small and medium-sized IT organizations to implement the prerequisite information security practices?

1.7 Client Organization

Small and medium-sized IT organizations in Ireland are conducting their business on financial services, IT services, and business services. 52 random SMEs were selected and surveys are conducted to collect information from the organizations about information security.

1.8 Rationale for the Study

Information is the most valuable asset for many organizations. So, it is important to secure it. Especially for SMEs. Information security is defined as "the task of resisting unauthorized entry, misuse, divulge, interruption, alteration, evaluation, documenting or loss of information." Information can take multiple shapes such as physical and digital ([Cisco, 2014](#), [Enisa, 2014](#), [European Commission, 2013](#), [Intel Security, 2014](#), [Pwc, 2013](#)). The protection of information carries four important roles:

- Safeguards the capacity of the organization to operate effectively.
- Allows the smooth handling of applications implemented on the IT systems of the company.
- Secures information collected and used by the organization.
- Aims to protect the organization's new tech.

In a globally connected environment, information is subjected to a greatly increased set of threats and a broader range of them. Threats including malware, cyber-crime, and denial-of-service threats became more popular, aggressive, and complex, rendering it even more of a challenge to introduce, manage, and upgrade information security within an organization. The security practices followed by the SME's are changing where new technologies are emerging, threats facing by the SME's are advancing and many barriers to implement the security practices for the SME's give scope for this research (Cisco, 2014, Enisa, 2014, European Commission, 2013, Intel Security, 2014, Pwc, 2013). So, it is important to investigate them which gives the scope for this research.

1.9 Structure of the Dissertation

1.9.1 Literature Review

In the literature review chapter, several theories by various researchers are discussed to examine the current information security practices following by the SME's, threats, and the barriers to the implementation of the prerequisite information security practices by the SME's. Key findings and gaps are observed in the literature review.

1.9.2 Methodology

In the methodology chapter, the research question, research design, research philosophy, secondary research data collection, type of research and methods, approach, primary research, sampling technique, primary research data collection, reliability, validity, triangulation, research ethics, participants and sampling survey are discussed.

1.9.3 Results

This chapter gives a detailed representation of the data obtained through the survey. As described in the methodology chapter, a survey is an effective way to gather the outcomes from the number of respondents from various SMEs. The data which is collected from the participants of the SME's on information security is represented in the form of charts and diagrams.

1.9.4 Discussion

The discussion chapter looks through the purpose, significance, and importance of the results which are obtained in the previous chapter. The researcher concentrated on describing and analyzing the results, demonstrating how it applies to the literature review and research questions by putting forward an argument to support the endpoint.

1.9.5 Conclusion:

In this chapter, key results have emerged while conducting this study. Consequently, conclusions are provided in this chapter based on the findings and study objectives. Recommendations are also emphasized which are important for the findings. Lastly, certain areas where future work is required are identified.

Chapter 2: Literature Review

2.1. Section 1: Introduction

A comprehensive and detailed analysis of literature is the basis and inspiration for extensive, valuable research. The dynamic nature of A comprehensive and detailed analysis of literature is the basis and inspiration for extensive, valuable research. The dynamic nature of academic research requires such comprehensive and detailed reviews (Boote.D.N & Beile.P, 2005). In this literature, several theories by various researchers are discussed to examine the current information security practices following by the SME's, threats, and the barriers to the implementation of the prerequisite information security practices.

The review of the literature in the paper is organized into sections. In section 2, the information security definition by various authors will be explained. Section 3 analyses the information security practices followed by small and medium IT enterprises. Section 4 deals with the threats facing by the organizations. Barriers to implementing prerequisite information security practices for the Small and medium-sized IT organizations in section 5. Finally, section 6 draws the key points and gaps found in the literature review.

2.2. Section 2: Information Security Definitions

Information Security is the means of securing the associated organization's resource possession, including "Intellectual Property Rights" (Pipkin, 2000). McDermott and Geer (2001) stated that information security is a restraint in managing risks, where its task is to control the organization 's information risk cost (McDermott and Geer, 2001). Generally, a chief information security officer is an intersection rectifier for that cluster. The security cluster is generally accountable for performing operational risks. A process by whom threats and risks to information resources are unending, evaluated, and then the appropriate securing measures are identified and implemented. A corporation's

importance exists within its information and its protection is important for business processes. Also, trustworthiness in keeping and earning the client's confidence (Josh Fruhlinger, 2019).

2.2.1 Principals of Information Security

Information security plans are intended around the key priorities of the CIA triad; ensuring IT practices and business knowledge confidentiality, integrity, and availability (Chad Perrin, 2012). Such priorities ensure that confidential information is barely exposed to licensees (privacy), forestall unauthorized information alteration (integrity), and ensure that once authorized (availability) the information can be collected by approved parties. First thought on data protection or confidentiality usually involves the use of coding and coding keys. The second thought, integrity, ensures that once information has been browsed back, it will be the same as when it was recorded. The third aspect is availability, being an aspect of the triad it aims to ensure that the data is accessible to authorized users. (Chad Perrin, 2012).

2.3. Section 3: Information Security Practices

Brett Valentine (2017) stated information security practices comply with how organizational leaders should conduct business about the expert need for IT systems. Information security practices in SMEs provide a collection of standards directed at accomplishing and preserving an acceptable level of protection including confidentiality rates, transparency, and information availability. Information security practices in SMEs are indeed an inseparable part of different organizational management of information technology which perceives the security threats, that technology tends to raise (Brett Valentine, 2017).

Andress.J (2014) found in the past decade the purpose of data security practices in SME's has developed and progressed substantially which provides five major areas of expertise, such as employees, policies and procedures,

network securing and associated infrastructure, risk management and business continuity management ([Andress.J, 2014](#)). Information security experts in organizations are anticipated to rise over 11 percent per annum between 2014 and 2019 in SME's, demonstrates the concern of the organizations about data security ([Threat Report, 2019](#)). The areas of expertise are discussed below to explain the importance of each area of expertise in information security practices.

2.3.1 Employees

Richardson (2007) stated that information security has become a more significant issue with the development of various advanced security activities ([Richardson, 2007](#)). No matter how professionally planned, security measures depend on the people (employees) who adopt them ([Gonzalez and Sawicka, 2002](#)). Supporting this view, Garrison (2006) stated that the employees are theoretically the greatest risk to information security protection in SMEs. The employees are responsible for the security activities like, downloading a trojan, integrates an unapproved program, uploads a virus from a storage device, introduces a malicious email, unattended a system registered in, discloses login details or chooses a simple password that puts the whole organization at risk ([Garrison, 2006](#)). Adams, Sasse, and their colleagues in their work identified by looking at password related employee experience problems. They discovered that the fear, to be a potential means to get employees to adopt the password policies ([Adams and Sasse, 1999](#); [Adams et al., 1997](#); [Weirich and Sasse, 2001](#)). The 3rd Big Red Cloud Business Sentiment Survey reported the top five security issues for Irish SME's are targeted attacks against employees such as ransomware (77%), phishing (79%), DDoS attacks (75%) and advanced persistent threats (77%) ([Irish Tech News, 2016](#)).

2.3.2 Policies and Procedures

Thomas R.Peltier (2016) stated that policies and procedures are indeed an extremely important part of the SME's. Policies and procedures can provide a road-map for regular operations. They can guarantee compliance with regulations, provide strategic planning guidelines, and improve business operations. He also mentioned that the policies and procedures are of no use, unless or until they are followed by the employees in the organization (Thomas R.Peltier, 2016). Whitten (2004) observed an overview of information security from an accessibility point of view and established functional safety designed policies (Whitten, 2004). Aytes and Connolly (2004) argued that information security also requires practice and compliance initiatives of policies and procedures. They also endeavored to examine the underlying explanation for violating or breaching security protocols and found the root cause for the violating or breaching security protocols is employee negligence (Aytes and Connolly, 2004).

The HR management of "Business & Finance" has reported that while an impressive 93% of Irish SMEs agree that HR management plays a key role in an organization, only a little over half currently invested in an HR management. 68% of Irish SME's employing up to 10 workers have no HR management, with this number falling to just 36% for Irish SME's employing 11-50 employees (small organization), and 29% for Irish SME' employing 50-250 employees (medium organization) (Business & Finance, 2020).

2.3.3 Network Security and Associated Infrastructure

Turner and Dawn.M (2016) stated network security begins with identity verification (authentication), usually by a login credential (Turner and Dawn.M, 2016). Once verified, a firewall upholds the access policies including the services which are permitted to access by the users (Oppliger and Rolf, 1997). Axelsson (2000) argued while efficient in restricting access, the firewall may struggle to monitor possibly dangerous content, like malware attacks or the transmission of trojans over its network. He also suggested antivirus software or perhaps an intrusion detection and prevention system will help to identify and prevent such attacks. Interaction between two hosts that use a network may be encrypted to preserve privacy (Axelsson, 2000).

Mohammed, Mohssen, Rehman, and Habib-ur (2015) stated honeypots, which effectively entice network available resources, can be implemented as monitoring and early alert techniques in a network. Honeypots are not usually made available for legitimate use. Methods being used by attackers trying to compromise such entice resources are being analyzed throughout and after an attack to maintain a focus on new methods of exploitation (Mohammed, Mohssen, Rehman and Habib-ur, 2015). 59% of the Irish SMEs said that they are lacking some network associated infrastructure such as highly reliable internet connection, firewalls, intrusion detection and prevention system, antivirus software, and honeypots (Irish Tech News, 2019).

2.3.4 Risk Management

Foreman.P (2010) argues that the management should define the information that is potentially important to the enterprise, the management processes of the said information, and their related vulnerabilities to evaluate risk effectively (Foreman.P, 2010). Newsome.B (2013) stated the risk management process consists of identifying vulnerabilities, identifying threats, and implementing appropriate control measures (Newsome.B, 2013). In addition to the Newsome.B statement, Chloe Biscoe (2017) suggested four ways to treat the identified risks. They are 'Terminate' the risk by fully removing it, 'mitigate' the risk by implementing security controls, 'transfer' the risk to a third party, or 'accept' the risk (Chloe Biscoe, 2017).

2.3.5 Business Continuity Management

Ellis Holman (2012) stated Management of Business Continuity is a process of risk management that addresses the risk of instability to business processes and practices. The effectiveness of business continuity management can help to achieve excellent organizational continuity in SMEs. Unfortunately, business Continuity management or disaster recovery is not adequate in SMEs because of a lack of expertise (Ellis Holman, 2012). Similarly, Intrieri and Charles (2013) stated, in case of a disaster, an appropriate business continuity management guarantees that the SME's can provide at-least lowest required facility and helps to protect the company's reputation and revenue. Business continuity management comprises procedures for creating, reviewing, and maintaining business continuity plans which will allow an organization to function properly after or during a disaster (Intrieri and Charles, 2013). Kim Lindros and Ed Tittel (2018) stated Business Continuity Management defines the measures of an organization that needs to do and to ensure that it can handle the potential losses, exploit and damage during and after a disaster (Kim Lindros and Ed Tittel, 2018).

2.4. Section 4: Threats to Information Security

Stewart & James (2012) stated, threats to personal and confidential data, like spam and virus attacks, identity fraud, and malicious software, are available in several alternative forms (Stewart, James, 2012). To discourage hackers and overcome vulnerabilities at various stages, many security checks are enforced and implemented as a part of an in-depth strategy of layered defense which is not possible in SMEs. It might reduce the associate's degree effect in the nursing attack. A thorough evaluation can be carried out to determine the efficiency of the business to take care of system security against a set of defined parameters (Michael; Chapple, Mike; Gibson, Darril, 2015).

Michael E. Whitman (2003) argued each new era brings new threats to SME's. Such threats are becoming increasingly complex and take total advantage over the weaknesses between applications and user-related infrastructure assets. Every device, if it is hardware or software, has security flaws which will cause intense damage once exploited (Michael E. Whitman, 2003). Supporting the statement, Tang.J, Wang.D, Ming.L, Li.X (2012) categorized the information security threats in SME's into three types. They are insider threats, technical threats (system-specific), and environmental threats (Tang.J, Wang.D, Ming.L, Li.X, 2012).

30% of Irish SMEs reported that breaches cost them less than \$100,000, whereas 20% reported that it cost them between \$1,000,000 to \$2,499,99. Irish SMEs facing more than 5000 average security alerts. 55.6% of security alerts were handled by Irish SME's. Phishing and insider threats are the most prevalent types of threats reported. And the other type of technical threats (system-specific) includes viruses and worms, botnets, drive-by downloads attacks, distributed denial-of-service (DDoS) attacks, ransomware, exploits kits, malvertising, and advanced persistent threats, etc (Irish Tech News, 2016).

2.4.1 Insider Threats

Cummings, Adam, Lewellen, Todd, McIntire, David, Moore, Andrew, Trzeciak and Randall (2010) argued, an insider threat arises when people related to an enterprise have deliberately or inadvertently misused connections to their network that adversely affects sensitive information or systems in the small and medium IT enterprises (Cummings, Adam, Lewellen, Todd, McIntire, David, Moore, Andrew, Trzeciak and Randall, 2010). Supporting the above argument Probst, Christian & Hunker, Jeffrey & Gollmann, Dieter & Bishop, Matt. (2012) categorized the insider threat into three types. They are malicious insiders, who inflict harm to the organization purposely with the help of their access advantage. Irresponsible insiders, who inflict harm to the organization by mistake due to ignoring policies. Hackers, who are foreign agents without authorization to receive valid login information. And reported malicious insiders is the most inflicting threat in SME's (Probst, Christian & Hunker, Jeffrey & Gollmann, Dieter & Bishop, Matt, 2012).

2.4.2 Technical Threats (System-specific)

The network security and associated infrastructure of the SME's are potentially weak because of the lack of resources and capital of SME's when compare to large organizations. So, technical threats associated with network and infrastructure inflict more damage to SME's. With the increase of technology, many new technical threats are inflicting more damage to the SMEs. Till now there are five generations of threats that are common to every IT organization, either small, medium, or large that are explained below (Geric.S and Hutinski.Z, 2007).

2.4.2.1 First Generation Threats

According to Information Systems Management (2015), the very first generation of threats to the security began in the 1980s. Such threats were usually boots viruses over a few weeks infected specific systems and system networks (Information Systems Management, 2015). A “virus” is the top form of threat with 42% being hit by Irish SMEs in 2016 (Irish Tech News, 2016).

2.4.2.2 Second Generation Threats

Gordon stated that in the 1990's the ransomware and denial-of-service threats were simultaneously prevailed and continue to be a problem mainly in SME's. Denial-of-service threats, which started in the 1990s, have intensified into attacks on the network and global technology. These threats are becoming popular these days by using numerous systems lacking user's knowledge to strike a single target. These kinds of threats are known as distributed denial-of-service attacks and are the top primary factor for corporate security failures. Currently, SME's became more vulnerable to requests for ransoms and denial-of-service threats (Gordon et al . , 2016). 20% of Irish SMEs were hit by ransomware attacks and also 93% of the Irish SMEs would not pay ransom to retrieve their data (Irish Tech News, 2016).

2.5.2.3 Third Generation Threats or Integrated Threats

Hilley (2003) stated that third-generation threats appeared in the early 2000s. An integrated threat may be a virus that has several techniques of replication, which proliferates via the application and network processes without human interference. They usually display similar responses like trojans. More than 60 percent of malicious program entries were within the kind of integrated threats in mid-2003 in SMEs (Hilley, 2003). 61% of SME's in Ireland represented in the study experienced a malware attack during 2016 (Irish Tech News, 2016).

2.4.2.4 Fourth Generation Threats

Wexler (2014) stated, the fourth generation threats are emerged in 2010, as SME's facing new types of threats that influence user machines, individual and complex networks, and sometimes even national networks ([Wexler, 2014](#)). Trojans have malware that dwells in a relatively trivial program and can damage the system once it is launched or deceased ([Basil Cupa, 2012](#)). Supporting the Basil Cupa (2012) statement, besides, Yusuf Bhaiji (2016) indicated that the trojans create back doors in systems that threaten information security. Numerous trojans are being designed for cracking passwords ([Yusuf Bhaiji, 2016](#)).

2.4.2.5 Fifth Generation Threats

The fifth-generation threats are advanced persistent threats, emerged in 2017's ([Margaret Rouse, 2019](#)). Saravanan. A and Bama. S (2019) argued, the fifth-generation threats are escalating threats to previous generations since, they are multi-vector and they can sabotage and continues to threaten the SMEs IT infrastructure such as networks, data centers, and servers, end devices, smart applications and websites ([Saravanan. A and Bama.S, 2019](#)). The 3rd Big Red Cloud Business Sentiment Survey reported the top five security issues for Irish SME's are targeted attacks against employees such as ransomware (77%), phishing (79%), DDoS attacks (75%) and advanced persistent threats (77%) ([Irish Tech News, 2019](#)).

2.4.3 Environmental and Physical Threats

Geric. S and Hutinski. Z (2007) stated that environmental and physical threats are undesirable site-specific chance occurrences that have less probability to occur and also unstoppable if occur. Environmental threats include lightning, floods, earthquake, fire accidents, tsunamis, electromagnetic interference, etc and physical threats include theft, vandalism, and arson, etc (Geric.S and Hutinski.Z, 2007). Mary Sumner (2009) argued, most SMEs ignore this kind of threat because they occur very rare and SMEs have to maintain good backups to minimize the damage inflicts by this kind of threats (Mary Sumner, 2009).

2.5. Section 5: Barriers for the SMEs to Implement the Prerequisite Information Security Practices

KanKanhalli et al., (2003) identified that the smaller value of protective measures imposed by the SMEs relative to the large organizations (KanKanhalli et al., 2003). Both Chapman & Smalov (2004); Mitchell et al., (1999) in their studies argued that SMEs ignore the knowledge of information security and explore alternative exposed threats to their organizations (Chapman & Smalov, 2004; Mitchell et al., 1999). Besides, Gupta & Hammond (2005) notes that several SME's are unable to concentrate on safety because of certain barriers such as implementation costs, lack of resources and capital (Gupta & Hammond, 2005). Supporting the view of Gupta & Hammond (2005), Ernst & Young (2005) included a lack of expertise and knowledge as another barrier for information security measures (Ernst & Young, 2005).

2.5.1 Lack of Expertise and Knowledge

Brodcrick (2006) stated, one of the potential barriers to implementing the prerequisite information security practices is the lack of expertise and knowledge on the information security of the administrators in SMEs. Some administrators are least worried about the security of information (Brodcrick, 2006). KanKanhalli (2003); Straub (1990) argued, many administrators collectively lack knowledge about the range of measures that are available to minimize misuse of information security (KanKanhalli et al., 2003; Straub, 1990). Administrators lack adequate IS expert knowledge (DE Lone, 1998; Gable, 1991; Spinellis et al., 1999).

2.5.2 Implementation Costs

Wiander (2007) argued that information security is usually not a full-time job in SMEs. As a result, there is indeed a threat that perhaps the person responsible for information security will see certain responsibilities as even more crucial, as information security task has been considered as cost (Wiander, 2007). Doherty & Fulford (2005) stated, the implementation of successful information security measures requires a lot of time, energy, and resources, where entities don't seem prepared to invest (Doherty & Fulford 2005). Wiander (2007) added, enforcing the standard requires total staff and this can entail higher salary costs. Hinson (2008) found implementation costs are a barrier originate from training and regular work reviews by managers and day to day processes to ensure quality-compliance. (Hinson, 2008).

2.5.3 Lack of Resources and Capital

Due to the challenging existence of security requirements, the shortage of resources and capital to purchase the SME 's expertise is again overloaded by the lack of resources to implement and approve the requirements. Effective information security management needs significant time and energy, where most SME's are reluctant to undertake (Doherty & Fulford, 2005; Moule & Giavara, 1995). In contrast, Mitchell et al., (1999) identified that the SME's who still haven't undergone a security breach are less willing to spend in security breaches are much less willing to spend in security projects and audits (Mitchell et al., 1999). The efficiency of data security audits relies mostly on the proficiency and reliability of the individuals who enforce and use it (Foreman.P, 2010).

2.6. Section 6 : Conclusion

In this literature review chapter, several theories are considered to examine the current information security practices following by the '**Small and Medium IT Enterprises**', threats, and the barriers for the implementation of the prerequisite information security practices.

In section 2.4, in the literature review of information security practices, the researcher found a relationship between the five major areas of expertise of information security practices: "**employees, policies and procedures, network securing and associated infrastructure, risk management, and business continuity management**" which are conceived, established and enforced within the SME's. Where other researchers or authors failed to identify the relationship and explained the five areas of expertise individually.

In section 2.5, in the literature review of threats currently facing by the SME's, some researchers argued "**insider threats**" play a major role in threatening

information security of the SME's. But they didn't discuss which insider threats inflict more damage among "**malicious insiders, irresponsible insiders, foreign agents/hackers**". Some researchers argued "**technical threats (system-specific)**" play a major role in threatening information security of the SME's. Also, many new threats are being generated every day which is almost an impossible task for the SMEs to establish potential security measures that require further investigation.

In section 2.6, in the literature review, statements and arguments of many researchers were observed related to the barriers to implement prerequisite information security measures that require further investigation. As some researchers argued "**lack of expertise and knowledge**" is the major barrier and some researchers argued "**implementation costs, lack of resources and capital**" are the major barriers. But the researcher of this study believes that all three barriers play an equal role and stand as major barriers for SMEs to implement prerequisite information security practices.

Witnessing the gap found in the above literature review indicating strong research criteria in information security practices adopted by the SME's. This research aims to investigate the current information security practices of SMEs, threats for information security, and barriers to implementing information security measures for SMEs.

Chapter 3: Methodology

3.1 Introduction

In this methodology chapter: the research question, research design, research philosophy, secondary research data collection, type of research and methods, approach, primary research, sampling technique, primary research data collection, reliability, validity, triangulation, research ethics, participants and sampling survey are discussed.

3.2 Research Questions

- What are the current information security practices following in small and medium-sized IT organizations?
- What are the threats to information security in small and medium-sized IT organizations?
- What are the barriers to small and medium-sized IT organizations to implement the prerequisite information security practices?

3.3 Research Philosophy

The deductive approach is used in this research. The deductive approach focuses on the hypothesis based on existing theory and then establishes the methodological approach to evaluate it (Silverman, 2013). The deductive approach is regarded specifically suitable to the positivist method, which allows the development of theories and statistical testing of predicted outcomes to an agreed degree of accuracy (Larner & Snieder, 2009). The deductive method utilizes a questionnaire to develop evaluation insight that allows the researcher to compare potential various public perceptions through empirical data. The collected data helps to validate or deny the query, and the cycle can be continued. The survey strategy is related to the deductive method. This is

one of the easiest and most effective approaches. This method helps to collect accurate data. Surveys appear to be used in quantitative areas of research, requiring a substantial percentage of the population being sampled ([Bell & Bryman, 2011](#)).

3.4 Research Design

The research design provides a suitable framework that collects data to answer the research objectives. It is a blueprint for data collection, measurement, and analysis. There are many research designs such as action research design, case study design, causal design, cross-sectional design, descriptive design, experimental design, exploratory design, observational design, etc. Every design has its purpose and researcher choose a design depends on their research study ([Wahyuni and Dina, 2012](#)).

This research employed descriptive design which includes quantitative methods. Descriptive study design aims to include responses to the inquiry of when, how, where, who, and what they contribute to a specific research question; descriptive research could not decide why. A descriptive study is used to collect data about the current state of the phenomenon and to explain "what does happen" about parameters or circumstances in a situation.

The main aim of the research is to investigate and explain the current information security practices of SMEs, threats for information security, and barriers to implementing information security measures for SMEs. Few researchers have researched on this and reported it. But the security practices followed by the SMEs are changing where new technologies are emerging, threats facing by the SME's are advancing and many barriers to implement the security practices for the SME's give scope for this research. The researcher chooses the quantitative methodology, descriptive method to study and explain the research objectives.

And the reason the researcher choose quantitative methodology is the size of the participants (52). There are many ways to gather data on current information security practices, threats, and barriers to the respective organizations from their respective participants (employees and information security managers). Among them, the quick and possible way is conducting the surveys in a given time frame. Liu & Fellows (2008) stated that usually quantitative research methods are implemented because they are analytical methods and deliver quick results in a given time frame (Liu & Fellows, 2008).

3.5 Quantitative Methodology, Descriptive Method, and Research Survey

3.5.1 Quantitative Methodology

Quantitative methodology is characterized as a systematic study of the phenomenon by gathering statistical information and carrying out empirical, mathematical, or computational techniques (Williamson, Kirsty, and Graeme Johanson, 2018). Quantitative research involves sampling methods to collect data from present and prospective SMEs by carrying out online surveys, questionnaires, etc., the results of which could be expressed in absolute form and displayed in graphs in the results section.

For the most part, quantitative analysis is carried out using the cross-tabulation statistical method to draw a correlation between variables mentioned above to obtain quantitative data for the study. The researcher observed the gaps in the literature review about the quantity at the question in this research process. Quantitative analysis is analytical, rigorous, and also investigative. The results of this investigative approach are logical, accurate, and unambiguous (Williamson, Kirsty, and Graeme Johanson, 2018). And also the advantages of using quantitative methodology are it collects reliable and accurate data, collects data quickly, wider scope to data analysis, and eliminates bias. In quantitative methodology, the researcher chooses the descriptive method among descriptive and casual research.

3.5.2 Descriptive Method

Descriptive research is described as a procedure of research that defines the elements of the phenomenon or phenomena of interest being investigated. This method is much more centered on the topic of research. Descriptive research primarily focuses on defining the nature of a demographic group where the participants are employees of the information security team of SME's who are well aware of the researcher's area of interest. Descriptive research is also known as the observational study process since none of the parameters which are essential to the research analysis are effected ([Williamson, Kirsty, and Graeme Johanson, 2018](#)). Descriptive research is also quick to conduct and cheap. In a descriptive method, survey research is conducted to gather information and was conducted on either small or larger samples, describing the selected subjects.

3.5.3 Survey Research

Survey used to pose questions to a population of participants, employing online surveys and questionnaires, etc. The researcher asked multiple questions by creating a questionnaire to gather information from a sample of individuals in two phases of surveys and evaluate the whole study aims to gather outcomes. This is the first step towards information gathering for research purposes. The key requirement for this method of study is indeed the random collection of the population of participants as members. The researcher thus conveniently preserved the quality of the data collected, as a wide number of participants would be answered using simple random sampling ([Adi Bhat, 2016](#)). Survey research is further classified into two types, longitudinal survey research which involves surveying over years or decades, and cross-sectional survey research which involves surveying a particular time interval ([Adi Bhat, 2016](#)). So, the researcher chooses the cross-sectional survey research because of the time frame of this research is limited.

3.5.4 Cross-Sectional Survey

A cross-sectional survey is an empirical survey carried out in a circumstance where the researcher aims to gather information at a specific moment in time from the targeted respondents (Anup Surendran, 2018). The researcher can test different aspects at a given time. Results obtained by the use of this form of the survey come from subjects who display correlation throughout all parameters of the study. A cross-sectional survey is common among SMEs. Information is gathered within the variable environment without changing any parameters. Multiple samples are analyzed and compared using a cross-sectional investigative method (Raj, Roy, 2016). A cross-sectional survey is perfect for this research because the information has to gather information at a specific moment in time from the targeted respondents. And also the researcher can test different aspects such as information security practices, threats, and barriers in this research in the given time frame.

3.6 Approach

In this research process, the researcher analyzed the previous articles, journals, conference reports, books, research, and related documents that are relevant to the area of interest of this research. And conducted surveys by approaching the participants in selected SMEs through emails to collect data on information security practices, threats, and barriers for SME's. The approaching process helps the researcher to examine the current information security practices, threats, and barriers for the SMEs in the present and past. The employees of the information security team of the SMEs are the participants of this research. The researcher approached them through emails with a questionnaire (surveys) to collect information which is helpful for the primary research. And the surveys were conducted in two phases.

Phase 1

In phase 1 (survey 1), the questionnaire is sent to the selected 52 SME'S to the employees of the information security team.

Phase 2

In phase 2 (survey 2), the second survey is conducted only to the participants who answered the survey 1 in phase 1. And the same questionnaire is used in both surveys.

The reason to conduct the surveys in two phases is to obtain reliable data. Reliable data is “Quality or a good state of being. The degree to which a method of experimenting, testing, or evaluating provides the same outcomes on repeated tests” (Loersch.C, Petty.R.E, Brinol.P & McCaslin.M.J, 2009). The logic behind how two surveys improve reliability if the same questions are asked is after attending the survey 1 in phase 1, the participants would have reconsidered their status (information security status) or discussed with their information security team. And when answering the survey 2 in phase 2, they will give correct or accurate data when they are answering the same questionnaire again.

3.7 Data Collection Methodology

Probability sampling: A probability sampling is being used to sort participants out of a group and to construct samples. Sample participants are selected by random selection methodology. Every target participant has equal chances of being selected in the survey (Fleetwood.D, 2020). Simple random sampling is selected among the four types of probability sampling because the subjects are relatively small. The other probability sampling types are stratified random sampling, random cluster sampling, and systematic sampling (Fleetwood.D, 2020).

Simple Random Sampling: Simple random sampling as the name implies, is nothing but a random collection of subjects for surveys. This sampling methodology is utilized where the selected subjects are relatively small ([Fleetwood.D, 2020](#)).

For this research process, a very well-prepared simple random method is being used to identify target subjects. Underneath the probability approach, simple random sampling is the true essence of the sample selection, random sampling offers equal opportunity to be selected for every person in the target subjects. The subjects involved in this research process are employees of the information security team of the SME's, who plays an important role in following the information security practices by the organizations.

For the surveys, a total of 52 random SMEs were selected which are providing professional services like financial services, business services, and IT services are in scope. The website "THE IRISH TIMES TOP 1000, Our Guide to Irish Business" helps the researcher to find and select 52 random SME's ([TOP 1000, 2020](#)). The website listed 1000 Irish small, medium, and large organizations along with the number of employees working in individual organizations and the IT sector the organization belongs to. The researcher selected 52 organizations randomly where the employee's number is below 250 (SME's are the organizations that have employees less than 250 ([Central Statistical Office\(CSO\), 2015](#))) and also SMEs which are providing financial services, business services, and IT services.

The targeted subjects or participants in these 52 random SMEs are employees of the information security team. Because the purpose of the survey is to identify the current information security practices following by the organizations, information security threats to the organizations, and barriers to implementing prerequisite information security measures. So, the researcher chose the members of the information security team as participants. The researcher mentioned in the emails which were sent to the organizations along with the survey link while conducting a survey, that this survey is for

“information security team members”. And the contact details (email addresses) of every participant were taken from their respective organization’s websites which are available in the “THE IRISH TIMES TOP 1000, Our Guide to Irish Business” website.

3.7.1 Primary Research Data Collection

The primary research data is collected through a descriptive primary data collection method, a survey. For the analysis of security practices, threats, and barriers for SMEs, the researcher needs data from the selected SMEs. To collect data, a quantitative approach is needed. Since the information has to be obtained is related to the information security of several small and medium-sized IT organizations. So, it is the only way formulated to collect data.

3.7.2 Secondary Research Data Collection

This research is integrated with various secondary research data sources. This secondary research data is a combined gathering of essential data from various sources such as articles, journals, conference reports, books, research, and related documents ([Collins, 1997](#)).

3.8 Research Data Analysis

Research data analysis is a method in which the raw data is collected and optimized to carry the defined structures, to define relevant trends and patterns for gaining insights. The descriptive statistics data analysis method is used to analyze the collected data from the selected participants. This method focuses on population (participants) and parameters simultaneously which is essential for this research. The parameters of this research are identifying the current security practices, threats, and barriers to the organizations. And the population (participants) is about the data obtained from the sampling research to address the survey research questions ([Adi Bhat, 2016](#)).

The data which is collected from the surveys mainly focus on information security practices, threats, and barriers for SMEs to implement information security measures. The correlation coefficient test is conducted for the data related to information security practices to find the relationship between the variable. Frequency tables are generated for some variables to show the number of occurrences of a particular data set. These frequency tables and correlation coefficient tests are done by using the “**SPSS tool**” (version 25).

3.9 Reliability and Validity

Reliability

The reliability of research defines the measure of obtained reliable and stable results. Reliable data is “Quality or a good state of being. The degree to which a method of experimenting, testing, or evaluating provides the same outcomes on repeated tests” (Loersch.C, Petty.R.E, Brinol.P & McCaslin.M.J, 2009). This study guarantees accurate and reliable data. To achieve this researcher conducted surveys in two phases to the employees of the information security team. The logic behind how two surveys improve reliability if the same questions are asked is after attending the survey 1 in phase 1, the participants would have reconsidered their status (information security status) or discussed with their information security team. And when answering the survey 2 in phase 2, they will give correct or accurate data when they are answering the same questionnaire again.

Validity

The validity of research in this study defines the degree to which the survey examined the current practices of information security, threats, and barriers for SMEs. To achieve this the questionnaire needs to frame properly which exactly measures the current practices of information security, threats, and barriers for SMEs. So, this study used the content validity where the questionnaire is designed with the help of an expert who has good knowledge of information security (CKirk, J. and Miller, M., 2005).

3.10 Triangulation

Triangulation aid researchers to analyze and evaluate the themes or patterns recognized in the quantitative analysis (CKirk, J. and Miller, M., 2005). The findings of this study which are obtained by the descriptive design method are compared and reviewed to establish a correlation between current practices of information security, threats, and barriers for SMEs. In this research, the researcher conducted the surveys in two phases. The results obtained from the two surveys were compared and validated to achieve triangulation. Comparing the results of both surveys is shown in the discussion chapter in section 5.3.

3.11 Research Ethical Issues

In research, it is essential to include evidence of consent when conducting the survey mostly during the information gathering process. The researcher has a duty in this process to obtaining information and use it responsibly with the consent of the respondents. On the first page of the questionnaire in the survey, a statement of consent is given to all participants by the researcher. This statement of consent outlines the subject of the study, details on the study, guidelines on participation, and restrictions. And also containing specifics about the respondents.

3.12 Limitations

There are a few considerable limitations of this research addressed while interpreting the responses of cross-sectional surveys. Firstly, this research does not generalize the results to other industries or organizations as the participants are only from SME's that to financial, business, and technology services organizations. As stated, the responses collected were based out of Ireland and majorly from 52 organizations that do not illustrate the scenario of other organizations. This research is limited in investigating only five major areas of expertise of information security practices: employees, policies and procedures,

network security and associated infrastructure, risk management, and business continuity management which plays an important role in protecting the organization's information to full scale. Three categories of threats: insider, technical, environmental and physical threats. Three major barriers: lack of expertise and knowledge, implementation costs, lack of resources and capital which are identified and discussed in the literature review.

3.13 Conclusion

The details gained from this chapter relates primarily to the research objectives and research questions. The purposes of the approach and the procedure used in this research are discussed in this chapter. This chapter clarified the methodology that was used in the research design, research philosophy, methods of data collection, approach, sampling techniques and procedure of sampling survey, sample data analysis, reliability, validity, triangulation, and finally ethical considerations practiced during the research.

Chapter 4: Results

4.1 Introduction

This chapter will give a detailed representation of the data obtained through the survey. As described in the methodology chapter, the survey is an effective way to gather the outcomes from the number of respondents from various SMEs. The researcher in this research study opted for a quantitative analysis in which a survey is conducted to collect data. The data which is collected from the participants of the small and medium IT enterprises on information security is represented in the form of charts and diagrams.

4.2 Quantitative Findings

The survey is conducted in two phases to 52 small and medium-sized IT organizations as a part of research to collect reliable data on information security which is analyzed and concludes the research questions. In phase 1, survey 1 a total of 21 responses were received out of 52 respondents. In phase 2, survey 2 a total of 16 responses were received out of 21 respondents. To achieve reliability the researcher conducted the survey second time to the 21 respondents of the first survey. In total sixteen questions were asked by the researcher of the participants. The results obtained for these sixteen questions from the surveys are shown and discussed below.

The data which was collected from the surveys were analyzed by using statistical data analysis methods such as frequency tables, descriptive statistics, and correlation coefficient tests using “SPSS tool”. These analyses were conducted to find the relationship between the variables. The questions that were asked in the surveys by the researcher to the participants emerged from the topics observed in the literature review. The topics and questions associated with them are listed in table 1.

Topics	Questions related to them.
1. Current information security practices. <ul style="list-style-type: none"> ● Employees. ● Policies and Procedures. ● Network Security and Associated Infrastructure. ● Risk Management. ● Business Continuity Management. 	Questions 3,4,5,6,7,8,9,10,11 ,12
2. Threats to information security. <ul style="list-style-type: none"> ● Insider threats. ● Technical threats (system-specific). ● Environmental and Physical Threats. 	Questions 13,14,15
3. Barriers to implementing prerequisite information security measures. <ul style="list-style-type: none"> ● Lack of expertise and knowledge. ● Implementation costs. ● Lack of resources and capital. 	Question 16

Table 1: Shows the topics and questions related to them.

4.3 Demographic Findings

A total of 52 small and medium-sized IT organizations were approached by the researcher through a survey in which 21 responded in phase1 and 16 out of 21 responded in phase 2. The size of the organization and the IT sector the organizations belongs to, were asked in questions 1 and 2 respectively.

Question 1: What is the size of the organization?

In response to survey1, Figure 1 shows that 66.7% (14 out of 21 organizations) of the participants belong to “**Medium Sized Organization**” and 33.3% (7 out of 21 organizations) of the participants belong to “**Small Sized Organization**” respectively. In response to survey2, Figure 2 shows that 62.5% (10 out of 16 organizations) of the participants reported “**Medium Sized Organization**” and 37.5% (6 out of 16 organizations) of the participants reported “**Small Sized Organization**” respectively.

Survey 1:

1. What is the size of your organization?

21 responses

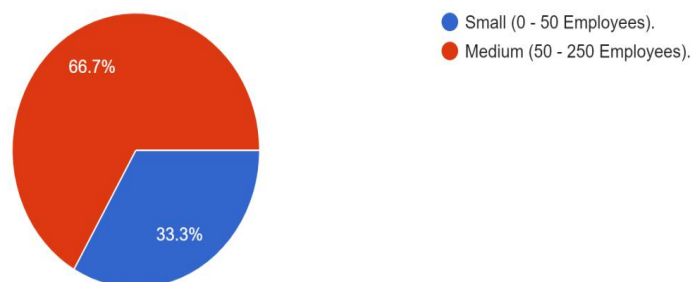


Figure 1: Represents the percentages of the magnitude of the organizations (survey 1).

Survey 2:

1. What is the size of your organization?

16 responses

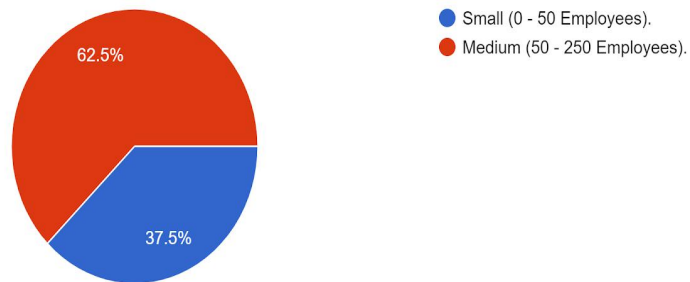


Figure 2: Represents the percentages of the magnitude of the organizations (survey 2).

Question 2: Your organization belongs to which of the following IT sector?

As per the organization's selection criteria described in the methodology chapter. Only three IT sectors: financial services, IT services, business services were in scope. And the survey is taken from the organizations belongs to these three IT sectors only. In response to survey 1, Figure 3 shows 47.6% of the participants reported that they are working in "**Financial Services**", 33.3% are working in "**IT Services**" and 19% are working in "**Business Services**" sectors respectively. In response to survey 2, Figure 4 shows 62.5% of the participants reported "**Financial Services**", 25% reported "**IT Services**" and 12.5% reported "**Business Services**" sectors respectively.

Survey1:

2. Your organization belongs to which of the following IT sector? (Select all that apply)

21 responses

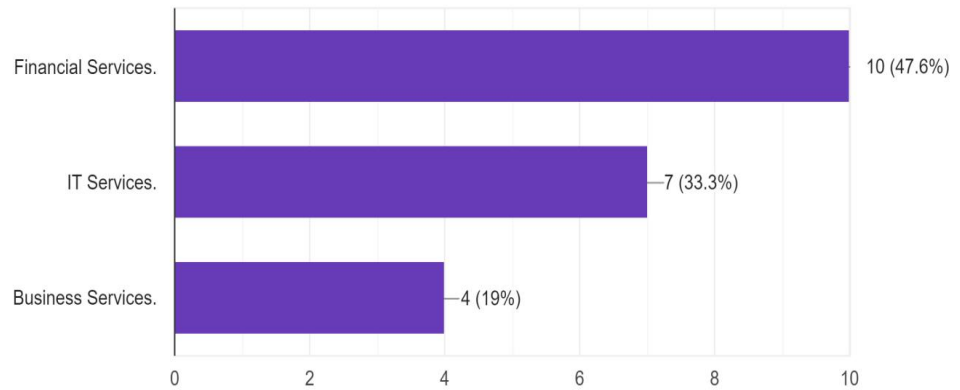


Figure 3: Represents the no.of organizations belongs to individual IT sectors (survey 1).

Survey 2:

2. Your organization belongs to which of the following IT sector? (Select all that apply)

16 responses

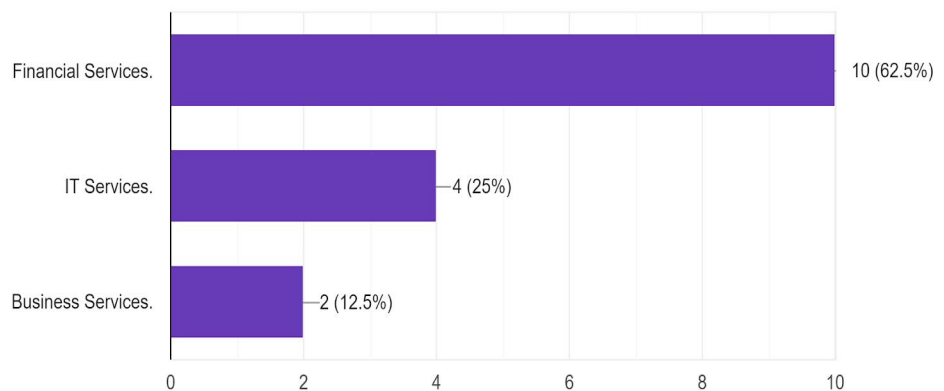


Figure 4: Represents the no.of organizations belongs to individual IT sectors (survey 2).

4.4 Current Information Security Practices

The questions related to “current information security practices” was framed by the researcher on employees, policies and procedures, network security and associated infrastructure, risk management, and business continuity management. The analysis for each of the individual questions was discussed below.

4.4.1 Employees

This section presents the findings related to employee role, the importance of information security and confidence in overall information security framework by the participants (employees) in their organizations, type of awareness briefings and training methods, and how often the employee awareness and training programs are conducted by their organizations.

Question 3: What is your role in your organization?

This research needs to find the participant’s role in their organizations because apart from the information security team or employees, most of the employees do not know much about the information security practices. An employee from an information security team can answer the survey more reliable than others. So, the researcher chose the members of the information security team as participants. The researcher mentioned in the emails which were sent to the organizations along with the survey link while conducting a survey, that this survey is for “information security team members”.

As follows from the figures 5 and 6 which shows 28.6% of the participants were “**Information Security Manager**”, 19% of the participants were “**IT Specialist and Information Security Specialist**”, 33.3% of the participants were “**Information Security Analyst**”, 19% of the participants were “**Technical Manager**” from survey 1. And 50% of the participants were “**Security Manager and Technical Manager**”, 31.3% of the participants were “**Security Analyst**”, 18.8% of the participants were “**Information Security Specialist**” from survey 2 respectively.

Note: Assumptions were made while conducting survey 2 in phase 2, as both “**Information Security Analyst and Security Analyst**” are the same. And both “**Information Security Manager and Security Manager**” are the same. This question is restructured when conducting survey 2 for a better understanding of the participants.

Survey 1:

3. What is your role in your organization?
21 responses

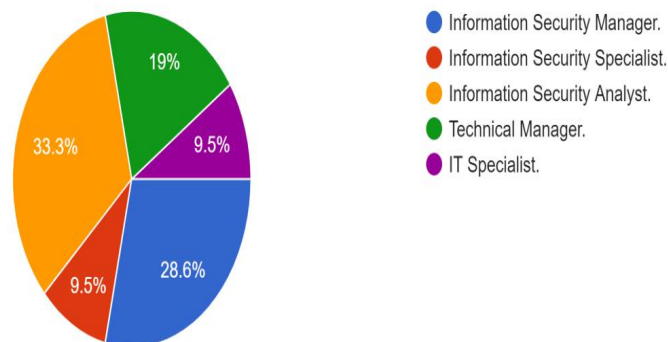


Figure 5: Represents the percentages of employment roles of the participants in the organizations (survey 1).

Survey 2:

3. What is your role in your organization?

16 responses

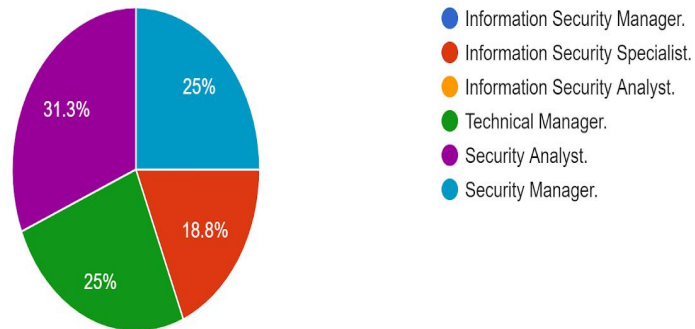


Figure 6: Represents the percentages of employment roles of the participants in the organizations (survey 2).

Question 4: How important is the information security within your organization?

In response to the survey 1 regarding the importance of the information security within the organizations, Figure 7 indicates that 57.1% of the participants reported a “5” rating, 28.6% reported a “4” rating and 14.3% reported a “3” rating respectively. In response to survey 2, Figure 8 indicates that 25% of the participants reported a “4” rating and 75% reported a “3” rating respectively. Surprisingly, there appears to be a big drop in the importance of information security between the two surveys which seems strange when 16 of the same organization are involved. Maybe the organizations had reconsidered their status after the first survey.

Survey 1:

4. On a scale from 0 to 5 (5 being highest rating), How important is the information security within your organization?

21 responses

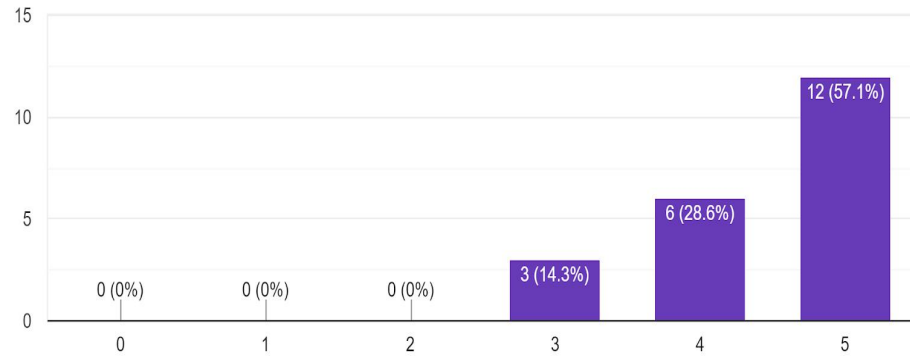


Figure 7: Represents the percentages of the importance of information security in organizations (survey 1).

Survey 2:

4. On a scale from 0 to 5 (5 being highest rating), How important is the information security within your organization?

16 responses

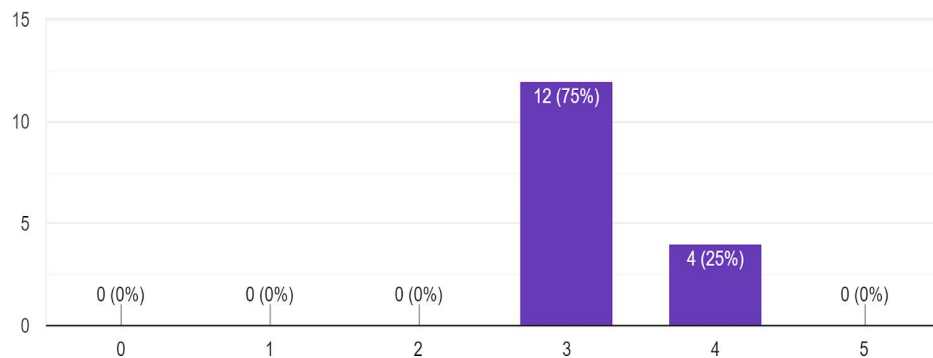


Figure 8: Represents the percentages of the importance of information security in organizations (survey 2).

Question 5: How confident are you about the overall information security framework of your organization?

As can be seen from figure 9 and 10, in response to survey 1, 19% of the participants are very much confident on “**Information security framework**” of their organization and reported a “**5**” rating, 47.6% reported a “**4**” rating and 33.3% reported a “**3**” rating respectively. In response to survey 2, 18.8% of the participants reported a “**4**” rating and 81.3% reported a “**3**” rating respectively. Similar to the previous question there appears to be a big drop in confidence on the overall information security framework between the two surveys. Maybe the confidence in the overall information security framework is related to the importance of information security is the reason which one affects the other.

Survey1:

5. On a scale from 0 to 5 (5 being highest rating), How confident are you about the overall information security framework of your organization?

21 responses

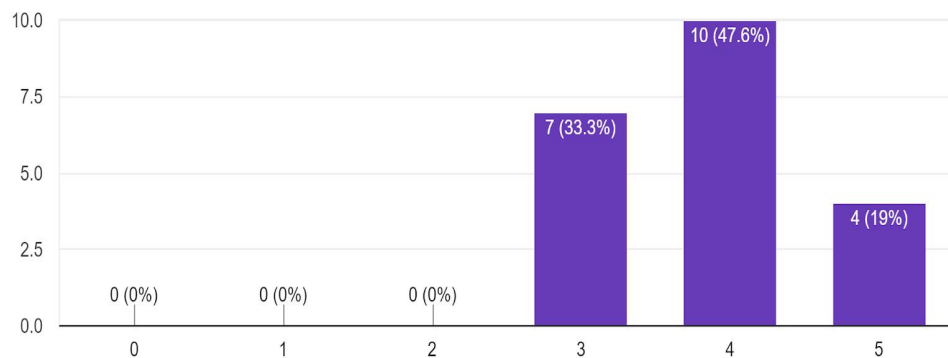


Figure 9: Represents the percentages of confidence of the organizations in their information security framework (survey 1).

Survey 2:

5. On a scale from 0 to 5 (5 being highest rating), How confident are you about the overall information security framework of your organization?

16 responses

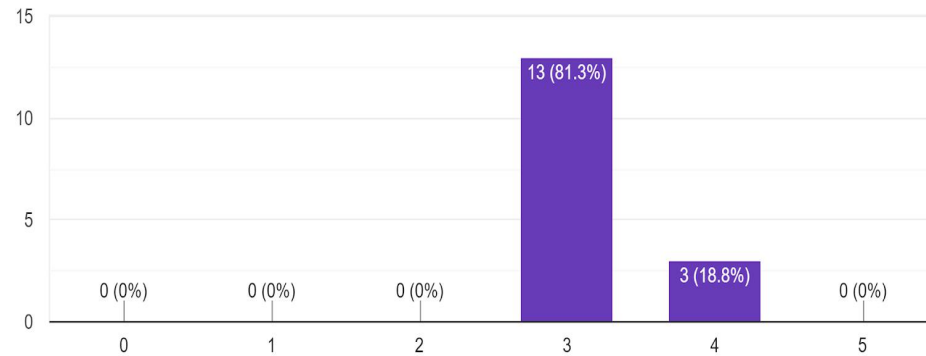


Figure 10: Represents the percentages of confidence of the organizations in their information security framework (survey 2).

Question 6: What type of awareness briefings and training methods are used by your organization to educate employees on information security?

In response to survey 1, Figure 11 shows that 66.7% of the organizations conducting **“Regular training sessions., Provide a training manual to the employee upon joining the organization”** each, 81% conducting **“General meetings and conferences”**, and 38.1% conducting **“Online training sessions”** respectively. In response to survey 2, Figure 12 shows that 62.5% of the organizations conducting **“Regular training sessions., Provide training manual to the employee upon joining the organization”**, 75% conducting **“General meetings and conferences”** and 37.5% conducting **“Online training sessions”** respectively. The results from the surveys were almost similar in which organizations using **“Regular training sessions., Provide a training manual to the employee upon joining the organization, General meetings and conferences”** methods more and giving less priority to **“Online training sessions”** to train and educate their employees on information

security. The frequencies table for survey 2 results shows the 8 combinations of data sets (refer to table 5 in appendices).

Survey1:

6. What type of awareness briefings and training methods are used by your organisation to educate employees on information security? (Select all that apply)

21 responses

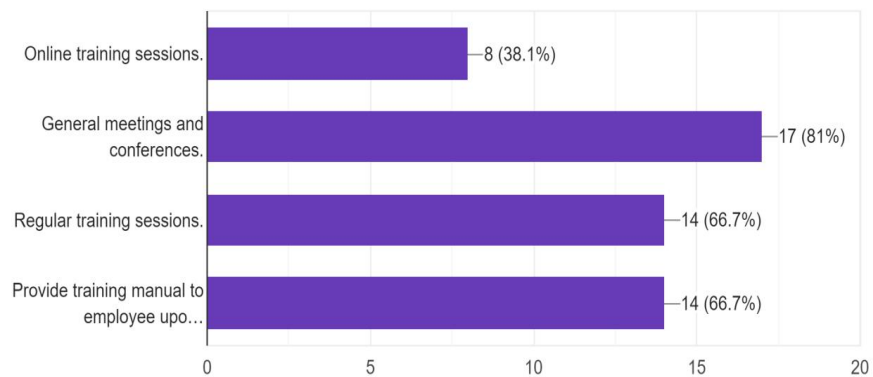


Figure 11: Represents the percentages of the type of awareness briefings and training methods in the organizations (survey 1).

Survey 2:

6. What type of awareness briefings and training methods are used by your organisation to educate employees on information security? (Select all that apply)

16 responses

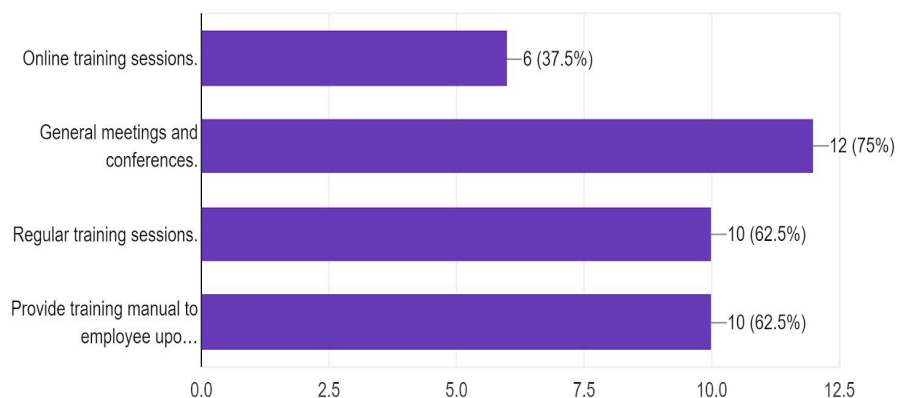


Figure 12: Represents the percentages of the type of awareness briefings and training methods in the organizations (survey 2).

Question 7: How often the employee awareness and training programs on information security are conducting by your organization?

As shown in figure 12 in response to survey1, 14.3% (3 out of 21 organizations) reported that the employee awareness and training programs on information security are being conducted for every “**Half-yearly**” by their organizations, 52.4% (11 out of 21 organizations) reported “**Quarterly**”, 33.3% (7 out of 21 organizations) reported “**Monthly**” respectively. In response to survey2, figure 13 shows 6.2% (1 out of 16 organizations) reported “**Half-yearly**”, 56.3% (9 out of 16 organizations) reported “**Quarterly**” and 37.5% (6 out of 16 organizations) reported “**Monthly**” respectively. The results from the surveys were almost similar in which most of the organizations conducting the awareness and training programs every three months and monthly wise, and half-yearly by few organizations.

Survey1:

7. How often the employee awareness and training programs on information security are conducting by your organization?

21 responses

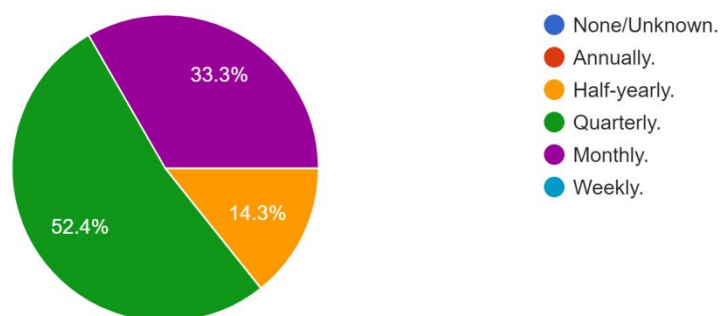


Figure 13: Represents the percentages of how often the training programs were conducted by your organizations (survey 1).

Survey2:

7. How often the employee awareness and training programs on information security are conducting by your organization?

16 responses

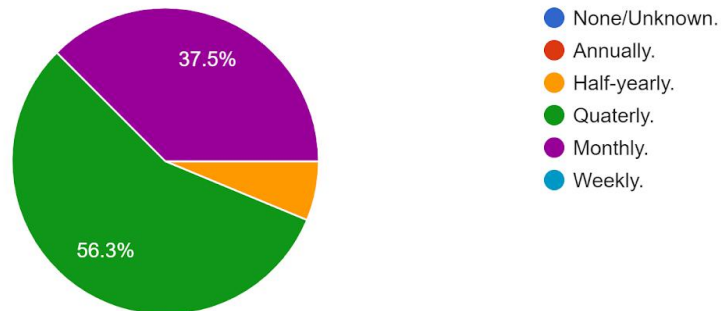


Figure 14: Represents the percentages of how often the training programs were conducted by your organizations (survey 2).

4.4.2 Policies and Procedures

This section presents the findings related to policies and procedures. As can be seen from fig 14 and 15, in response to survey 1, 42.9% of the participants are more confident on “**Policies and Procedures**” of their organization and reported a “**5**” rating, 38.1% reported a “**4**” rating and 19% reported a “**3**” rating respectively. In response to survey 2, 12.5% of the participants reported a “**4**” rating and 87.5% reported a “**3**” rating respectively. There seems to be a significant drop in the confidence in information security policies and procedures between the two surveys which seems odd.

Question 8: How confident are you about the information security "Policies and Procedures" of your organization?

Survey1:

8. On a scale from 0 to 5 (5 being highest rating), How confident are you about the information security "Policies and Procedures" of your organization?

21 responses

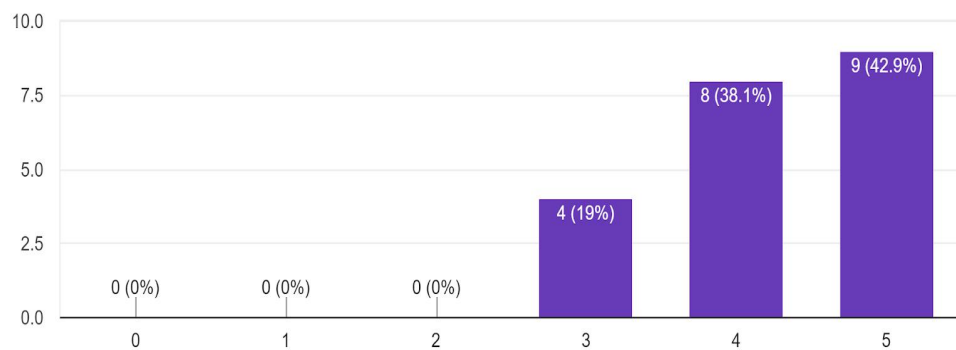


Figure 15: Represents the percentages of confidence of the organizations on information security policies and procedures (survey 1).

Survey2:

8. On a scale from 0 to 5 (5 being highest rating), How confident are you about the information security "Policies and Procedures" of your organization?

16 responses

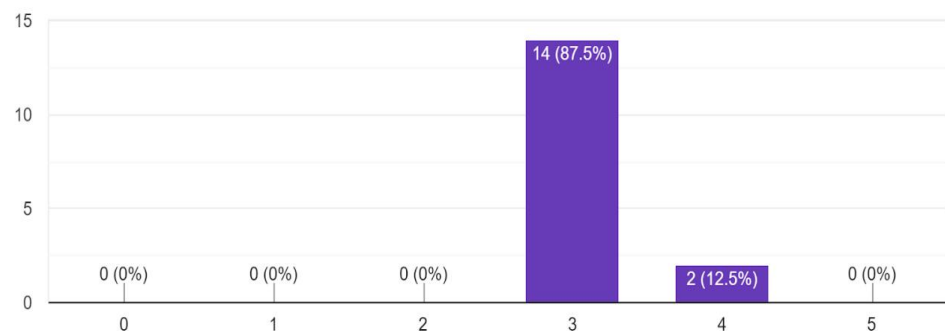


Figure 16: Represents the percentages of confidence of the organizations on information security policies and procedures (survey 2).

4.4.3 Network Security and Associated Infrastructure

This section presents the findings related to network security and associated infrastructure. In response to survey 1, Figure 16 shows that 71.4% of the organizations implemented “**Multi-factor authentication**”, 42.9% implemented “**Data encryption**”, 85.7% implemented “**Firewalls**”, 52.4% implemented “**Intrusion detection and prevention systems**”, 90.5% implemented “**Antivirus software**”, and 23.8% implemented “**Honeypots**” respectively. In response to survey 2, Figure 17 shows that 56.3% of the organizations implemented “**Multi-factor authentication**”, 43.8% implemented “**Data encryption**”, 81.3% implemented “**Firewalls**”, 31.3% implemented “**Intrusion detection and prevention systems**”, 81.3% implemented “**Antivirus software**”, and 6.3% implemented “**Honeypots**” respectively. By observing both results “**Firewalls and Antivirus software**” were implemented by most of the organizations and “**Honeypots**” were implemented by very few organizations.

Question 9: Which of the following information security measures has your organization implemented?

Survey1:

9. Which of the following information security measures has your organization implemented?(Select all that apply)

21 responses

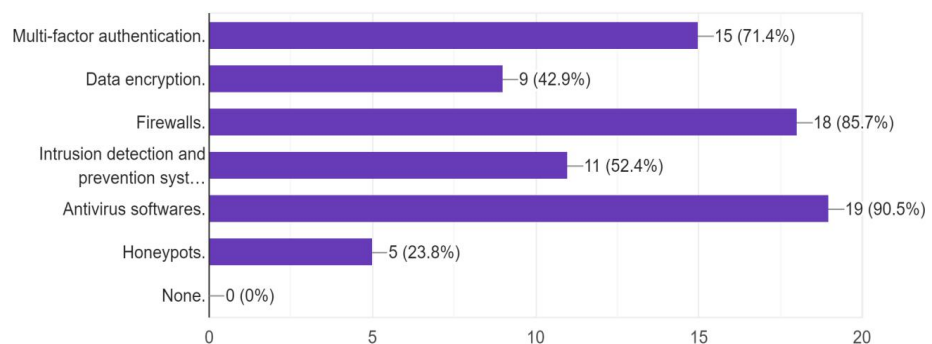


Figure 17: Represents the percentages of information security measures implemented in the organizations. (survey 1).

Survey 2:

9. Which of the following information security measures has your organization implemented?(Select all that apply)

16 responses

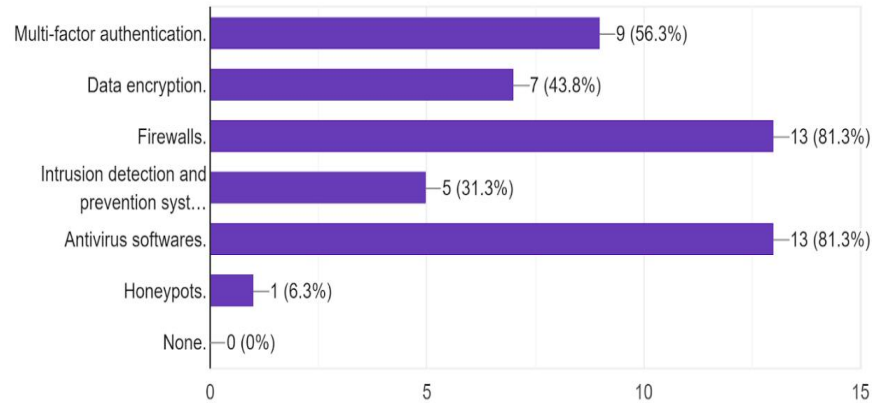


Figure 18: Represents the percentages of information security measures implemented in the organizations. (survey 2).

4.4.4 Risk Management

This section presents the findings related to risk management. Figures 17 and 18 show, in response to survey 1, 23.8% of the participants are very much confident in information security “**Risk Management**” in their organization and reported a “**5**” rating, 38.1% reported a “**4**” rating and 38.1% reported a “**3**” rating respectively. There seems to be a significant drop in the confidence in information security risk management in survey 2 which seems odd. In response to survey 2, 6.3% of the participants reported a “**4**” rating, 68.8% reported a “**3**” rating, and 25% reported a “**2**” rating respectively. Maybe the organizations had reconsidered their status after the first survey.

Question 10: How confident are you about the information security "Risk Management" of your organization?

Survey1:

10. On a scale from 0 to 5 (5 being highest rating), How confident are you about the information security "Risk Management" of your organization?

21 responses

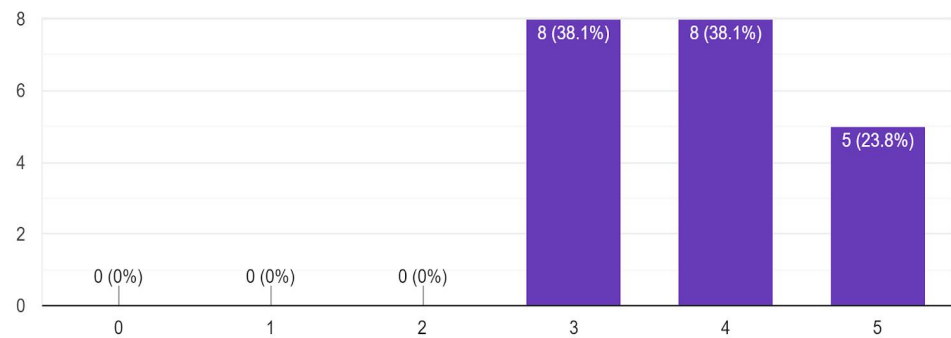


Figure 19: Represents the percentages of confidence of the organizations on information security risk management (survey 1).

Survey 2:

10. On a scale from 0 to 5 (5 being highest rating), How confident are you about the information security "Risk Management" of your organization?

16 responses

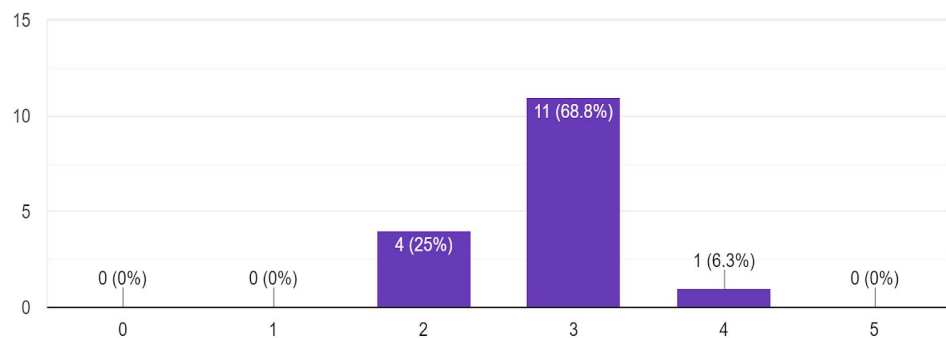


Figure 20: Represents the percentages of confidence of the organizations on information security risk management (survey 2).

Question 11: Does your organization have any "Business Continuity Plan" in case of an information security disaster?

In response to survey 1, Figure 19 shows 76.2% (16 out of 21 organizations) of the participants reported “**Yes**” and 14.3% (3 out of 21 organizations) of the participants reported “**No**” respectively. In response to survey 2, Figure 20 shows 62.5% (10 out of 16 organizations) of the participants reported “**Yes**” and 18.8% (3 out of 16 organizations) of the participants reported “**No**” respectively. The results from both surveys were almost similar and most of the organizations have a business continuity plan in case of an information security disaster.

Survey 1:

11. Does your organization have any "Business Continuity Plan" in case of an information security disaster?

21 responses

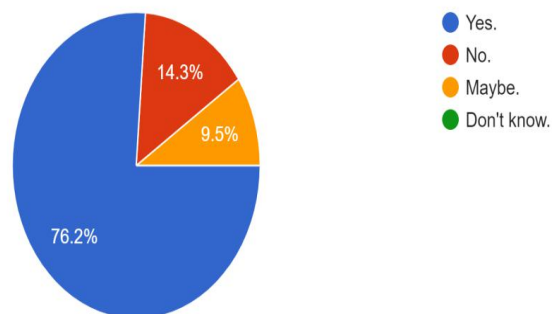


Figure 21: Shows the percentage of the organizations that implemented a business continuity plan (survey 1).

Survey 2:

11. Does your organization have any "Business Continuity Plan" in case of an information security disaster?

16 responses

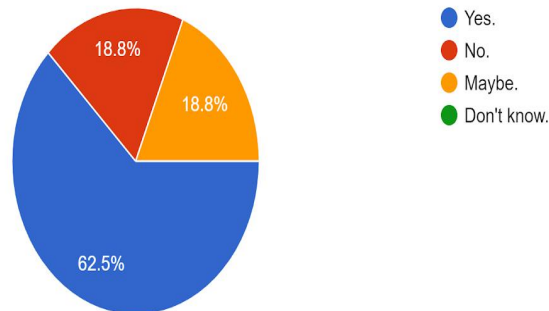


Figure 22: Shows the percentage of the organizations that implemented a business continuity plan (survey 2).

4.4.5 Business Continuity Management

This section presents the findings related to business continuity management. In response to survey 1, Figure20 shows 23.8% of the participants are very much confident on "**Business continuity management**" in their organization and reported a "**5**" rating, 23.8% reported a "**4**" rating, 38.1% reported a "**3**" rating and 14.3% reported a "**3**" rating respectively. In response to survey 2, Figure 21 shows 6.3% of the participants reported a "**4**" rating, 56.3% reported a "**3**" rating, 25% reported a "**2**" rating, and 12.5% reported a "**1**" rating respectively. The results from both surveys were contrasting with each other and doesn't make any sense. Only the organizations which gave rating "**3**" were constant in survey 2.

Question 12: How confident are you about the "Business Continuity Management" of your organization in case of an information security disaster?

Survey1:

12. On a scale from 0 to 5 (5 being highest rating), How confident are you about the "Business Continuity Management" of your organization in case of an information security disaster?

21 responses

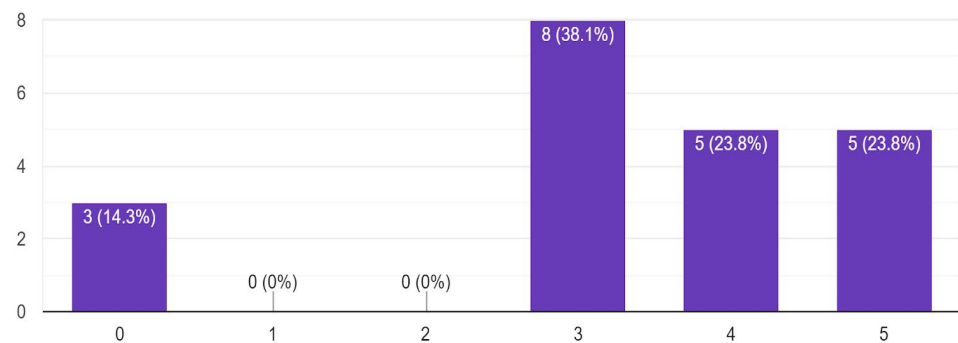


Figure 23: Represents the percentages of confidence of the organizations on their business continuity management (survey 1).

Survey 2:

12. On a scale from 0 to 5 (5 being highest rating), How confident are you about the "Business Continuity Management" of your organization in case of an information security disaster?

16 responses

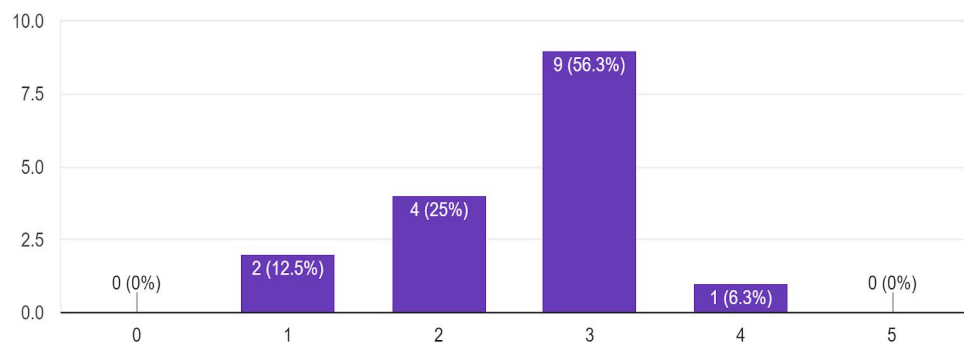


Figure 24: Represents the percentages of confidence of the organizations on their business continuity management (survey 2).

4.4.6 Correlation coefficient test

Correlation coefficient test statistics evaluate the statistical relationship or interconnections between two or more variables. This provides information regarding the relationship's potential impact or correlation and the nature of the interaction between variables.

The P-value is the probability of the correlation coefficient. When this probability is less than the standard 5% ($P < 0.05$) the correlation coefficient is called statistically relevant. $P > 0.05$ is a chance the test is correct. A statistically significant test outcome ($p\text{-value} \leq 0.05$) indicates that the test is incorrect or will be dismissed. A p-value higher than 0.05 indicates that no impact has been detected. The correlation coefficient(r) usually reflects the degree to which two variables differ proportionately on an average. The correlation coefficient(r) is between -1 and 1. If the value is between 0 and 1, it means the relationship between variables is strong. If the value is between -1 and 0, it means the relationship between variables is weak (SPSS Tutorials - Correlation Coefficient Test, 2017).

Correlation coefficient test is conducted for the questions 4, 5, 8, 10 and 12 respectively for the results of both surveys to evaluate the statistical relationship or interconnections between the variables: **“Importance of information security within Organization, Information Security Framework, Policies and Procedures, Risk Management and Business Continuity Management”**. The P-values for all the variables in the table were either standard ($P < 0.05$) where the correlation coefficient is called statistically relevant or $P > 0.05$ is a chance the test is correct. The correlation coefficient (r) was between 0 and 1, it means the relationship between variables is strong. The correlation coefficient(r) and p-values in the below table 2 and table 3 show that there is a strong relationship between the variables and the correlation coefficient test is correct. Which means one variable changes when the other

one does. If we observe the results of questions 4, 5, 8, 10, and 12, they were almost similar which proves that there is a strong relationship between them.

Survey 1:

Correlation coefficient test for questions 4, 5, 8, 10, and 12 for survey 1 results.

Confidence							
I m p o r t a n c e		Correlation coefficient	Q4.Importance of information security within the Organization	Q5.Information Security Framework	Q8.Policies and Procedures	Q10.Risk Management	Q12.Business Continuity Management
	Q4.Information security within the Organization	(r)					
		P-value					
	Q5.Security Framework	(r)	0.671***				
		P-value	< .001				

Q8.Policies and Procedures	(r)	0.772***	0.690			
	P-value	< .001	< .001			
Q10.Risk Management	(r)	0.785	0.657	0.633**		
	P-value	< .001	0.001	0.002		
Q12.Business Continuity Management	(r)	0.779	0.601**	0.680	0.790	
	P-value	< .001	0.004	< .001	<.001	

Table 2: Correlation coefficient test values for survey 1 results.

Survey 2:

Correlation coefficient test for questions 4, 5, 8, 10, and 12 for survey 2 results.

Confidence							
I m p o r t a n c e		Correl ation coeffic ient	Q4.Importan ce of information security within the Organizatio n	Q5.Infor mation Security Framework ork	Q8.Poli cies and Proced ures	Q10.Ris k Manage ment	Q12.B usiness Contin uity Manag ement
	Q5.Se curity Frame work	(r)	0.832**				
		P-valu e	< .001				
	Q8.Pol icies and Proced ures	(r)	0.655**	0.787*			
		P-valu e	0.006	< .001			

Q10.R isk Manag ement	(r)	0.206	0.475	0.493		
	P-value	0.445	0.063	0.052		
Q12.B usines s Contin uity Manag ement	(r)	0.137	0.267	0.450	0.254	
	P-value	0.612	0.318	0.081	0.342	

Table 3: Correlation coefficient test values for survey 2 results.

4.5 Threats to Information Security

The questions related to “Threats to the information security” were framed by the researcher on insider threats, technical threats (system-specific), and environmental and physical threats. The analysis for each of the individual questions was discussed below.

Question 13: Did your organization experience an information security breach and when?

In response to the question, whether the organization experienced any information security breach and when. In response to the survey1, Figure 22 shows 14.3% (3 out of 21 organizations) of the participants reported “**Yes, In the last month**”, 38.1% (8 out of 21 organizations) reported “**Yes, In the last year**”, 33.3% (7 out of 21 organizations) reported “**Yes, In the last two years**” and 14.3% (3 out of 21 organizations) reported “**Don’t know**” respectively. In response to the survey2, Figure 23 shows 18.8% (3 out of 16 organizations) of the participants reported “**Yes, In the last month**”, 37.5% (6 out of 16 organizations) reported “**Yes, In the last year**”, 37.5% (6 out of 16 organizations) reported “**Yes, In the last two years**” and 6.2% (1 out of 16 organizations) reported “**No Breach**” respectively. By observing both results in most of the organizations there were information security breaches which were happened most in the last year and the last two years, and only a few happened in the last month in some organizations.

Survey1:

13. Did your organization experience an information security breach and when?

21 responses

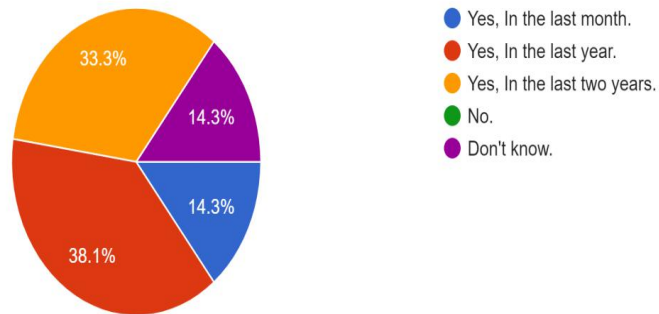


Figure 25: Shows the percentages of organizations experienced an information security breach and when (survey 1).

Survey2:

13. Did your organization experience an information security breach and when?

16 responses

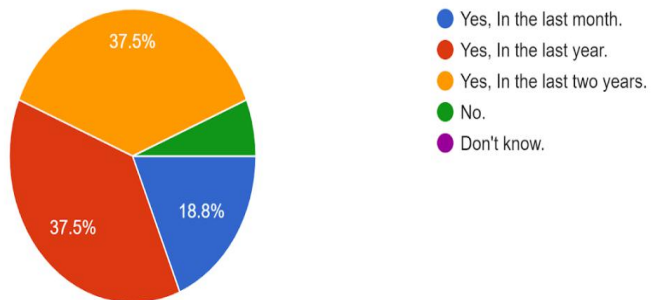


Figure 26: Shows the percentages of organizations experienced an information security breach and when (survey 2).

4.5.1 Insider threats, Technical Threats (System-specific), and Environmental and Physical threats

This section presents the findings related to insider threats, technical threats (system-specific), and environmental and physical threats. In response to the question, to find the probability of the information security threats posed within their organization such as insider threats, unauthorized access, malware threats, (DoS/DDoS) threats, phishing threats, advanced persistent threats and environmental or physical threats which are rated individually by the participants. Most of the threats were rated “**3 and 4**” in survey 1 and “**2 and 3**” in survey 2. All most all threats were rated uniformly by the participants in both surveys. Refer table 6 and 7 in appendices to know the number of individual participants rated individual threats.

Question 14: Rate each of the following information security threats posed within your organization?

Survey 1:

14. On a scale from 0 to 5 (5 being highest rating), rate the each of following information security threats posed within your organization ?

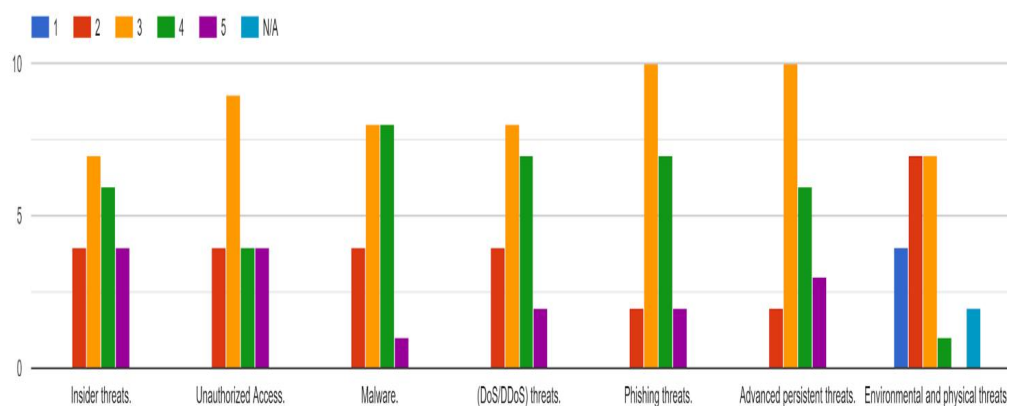


Figure 27: Shows the individual ratings of the information security threats posed within the organizations (survey 1).

Survey 2:

14. On a scale from 0 to 5 (5 being highest rating), rate the each of following information security threats posed within your organization ?

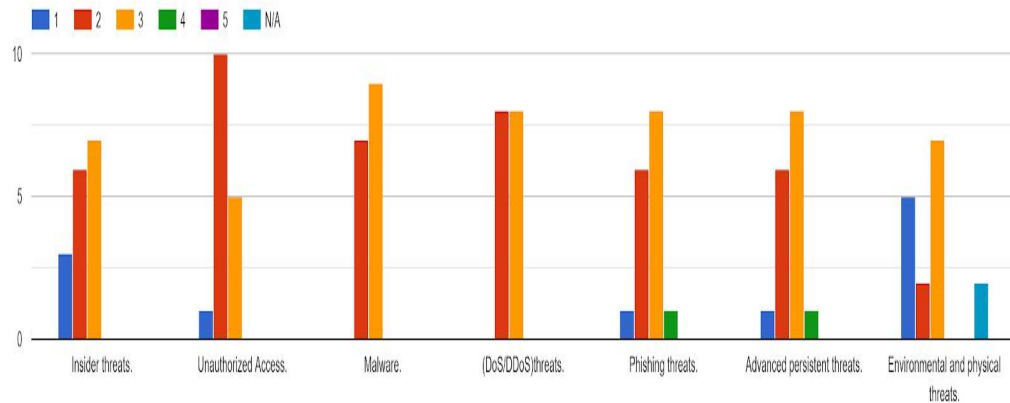


Figure 28: Shows the individual ratings of the information security threats posed within the organizations (survey 2).

Question 15: Which of the following insider threat do you consider the most "LIKELY" to happen to your organization?

In response to the survey1, Figure 22 shows 14.3% of the participants reported “**Malicious Insider**”, 66.7% reported “**Irresponsible Insider**” and 85.7% reported “**Foreign Agents**” respectively. In response to the survey2, Figure 23 shows 18.8% of the participants reported “**Malicious Insider**”, 75% reported “**Irresponsible Insider**” and 68.8% reported “**Foreign Agents**” respectively. By observing the results from both surveys, irresponsible insider and foreign agents were the most likely happening threats in the organizations where organizations were less affected by a malicious insider. The frequencies table for survey 2 results shows the 4 combinations of data sets (refer to table 7 in appendices).

Survey1:

15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)

21 responses

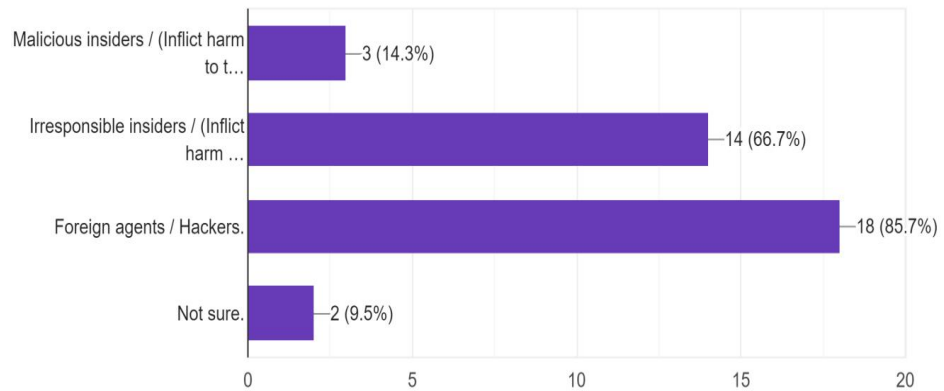


Figure 29: Shows the percentages of insider threats the most likely to happen in the organizations (survey 1).

Survey2:

15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)

16 responses

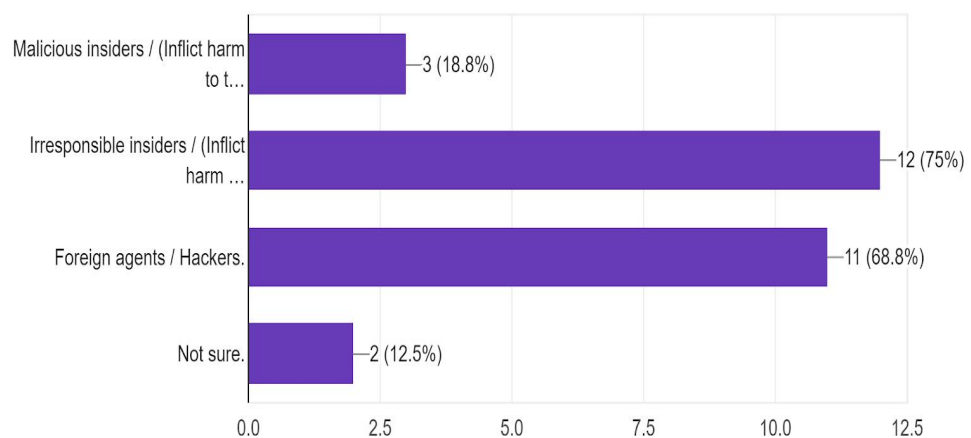


Figure 30: Shows the percentages of insider threats the most likely to happen in the organizations (survey 2).

4.6 Barriers to Implement Prerequisite Information Security Measures

The questions related to the theme 3 “Barriers to implementing prerequisite information security measures” were framed by the researcher on lack of expertise and knowledge, implementation costs, lack of resources and capital.

4.6.1 Lack of Expertise and Knowledge, Implementation Costs, and Lack of Resources and Capital

This section presents the findings related to lack of expertise and knowledge, implementation costs, lack of resources and capital. In response to survey 1, Figure 22 shows 38.1% of the participants reported “**Lack of expertise and knowledge**”, 85.7% reported “**Implementation costs**” and 61.9% reported “**Lack of capital and Resources**” respectively. In response to survey 2, Figure 23 shows 43.8% of the participants reported “**Lack of expertise and knowledge**”, 87.5% reported “**Implementation costs**” and 75% reported “**Lack of capital and Resources**” respectively. The results show that organizations were effected by implementation costs followed by a lack of capital and resources which stood as barriers to implement prerequisite information security measures. Lack of expertise and knowledge stood last among the three barriers. The frequencies table for survey 2 results shows the 5 combinations of data sets (refer to table 8 in appendices).

Question 16: Which of the following barriers prevents your organization to implement prerequisite information security measures?

Survey1:

16. Which of the following barriers prevents your organization to implement prerequisite information security measures?(Select all that apply)

21 responses

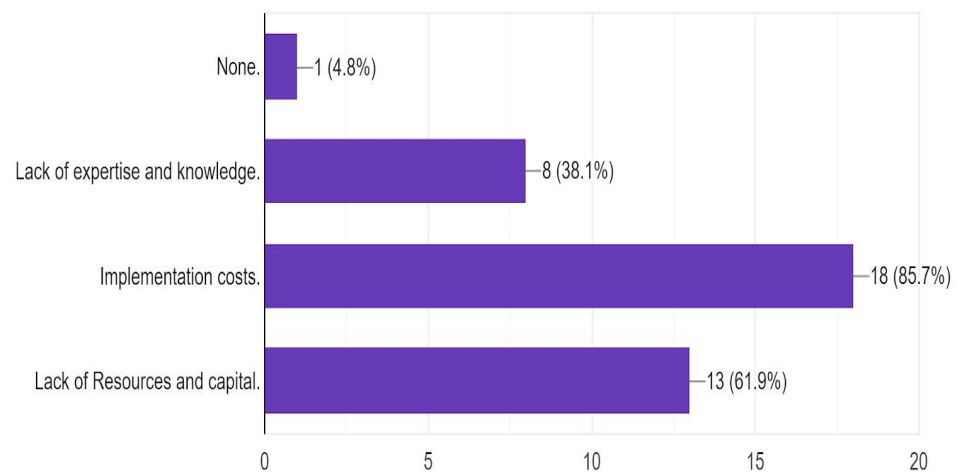


Figure 31: Represents the percentages of barriers that prevent organizations to implement prerequisite information security measures (survey 1).

Survey2:

16. Which of the following barriers prevents your organization to implement prerequisite information security measures?(Select all that apply)

16 responses

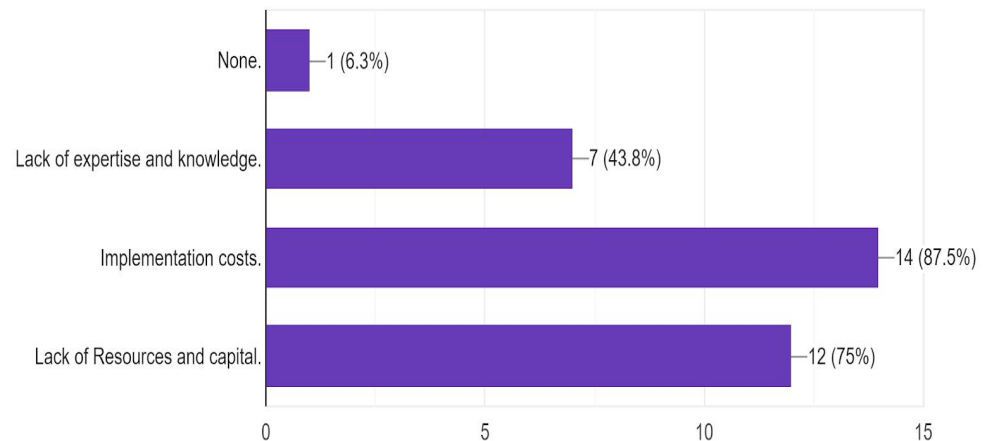


Figure 32: Represents the percentages of barriers that prevent organizations to implement prerequisite information security measures (survey 2).

4.7 Conclusion

The data which is collected from both surveys is represented in the form of charts and diagrams and analyzed. After analyzing the results, the researcher found that there was a strong relationship between the variables: “**Importance of information security within Organization, Information Security Framework, Policies and Procedures, Risk Management, and Business Continuity Management**” related to the topic information security practices. Where the authors and researchers of the previous studies didn’t mention the relationship and explained those variables individually. Also most of the results related to the topics “**Threats to the information security and Barriers to implementing prerequisite information security measures**” were a contrast to the statements made by the researchers in previous studies, discussed in literature review which were further discussed in the next chapter.

Chapter 5: Discussion

5.1 Introduction

This discussion chapter looks through the purpose, significance, and importance of the results which are obtained in the previous chapter. The researcher concentrated on describing and analyzing the results, demonstrating how it applies to the literature review and research questions by putting forward an argument to support the endpoint.

5.2 Profile of the Participants

Surveys were conducted in two phases. In phase 1, survey 1, a total of 21 out of 52 responses were received. In phase 2, survey 2, a total of 16 out of 21 responses were received. All the participants were responded from three SME IT sectors such as financial services, IT services, and business services. Also, all the participants are from the information security team of their respective organizations which indicates that they are very well known about the information security of their organization.

5.3 Data Triangulation

Data triangulation is chosen when two distinct, separate (but practically similar) data sets are used and the data should be collected at various points in time, or in dimension or at different locations. The term triangulation refers to the method of using different data sources or multiple methods to interpret data to improve the validity of the research ([Czarzasty, 2000](#)).

In this research, the researcher had conducted surveys in two phases. The results obtained from the two surveys were compared and validated to achieve triangulation. Comparing the results of both surveys.

Questions	Results	
	Phase1, Survey1 Out of 21 respondents	Phase1, Survey1 Out of 16 respondents
1. What is the size of your organization? <ul style="list-style-type: none"> ● Small (0 - 50 Employees). ● Medium (50 - 250 Employees). 	<ul style="list-style-type: none"> ● Medium - 14. ● Small - 7. 	<ul style="list-style-type: none"> ● Medium - 10. ● Small - 6.
2. Your organization belongs to which of the following IT sector? (Select all that apply) <ul style="list-style-type: none"> ● Financial Services. ● IT Services. ● Business Services. 	<ul style="list-style-type: none"> ● Financial services - 10. ● IT services - 7. ● Business services - 4. 	<ul style="list-style-type: none"> ● Financial services - 10. ● IT services - 4. ● Business services - 2.
3. What is your role in your organization? <ul style="list-style-type: none"> ● Information Security Manager. ● Information Security Specialist. ● Information Security Analyst. ● Technical Manager. ● IT Specialist. 	<ul style="list-style-type: none"> ● Information Security Manager - 6. ● Information Security Specialist - 2. ● Information Security Analyst - 7. ● Technical Manager - 4. ● IT Specialist - 2. 	<ul style="list-style-type: none"> ● Information Security Manager - 4. ● Information Security Specialist - 3. ● Information Security Analyst - 5. ● Technical Manager - 4.

4. On a scale from 1 to 5 (5 being the highest rating), How important is the information security within your organization?	<ul style="list-style-type: none"> ● 5 rating - 12. ● 4 rating - 6. ● 3 rating - 3. 	<ul style="list-style-type: none"> ● 4 rating - 4. ● 3 rating - 12.
5. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the overall information security framework of your organization?	<ul style="list-style-type: none"> ● 5 rating - 4. ● 4 rating - 10. ● 3 rating - 7. 	<ul style="list-style-type: none"> ● 4 rating - 3. ● 3 rating - 13.
6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply) Online training sessions. General meetings and conferences. Regular training sessions. Provide a training manual to the employee upon joining the organization.	<ul style="list-style-type: none"> ● Online training sessions - 8. ● General meetings and conferences - 17. ● Regular training sessions - 14. ● Provide a training manual to the employee upon joining the organization - 14. 	<ul style="list-style-type: none"> ● Online training sessions - 5. ● General meetings and conferences - 12. ● Regular training sessions - 14. ● Provide a training manual to the employee upon joining the organization - 10.

<p>7. How often the employee awareness and training programs on information security are conducting by your organization?</p> <ul style="list-style-type: none"> ● Annually. ● Half-Yearly. ● Quarterly. ● Monthly. ● Weekly. 	<ul style="list-style-type: none"> ● Half-Yearly - 3. ● Quarterly - 11. ● Monthly - 7. 	<ul style="list-style-type: none"> ● Half-Yearly - 1. ● Quarterly - 9. ● Monthly - 6.
<p>8. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the information security "Policies and Procedures" of your organization?</p>	<ul style="list-style-type: none"> ● 5 rating - 9. ● 4 rating - 8. ● 3 rating - 4. 	<ul style="list-style-type: none"> ● 4 rating - 2. ● 3 rating - 14.
<p>9. Which of the following information security measures has your organization implemented? (Select all that apply)</p> <ul style="list-style-type: none"> ● Multi-factor authentication. ● Data encryption. ● Firewalls. ● Intrusion detection and prevention systems. ● Antivirus software. ● Honeypots. ● None. 	<ul style="list-style-type: none"> ● Multi-factor authentication - 15. ● Data encryption - 9. ● Firewalls - 18. ● Intrusion detection and prevention systems - 11. ● Antivirus software - 19. ● Honeypots - 5. ● None - 0. 	<ul style="list-style-type: none"> ● Multi-factor authentication - 9. ● Data encryption - 7. ● Firewalls - 12. ● Intrusion detection and prevention systems - 5. ● Antivirus software - 14. ● Honeypots - 3. ● None - 0.

10. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the information security "Risk Management" of your organization?	<ul style="list-style-type: none"> ● 5 rating - 5. ● 4 rating - 8. ● 3 rating - 8. 	<ul style="list-style-type: none"> ● 4 rating - 1. ● 3 rating - 11. ● 2 rating - 4.
11. Does your organization have any "Business Continuity Plan" in case of an information security disaster? <ul style="list-style-type: none"> ● Yes. ● No. ● Maybe. ● Don't know. 	<ul style="list-style-type: none"> ● Yes - 16. ● No - 3. ● Maybe - 2. ● Don't know -0. 	<ul style="list-style-type: none"> ● Yes - 10. ● No - 3. ● Maybe - 3. ● Don't know -0.
12. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the "Business Continuity Management" of your organization in case of an information security disaster?	<ul style="list-style-type: none"> ● 5 rating - 5. ● 4 rating - 5. ● 3 rating - 8. ● 0 rating - 3. 	<ul style="list-style-type: none"> ● 4 rating - 1. ● 3 rating - 9. ● 2 rating - 4. ● 1 rating - 2.
13. Did your organization experience an information security breach and when? <ul style="list-style-type: none"> ● Yes, In the last month. ● Yes, In the last year. ● Yes, In the last two years. ● No. ● Don't know. 	<ul style="list-style-type: none"> ● Yes, In the last month - 3. ● Yes, In the last year - 8. ● Yes, In the last two years - 7. ● No - 0. ● Don't know - 3. 	<ul style="list-style-type: none"> ● Yes, In the last month - 3. ● Yes, In the last year - 6. ● Yes, In the last two years - 6. ● No - 1. ● Don't know - 0.

<p>14. On a scale from 0 to 5 (5 being the highest rating), rate each of following information security threats posed within your organization?</p> <ul style="list-style-type: none"> ● Insider threats. ● Unauthorized Access. ● Malware. ● (DoS/DDoS) threats. ● Phishing threats. ● Advanced persistent threats. ● Environmental and physical threats. 	<p>Refer to tables 6 and 7 in appendices.</p>	
<p>15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)</p> <ul style="list-style-type: none"> ● Malicious insiders / (Inflict harm to the organization purposely). ● Irresponsible insiders / (Inflict harm to the organization by mistake). ● Foreign agents / Hackers. ● Not sure. 	<ul style="list-style-type: none"> ● Malicious insiders - 3. ● Irresponsible insiders - 14. ● Foreign agents or Hackers - 18. ● Not sure - 2. 	<ul style="list-style-type: none"> ● Malicious insiders - 3. ● Irresponsible insiders - 11. ● Foreign agents or Hackers - 11. ● Not sure - 2.

16. Which of the following barriers prevents your organization to implement prerequisite information security measures? (Select all that apply) <ul style="list-style-type: none"> ● None. ● Lack of expertise and knowledge. ● Implementation costs. ● Lack of Resources and capital. 	<ul style="list-style-type: none"> ● None - 1. ● Lack of expertise and knowledge - 8. ● Implementation costs - 18. ● Lack of Resources and capital - 13. 	<ul style="list-style-type: none"> ● None - 1. ● Lack of expertise and knowledge - 7. ● Implementation costs - 14. ● Lack of Resources and capital - 12.
--	--	--

Table 4: Data triangulation.

Observing the results and number of respondents reported the answers to the individual questions in table 4 are almost similar which proves the validity of the data. Also, the results section 4.4.6, Correlation coefficient tests for both surveys shows that they are almost the same.

5.4 Current Information Security Practices

The findings of this research show that there is a strong relationship between employees, policies and procedures, and different managements such as network security management, risk management, and business continuity management of the organization in which one affects the other. Similarly, Brett Valentine (2017) stated, information security practices in SMEs are indeed an inseparable part of different organizational management of information technology which perceives the security threats, that technology tends to raise. In support of the researcher finding the results section 4.4.6, Correlation coefficient tests for both surveys shows that there is a strong relationship between employees, policies and procedures, and different managements such as network security management, risk management, and business continuity

management of the organization. The P-values for all the variables in tables 2 and 3 were either standard ($P < 0.05$) where the correlation coefficient is called statistically relevant or $P > 0.05$ is a chance the test is correct. The correlation coefficient (r) was between 0 and 1, it means the relationship between variables is strong. The correlation coefficient (r) and p-values in tables 2 and 3 show that there is a strong relationship between the variables and the correlation coefficient test are correct.

Surprisingly, Gonzalez and Sawicka (2002) stated, no matter how professionally planned, security measures depend on the people (employees) who adopt them (Gonzalez and Sawicka, 2002). Supporting this view, Garrison (2006) stated that the employees are theoretically the greatest risk to information security protection. Garrison (2006) stated that the employees are theoretically the greatest risk to information security protection in SMEs. The employees are responsible for the security activities like, downloading a trojan, integrates an unapproved program, uploads a virus from a storage device, introduces a malicious email, unattended a system registered in, discloses login details or chooses a simple password that puts the whole organization at risk (Garrison, 2006). Thomas R.Peltier (2016) stated that the policies and procedures are of no use, unless or until they are followed by the employees in the organization (Thomas R.Peltier, 2016). And the HR management of “Business & Finance” has reported that while an impressive 93% of Irish SMEs agree that HR management plays a key role in the organization, only a little over half currently invested in HR management. 68% of Irish SMEs employing up to 10 workers have no HR management, with this number falling to just 36% for Irish SME's employing 11-50 employees (small organization), and 29% for Irish SME' employing 50-250 employees (medium organization) (Business & Finance, 2020). In contrast to the all above literature review statements, this study found that employees especially the information security team has a critical role to play in SMEs to protect information. The information security team in SMEs is responsible for:

- Designing policies and management of an organization's security posture.
- Providing the organization's strategy from an information security viewpoint.
- Carrying out various security programs.
- Maintaining firewalls, antivirus software, data encryption, intrusion detection and prevention, honeypots, and strong passwords.
- Conducting awareness and training sessions for other employees on information security.
- Coordination and escalating incidents.
- Risk management.
- Business continuity plan.

Considering survey 2 results were the final survey results. The results supporting the research show that almost all the participants from survey 2 reported that they are confident in “**Information security framework, Policies and Procedures**”. The results of survey 2 were as follows: 18.8% of the participants were confident in the “**Information security framework**” of their organization and reported a “4” rating and 81.3% of the participants reported a “3” rating respectively. And for the “**Policies and Procedures**”, 12.5% of the participants reported a “4” rating and 87.5% of the participants reported a “3” rating respectively. Also, respondents reported regular awareness and training sessions on information security were conducting in all possible ways such as online training sessions (37.5%, 6 out of 16 organizations), general meetings and conferences (75%, 12 out of 16 organizations), regular training sessions (62.5%, 10 out of 16 organizations) respectively. And these awareness and training sessions are mostly conducting monthly (37.5%, 6 out of 16 organizations) and quarterly (56.3%, 9 out of 16 organizations) periods which is good for the organizations providing employees the information security knowledge up-to-date.

Surprisingly most of the participants were not that confident when it comes to **“Risk management, Business continuity management, Network security and associated infrastructure”** of their organization. And the final results (survey 2 results) from the findings were as follows: For **“Risk management”**, 6.3% (1 out of 16 organizations) reported a “4” rating, 68.8% (11 out of 16 organizations) reported a “3” rating and 25% (4 out of 16 organizations) reported a “2” rating respectively. For **“Business continuity management”**, 6.3% (1 out of 16 organizations) reported a “4” rating, 56.3% (9 out of 16 organizations) reported a “3” rating, 25% (4 out of 16 organizations) reported a “2” rating and 12.5% (2 out of 16 organizations) reported a “1” rating respectively. For **“Network security and associated infrastructure”**, only “Firewalls and Antivirus software” (81.3%, 13 out of 16 organizations) was implemented by most of the organizations. Followed by “Multi-factor authentication (56.3%, 9 out of 16 organizations), Data encryption (43.8%, 7 out of 16 organizations), Intrusion detection and prevention systems (31.3%, 5 out of 16 organizations), and honeypots (6.3%, 1 out of 16 organizations) were implemented by the organizations respectively. Similar to this Manuele (2016) stated managing risk of data security in small and medium IT organizations is the continuous process of identifying, fixing, and minimizing security risks. Risk assessment has become critical in SMEs because of the cost-benefit ratio (Manuele, 2016). And, Ellis Holman (2012) stated, Management of Business Continuity is a process of risk management that addresses the risk of instability to business processes and practices. The effectiveness of business continuity management can help to achieve excellent organizational continuity in SMEs. Unfortunately, business Continuity management or disaster recovery is not adequate in SMEs because of a lack of expertise (Ellis Holman, 2012). Also, 59% of the Irish SMEs said that they are lacking some network associated infrastructure such as highly reliable internet connection, firewalls, intrusion detection and prevention systems, antivirus software, and honeypots (Irish Tech News, 2019) in literature review supporting each statement.

5.5 Threats to Information Security

The findings of this research found that almost every organization that participated in the surveys had experienced breaches. Most of the SMEs experienced the breaches in the last year (37.5%, 6 out of 16 organizations) and the last two years (37.5%, 6 out of 16 organizations). The previous studies on threats to information security stated that many threats inflict damage to SMEs. Ming.L, Li.X (2012) categorized these information security threats in SME's into three types. They are insider threats, technical threats (system-specific), and environmental threats (Tang.J, Wang.D, Ming.L, Li.X, 2012). The findings of this research identified the threats which inflicting most damage in organizations point of view among insider threats, technical threats (system-specific), and environmental threats. In support of this, the results show that almost all respondents reported that technical threats are inflicting the most damage to the organizations. In technical threats, almost all **“Insider threats, Unauthorized access, Malware threats, (DoS/DDoS) threats, Phishing threats, Advanced persistent threats, and Environmental or physical threats”** were rated uniformly (mostly rated 2 and 3) by the participants in the final survey 2. Environmental and physical threats (mostly rated 1 and 2), and insider threats (18.8%, 3 out of 16 organizations) were rated moderately by the respondents. Following the insider threats, Cummings, Adam, Lewellen, Todd, McIntire, David, Moore, Andrew, Trzeciak, and Randall (2010) categorized the insider threat into three types. They are malicious insiders, who inflict harm to the organization purposely with the help of their access advantage. Irresponsible insiders, who inflict harm to the organization by mistake due to ignoring policies. Hackers, who are foreign agents without authorization to receive valid login information. And reported malicious insiders are the most inflicting threat in SMEs (Probst, Christian & Hunker, Jeffrey & Gollmann, Dieter & Bishop, Matt, 2012). In contrast to the above literature review statement, the researcher from the results found that foreign agents (68.8%, 11 out of 16 organizations) and irresponsible insiders (75%, 12 out of 16 organizations) were the threats experienced by the

organizations the most when compared to the malicious insider threats (18.8%, 3 out of 16 organizations).

5.6 Barriers to Implement Prerequisite Information Security Measures

The findings of this research identified that implementation costs (87.5%, 14 out of 16 organizations reported), lack of resources and capital (75%, 12 out of 16 organizations reported) were the main barriers for the small and medium IT organizations to implement prerequisite information security measures. Brodcrick (2006) stated the main potential barrier to implementing the prerequisite information security practices is a lack of expertise and knowledge on the information security of the administrators in SMEs. Some administrators are least worried about the security of information (Brodcrick, 2006). KanKanhalli (2003); Straub (1990) argued, many administrators collectively lack knowledge about the range of measures that are available to minimize misuse of information security in SME's (KanKanhalli et al., 2003; Straub, 1990). Administrators lack adequate IS expert knowledge (DE Lone, 1998; Gable, 1991; Spinellis et al., 1999). In contrast to the all above literature review statements which stated that lack of knowledge and expertise was the major barrier, but the results found that it was the least reported barrier (43.8%, 7 out of 16 organizations) compared to implementation costs, lack of resources and capital.

Wiander (2007) argued that information security is usually not a full-time job in SMEs. As a result, there is indeed a threat that perhaps the person responsible for information security will see certain responsibilities as even more crucial, as information security task has been considered as cost (Wiander, 2007). Doherty & Fulford (2005) stated, the implementation of successful information security measures requires a lot of time, energy, and resources, where entities don't seem prepared to invest (Doherty & Fulford 2005). Wiander (2007) added, enforcing the standard requires total staff and this can entail higher salary costs. Due to the challenging existence of security

requirements, the shortage of resources and capital to purchase the SME 's expertise is again overloaded by the lack of resources to implement and approve the requirements. Effective information security management needs significant time and energy, where most SME's are reluctant to undertake (Doherty & Fulford, 2005; Moule & Giavara, 1995). In support to the all above literature review statements, the final results (survey 2) of this study found implementation costs (87.5%, 14 out of 16 organizations reported) and, lack of resources and capital (75%, 12 out of 16 organizations reported) are the major barriers reported by the participants.

5.7 Conclusion

The researcher after examining the individual responses from the findings of this research found that almost all SMEs that responded were trying their best to implement adequate information security practices. The results in support of the above statement were as follows. Almost all SMEs that responded were conducting online training sessions (37.5%, 6 out of 16 organizations), general meetings and conferences (75%, 12 out of 16 organizations), regular training sessions (62.5%, 10 out of 16 organizations) respectively. And these awareness and training sessions are mostly conducting monthly (37.5%, 6 out of 16 organizations) and quarterly (56.3%, 9 out of 16 organizations) periods to provide employees the information security knowledge up-to-date. When it comes to network and associated infrastructure most of the organizations implemented firewalls and antivirus software (81.3%, 13 out of 16 organizations) followed by “Multi-factor authentication (56.3%, 9 out of 16 organizations), Data encryption (43.8%, 7 out of 16 organizations) and Intrusion detection and prevention systems (31.3%, 5 out of 16 organizations) respectively. And when it comes to the confidence in information security framework, policies and procedures, and risk management almost all organizations gave ratings “3 and 4” respectively. Even though the organizations were not confident in business continuity management, 62.5% (10 out of 16 organizations) have a business continuity plan in case of an information security disaster. These results show that almost all SMEs that

responded were trying their best to implement adequate information security practices. But the implementation costs (87.5%, 14 out of 16 organizations reported), lack of resources and capital (75%, 12 out of 16 organizations reported) became major barriers for them. Even though SMEs implementing some of the information security practices which can afford and can be handled by them. Also, each new era brings new threats to SMEs. Such threats are becoming increasingly complex and taking total advantage over the weaknesses of user-related infrastructure assets. Every device, if it is hardware or software, has security flaws which will cause intense damage to the organization once it is exploited. Also, almost all respondents reported the issues of threats posed to their organizations. The respondents in the final survey (survey 2) reported that hackers or foreign agents (68.8%, 11 out of 16 organizations) became a serious problem for the SMEs. To discourage hackers and overcome vulnerabilities at various stages, many security checks are enforcing and implementing as a part of an “in-depth strategy of layered defense” by SME’s. Which is allowing them to control and restrict the damage, eliminate the source, and apply modified control measures on security. This study mainly found that the respondents reported a high number of threats posed to their organizations even though they have no barriers to implement prerequisite information security measures and following good information security practices.

This chapter discussed the findings around the three research questions: Information security practices, Threats to the information security and Barriers to implementing prerequisite information security measures, and the literature review related to the three research questions. Also compared and validated the surveys which were conducted in two phases to achieve data triangulation and validation.

Chapter 6: Conclusion

6.1 Introduction

This study was conducted by the researcher to examine and investigate the information security practices, threats, and barriers in SMEs in Ireland. The objectives of this study were:

- To investigate the current information security practices following in small and medium-sized IT organizations.
- To analyze the major threats to information security in small and medium-sized IT organizations.
- To examine the major barriers to implement prerequisite information security practices for small and medium-sized IT organizations.

Key results have emerged while conducting this study. Consequently, conclusions are provided in this chapter based on the above-mentioned findings and study objectives. Recommendations are also emphasized which are important for these findings. Lastly, certain areas where future work is required are identified.

6.2 Current Information Security Practices

The findings of this research found that there is a strong relationship between employees, policies and procedures, and different managements such as network security management, risk management, and business continuity management of the organization in which one affects the other and results of the correlation coefficient test supports this finding (referring section 4.4.6). The information security team plays a crucial role in SMEs and is responsible for following information security practices in the organizations. Almost all organizations who had participated in this study have confidence on their information security framework, policies and procedures but surprisingly not that confident when it comes to risk management, business continuity

management, and network security and associated infrastructure which gives scope to the threats to inflict damage to the SME's in one way or another way. The current information security practices following the small and medium IT organizations found by this study were:

- Awareness and training programs on information security conducting monthly and quarterly periods.
- Framing good policies and procedures on information security.
- Using firewalls, encrypting data, multi-factor authentication, antivirus software, intrusion detection and prevention systems for network protection.
- Risk management and business continuity management in case of an information security disaster.

6.3 Threats to Information Security

Most of the SMEs experienced the information security breaches in the last year and the last two years. This study identified the technical threats (system-specific) such as malware, Dos/DDos threats, phishing threats, and advanced persistence threats were the threats posed to the organizations the most when compared to the insider and environmental or physical threats. Also, the foreign agents and irresponsible insiders were the threats posed to the organizations the most when compared to the malicious insider threats. Environmental and physical threats were almost negligible in SMEs. Also, each new era brings new threats to SMEs. Such threats are becoming increasingly complex and taking total advantage over the weaknesses of user-related infrastructure assets. Every device, if it is hardware or software, has security flaws which will cause intense damage to the organization once it is exploited. The key threats to the information security in SMEs found by this study were:

- Foreign agents (68.8%, 11 out of 16 organizations) and irresponsible insiders (75%, 12 out of 16 organizations) were the threats experienced by the organizations compared to the malicious insider threats (18.8%, 3 out of 16 organizations).
- Technical threats were inflicting the most damage to the organizations. In technical threats, all most all “**Insider threats, Unauthorized access, Malware threats, (DoS/DDoS) threats, Phishing threats, Advanced persistent threats and Environmental or physical threats**” were rated uniformly (mostly rated 2 and 3) by the participants.

6.4 Barriers to Implement Prerequisite Information Security Measures

The implementation costs, lack of resources and capital were the main barriers for SMEs to implement prerequisite information security measures when compared to lack of knowledge and expertise. Organizations conducting regular awareness and training sessions on information security are in all possible ways such as online training sessions, general meetings, and conferences, regular training sessions. And these awareness and training sessions are mostly conducting monthly and quarterly periods which is good for the organizations providing employees the information security knowledge up-to-date. Lack of knowledge and expertise can be overcome by the SMEs by conducting awareness and training sessions. But the implementation costs, lack of resources and capital can not be overcome by the SMEs. SMEs need to plan and follow adequate information security practices with the available resources and capital. The key barriers to implementing prerequisite information security measures in SMEs found by this study were implementation costs (87.5%, 14 out of 16 organizations reported), lack of resources and capital (75%, 12 out of 16 organizations reported).

6.5 Recommendations

The researcher concluded after examining some key findings, objectives, and literature review of this study. The recommendations proposed by the researcher reflects the conclusions which set out the measures further to be taken by the SMEs.

1. The results of this research can be considered as factors for creating information security policies and procedures.
2. Implementation of information security policies and procedures at the organizational level in SME's can be found in the quantitative results.
3. SME's need to take protective measures for irresponsible insider threats and foreign agents as they are inflicting more damage to the organizations.
4. Investigation shows the application of honeypots, intrusion detection and prevention systems are lack in most of the SMEs which makes their systems more vulnerable. Implementation of these measures can make the network infrastructure of their organizations more secure.
5. New methods of training for different categories of employees based on their employment role are needed like online training sessions, general meetings and conferences, provide training manual to the employee upon joining in the organization.
6. Quarterly and monthly awareness and training programs were not found to be effective, new measures of creating these awareness and training programs need to be considered.
7. Although 70% of the respondents pointed out the presence of the business continuity plans but failed to address the confidence during the time of information security disaster, which needs to be taken care of.
8. Phishing and advanced persistent threats are recorded to be most happening threats in the SME's when compared to others, relevant measures during the awareness and training sessions need to be focused to prevent these threats.

Small and medium-sized IT organization which has limited number of employees, lack of resources and capital, and high implementation cost to implement prerequisite information security measures. The probability of threats to inflict damage to the SMEs is high. There are less opportunities for SMEs to implement proper information security practices due to a lack of resources and capital, and implementation costs. So, organizations need to plan and implement adequate information security practices within their budget.

6.6 Future Research:

This research mainly found that there are many threats posed to SMEs even though the organizations have no barriers to implement prerequisite information security measures and following adequate information security practices. This gives the scope to future research to find the reasons why many threats are posed to SME's even though there are following adequate information security practices. Also, the research is mainly carried out on 52 small and medium-sized IT organizations in which financial services, IT Services, and business services were only in scope. So, there is a large scope to research other IT sectors as well.

Also, this research is limited in investigating only five major areas of expertise of information security practices: employees, policies and procedures, network security and associated infrastructure, risk management, and business continuity management which plays an important role in protecting the organization's information to full scale. Three categories of threats: insider, technical, environmental and physical threats. Three major barriers: lack of expertise and knowledge, implementation costs, lack of resources and capital which are identified and discussed in the literature review. There is a scope to research other areas of expertise of information security practices, threats, and barriers that are not discussed in this study.

7. References

1. Ismail, N., 2020. 7 Cyber Security Threats To Smes And How To Secure Against Them. [online] Information Age. Available at: <<https://www.information-age.com/7-nightmare-cyber-security-threats-smes-secure-123466495/>> [Accessed 4 February 2020].
2. ComputerWeekly.com. 2020. The Top Five SME Security Challenges. [online] Available at: <<https://www.computerweekly.com/feature/The-top-five-SME-security-challenges>> [Accessed 8 February 2020].
3. Isc2.org. 2020. (ISC)² Research Report Indicates That Small Businesses May Not Be The Weakest Link In The Supply Chain. [online] Available at: <<https://www.isc2.org/News-and-Events/Press-Room/Posts/2019/06/20/ISC2-Research-Report-Indicates-That-Small-Businesses-May-Not-Be-the-Weakest-Link-in-the-Supply-Chain>> [Accessed 16 February 2020].
4. Irwin, L., 2020. 61% Of Data Breaches Hit Smes - IT Governance Blog En. [online] IT Governance Blog En. Available at: <<https://www.itgovernance.eu/blog/en/61-of-data-breaches-hit-smes>> [Accessed 16 February 2020].
5. Small Business Trends. 2020. 43% Of Cyber Attacks Still Target Small Business - Ransomware On Rise. [online] Available at: <<https://smallbiztrends.com/2019/05/2019-small-business-cyber-attack-statistics.html>> [Accessed 17 February 2020].
6. Segal, C., 2020. 8 Cyber Security Best Practices For Your Small To Medium-Size Business. [online] Coxblue.com. Available at: <<https://www.coxblue.com/8-cyber-security-best-practices-for-your-small-to-medium-size-business-smb/>> [Accessed 24 February 2020].

7. Kaila, U., 2018. Information Security Best Practices: First Steps for Startups and SMEs. *Technology Innovation Management Review*, 8(11), pp.32-42.[Accessed 11 March 2020].
8. S. Todd, M. and M. Rahman, S., 2013. Complete Network Security Protection for SME's within Limited Resources. *International Journal of Network Security & Its Applications*, 5(6), pp.1-13.[Accessed 15 March 2020].
9. Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M., 2005. Information Security Threats and Practices in Small Businesses. *Information Systems Management*, 22(2), pp.7-19.[Accessed 15 March 2020].
10. Kurpjuhn, T., 2015. The SME security challenge. *Computer Fraud & Security*, 2015(3), pp.5-7.[Accessed 15 March 2020].
11. Huang, D., Patrick Rau, P., Salvendy, G., Gao, F. and Zhou, J., 2011. Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, 69(12), pp.870-883.[Accessed 3 April 2020].
12. Chenoweth, J., 2005. Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. *Journal of Information Privacy and Security*, 1(1), pp.43-44.[Accessed 3 April 2020].
13. Jouini, M., Rabai, L. and Aissa, A., 2014. Classification of Security Threats in Information Systems. *Procedia Computer Science*, 32, pp.489-496.[Accessed 11 April 2020].
14. Sumner, M., 2009. Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. *Information Systems Management*, 26(1), pp.2-12.[Accessed 11 April 2020].
15. Paulsen, Celia. "Cybersecuring Small Businesses." *Computer*, vol. 49, no. 8, Institute of Electrical and Electronics Engineers (IEEE), Aug. 2016, pp. 92–97. Crossref, doi:10.1109/mc.2016.223.[Accessed 11 April 2020].

16. Chun, Yong-Tae. "Cyber Security Management of Small and Medium-Sized Enterprises with Consideration of Business Management Environment." *Korean Security Science Review*, vol. 59, Korean Security Science Association, June 2019, pp. 9–35. Crossref, doi:10.36623/kssa.2019.59.1.[Accessed 11 April 2020].
17. "Structure and Challenges of a Security Policy on Small and Medium Enterprises." *KSII Transactions on Internet and Information Systems*, vol. 12, no. 2, Korean Society for Internet Information (KSII), Feb. 2018. Crossref, doi:10.3837/tiis.2018.02.012.[Accessed 9 May 2020].
18. Brewer, Ross. "Advanced Persistent Threats: Minimising the Damage." *Network Security*, vol. 2014, no. 4, Elsevier BV, Apr. 2014, pp. 5–9. Crossref, doi:10.1016/s1353-4858(14)70040-6.[Accessed 9 May 2020].
19. Kurpjuhn, Thorsten. "The SME Security Challenge." *Computer Fraud & Security*, vol. 2015, no. 3, Elsevier BV, Mar. 2015, pp. 5–7. Crossref, doi:10.1016/s1361-3723(15)30017-8.[Accessed 9 May 2020].
20. Freeman A., Doyle L. (2010) The Utilization of Information Systems Security in SMEs in the South East of Ireland. In: D'Atri A., De Marco M., Braccini A., Cabiddu F. (eds) *Management of the Interconnected World*. Physica-Verlag HD [Accessed 13 June 2020].
21. Fruhlinger, J., 2020. Does It Matter Who The CISO Reports To?. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3278020/does-it-matter-who-the-ciso-reports-to.html>> [Accessed 13 June 2020].
22. TechRepublic. 2020. The CIA Triad. [online] Available at: <<https://www.techrepublic.com/blog/it-security/the-cia-triad/>> [Accessed 13 June 2020].

23. Stewart, James (2012). CISSP Study Guide. Canada: John Wiley & Sons, Inc. pp. 255–257. ISBN 978-1-118-31417-3.[Accessed 13 June 2020].
24. Services, P., 2020. What Is An Incident Response Plan For IT?. [online] Cisco. Available at: <<https://www.cisco.com/c/en/us/products/security/incident-response-plan.html>> [Accessed 13 June 2020].Stewart, James Michael; Chapple, Mike; Gibson, Darril (2015).[Accessed 13 June 2020].
25. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. [Accessed 13 June 2020].
26. Security Intelligence. 2020. Security Is An Organizational Behavior Problem. [online] Available at: <<https://securityintelligence.com/security-is-an-organizational-behavior-problem/>> [Accessed 14 June 2020].
27. Basil Cupa, Trojan Horse Resurrected: On the Legality of the Use of Government Spyware (Govware), LISS 2013, pp. 419–428[Accessed 14 June 2020].
28. BHAIJI, Y., 2016. Network Security Technologies And Solutions (Ccie Professional Development Series). [Place of publication not identified]: CISCO Press.[Accessed 14 June 2020].
29. Malware Revolution: A Change in Target. March 2007.[Accessed 14 June 2020].
30. Andress, J. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Syngress. p. 240. ISBN 9780128008126.[Accessed 16 June 2020].
31. PDF4PRO. 2020. Information Security Policies, Procedures, And Standards ... / Information-Security-Policies-Procedures-And-Standards.Pdf /

PDF4PRO. [online] Available at:
<<https://pdf4pro.com/view/information-security-policies-procedures-and-standards-5aba91.html>> [Accessed 16 June 2020].

32. PowerDMS. 2020. Following Policies And Procedures And Why It's Important. [online] Available at:
<<https://www.powerdms.com/blog/following-policies-and-procedures-why-its-important/>> [Accessed 16 June 2020].

33. Turner, Dawn M. "Digital Authentication: The Basics". Cryptomathic.[Accessed 16 June 2020].

34. Oppliger, Rolf (May 1997). "Internet Security: FIREWALLS and BEYOND". Communications of the ACM. **40** (5): 94. doi:10.1145/253769.253802.[Accessed 16 June 2020].

35. Axelsson, S (2000). "Intrusion Detection Systems: A Survey and Taxonomy"
Mohammed, Mohssen; Rehman, Habib-ur (2015-12-02). Honeypots and Routers: Collecting Internet Attacks. CRC Press. ISBN 9781498702201. [Accessed 17 June 2020].

36. Rapid7. 2020. Information Security Risk Management (ISRI). [online] Available at:
<<https://www.rapid7.com/fundamentals/information-security-risk-management/#:~:text=Information%20security%20risk%20management%2C%20or,availability%20of%20an%20organization's%20assets.>> [Accessed 17 June 2020].

37. Foreman, P: Vulnerability Management, page 1. Taylor & Francis Group, 2010. ISBN 978-1-4398-0150-5. [Accessed 17 June 2020].

38. Manuele, F.A. (2016). "Chapter 1: Risk Assessments: Their Significance and the Role of the Safety Professional". In Popov, G.; Lyon, B.K.; Hollcraft, B. (eds.). Risk Assessment: A Practical Guide to Assessing Operational Risks.

John Wiley & Sons. pp. 1–22. ISBN 9781118911044. [Accessed 17 June 2020].

39. Campbell, T. (2016). "Chapter 1: Evolution of a Profession". Practical Information Security Management: A Complete Guide to Planning and Implementation. APress. pp. 1–14. ISBN 9781484216859. [Accessed 17 June 2020].

40. Newsome, B. (2013). A Practical Introduction to Security and Risk Management. SAGE Publications. p. 208. ISBN 9781483324852. [Accessed 17 June 2020].

41. Biscoe, C., 2020. 7 Steps To A Successful ISO 27001 Risk Assessment - IT Governance UK Blog. [online] IT Governance UK Blog. Available at: <<https://www.itgovernance.co.uk/blog/7-steps-to-a-successful-iso-27001-risk-assessment#:~:text=An%20information%20security%20risk%20assessment%20is%20the%20process%20of%20identifying,and%20conduct%20a%20risk%20assessment.>> [Accessed 17 June 2020].

42. Itgovernance.eu. 2020. Business Continuity | IT Governance Ireland. [online] Available at: <<https://www.itgovernance.eu/en-ie/business-continuity-ie>> [Accessed 18 June 2020].

43. Ellis Holman. 2012. A Business Continuity Solution Selection Methodology. IBM Corp.

44. SearchSecurity. 2020. What Is Elk Cloner? - Definition From Whatis.Com. [online] Available at: <<https://searchsecurity.techtarget.com/definition/Elk-Cloner>> [Accessed 18 June 2020].

45. Saravanan, A. and Bama, S., 2019. A Review on Cyber Security and the Fifth Generation Cyberattacks. *Oriental journal of computer science and technology*, 12(2), pp.50-56. [Accessed 18 June 2020].
46. Williamson, Kirsty, and Graeme Johanson. *Research Methods*. Chandos Publishing, 2018. [Accessed 18 June 2020].
47. Roy, Raj. "Survey Research: Definition, Examples and Methods | QuestionPro." *Free Online Survey Software and Tools | QuestionPro®*, QuestionPro, 17 July 2016, <https://www.questionpro.com/article/survey-research.html>. [Accessed 18 June 2020].
48. Cummings, Adam; Lewellen, Todd; McIntire, David; Moore, Andrew; Trzeciak, Randall (2012), *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*, Software Engineering Institute, Carnegie Mellon University, (CMU/SEI-2012-SR-004). [Accessed 22 June 2020].
49. Veriato.com. 2020. *Insider Threat Report 2018*. [online] Available at: <<https://www.veriato.com/resources/whitepapers/insider-threat-report-2018>> [Accessed 22 June 2020].
50. Geric S, Hutinski Z. 2007. Information system security threats classifications. *Journal of Information and Organizational Sciences*. [Accessed 22 June 2020].
51. Fleetwood, D., 2020. *Probability Sampling: Definition, Methods And Examples*. [online] QuestionPro. Available at: <<https://www.questionpro.com/blog/probability-sampling/>> [Accessed 22 June 2020].
52. Top 1000. 2020. *The Top Professional Services Companies On Top1000.Ie*. [online] Available at:

<<https://www.top1000.ie/industries/professional-services>> [Accessed 22 June 2020].

53. Pal, Parashu & Jain, Jitendra. (2017). A Recent Study over Cyber Security and its Elements. Journal of Advanced Research in Law and Economics.[Accessed 22 June 2020].

54. Peltier, T., 2004. Information Security Policies And Procedures. Boca Raton, FL: Auerbach Publications.[Accessed 22 June 2020].

55. Tang J, Wang D, Ming L, Li X. 2012. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory.[Accessed 22 June 2020].

56. Wahyuni, Dina.(2012).The Research Design Maze: Understanding Paradigms, Cases, Methods and Methodologies. Journal of Applied Management Accounting Research, Vol. 10, No. 1, pp. 69-80, 2012. Available at SSRN: <https://ssrn.com/abstract=2103082>. [Accessed 22 June 2020].

57. Probst, Christian & Hunker, Jeffrey & Gollmann, Dieter & Bishop, Matt. (2010). Insider Threats in Cyber Security. 10.1007/978-1-4419-7133-3.[Accessed 22 June 2020].

58. Probst, C., 2010. Insider Threats In Cyber Security. New York: Springer.[Accessed 22 June 2020].

59. Mary Sumner (2009) Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness, Information Systems Management, 26:1, 2-12, DOI: 10.1080/10580530802384639.[Accessed 22 June 2020].

60. Kirk, J. and Miller, M., 2005. Reliability And Validity In Qualitative Research. Newbury Park, Calif: Sage.[Accessed 22 June 2020].

61. Boote, D. N., & Beile, P. (2005). Scholars Before Researchers: On the Centrality of the Dissertation Literature Review in Research Preparation.

Educational Researcher, 34(6), 3–15.
<https://doi.org/10.3102/0013189X034006003>. [Accessed 22 June 2020].

62. Irish Tech News. 2020. Survey: 4 In 10 Irish Smes Have Been The Victim Of A Cyber Security Attack - Irish Tech News. [online] Available at: <<https://irishtechnews.ie/survey-4-in-10-irish-smes-have-been-the-victim-of-a-cyber-security-attack/>> [Accessed 29 June 2020].

63. Irish Tech News. 2020. Smbs Cybersecurity Risk, Their Opportunity - Irish Tech News. [online] Available at: <<https://irishtechnews.ie/smbs-cybersecurity-risk-their-opportunity/>> [Accessed 29 June 2020].

8. Appendices

Question 6: What type of awareness briefings and training methods are used by your organization to educate employees on information security?

In response to the question, type of awareness briefings and training methods are used by your organization to educate employees on information security. The frequencies table shows that 3 out of 16 organizations conducting “Online training sessions., General meetings and conferences., Provide a training manual to the employee upon joining the organization” and 3 out of 16 organizations conducting “General meetings and conferences., Regular training sessions”. A total of 8 combinations of data sets are observed in the below frequencies table.

Frequencies for Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)				
Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)	Frequency	Percent	Valid Percent	Cumulative Percent
General meetings and conferences., Provide a training manual to the employee upon joining the organization.	2	12.500	12.500	12.500
General meetings and conferences., Regular training sessions.	3	18.750	18.750	31.250

Frequencies for Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)				
Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)	Frequency	Percent	Valid Percent	Cumulative Percent
General meetings and conferences., Regular training sessions., Provide a training manual to the employee upon joining the organization	1	6.250	6.250	37.500
Online training sessions., General meetings and conferences.	1	6.250	6.250	43.750
Online training sessions., General meetings and conferences., Provide a training manual to the employee upon joining the organization	3	18.750	18.750	62.500
Online training sessions., General meetings and conferences., Regular training sessions., Provide a training manual to the employee upon joining the organization.	2	12.500	12.500	75.000
Regular training sessions.	2	12.500	12.500	87.500

Frequencies for Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)				
Q6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)	Frequency	Percent	Valid Percent	Cumulative Percent
Regular training sessions., Provide a training manual to the employee upon joining the organization.	2	12.500	12.500	100.000
Missing	0	0.000		
Total	16	100.000		

Table 5: Frequency table for the type of awareness & training methods.

Question 14: Rate each of the following information security threats posed within your organization?

In response to the question, to find the probability of the information security threats posed within their organization such as insider threats, unauthorized access, malware threats, (DoS/DDoS) threats, phishing threats, advanced persistent threats and environmental or physical threats which are rated individually by the participants. Tables 6 and 7 show the number of respondents reported the individual ratings of individual threats.

Survey1:

Rating	Number of Participants						
	Insider Threats	Unauthorized Access	Malware Threats	(DoS/DDoS) Threats	Phishing Threats	Advanced Persistent Threats	Environmental or Physical Threats
5	4	4	1	2	2	3	0
4	6	4	8	7	7	6	1
3	7	9	8	8	10	10	7
2	4	4	4	4	2	2	7
1	0	0	0	0	0	0	4
0	0	0	0	0	0	0	2
Total	21	21	21	21	21	21	21

Table 6: Shows the no.of participants rated individual threats (survey 1).

Survey2:

Rating	Number of Participants						
	Insider Threats	Unauthorized Access	Malware Threats	(DoS/DDoS) Threats	Phishing Threats	Advanced Persistent Threats	Environmental or Physical Threats
5	0	0	0	0	0	0	0
4	0	0	0	0	1	1	0
3	7	5	9	8	8	8	7
2	6	10	7	8	6	6	2
1	3	1	0	0	1	1	5
0	0	0	0	0	0	0	2
Total	16	16	16	16	16	16	16

Table 7: Shows the no.of participants rated individual threats (survey 2).

Question 15: Which of the following insider threat do you consider the most "LIKELY" to happen to your organization?

In response to the question, which of the following insider threat do you consider the most "LIKELY" to happen to your organization. The frequencies in table 8 show that 9 out of 16 organizations reported “Irresponsible insiders., Foreign agents / Hackers” and 3 out of 16 organizations reported “Malicious insiders; Irresponsible insiders”. A total of 4 combinations of data sets were observed in the below frequencies table.

Frequencies for Q15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)						
Q15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)	Frequency	Percentage	Valid Percent	Cumulative Percent		
Foreign agents / Hackers.	2	12.500	12.500		12.500	
Irresponsible insiders / (Inflict harm to the organization by mistake)., Foreign agents / Hackers.	9	56.250	56.250		68.750	
Malicious insiders / (Inflict harm to the organization purposely)., Irresponsible insiders / (Inflict harm to the organization)	3	18.750	18.750		87.500	
Not sure.	2	12.500	12.500		100.000	
Missing	0	0.000				
Total	16	100.000				

Table 8: Frequency table for information security measures implemented in the organizations.

Question 16: Which of the following barriers prevents your organization to implement prerequisite information security measures?

In response to the question, which of the following barriers prevents your organization to implement prerequisite information security measures. The frequencies in table 9 show that 6 out of 16 organizations reported “Implementation costs., Lack of Resources and capital.” and 5 out of 16

organizations reported “Lack of expertise and knowledge., Implementation costs., Lack of Resources and capital”. A total of 5 combinations of data sets were observed in the below frequencies table.

Frequencies for Q16. Which of the following barriers prevents your organization to implement prerequisite information security measures? (Select all that apply)				
Q16. Which of the following barriers prevents your organization to implement prerequisite information security measures? (Select all that apply)	Frequency	Percent	Valid Percent	Cumulative Percent
Implementation costs.	2	12.500	12.500	12.500
Implementation costs., Lack of Resources and capital.	6	37.500	37.500	50.000
Lack of expertise and knowledge., Implementation costs.	1	6.250	6.250	56.250
Lack of expertise and knowledge., Implementation costs., Lack of Resources and capital.	5	18.750	18.750	87.500
Lack of expertise and knowledge., Lack of Resources and capital.	1	6.250	6.250	93.750
None.	1	6.250	6.250	100.000
Missing	0	0.000		
Total	16	100.000		

Table 9: Frequency table for information security barriers in the organizations.

8.1 Questionnaire:

Survey on current information security practices, threats, and barriers for Information security in IT SME's in Ireland.

1. What is the size of your organization?

- Small (0 - 50 Employees).
- Medium (50 - 250 Employees).

2. Your organization belongs to which of the following IT sector?

- Financial Services.
- IT Services.
- Business Services.

3. What is your role in your organization?

- Information Security Manager.
- Information Security Specialist.
- Information Security Analyst.
- Technical Manager.
- IT Specialist.
- Other.

4. On a scale from 1 to 5 (5 being the highest rating), How important is the information security within your organization?

5. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the overall information security framework of your organization?

6. What type of awareness briefings and training methods are used by your organization to educate employees on information security? (Select all that apply)

- Online training sessions.
- General meetings and conferences.
- Regular training sessions.
- Provide a training manual to the employee upon joining the organization.
- Other.

7. How often the employee awareness and training programs on information security are conducting by your organization?

- Annually.
- Half-Yearly.
- Quarterly.
- Monthly.
- Weekly.
- Other.

8. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the information security "Policies and Procedures" of your organization?

9. Which of the following information security measures has your organization implemented? (Select all that apply)

- Multi-factor authentication.
- Data encryption.
- Firewalls.
- Intrusion detection and prevention systems.
- Antivirus software.
- Honeypots.
- None.

10. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the information security "Risk Management" of your organization?

11. Does your organization have any "Business Continuity Plan" in case of an information security disaster?

- Yes.
- No.
- Maybe.
- Don't know.

12. On a scale from 1 to 5 (5 being the highest rating), How confident are you about the "Business Continuity Management" of your organization in case of an information security disaster?

13. Did your organization experience an information security breach and when?

- Yes, In the last month.
- Yes, In the last year.
- Yes, In the last two years.
- No.
- Don't know.

14. On a scale from 0 to 5 (5 being the highest rating), rate each of the following information security threats posed within your organization?

- Insider threats.
- Unauthorized Access.
- Malware.
- (DoS/DDoS) threats.
- Phishing threats.
- Advanced persistent threats.
- Environmental and physical threats.

15. Which of the following insider threat do you consider the most "LIKELY" to happen to your organization? (Select all that apply)

- Malicious insiders / (Inflict harm to the organization purposely).
- Irresponsible insiders / (Inflict harm to the organization by mistake).
- Foreign agents / Hackers.
- Not sure.

16. Which of the following barriers prevents your organization to implement prerequisite information security measures? (Select all that apply)

- None.
- Lack of expertise and knowledge.
- Implementation costs.
- Lack of Resources and capital.

Declaration of Ethical Consideration:

FORM REC 1/L6-8/9T

DECLARATION OF ETHICAL CONSIDERATION

NOTE: This form, (together with sample participant information sheet and sample informed consent form in the case of research to which Section C of this form applies) must be submitted to the supervisor with research proposal prior to commencement of research project.

This form (and additional documentation where Section C applies) shall be retained by the supervisor. The documentation shall be retained to be available for inspection by the REC as required and shall subsequently be attached to the completed research project once submitted for assessment.

In the case of research to which Section C of this form applies, the signature of a second supervisor is required to independently confirm that all relevant ethical issues have been adequately considered and addressed.

Research projects submitted for assessment which have not followed this procedure, shall not be assessed.

Section A

Learner Details:	
Name	Srikanth Chundu
Email	srikanthrvn37@gmail.com
Department	LLL
Programme	MSc Information Technology Management
Year	5
Module	Dissertation
Project Title:	
Main Research Supervisor	
Name	MARTIN MCNAMARA
Email	MCNAMARAM@ITCARLOW.IE
Department	LIFE LONG LEARNING

Section B

TO BE COMPLETED PRIOR TO COMMENCEMENT OF RESEARCH

Does your proposed research project involve (circle as appropriate):

1. A requirement for participant information sheets and receipt of informed consent?

YES ↑

☒ NO ↓

2. Management and retention of personal data of participants?

YES ↑

☒ NO ↓

3. Vulnerable groups (e.g. children, prisoners, individuals who require assisted living or individuals for whom English is not the primary language)

YES ↑

☒ NO ↓

4. Sensitive topics that may make subjects uncomfortable (e.g. sexual behaviour, illegal activities, racial bias or religious affiliation)

YES ↑

☐ NO ↓

5. Use of Drugs

YES ↑

☐ NO ↓

6. Invasive procedures (e.g. blood or tissue sampling)

YES ↑

☐ NO ↓

7. Physical stress or discomfort

YES ↑

☐ NO ↓

8. Psychological distress

YES ↑

☐ NO ↓

9. Deception of, or withholding information from subjects

YES ↑

☐ NO ↓

10. Access to data by individuals or organisations other than the researcher

YES ↑

☐ NO ↓

11. Any conflict of interest relating to or arising from the research project

YES ↑

☐ NO ↓

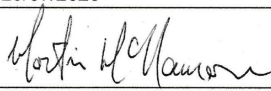
12. Any ethical dilemma relating to or arising from the research project.

YES ☐

NO ☒

If the answer to all of the above is NO, please sign this form and include it in your final project/thesis/dissertation

If the answer to any of the above questions is YES, please proceed to complete Section C

Learner Signature	ch.srikanth
Date	29/07/2020
Main Supervisor Signature	
Date	29/7/20