Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective.

Gerard Whitehead

MASTER OF BUSINESS ADMINISTRATION

This thesis is submitted to the School of Business at the National College of Ireland in partial fulfilment of the requirements for the degree of Master in Business Administration

August 2020

Abstract

Cybercrime is one of the biggest threats to modern businesses. The threat is particularly poignant for SMEs with limited budgets and resources to protect themselves. The inadequate cyber security protection in SMEs has led to an increasing number of attacks and subsequent cyber security incidents. SMEs need to increase investment in this area but have to balance these with other business priorities. The purpose of this research is to analyse the perceptions of senior managers/owners of Irish SMEs to understand the factors that influence decision making related to additional cyber security investment. Understanding these factors will assist when forming governance and standards policies in the future. A qualitative approach using semi-structured interviews was chosen to best answer the research question and accomplish all research objectives. Five participants were selected using purposive sampling that fit the outlined criteria. A conceptual model derived from existing literature consisted of 9 themes forming the basis of questions for semi-structured interviews. Interviews were analysed using thematic analysis and findings were critically assessed in the context of extant literature. The six factors influencing cybersecurity investment decisions in Irish SMEs were identified as (i) cost, (ii) company reputation, (iii) monetary loss, (iv) awareness, (v) regulation and (vi) expertise. Critically, this research showed that SMEs acknowledge the need to invest and are willing, but more guidance is required to ensure investment targets the areas most impactful for the business.

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form
(Thesis/Author Declaration Form)

Name: Gerard Whitehead

Student Number: 18133215

Degree for which thesis is submitted: Masters of Business Adminitration

Title of Thesis: Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior managers/owner perspective

Date: 16/08/2020

Material submitted for award

A. I declare that this work submitted has been composed by myself. ☑

B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged. ☑

C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA. ☑

D. ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award.
Or *I declare that the following material contained in the thesis formed part of a submission for the award of ☑

Master of Business Administration

Signature of research student:

Ger Whitehead

16th August 2020

Submission of Thesis to Norma Smurfit Library, National College of Ireland

Student name: Ger Whitehead

Student number: x118133215 School: National College of Ireland

Course: MBA

Degree to be awarded: Master of Business Administration

Title of Thesis: Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior managers/owner perspective**.**

One hard bound copy of your thesis will be lodged in the Norma Smurfit Library and will be available for consultation. The electronic copy will be accessible in TRAP (http://trap.ncirl.ie/), the National College of Ireland's Institutional Repository.

In accordance with normal academic library practice all theses lodged in the National College of Ireland Institutional Repository (TRAP) are made available on open access.

I agree to a hard bound copy of my thesis being available for consultation in the library.

I also agree to an electronic copy of my thesis being made publicly available on the National College of Ireland's Institutional Repository TRAP.

Signature of Candidate: Ger Whitehead

For completion by the School: The aforementioned thesis was received

by_________________________ Date:______________

This signed form must be appended to all hard bound and electronic copies of your thesis

submitted to your school

Acknowledgements

I would like to thank my supervisor Dr. Colette Darcy for her patience and support throughout the MBA and especially in the last few weeks completing the dissertation. The advice, guidance and feedback have been invaluable in helping me complete this research.

I would like to thank the five participants who voluntarily gave up their time and honest opinions to make this research possible.

I would like to thank Mark Hurley and the team at Spector for giving me the freedom to help reach my goals.

Most importantly, I would like to thank my wife who has been there for me throughout my MBA journey providing encouragement, inspiration and unwavering support.

.

Table of Contents

List of Figures

List of Tables

List of Appendices

List of Abbreviations

COBIT	Control Objectives for Information and Related Technology
NIST	National Institute of Standards and Technology
SME	Small to medium enterprises
GDPR	General Data Protection Regulation
IT	Information Technology
CSO	Central Statistics Office
DCCAE	Department of Communications, Climate Action and Environment
EU	European Union
NCI	National College of Ireland
PRISM	Probability Risk and Impact System
CE	Cyber Essentials
MSP	Managed Service Provider

Problem: **Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior managers/owner perspective.**

1.0. Introduction

1.1. Background and context

With the increasing reliance on technology and ongoing digital transformation, cybercrime is quickly becoming the fastest growing form of criminal activity and is estimated to cost businesses $5.2 trillion by 2024 (Abbosh and Bissell, 2019). Cybersecurity threats and attacks in the past were primarily focused on large organisations where attackers could reap the biggest rewards. Sophisticated hacking has accounted for over 4 billion stolen records such as financial information, login credentials or personal data in the last decade with the majority from larger organisations such as Marriott and Adobe (Holmes, 2019). Mijnhardt, Baars and Spruit (2016) inform us that larger organisations have responded by adopting security standards such as ISO 27000x series, COBIT, NIST, and related frameworks but these frameworks are complicated and expensive for small and medium enterprise (SME) businesses to adopt and implement. According to Rebner (2019), this inherent gap in cybersecurity has made small to medium enterprises a primary target for cybercriminals with 43% of all attacks in 2019 aimed at small to medium-sized businesses (Verizon, 2020).

1.2 Identified problem

In recent years high profile ransomware attacks such as WannaCry and Peyta in 2017 alongside the introduction of General Data Protection Regulation (GDPR) in 2018 have raised the public awareness levels for the necessity of heightened information and cybersecurity processes (European Union, 2020). A high percentage of previous research in information and cybersecurity has been aimed at large organisations. With the growing and evolving threat to small to medium-sized businesses, more detailed research is required to understand attitudes towards cybersecurity from their perspective.

1.2. Proposed research

This study will aim to understand the factors that are influencing decision makers when making cybersecurity investment decisions. Previous research from Ng, Ahmad and Maynard (2013) and De Vries (2017) examine this topic and provide insight into some of the factors but the former is outdated while the latter is not aimed specifically at SMEs. Additionally, previous research in this area is aimed at SMEs globally while this research will analyse SMEs from an Irish only context.

Cybercrime is a global threat but legislation and culture towards security are different in different regions. Van Omenn (2014) discusses cost/benefit analysis as key when making IT security investment decisions so comparing all SMEs globally is both difficult and not accurate. The factors will be similar but the weighting on those factors may be significantly different. For the purpose of this research, the focus will be on the decision makers in Irish SMEs. An SME is defined as having a staff headcount of less than 250 and an annual turnover of less than €50m (European Commission, 2018).

According to the Central Statistics Office (2019), SMEs in Ireland account for 99.8% of all businesses and 68% of all employment. They are hugely important to the Irish economy. Approaching a technical subject as cybersecurity can be a challenge for owners/managers if it is not within their area of expertise. This research aims to provide guidance in approaching these decisions and allow them to assess similarities with SMEs facing similar challenges. In December the Department of Communications, Climate Action and Environment (DCCAE, 2019) launched a revamped National Cyber Security Strategy which in part is aimed at educating and training SMEs to better protect themselves online. Adoption of this strategy will require investment. Studying the perceptions of decision makers and the factors that influence cybersecurity investment decisions will give a clearer understanding of how the adoption of this and similar security standards can be improved in the future.

2.0. Literature Review

2.1. Introduction

In the literature chapter, the term cybersecurity will be defined along with an explanation of its relationship to information security. The literature will then be examined to highlight the growth in cybercrime and the effects it may have on organisations followed by evidence of a disparity between the readiness of cyber defences between large organisations and SMEs. Previous research related to SME cybersecurity deficiencies and approaches will be examined with a focus on factors that influence SME investment. Gaps in the literature will be examined and put forward as evidence of the need for further research in this area. A conceptual model will be derived from the literature and used as a basis for this research to build upon.

2.2. Cybersecurity v Information Security

According to Longley (2019), cybersecurity is the collection of technologies, processes, and practices that combine to protect computer hardware, software, networks and data from unsolicited attack. The goal of cybersecurity is to limit risk and mitigate the potential risks associated with cyber-attacks. Cybersecurity and information security are often confused and used interchangeably but Tungaa (2020) informs us of the key differences. Cybersecurity is focused on protecting electronic data from being compromised or attacked while Information security is concerned with the confidentiality, integrity and availability of data. Solms and Niekerk (2013) argue that cybersecurity goes beyond information security but that is not the case. They serve different purposes but are both critical. With the terms being used so interchangeably and this study focused on investment decisions, literature relating to both will be reviewed.

2.3. Key concepts, theories and studies

There is a consensus on the need for enhanced cybersecurity measures. Longley (2013) discusses cyber-attacks being regularly reported on the news causing a growing realisation that organisations need to protect themselves from cybercrimes. Kaila and Nyman(2018) highlight that almost a third of online computers encountered an attack in 2017 while Čelik(2019) discusses the threat from an EU perspective with official EU reports showing an increased theft of business secrets and personal data along with a disruption of service and significant financial loss.

When researched further, the picture looks even bleaker for SMEs. Mijnhardt et al (2016) inform us that 18% of all Dutch SMEs are hit with a cyber-attack each year. Browne, Lang, and Golden (2015) discuss the trend of cybercriminals to target SMEs as they conduct more high volume and low-risk attacks against what is considered weaker targets and Čelik(2019) tells us that there is great concern among SMEs as they do not have the capability to respond adequately to such cyber-attacks, unlike bigger organisations. Hiscox (2018) in the UK released a study showing the average cost of a cyber-attack to a small business is £25,700 and that is before reputational damage is considered. The severity of the problem is clear and the impact for small to medium-sized businesses can be fatal.

2.4. Gaps in existing research

The majority of the research in the area acknowledges that SMEs are at a distinct disadvantage to larger organisations who have the budget and qualified personnel to implement cybersecurity strategies. The researchers generally provide a set of tools or techniques to implement risk-based assessments and subsequent strategies to mitigate risks and improve cybersecurity resilience. Kaila and Nyman (2018) provide a three-step plan including identification of assets, protecting your accounts and making a business continuity plan. Parra, Crespo, Caballero and Camacho (2016) create a framework called “Marisma" specifically aimed at the challenge of incorporating information security management systems into SMEs. The research is conclusive in the need for SMEs to improve cybersecurity defences and often discuss cost as a prohibitive factor, but the research excludes the detailed perspective of the decision makers within SMEs. Cost is a factor which will only be exacerbated by the shortage of qualified professionals highlighted by Department of Education and Skills (2019) but multiple other potential factors need to be explored such as the effect of recent regulatory changes and overreliance on abilities of inhouse IT function or IT service provider.

Ng et al (2013) and De Vries (2017) mentioned previously, performed research in the area of cybersecurity investment influences and decision making. De Vries (2017) research is based on organisations who have Chief Information Officers or Chief Information Security Officers which a large percentage of SMEs would not have. Ng et al (2013) researched in 2013 and there have been significant developments since then with increasing threat landscape for SMEs, legislative changes, awareness among decision makers and an increased prioritisation added to cybersecurity initiatives. De Vries (2017) discusses the need for larger organisation to be compliant with rules and regulations as a key driver. Advancing regulation is making this more prevalent so investigation is needed from an SME context. Awareness is not highlighted as a key component in the examined research and is critical if trying to understand the mentality of decision makers in choosing to make cybersecurity assessments and investments. Jordaaan (2014) researched this topic specifically from a South African context concluding a low level of threat awareness leading to greater risk to businesses. Ključnikov, Mura, and Sklenár (2019) also make the connection between awareness and risk, discussing how 58% of SME managers do not consider cyber-attacks a significant risk. This study will examine these factors and do so from a purely Irish SME perspective giving consistency in culture, economic situation and exposure to the same media and news sources that are carrying increasing alarming warnings about cyber threats.

2.5. Conceptual Model

Using the study by Ng et al (2013) as a basis and expanding it to include additional factors examined in the literature above, this research aims to comprehensively examine the factors influencing senior managers/owners in modern Irish SMEs. Čelik(2019) discusses the exponential growth of digital technologies affecting all spheres of business and personal lives. Malter and Rindfleisch (2019) inform that digital innovation is currently dominating customer and business life and advise that the latest digital innovations were largely unanticipated as recently as 1999. Consequently, research in this field will additionally need to be perpetually updated.

This literature review presented the following conceptual model with the below themes that will be utilised throughout the course of this research.

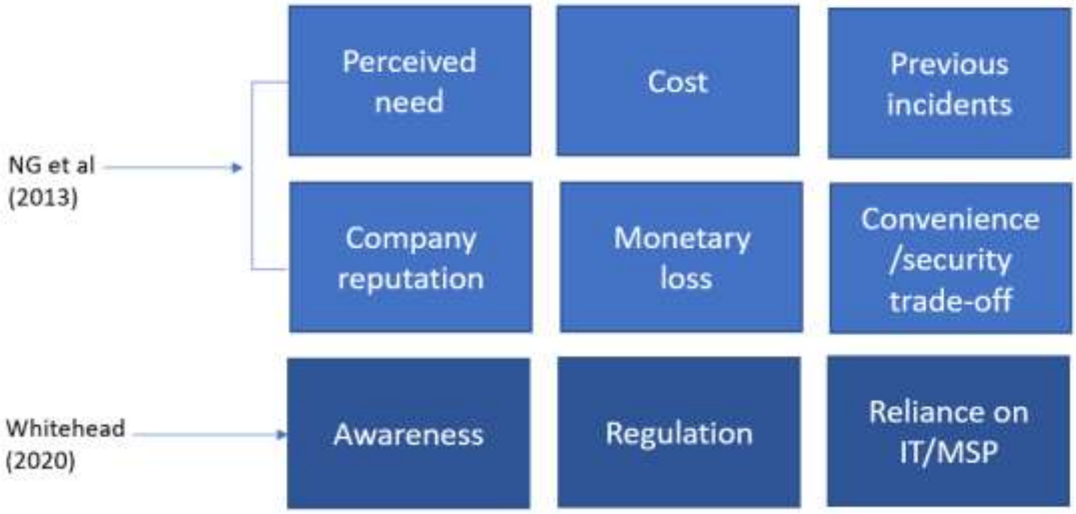


Figure 1. Conceptual model

2..6. Conclusion

The research examined above shows consensus in the growth of the threat from cybercrime and consensus that SMEs are at a disadvantage to larger organisations in being prepared for such attacks. With a shortage of qualified cybersecurity professionals, SMEs could be worse off again as larger organisations are more likely to be able to pay larger salaries for the in-demand workers. Gaps have been identified in previous research and it is the purpose of this study to explore some of these gaps to add a new dimension to existing research. A conceptual model has been presented to provide a framework and ascertain legitimacy with subsisting literature. In the next chapter, the research question and research objectives will be outlined.

3.0. Research Question

3.1. Research question

Given the demonstrated increasing cyber threat, the lack of cybersecurity controls in place in SMEs, the focus of cybercriminals on SMEs and the importance of these SMEs to the Irish economy, this research will aim to answer the following research question:

What factors influence Irish SMEs level of investment in cybersecurity from a senior managers/owner perspective?

3.2. Research objectives

The research objectives are

- Analyse the extent Irish SMEs are aware of the prevalence and impact of cybercrimes.
- Assess the attitudes and perceptions of key decision makers towards cybersecurity.
- Identify barriers for SMEs investing in cybersecurity defence mechanisms.
- Complete a thematic analysis of qualitative research findings from multiple sources to identify patterns and provide findings of the predominant factors influencing cybersecurity investment decisions in Irish SMEs.

3.3. Conclusion

This chapter has detailed the research question to be answered along with specific research objectives. The next chapter outlines the chosen research methodology deemed most appropriate to ensure objectives are reached and the research question is answered.

4.0. Methodology

4.1. Introduction

Kennedy (2019) describes methodology as the research design that links the chosen methods with the research objectives and provides justification for the researcher’s choice. This chapter aims to outline the methodology chosen by the researcher and provide the rationale to validate choices that were made. It outlines the philosophical assumptions the research is based up and approach taken to best answer the research question. The methods employed for sampling, data collection, and analysis will be provided. Ethical considerations and validity of the research will also be assessed.

This research follows the research onion model to ensure validity and credibility at each stage of the research methodology (Saunders, Lewis and Thornhill, 2009). According to Sahay (2019), this approach leads to a structured unified approach where the understandings and decisions made in the outer layers provide context for the approaches and decisions made in inner layers of the onion and associated boundaries.

4.2. Research Philosophy

Saunders et al. (2009) describe research philosophy as the development of knowledge for a specific domain. It contains assumptions and beliefs about how the researcher views the world. These assumptions and beliefs underpin strategy and methods used in conducting research (Saunders et al, 2009). The two main concepts when discussing research philosophy are ontology and epistemology. According to Creswell (2007), ontology is concerned with the nature of reality, while epistemology is concerned with knowledge and understating and how we came to know about that reality. In practical terms, epistemological research involves spending time in the field and building relationships with the participant, a method preferred by this researcher.

Regardless of the research position, Saunders et al (2009) discuss the research question as a key consideration when choosing the appropriate research philosophy. The philosophy most apt to answer the research question for this research is an interpretivist philosophy. Thanh and Thanh (2015) inform us that an Interpretivist philosophy allows the researcher to view the world through the perception of the participant in the belief that reality and knowledge are subjective and influenced directly by people and their environment. Interpretivist philosophy deems it necessary to recognise the difference between humans as social actors as opposed to objects (Saunders et al, 2009). The term 'social actors' is taken from the theatre where actors interpret and play a role in their own specific way similar to how people adapt to different daily social roles and interpret these in accordance to their own set of values and meanings (Saunders et al, 2009). Weber (2004) informs us that interpretivists understand that knowledge is built from experience, history, culture, etc. and the foundation of this research is to understand these factors and how they influence the participant's decision-making process. This research is identifying factors influencing cybersecurity decision making in Irish SMEs. Key to this will be understanding the perspective of participants, empathising and helping provide meaning, making an interpretivist philosophy the best approach.

4.3. Approach & Design

According to Bryman and Bell (2011), deductive reasoning is the most frequent view of the nature between theory and research. A deductive approach uses knowledge already known of a domain which is then subjected to empirical scrutiny (Bryman and Bell, 2011). Dudovskiy (2016) advises that a deductive approach begins with an expected pattern which is later tested against observations. An inductive approach, on the other hand, emerges from the ground up and is shaped by the researcher's experience in collecting and analysing data (Creswell, 2007).

According to Yin (2016), a deductive approach can help remove uncertainty during research as you start with relevant concepts instead of waiting on them to emerge (Yin, 2016). Yin (2016) advises that an inductive approach is most associated with qualitative research. This research is building on previous research in this field and using a conceptual model derived from the literature review, therefore a deductive approach is most appropriate.

Kennedy (2019) discusses qualitative research as the study of a research topic that cannot be subjected to statistical analysis, instead focusing on interpreting meaning, viewpoint or experience from the perspective of the participants. When it is important to understand the reasons for decisions your participants have taken or their attitudes and opinions, qualitative research is used (Saunders, 2009). Furthermore, Creswell (2007) states a qualitative method is used when there is a need a complex detailed understanding of the issue. Given these factors, a qualitative approach is most suitable for this research. This methodology was used by both Ng et al (2013) and Jordaan (2014) and is appropriate to make a connection with the participant to provide adequate depth and detail required to understand the rationale behind their decision making. It will be used to stimulate their individual experience and perceptions to unearth reasons for how they arrived at these decisions.

4.4. Research Method

According to Kennedy (2017), research methods are the tools, techniques and procedures used to gather and analyse data. Myers (1997) describes them as a strategy of inquiry that provides direction to the research to progress from philosophical assumptions to research design and data collection. They encompass both qualitative and quantitative research and take the form of interviews, surveys, questionnaires etc.

For the purpose of this research, semi-structured interviews will be the adopted research method. Clifford, French and Valentine (2010) discuss semi-structured interviews as a form of interview where the questions are open-ended. The conversation is allowed to unfold in a conversational manner allowing participants to delve deeper on issues they feel important. Saunders et al (2009) refer to semi-structured interviews as qualitative interviews where the research will have a set of themes and questions to cover but also probe to allow participants to build on their responses. This research will contain a number of open-ended questions relating to the themes set out in the conceptual model provided below. Not all decision-makers in SMEs are fully informed or up to date with cybersecurity trends or language used, clarifying questions may be required. Yin (2016) highlights conversational mode with two-way interaction as an advantage of semi-structured interviews, aiding relationship building and facilitating clarification questions. A Deloitte report (2017) discusses the rapidly evolving cybersecurity threats that companies are struggling to keep pace with. Getting participants to be open, honest and discuss the topic will require a delicate approach. Semi-structured interviews allow the development of a social relationship between researcher and participant that will help overcome that obstacle Yin (2016) and Saunders (2009).

Multiple research methods were examined in the literature review; however, the conceptual model is building on the research completed by Ng et al (2013) which was exploratory in nature and set out themes discovered during semi-structured interviews further justifying the choice of research method.

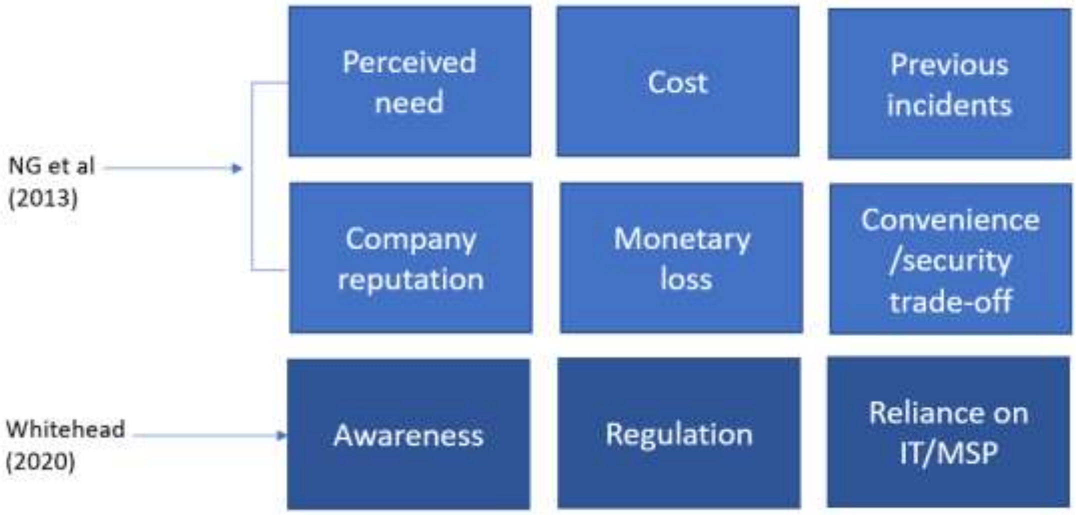


Figure 2. Conceptual model

4.5. Sample Selection

Dudovskiy (2016) defines sampling as a principle to select members of the population to be a part of the research, acknowledging due to the potential target size, the need to select elements of the population and draw conclusions to represent the population. According to Yin (2016), in qualitative research, participants are likely to be chosen in a deliberate manner known as purposive sampling. Purposive sampling is a form of non-probability sampling that involves the selection of instances who are the most relevant and information-rich to the area of study (Yin, 2016) and (Saunders, 2009). This research seeks to gain perspective on factors influencing decision-makers in Irish SMEs. The target is specific and therefore purposive sampling will be adopted. This approach was also adopted by both Ng et al (2013) and De Vries (2017) to ensure participants in their research had the required level of knowledge to contribute effectively to the research. The participants for this study must adhere to the following criteria:

- Work for a company based in Ireland.
- Work for a company that employees between 1 and 250 employees.
- Owner or senior manager with responsibility for strategic decision making.
- Owner or senior manager with responsibility for IT function.

Yin (2016) discusses needing to select the sample to obtain the broadest range of knowledge, information and perceptions on the subject of the research. Dudovskiy (2016), informs of the reliance on the judgement of the researcher and the potential for bias. Both these factors were weighed up and formed part of the rationale when selecting participants.

Based on the criteria, after filtering, the researcher contacted ten possible participants in a broad range of industries. The participants are contacts or associates of the researcher's business network. The population was reduced to the five participants that could best contribute to the successful completion of the research objectives. The selected candidates are shown in figure 2.

Unique ID	**Job Title**	**Company size**	**Industry**
Participant one	Financial Director	20 employees	Manufacturing
Participant two	Managing Director	80 employees	Retail
Participant three	Operations Manager	120 employees	Professional Services
Participant four	Financial Controller	30 employees	Retail
Participant five	Operations Manager	16 employees	Financial Services

Table 1. Table of participants for this research

4.6. Time Horizon

An important layer of the research onion when considering research design is related time horizon. Saunders et al (2009) explain research can be a snapshot in time referred to as cross-sectional or a diary-like series of snapshots referred to as longitudinal.

For this research, a cross-sectional approach was taken, allowing a study of a phenomenon at a point in time (Saundes, 2009). The snapshot was captured through semi-structured interviews over a two-week period. Building on research by Ng et al (2013), cross-sectional allowed to contrast changes in internal and external factors affecting decision-makers that occurred since their research in 2013. Cyber security has a rapid pace of change, cross-sectional facilitates future research to compare the snapshot created at the time of this research.

4.7. Data Collection & Analysis

Once the sample was narrowed to five participants, an initial email was sent with the research topic, consent form, a summary of the objectives and a request for a 1-hour online meeting if they were amenable to participation. Upon acceptance, the interviews were scheduled, and a copy of the conceptual model was attached to the meeting invite to give participants a preliminary indication of the themes to be discussed. Greener (2008) and Yin (2016) discuss the importance of facial expressions and body language when analysing qualitative interviews. With the reduced possibility for face to face interviews due to Covid-19, online video platform Zoom was chosen. All participants had the requisite IT equipment. Yin (2016) and Creswell (2007) describe qualitative interviews as taxing for inexperienced researchers and recommend practice and preparation. An open-ended question set was developed based on each stage of the conceptual model, and a pilot exercise was executed to help the researcher prepare and field test the technology to be used during the interviews. When conducting interviews, a relaxed environment with a friendly non-threatening atmosphere is essential (Dudovskiy, 2016). Online meetings facilitated a natural environment and allowed participants to remain in the physical context of their office environment, aiding scheduling. In the beginning, each participant was advised of anonymity. Yin (2016) advises permission to record is essential and better received in written format. Permission was sought and granted via the consent form in advance and reiterated at the start of each interview. This aided the conversational nature of the interview as detailed note-taking was not required. Each interview lasted between 50 and 65 minutes.

According to (Dudovskiy, 2016), data analysis involves identifying patterns in collected data, organising the data, and transforming it into a useful form to help achieve research objectives.

After collection, the data was analysed using thematic analysis. Thematic analysis according to Willig (2013) is a way of identifying patterns in your data and reorganising your data into themes. A theme is described as a recognisable reoccurrence of meaningful patterns in your data that are systematic as opposed to random and arbitrary (Willig, 2013). Vaismoradi (2013) informs us that thematic analysis can be used for identifying common threads in a series of interviews and is suitable for answering questions such as “what are the concerns” or “what are the reasons” This study aims to understand the reasons behind investment decisions in SMEs concerning cybersecurity making this approach suitable. This research is building on research by Ng et al (2013) who discuss a similar approach transcribing the data and developing themes, further validating this choice of approach.

Willig (2013) discusses a concern for thematic analysis if not performed correctly that the researcher needed to be cognisant of. Without a theoretical basis, the researcher can end up with a shopping list of themes that do not provide an accurate representation of the data collected and therefore provide little value. This research aimed to mitigate this by utilising the conceptual model to extract themes from literature to provide a theoretical base for the interview questions. Braun and Clarke (2006) discuss the potency and flexibility of thematic analysis in qualitative research but highlight no clear agreement in the literature on how to properly conduct it. They provide a six-phase framework that this researcher used during data analysis.

1. Familiarise with the data
2. Generate initial codes
3. Search for themes
4. Review themes
5. Define and name themes
6. Produce the report

Within the framework, Braun and Clarke (2006) provide guidance on key decisions when doing qualitative research. They provide detail on what constitutes a theme and explore the difference between inductive and theoretical (deductive) thematic analysis. Inductive is data-driven and coded analysed without trying to fit into a pre-established coding frame. Theoretical analysis is more explicitly analyst driven, guided by the analysts theoretical or analytic interest in the area of research (Braun and Clarke (2006). This literature review has presented a conceptual model that established a number of themes. The generated themes formed the basis for the questions for the interviews, thus theoretical thematic analysis is most appropriate.

For this research, the Braun and Clarke (2006) framework was utilised in the following way. Recorded interviews were listened to multiple times to become familiar with the data and interviews were transcribed. Theory-driven coding was then used to extract key points within the data relevant to existing themes in the conceptual model. Additional codes found within the data were also detailed and documented. Coding was completed by working systematically through all the data given equal time and attention to each element of data (Braun and Clarke, 2006). Pre-existing themes and newly created themes were sought within the coding and formed an initial list. The list was reviewed and defined. A confirmed list of validated themes emerged which will be discussed in detail in the analysis and findings chapter.

4.8. Reliability and Validity

According to Saunders (2009), reliability is concerned with the extent to which chosen data collection tools and techniques will produce consistent results. Bryman and Bell (2011) discuss the need for the research to be repeatable. The reliability of qualitative data as opposed to quantitative is affected by the judgement of the researcher (Denzin and Lincoln, 2018). Leung (2015) agrees that reliability is challenging but stresses the essence of reliability being consistency. The most important test of any qualitative research is its quality (Golafshani. 2003). According to Yin (2016), validity in qualitative research is linked to accuracy. Data is accurately Interpreted and results accurately reflect the real world that was studied. Leung (2015) describes it as the appropriateness of the tools, process and data. Reiter (2013) advises transparency and honesty when conducting exploratory studies, adding validity. Morse, Barrett, Spiers and Olson (2002) critique the rejection of reliability and credibility in qualitative research and promote a change of agenda by implementing rigorous verification steps. These verification steps along with techniques from the above reviewed literature were integrated into research.

To ensure reliability and validity, the following measures implemented.

- A similar research method was utilised as per peer-reviewed literature. Methods were thoroughly evaluated and critiqued to ensure congruence with the research question.
- The sample was selected with a population capable and knowledgeable to the area of study.
- A flexible and iterative approach was chosen between design and implementation for consistent verification at each stage.

- A consistent and standardised approach was used for each element of data collection and analysis.
- Interviews were recorded to allow consistent and accurate revision.
- Questions were framed appropriately to ensure no bias.
- Regular internal reflection throughout the research was executed to determine and remove any inherent personal bias.
- Interviews and follow-ups were conducted honestly and transparently.

4.9. Ethical considerations

To ensure approval to conduct this research, the National College of Ireland (NCI) ethics form was completed as part of the proposal in January 2020 and submitted to the NCI ethics committee.

Participation was on a voluntary basis. Participants were given information on the research topic and provided with full details of the aims and objectives of the research. Following this, participants were asked to sign an informed consent form. The consent form provided assurances of anonymity and the right to withdraw at any time. The contents of the form were reiterated verbally by the researcher. Each participant was assigned a unique identification number. No reference to names or organisation names will appear in the research.

Primary data collected during the research in the form of video and audio files were stored on an encrypted hard drive only accessible to the researcher. This drive will be formatted on receipt of the grade for this study

4.10 Conclusion

This chapter has provided detail on the research methodology that was used to ensure the research question is effectively answered. The philosophy of the researcher was outlined along with the research method, approach and chosen sample. Details on data collection and analysis were provided along with steps taken to ensure reliability and validity. Finally, details of ethical consideration taken throughout were provided. The next chapter will present the analysis and findings from the qualitative interviews.

5.0. Analysis and Findings

5.1. Introduction

This research aims to identify factors that influence cybersecurity decision making in Irish SME's from a senior managers/owner perspective using the thematic analysis framework produced by Braun and Clarke (2006).

The literature review produced a conceptual model with 9 themes. Each will be analysed relating to the experience of the five participants involved in the semi-structured interview process. They will be ordered in accordance to the themes found most interesting to the researcher. Participants will be numbered by their unique identifier provided in table 1.

Some factors in the conceptual model are closely related. It is therefore acknowledged that some of the content provided below from participants could be attributed to more than one theme.

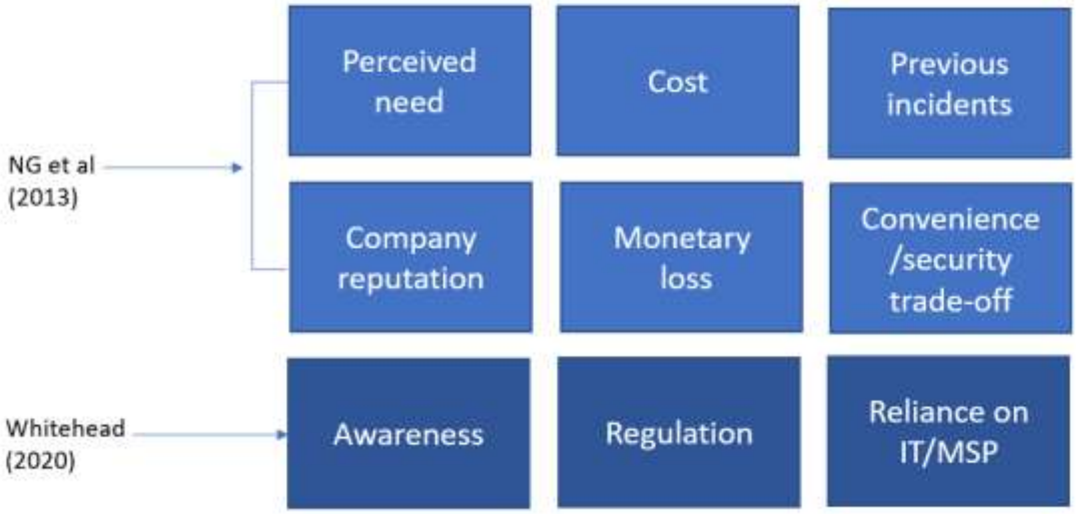


Figure 3. Conceptual model

5.2. Thematic Analysis

5.2.1. Company Reputation

This theme looks at how big an influence company reputation has when making cybersecurity decisions. All participants highlighted reputation as a key concern and discussed the impact a cybersecurity incident could have on their business.

Participant three painted a bleak picture for the future of their company in the event of customers losing faith in utilizing their systems

> *"It's huge. Essentially, everything we do. If our infrastructure is compromised in any way, or customers don't feel it's safe to use our online banking or all that kind of stuff, that's end game for us"* (Participant three).

This point was echoed by Participant five but intriguingly they fixate on the one-shot nature of reputation – the idea that it can years to build but a single incident to destroy. Trust and confidence are crucial to customer and supplier relationships. With one cybersecurity incident, they can be eradicated.

> "*It's reputationally critical. You never get a second. If we got compromised now, the damage that will do to our business and our reputation would be horrendous"* (Participant five).

Participant two explicitly refers to confidence. indicating customers may look to shop elsewhere if they lose confidence in their systems. Retail businesses like this rely heavily on online transactions.

> "*I think it would be very damaging to our reputation, and it would totally undermine confidence"* (Participant two).

The below participant discusses a recent security incident involving a suspicious email sent from his account and discusses the effect a small isolated incident can have on his individual and company reputation. Again, an example of how a minor incident in a split second can tarnish the reputation and cast doubts on future customer/supplier relationships.

> "*The simple little knock-on effects would be, that individual is afraid of their life of any kind of an email from me now. And second guesses, if they see my name, if they see the company's name, there's an instant paranoia, that's an indirect damage"* (Participant four).

An interesting subtheme which came to the fore during analysis was the loss of availability of systems. A participant described it as disruptive and discussed plans they have in place to get back up and running quickly. However, they again had more concern for the impact it had on external parties' trust in using their systems in the future.

> “*We support financial institutions on a day to day basis. So, during office hours, that's would be very hard for us to take. That would obviously impact our ability to support them and undermine their confidence in our ongoing support”* (Participant five).

5.2.2. Regulation

Increases in cybersecurity and data protection legislation have caused businesses to take a more proactive approach to defend against cyber-attacks.

Discussing the impact of the recent GDPR legislation, a participant discussed the short-term impact on their business but critically implied there was no long-term effect or improvement on cybersecurity policies within the business.

> *“We had to communicate with each customer to let them know, obviously that we had their data, and gave them the option for us to disregard it and destroy any information that we had. Some requested it, majority didn't, and other than that there have been no advancements in our cybersecurity policies whatsoever”* (Participant two).

A second participant gave more credence to the necessity of compliance for all businesses no matter the size or industry.

> *"It plays a big factor for everybody now, irrespective of what business you're in, whether you're manufacturing services, whether you're a big company, a small company, GDPR is all about protecting people's privacy and that's something for everybody"* (Participant four).

However, when probed further on the day to day impact within the company, the same participant could not provide explicit detail on what GDPR controls currently exist in their business and highlighted the critical dependency organisations can have on outsourced IT partners.

> *“I don't think it's anything I'd be interested, trust me, in managing or monitoring. And again, that's the beauty of having an outsourced IT company. They talked a lot about it, but it has not been on the agenda in our recent meetings”* (Participant four).

Emerging from the analysis was a stark contrast between regulated and non-regulated entities. Regulated entities in the financial sector are upheld to stringent central bank rules. Although participant five works in the financial services industry, his organisation is not classified as a regulated entity and therefore not subject to the same stringent regulations.

> "*If you're a regulated entity, you're effectively held to a whole set of procedures around risk management and risk appetite. Now we're not a regulated entity, which means we don't have the central bank knocking on our door and coming in and inspecting us*" (Participant five).

In contrast, participant three must adhere to strict prudential supervision by the Central Bank of Ireland using the Probability Risk and Impact System (PRISM) that adds huge regulatory overhead to day to day operations (Central Bank, 2020).

> "*Every time we get an examination, a prism examination, they report on various different factors, like co-ordinance and all these things, but IT is one of if you don't comply, they have the power just to make your life hell in other areas"* (Participant three).

The point was reinforced when they stressed the bureaucracy involved in ensuring they adhered to governance standards set down by the regulators. The other participants did not have any such oversight or complexities in their businesses.

> "*Businesses like ours, you end up getting governed or run by reports that we comply with the standards that are set down for us by the Central Bank*" (Participant three).

5.2.3. Cost

This theme analyses the relative impact cost of IT security investment has when deciding to increase cybersecurity defences. Van Ommen (2014) discusses cost-benefit analysis as being key when making IT Security investment decisions. This or some variant was corroborated by each participant.

Participant one was cognisant of the high potential for risk but also aware mitigating every possible risk would take substantial investment. In this organisation, the likelihood of suffering, the cost to alleviate/mitigate and the potential impact of each risk on the business are calculated before investment is made.

> "*I think the important thing is to have a balance in what you're looking at and whether the risk is a real risk to the business or not. Because if you went down the route of I need to cover everything, then it becomes cost-prohibitive. Each individual risk must be analysed on its merits and how likely it will strike us*" (Participant one).

Participants four and five below looked at investment from specifically an SME perspective. Participant four highlighted the cost-conscious nature of SMEs but stressed the concern if they opt against investing.

> "*It's very, very hard to put a price on the likely loss of not investing in it. But again, obviously, SMEs are typically very, very conscious about every spent penny that they spend, and it has to be spent wisely*" (Participant four").

Participant five furthered this by discussing the increased burden and perpetual nature of the required investment. The constantly evolving threat landscape is adding pressure to already limited SME budgets.

> "*We're a small business, we're an SME with financial activities. The operating costs around this whole technology area now are a big burden on us. Not only that, they never end*" (Participant five).

A final point related to above picked up by multiple participants is the IT service provider's incessant upsell of new software designed to mitigate new risks. A participant openly questioned the requirement but did not have the expertise the judge the validity of the proposed solutions.

> "*There'll be their findings and recommendations in the report. But then our provider's solution to everything will be, if you buy this piece of software, you will be protected but this cycle never ends. Every meeting is a new piece of software. We fear saying no and exacerbating what could be a serious risk*" (Participant three).

5.2.4. Awareness

This theme sets out to gauge the level of understanding of the risks associated with cybersecurity to businesses, the knowledge among participants of the potential impacts to Irish SMEs and obtain indications of the effect awareness has when faced with cybersecurity investment decisions.

When discussing awareness, all participant referenced the barrage of information relating to cybersecurity incidents in the media pertaining to the misfortune of individuals or companies. The constant media coverage is increasing the level of fear in a topic people are already apprehensive about.

> "*I'm increasingly aware. And again, it's based on my own personal experience, listening every day, hearing horror stories and not even within the context of my interaction or engagement with our IT provider"* (Participant four)

Of the five participants, four could give specific examples of companies that had attacks in recent years with participant five relating to a specific example Irish example that took place in 2016. The readiness of examples further demonstrates the constant media coverage.

> "*it's constantly on the agenda and you constantly hear about it in the media. A big one I read about was the Meath County Councils for 3 million or something or more. When you read something like that, it definitely sets off the alarm bells*" (Participant five).

Only three of the companies had security awareness training programs to distil awareness and best practices down to employees. Two of these companies operated in the financial services potentially highlighting more evolved practices within this industry.

> "*Now obviously we do the training. We just finished the training now, a series of training we do once a year just to create awareness among the team*" (Participant five).

Interestingly, when looking through the lens of the regulated entity, awareness took a whole new meaning. There was a clear expectancy on the individual in charge to be fully aware of potential threats to the business but also be able to decipher potential incidents and escalate when required.

> "*For someone in my position, 24 hours a day, 365 days a year, it doesn't matter what time, the instant that I become aware of an incident, I must act immediately. We have a special emergency number for our insurers, for our cyber insurance. That's my first call. It doesn't matter the time. The first call is*

> *the insurers and that's drilled into us. We would have annual training, just general awareness for staff*" (Participant three).

5.2.5. Perceived need

Perceived need for this research analyses how high business owners/managers in Irish SMEs feel mitigating cybersecurity risk is necessary for their business. The views of participants were mixed with the level of security required dependent on the type of business and type of information they hold.

Participant two views it as significant for all businesses but being a retail business focused on the online financial transactions that are critical for their business.

> "*It's obviously paramount to any business, certainly with us having an online platform, we have a lot of financial transactions that take place online day to day*" (Participant two).

Participant three emphasised the importance and again pointed to the sensitivity of financial records discussing the damaging implications of a data leak from inside their network. There was no doubt that it was a requirement in their business.

> "*Look, I suppose the way we look at it is it's protecting our infrastructure from attacks from the outside in and preventing, I suppose, something happening on our network that causes a loss of data or stuff to leak out. Obviously, for us, that's hugely important in terms of the financial records we have*" (Participant three).

In comparison, the necessity and importance were downplayed by participant one due to the nature of their business. There was an understanding of the type of data they presently hold, and the fact a cybersecurity incident would not damage other organisations somewhat eased the burden.

> *"Well, I would say that every business has a requirement, probably. But to what degree, it depends on the business itself. So, I suppose, our business is not such that it's crucial that we're not holding other people's information, and we're not holding credit card details or any of that sort of stuff that might be a major risk to other people if it was leaked out of the place. It is important to us because of the impact that it could have on our own business ourselves and the damage it could do to us, but we don't have that additional worry and risk*

> *of damaging somebody else in the process. So, important, but it's not absolutely top of our list" (Participant one).*

Although its importance was not paramount for participant one above, there appeared to be a logical risk assessment completed weighing up likelihood and impact. For participant four, the perception was that their business would not be a target due to its size until faced with the stark reality. Unfortunately, with the increased attacks, more and more businesses will be faced with this reality.

> "*I did not think a small retail business would need much protection. But there was an email of mine was intercepted, and it ended up some scammer was communicating back and forth with it with a client of ours under the guise of me. So, I mean, it's really only since I got that in-depth and knowledge, and I can see the hard, cold face of it, that I have an appreciation for the need and importance of It*" (Participant four).

5.2.6. Reliance on IT/MSP

This research has established that SMEs tend to outsource some/all of the IT security function as they have inadequate security resources in place to defend against cybercriminals. For those that don't outsource, they rely on internal IT teams. The trust put in these relationships to protect the business is substantial. This theme aims to establish the type of relationship, how frequently updated owners/senior managers are advised of new security threats and the level of reliance that exists on this relationship in ensuring the protection of the business.

All participants in this research outsourced their IT function to a managed service provider. Participant one discussed the type of relationship required from their IT company and the trust once the technical aspects are explained effectively.

> "*Yeah. I think the ideal thing is to be able to deal with the likes of an IT person from an IT company who might know what they're talking about, break down all the levels of things that there's a potential to cover within your business. And identify within those, then, which ones are the real risks from your perspective and which ones are sort of fake. We trust in what they tell us as long as it is broken down to plain English*" (Participant one).

Participant four is equally impressed with their outsourced managed services provider indicating a strong bond had been formed between the decision maker and MSP.

> "*It's only true with the involvement of x that I've even achieved the level of understanding and knowledge that I have. When you outsource it, you're dealing now with a service provider who's going out of their way to constantly impress and make you acutely aware of why they're needed and the various things they are needed for. So I would rely very, very heavily on x"* (Participant four).

They did, however, take a dim view if a new threat emerged which they were neither aware nor protected against. The role of the MSP in keeping updated with the latest threats is vital.

> *"Not only would I rely on them, the absence of me not knowing something, I would blame them"* (Participant four).

By contrast, participant two had a completely different relationship. In doing so, they demonstrated the two-way nature required for the relationship to work.

> *"So, typically, I suppose there's an element of proactiveness because they're there when we need them, but it's more reactive"* (Participant two).

> *"Yeah. Unfortunately, they actually wouldn't keep you informed, because they'd be so fed up with having done extensive work for the business through quotes, through what their understanding of business needs are, where they find that they don't develop into actual business for them" (Participant two).*

Participant three had an ultra-cautious approach. They outsource to an MSP but also utilise independent consultants who know the industry well. Critically they are not selling so trusted to put the needs of the client above their own.

> *"We utilize two guys who used to be involved in serving our industry. Now basically operate kind of independently, so to speak. But they sell nothing. They're not selling anything. They create a framework and a matrix of what our needs were based on input from us saying and basically taking the technical stuff and translating that into non-technical language for our non-technical*

> *managers. We can then bring this to our MSP or another provider depending on the type of service required"* (Participant three).

5.2.7. Monetary Loss

Abbosh and Bissell (2019) advise that cybercrime will cost businesses $5.2 Trillion globally by 2024. This theme aims to determine if monetary loss for SMEs is a key concern when weighting up factors designed to protect their businesses. Monetary loss for this research was scrutinised for both direct losses (direct loss to the company from the crime) and indirect losses (knock-on effects such as loss of availability of systems, lost opportunity costs or defence costs).

When advised the average cost of a cyber-attack in the UK was £25,700 according to Hiscox (2018), participants had mixed opinions. Participant one viewed it purely from a once-off direct financial hit perspective.

> *"£25,000 is a big amount of money. We certainly wouldn't want to be losing it off the bottom line, no, absolutely not, for no good reason. Some of the money that's not spent of our own accord and is just taken from us. Absolutely, yeah, that would be terrible for us*" (Participant one).

The below participant concurred with regards to the monetary loss but focused more on their own experience and provided a chilling example of the long-term financial impacts a cyber-attack can have. These types of attacks are common and long-term costs to businesses can be crippling.

> "*Nobody wants to lose that kind of money, but the long term can hurt more. We lost 30,000 plus customer loyalty records on a loss of information from an attack, and we break it down into most of those customers make four visits, three to four visits a year, our average transaction 95 euros. So, you're talking between 285 - 380 euros by 30,000 customers*" (Participant two).

Interestingly, participant five also chose to focus on the longer-term ramifications with the initial monetary loss a secondary concern. Reputational damage was a key concern yet again.

> "*It's a financial record of cost because the cost would be wider than that. There would be downtime, disruption of staff. The knock-on effect of the reputation*

> *wouldn't be pretty - more significant damage, more significant than the money itself*" (Participant 5).

Participant three viewed it differently by contrasting the £25,700 with the average costs incurred trying to protect the business from cyber-attacks - perhaps emphasising the different expenditure required in their industry.

> "*Yeah, 25,700 would be a loss. We'd feel it, but it wouldn't be massive. I don't know what the spend in average SMEs would be on cybersecurity. But it'll probably be multiples of that for the likes of us*" (Participant three).

5.2.8. Previous Incidents

For the purpose of this research, previous incidents are viewed as cyber-attacks attacks against the participant company in the last 5 years that the participant had knowledge of. The distinction is important as cyber-attack often go undetected. Undetected attacks are unlikely to influence senior managers/owners to invest further in protecting their business.

All five participants admitted they were the victims of at least one cybersecurity incident that affected them personally or their organisation, further emphasising the prevalence of cybercrime in Irish SMEs. Participant four was acceptant that incidents will occur and discussed the improbability of mitigating all attacks.

> "*But I have, again with my involvement, and I had a very, very direct experience there recently, where my own email was hacked, and I would consider us to be very protected I suppose, up to a point. you cannot keep all the bad guys out but you do need to make sure you are as secure as possible*" (Participant four).

Participant one also suffered a targeted attack on their mail, highlighting this vector of attack as popular among cybercriminals. Interestingly, they downplayed their concern due to the type of data held in the business.

> "*We've had probably three or four of those, I would say, in the past five years. It's the biggest one that we see. Again, this goes back to the nature of our business to some extent, because we don't hold bank details on the system, we don't hold credit card information, we do not get as concerned as some others would*" (Participant one).

Participants three and five below both had previous incidents that have spurred them onto increasing their cybersecurity protection. Participant three discusses another common form of attack with ransomware that encrypts all company files. Participant four again reinforces the commonality of mail related attacks.

> "*It was about four and a half years ago we did get one of these CryptoLocker things. And so essentially it manifests itself that as soon as we tried to access files in our file server, we're getting this message popping up looking for money. That's the reason why we now have multiple backup solutions and replication*" (Participant three).

> "*Two minutes later, I got a message saying my mail's been hacked so if you get a message, ignore it. At the same time, a message went to the CFO and the CEO, "have an invoice paid urgently for something," which was purporting to come from me, but I knew nothing about it. I'm lucky enough they caught it, and I think that kind of spurred us on then to just look at the whole thing again. We installed multi-factor authentication and other tools to protect Office365*" (Participant five).

5.2.9. Convenience/Security trade off

This theme sets off to analyse if participants perceive increased IT security measures will hamper productivity or efficiency in their organisations. If the answer is in the affirmative, what measure of impact does that have on further investment?

Participants had mixed opinions on the impact but were aligned to the fact that higher degrees of security and associated steps to complete daily processes were a permanent fixture in modern business

Participant four discussed the commonplace nature of additional security steps, referencing his personal email as an example that both businesses and personal lives are affected. Commonality appears to lead to acceptance.

> "*It's part and parcel of daily life now. Even with my Gmail account, I get a code on my phone to access. Yes. it slows things down slightly but it is a necessary evil.*" (Participant four)

Participant five was equally decisive on the necessity of cybersecurity in their business. Interestingly, they alluded to the fear that exists among management teams when faced with cybersecurity choices.

> "*We have viewed it as a must have in terms of the advancing threat. It hasn't impacted. It's not a burden. If it came to a trade-off between doing something else and doing something around cybersecurity, it will be a brave management team now that would go against cybersecurity"* (Participant five).

Participant three accepted that in their industry, delays are inevitable with extra governance controls causing a process that was instantaneous to now take overnight.

> "*We just accept it that's it. We just accept it as a delay. So from that point of view, it does impact productivity but the staff just have to work around it. My staff will have to submit reports to the bank on a Friday evening, let it go through the red tape so that they could get them back on the Saturday morning and they can actually get worked on. It used to be instant."* (Participant three)

A slightly different view from within their organisation was given from participant two. They indicated an entrenched culture with resistance to change seemingly at odds with the other participant's organisations.

> "*The problem with organizations of our size it's typically learning through experience and experience of your organization, rather than learning through what's happened to others of similar size. If you spend the time to review issues that have occurred before that, you realize how beneficial something like two-step verification could be. Some people in our organisation would say, "this takes just too long and it's a waste of resources, or it's too cumbersome*" (Participant two).

5.3. Conclusion

This chapter aimed to present the finding from the five participants relevant to each of the nine stages of the conceptual model. The next chapter will test the validity of the conceptual model by discussing the views of participants in relation to the extant literature.

6.0 Discussion

6.1. Introduction

This research aims to investigate the factors influencing cybersecurity decision making in Irish SME's from a senior managers/owner perspective. The research findings were derived with the use of semi-structured interviews. This section will analyse the empirical data from the analysis chapter in relation to the extant literature. As a result of this research, a revised and updated conceptual model will be presented.

6.2. Factors influencing cybersecurity investment decisions

6.2.1. Prevalence of cybersecurity in modern business

Malter and Rindfleisch (2019) discuss the rapid pace of change and adoption of digital technologies in every aspect of business and personal lives. Unfortunately, as shown by Abbosh and Bissell (2019), cybercriminals are equally as innovative - cybercrime is quickly becoming the fastest growing form of criminal activity expected to cost businesses $5.2 trillion by 2024.

The fact that cybersecurity incidents have become so prevalent was reflective in the analysis compared to previous literature. 100% of participants had first-hand knowledge of their organisation being subject to at least one cybersecurity incident compared to 40% of participants studied by Ng et al (2013). Similarly, Van Ommen (2014) reported very few cybersecurity incidents volunteered by participants indicating attacks were not as prevalent in 2014, the chosen sample had adequate protection measures in place or a lack of awareness existed among participants.

There was consensus among participants on the importance of cybersecurity for every business, however, the level of protection required is dependent on other factors – namely nature of the business and type of information held. Conversely, Ng et al (2013) found misconceptions about the need for cybersecurity with participants believing small firms are unlikely to be attacked. Ng et al (2013) also found perceptions among participants to be of particular concern, whether not investing due to the infeasibility of stopping all attacks or ignoring such attacks due to their frequency. The increasing prevalence of attacks since 2013 could potentially exacerbate this, however, there was an understanding among participants that doing nothing is not an option. Two participants did discuss the impossibility of stopping all attacks but discussed taking a logical approach to analyse each risk and potential impact.

A final reason provided by Ng et al (2013) for organisations not investing in cybersecurity was the perception for small business that it would "add too many layers" and impact the efficiency of business processes. De Vries (2017) describes this as a trade-off where additional security costs time and resources - outlining a tension that exists between security and usability. Like the literature, it was found that additional security measures can impact productivity and efficiency but a recognition that the associated delays were inevitable and a necessary component of modern business.

Research by Jordaan (2014) focused on awareness with a key finding being lack of awareness initiatives in place within organisations. The importance of awareness was backed up by Ključnikov (2019), stating "*organisation awareness is the most obvious and important factor in information security management*" All participants discussed the barrage of information relating to cybersecurity incidents in the media and four of the five could provide specific examples of company's victim of attacks in recent years. Combined with previous incidents, this appears to have led to a heightened state of awareness not found in previous literature. The awareness has led to an acceptance that additional security measures are necessary across all businesses and nullified arguments focusing on the impact on efficiency.

A concern for this researcher is that the awareness in question above is happening by chance and not explicitly being supplemented through awareness programs within the organisation. Both Jordaan (2014) and Ključnikov (2019) discuss the importance of organisation awareness and awareness programs but only two of the five participants had such programs in place.

6.2.2. Knock-on effects from a cyber attack

. According to De Vries (2017), people's perception of risk guides their behaviour in the decision making process related to cybersecurity. The problem for SMEs is quantifying the risk and potential impact which extends much further than an isolated cyber-attack. Like the literature, the finding from the analysis show participants are far more concerned with the longer-term impact an incident can have than any short-term disruption. Participants acknowledged the loss of system availability, disruption of staff and short-term financial loss as potential outcomes of a security incident but similarly to Ng et al (2013) the focus was on how the organisation is perceived from an external perspective and the effect this may have on business in the future.

De Vries (2017) highlights financial losses as a key factor influencing senior management in large public organisations, however, monetary loss was not the key factor in research aimed specifically at SMEs (NG et a, 2013). This was corroborated by participants who advised losing money directly from the bottom line as not ideal but secondary to any impact that negatively affects customers or suppliers.

Ng et al (2013) discuss protecting the confidentiality of client data and consistent delivery of a quality product as the key to establishing and building trust, creating a clear correlation between information security and trust. Furthermore, any erosion of that trust due to a security incident can damage the organisations' reputation. Trust, confidence, safety and paranoia were mentioned by different participants, but the central theme was the same. The reputation of the organisation is critical to the long-term success of their business. Reputation takes years to build and can be tarnished by a single incident. Participants were cognisant of the effects a security incident can have on reputation with one describing how it would "totally *undermine confidence* ", while another describing the damage to the business and reputation as “*horrendous* “. One participant alluded to the potential finality stating of customers did not feel safe using their systems, it would be “end game for us”.

What is clear from the analysis and in agreement with Ng et al (2013), reputation is a key factor influencing cybersecurity investment decisions. SMEs are more likely to invest when reputation is involved, With the understanding that an incident can lose something that has taken so long to develop, questions can be asked of owners/senior managers who do not put strategies in place to at the very least minimise the risk.

6.2.3. Nature of the organisation

According to De Vries (2017), a key driver for large public organisations investing in cybersecurity is compliance with rules and regulations. De Vries (2017) points out that financial damage is largest in public organisations but poses the question if that is really the case or is it because they are under obligation to report incidents. This research aimed to look at the influence regulations has on Irish SMEs

The analysis showed a disparity among participant organisations. The first disparity relates to the general data protection regulation (GDPR) introduced in 2018. Van Ommen (2014) discusses a lack of reported incidents in his research while De Vries (2017) highlights the necessity of large public organisations to report incidents. GDPR brought strict new rules around the protection of data and enforces reporting of data breaches to the data commissioner should they occur (European Union, 2020). Four of the five participants admitted adherence to GDPR and protection of people's data as an important factor for their business. The fifth participant's organisation did not hold any personal data, thus GDPR was not applicable. The increased regulation is having an impact but the long-term effect on businesses practices is questionable. Participants discussed a surge of activity to comply when GDPR was first announced but there is a lack of evidence to support sustained efforts.

The second disparity not discussed in reviewed literature related to regulated versus unregulated entities. Two of the participants in this research are in financial services but only one is classed as a regulated entity. The other three participants were not regulated. Over 10,000 firms providing financial services in Ireland are regulated by the central bank of Ireland through risk-based supervision with the legal power of enforcement (Central Bank, 2020). The Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks shows the sophisticated processes with regards to cybersecurity risk and governance required for firms who operated under this umbrella (Central Bank, 2016). Looking further at regulation, only key sectors are regulated. The European Union NIS directive transposed into law in Ireland in 2016 aims to enhance cybersecurity across the EU crucially only targets key sectors - health, transport, water, digital infrastructure, energy, and finance (ENISA, 2016).

The participant from the regulated entity discussed how regulators can make their life hell and businesses like theirs being governed by reports. This is a stark contrast to the other participants where no formal supervision exists. The UK have a cyber essentials certification where businesses of any size can show their commitment to cybersecurity (itgovernance, 2020). Cyber essentials is required for all companies doing business with any government contracts. This forces compliance with cyber essentials requirements and the fee to obtain the certification is only £300. Affordable for any business. No such certification exists here. From a customer-supplier perspective, a regulated entity would be low risk and therefore preferential to buy from or work with. A European pilot scheme with a simplified security approach to risk management for SMEs is underway and has been validated but there is a long way to go to bridge the gap (Enisa, 2020). The question from this analysis is how to extend the guidance and regulation to all organisations. This leads to other questions like how would it be governed, and could small businesses afford it? Having an international standard that all businesses must meet should be a priority for governments.

6.2.4. Expertise and associated costs of protection

The literature presents four clear issues for SMEs - lack of understanding of the risks, unclear benefits from investment, lack of skilled resources to mitigate the risk and limited budget. During the analysis, each of these factors was touched on by participants. Cost is contributing factor throughout the literature when analysing factors influencing cybersecurity investment decisions (De Vries, 2017; Ng et al, 2013; Van Ommen, 2014). The was corroborated by participants with one advising SMEs having to spend every penny wisely and another describing cost in this area as a burden.

De Vries (2017) discusses budget constraints, citing the difficulty assigning costs and especially the benefits derived from cybersecurity. Cost-benefit analysis for SMEs was also highlighted by Ommen (2014), advising of limited budget and resources to devote to IT Security. Like the literature, one participant exemplified a typical SME speaking of the difficulty putting a price on not investing but appeared to be investing out of fear instead of through a structured risk assessment process. Only one participant spoke of analysing each risk in the context of its criticality to the business

Van Ommen (2014) advises that large organisations are likely to have built extensive security controls to reduce exposure to IT security risk. Large organisations are further distinguished from SMEs by the likelihood of having dedicated IT security resources. All participants outsourced their IT function to a managed service provider and barring the organisation that is regulated, recommendations around cybersecurity measures came solely from them. This research aimed to look at the reliance on IT/MSP as a central factor but found the truth to be much bigger. SMEs demonstrated a lack of expertise in this area and were happy to outsource the function to a third party. Ng et al (2013) advise that SMEs have a limited set of information skills and are more likely to focus on their core competency than focus on cybersecurity. Outsourcing to experts is a common move but there has to be a level of understanding and oversight of what is expected and being delivered. The relationship with their MSP varied between participants with one describing it as "more reactive than proactive" and another discussing the constant upsell of more security tools to protect against the latest threat. Most participants spoke of the strong relationship with their MSP and consequently the full trust they put in them to keep their business protected. With the acknowledged lack of expertise within SMEs, how can they verify what they are being told is correct? How do they know MSPs are not putting their own interests first by selling solutions that may not be required? Only one of the five participants used independent external consultants to translate the technical requirement into non-technical language to aid informed decision making. Utilising independent consultants like this who are not selling would be a benefit to all SMEs. MSPs or internal IT resources have a difficult task in keeping up with the latest threats and developments in cybersecurity. Some will be more skilled than others in this area – relying on a single source for something so critical to the business is not enough

6.3. Updated Conceptual Model

The outcomes of this research have provided an updated conceptual model highlighting the key factors influencing owners/senior managers when making cybersecurity investment decisions. Some factors found to be central in literature are no longer applicable or subsumed within other factors as highlighted in the discussion above. This model can be utilised for future research in this area. The changes to the model compared with previous literature of just a few years ago shows the fast-paced nature of evolution in this field. The biggest changes have come through the heightened state of awareness. Perceived need is no longer in question. Each company is aware of the danger and possible ramifications for their business. Similarly, previous literature discussed convenience/security trade-off but there is now acceptance that additional measures are requited and part of modern business. Each participant was also fully aware of previous incidents that affected their business and other businesses though the media. Awareness is a key topic for businesses that needs to be highlighted in each discussion regarding cyber security.

The additional key change to the model is the addition of expertise. Highlighted in the discussion, SMEs lack expertise in this area of the business and the need to ensure the advice and guidance they receive is both adequate and appropriate for their business.

The research will recommend testing and validation of the model against a larger sample to ensure accuracy. The model gives a clear picture of the factors influencing modern Irish SMEs when faced with one of the biggest modern challenges to their businesses.

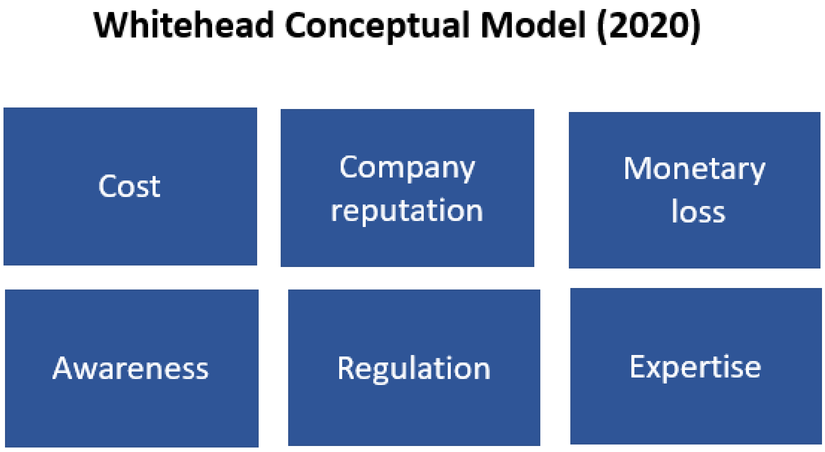


Figure 4. Updated Conceptual model

6.4. Research Limitations

This research had a set timeframe and utilised purposive sampling leading to a limited sample size. Yin (2016) informs that qualitative studies are intended to maximise information, and even an individual sample can provide value. However, a contrast emerged from the research between regulated and unregulated entities which have benefitted from additional regulated entities for comparative purposes.

Additional time could have allowed more in-depth interviews and glean a deeper understanding and perspective from participants.

Face to face interviews as opposed to online would have allowed for better rapport to develop between researcher and participant.

The study looked at factors influencing cybersecurity investment decision making from an Irish SME only context.

Every effort was made to ensure validity. However, reliability of qualitative data as opposed to quantitative is affected by the judgement of the researcher and is therefore not assured (Denzin and Lincoln, 2018).

Finally, according to the CSO (2019), an SME is a company with between 1 and 250 employees with less than €5m turnover. The largest company in this research had 120 employees. Companies with closer to 250 employees may have different attitudes to risk and cybersecurity.

6.5. Recommendations for future research

This research has presented an updated conceptual model that can be utilised to build on this research and expand to a greater population. Validation of this model with a larger sample would be a first step. Once validated in Ireland, the model can be used for analysis from a European context to measure the likely success of standards and policies set by the EU.

This research has highlighted a contrast between regulated and unregulated entities. More regulation and guidance have been lobbied for and worked on for SMEs. A comparative study between regulated entities who have stringent regulations in place now and non-regulated entities would provide a clear indication of the effectiveness if policies were pushed to all SMEs. An element of the study should include affordability to assess viability.

7.0. Conclusion

Cybercriminals are increasingly turning their attention towards SMEs who view them as weaker targets than larger organisations. Using qualitative analysis, this research provides a contribution to theory on the perceptions of senior managers/owners of Irish SMEs when faced with cybersecurity investment decisions. It is concluded six factors are influencing these decisions which are applicable to modern business – (i) cost, (ii) company reputation, (iii) monetary loss, (iv) awareness, (v) regulation and (vi) expertise

The factors outlined are not independent of each other. Each factor has a bearing in the decision-making process, but the weighting alters for different organisations. It is acknowledged that additional security measures come at a cost and the cost can be a burden on SMEs with limited resources and budget. It is, therefore, more important than ever to have adequate risk assessments in place to ensure expenditure is where it is required most. Similarly, SMEs with limited budgets are naturally concerned with having a security incident that results in monetary loss but need investment to reduce the probability of this occurring.

The primary concern found in the research is the requirement to protect the company's reputation. Participants care more about how the company is viewed externally and what an erosion of trust would mean for their business in the future. This fear contributed to a heightened state of awareness amplified by the incessant reports in the media of cyberattacks highlighting the damage done to other organisations. Awareness is also driven by an influx of cybersecurity incidents happening within their organisations. It has led to an acceptance that heightened cybersecurity measures are required, and SMEs no longer see themselves as too small to be a target.

SMEs were found to differ from large organisations by not having dedicated IT security resources. This lack of expertise within the business resulted in outsourcing this function. Understanding the risks and benefits of solutions recommended from outsourced partners proved challenging. The SMEs feared not investing and implementing what they are told they require but the advice given is complicated and often not corroborated. The majority rely solely on the judgement and skill of their outsourcing partner to protect a critical element of their business.

A key finding not anticipated at the beginning of this research was the comparison between regulated and non-regulated entities. Ireland has provided very limited guidelines to SMEs to be able to measure themselves against other organisations with the exception of regulated entities. Regulated entities are upheld to strangest regulation and under strict prudential supervision from authorities. Utilising this approach leads to conformity among entities who are all subject to a minimum IT security standard.

This research provides several recommendations. For Ireland, more guidance is needed for SMEs. The National Cyber Security Strategy aims to provide education to help citizens and SMEs protect themselves online, but this research found no evidence of any impact thus far (DCCAE, 2019). Adoption of the UK cyber essential or similar standard by the Irish government would allow Irish SMEs demonstrate their commitment to cybersecurity and ensure commonality of protection levels across companies adhering to the standard (itgovernance, 2020).

At the EU level, cybersecurity requires a consistent approach. The EU is imposing new standards across member states which are welcome, but they are not directed at SMEs. A slimmed down approach to IT security and risk is required for SMEs that is lower cost and more flexible. ENISA's pilot program aimed at SMEs could provide real benefit if widespread rollout and adoption occurs (Enisa, 2020). Involvement from stakeholders in business and government will be needed to ensure changes are applicable and affordable to all size of SMEs.

From an SME perspective, with the increasing number of attacks, a key line of defence is employees. Phishing and spoofing were common in the analysis; therefore, employees need to be educated. Awareness programs need to be a component of all company's cybersecurity strategy. A structured risk assessment should be implemented by senior managers/owners to find the risks pertinent to their business. Risks should be assessed individually based on probability and impact to the business. Recommendations from MSPs to mitigate risks should be validated by independent consultants.

This dissertation shows growing concern among Irish SMEs and highlighted a fragmented and disparate approach to cybersecurity. New dimensions have been added to previous literature fuelled by the fast pace of change in IT. SMEs have shown a willingness to invest but lack expertise, making guidance essential. The need for a standardised approach to help SMEs is evident.

"The only limit to our realization of tomorrow will be our doubts of today."

Franklin D. Roosevelt

Reference List

Abbosh, O and Bissell, K (2019) SECURING THE DIGITAL ECONOMY, Available at: https://www.accenture.com/us-en/insights/cybersecurity/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50

AON Global (2019) Global Risk Management Survey 2019, London: AON.

Bradford, A (2017) Deductive Reasoning vs. Inductive Reasoning, Available at: https://www.livescience.com/21569-deduction-vs-induction.html

Braun, V and Clarke, V (2006) 'Using Thematic Analysis in Psychology, Qualitative Research in Psychology', Qualitative Research in Psychology. 3(2): pp. 77-101

Browne, S., Lang, M. and Golden, W. (2015) Linking threat avoidance and security adoption: a theoretical model For SMEs

Bryman, A and Bell, B (2011) Business Research Methods, 3rd edn., New York: Oxford University Press.

Čelik, P. (2019) 'Institutional Measures for Increasing the Cyber Security for Business in the European Union', Economic Themes, 57(3), pp. 351–364.

Central Bank of Ireland (2020) What we do – authorise, monitor, enforce, Available at: https://www.centralbank.ie/regulation

Central Bank of Ireland (2016) Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks, Dublin: Central Bank of Ireland

Clifford, N., French,S & Valentine, G (2010) Key Methods in Geography, 2nd edn. London: SAGE Publications Ltd

Creswell, J. (2007) Qualitative Inquiry and Research Design: Choosing Among Five Approaches 2nd edn. Thousand Oaks, London: Sage Publications.

CSO (2019) Statistical Yearbook of Ireland 2019, Available at: https://www.cso.ie/en/releasesandpublications/ep/p-syi/statisticalyearbookofireland2019/bus/businessinireland/

DCCAE (2019) National Cyber Security Strategy published, Available at: https://www.dccae.gov.ie/en-ie/news-and-media/press-releases/Pages/National-Cyber-Security-Strategy-published.aspx

Delotte (2017) Global Survey on Reputation Risk, South Africa: Deloitte.

Denzin, N. and Lincoln, Y. (2011) The SAGE Handbook of Qualitative Research. Thousand Oaks: SAGE.

Department of Education and Skills (2019) Technology Skills 2022 Ireland's Third ICT Skills Action Plan, Dublin: Government of Ireland.

De Vries, J. (2017) 'What drives cyber security investment? Organizational factors and perspectives from decision-makers ', [Online]. Available at: https://pdfs.semanticscholar.org/7e70/f2ab3a3c230a4055580220abf6c230350616.pdf?_ga=2.206370387.177208897.1579339534-1627028690.1578732181

Dudovskiy, J. (2016) 'The ultimate guide to writing a dissertation in business studies: A step-by-step assistance'. eBook Journal of Mixed Methods Research, 4(1): pp.6–16

ENISA (2016) NIS Directive, Available at: https://www.enisa.europa.eu/topics/nis-directive

ENISA (2020) Risk Management and Risk Assessment for SMEs, Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/approaches-for-smes/infosec-smes/pilot-study

European Commission (2018) Internal Market, Industry, Entrepreneurship and SMEs, Available at: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

European Union (2018) General Data Protection Regulation (GDPR), Available at: https://gdpr.eu/tag/gdpr/

Golafshani, N. (2003) Understanding reliability and validity in qualitative research' The Qualitative Report, 8(4): pp. 597-607.

Greener, S. (2008). Business Research Methods. London: Ventus Publishing.

Hiscox (2918) The Small Business Guide to Cyber Attacks, Available at: https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/faq/small-business-guide-to-cyber-attacks

Holmes, A (2019) Hackers have become so sophisticated that nearly 4 billion records have been stolen from people in the last decade alone. , Available at: https://www.businessinsider.com/biggest-hacks-2010s-facebook-equifax-adobe-marriott-2019-10?r=US&IR=T

IT Governance (2020) The Cyber Essentials Scheme, Available at: https://www.itgovernance.eu/en-ie/cyber-essentials-ie

Jordaan, P. (2014) Information security awareness in small information technology-dependent business organisations , Available at: https://core.ac.uk/download/pdf/54201845.pdf

Kaila, U., Nuyman, L. (2018). Information Security Best Practices: First Steps for Startups and SMEs. Technology Innovation Management Review. 8. pp:32-42.

Kennedy KM. (2019). Promoting the qualitative research approach in the discipline of forensic and legal medicine: Why more qualitative work should be promoted and how that can be achieved. J Forensic Leg Med. 2019 Feb;62 72-76.

Ključnikov, Aleksandr & Mura, Ladislav & Sklenar, David. (2019). Information security management in SMEs: factors of success. Entrepreneurship and Sustainability Issues. 6. 2081-2094.

Lee, A. (2004). Thinking about Social Theory and Philosophy for Information Systems. Social Theory and Philosophy for Information Systems.

Leung, L. (2015) Validity, reliability, and generalizability in qualitative research. J Fam Med Prim Care, 4(3): pp. 324-338

Longley, A. (2019) ‘Understanding and managing cyber security threats and countermeasures in the process industries’, Loss Prevention Bulletin, (268), pp. 2–6.

Malter, Alan & Rindfleisch, Aric. (2019). Transitioning to a Digital World.

Mijnhardt, F., Baars, T. and Spruit, M (2016) 'Organizational Characteristics Influencing SME Information Security Maturity', Journal of Computer Information Systems, 56(02), pp. 106-115

Morgan, S. (2018) Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021, Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Morse, J., Barrett, M., Olson, K and Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. International Journal of Qualitative Methods. 1. 13-22.

Myers, M. (1997). Qualitative Research in Information Systems. MIS Quarterly. 21. 10.2307/249422.

NG, Z.X., Ahmad , A. and Maynard, S.B. (2013) Information Security Management: Factors that Influence Security Investments in SMES, Available at: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1156&context=ism

Ommen, V.B. (2014) IT Security in SMEs: Necessary or Irrelevant? , Available at: https://pdfs.semanticscholar.org/ca68/7bb0a9e12d28875caa0a25fcc5d610d03a1d.pdf

Parra, A.S., Crespo, L.E.S., Caballero, I. and Camacho, S. (2016) The Importance of the Security Culture in SMEs as Regards the Correct Management of the Security of Their Assets, Available at: https://www.semanticscholar.org/paper/The-Importance-of-the-Security-Culture-in-SMEs-as-Parra-Sanchez/b58b1618accc504151743c9bf92f6234350885a9

Rebner, S. (2019) The State Of Cybersecurity Pertaining To Small Business , Available at: https://www.forbes.com/sites/theyec/2019/09/18/the-state-of-cybersecurity-pertaining-to-small-business/#19e94ea731a0

Reiter, B. (2013) The epistemology and methodology of exploratory social science research: crossing popper with Marcuse. Florida: Government and International Affairs Faculty Publications.

Saunders, M., Lewis, P. and Thornhill, A. (2009) ‘Research methods for business students’.5th edn. Pearson Education.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students, (6th ed.) London: Pearson.

Sahay, Arunaditya. (2016). Peeling Saunder's Research Onion. Shodh Gyan. ISSN 2395-0617.

Solms, R.V. and Niekerk, J.V (2013) 'IT Security in SMEs: Necessary or Irrelevant? ', Computers & Security, 38(), pp. 97-`102

Thanh, N.C. and Thanh, T.T.L. (2015) 'The Interconnection Between Interpretivist Paradigm and Qualitative Methods in Education ', American Journal of Educational Science , 01(02), pp. 24-27

Tunggal, A.T. (2020) Cyber Security Vs. Information Security: The Key Differences, Available at: https://www.upguard.com/blog/cyber-security-information-security

Vaismorad, M. (2013) 'Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study', Nursing & Health Sciences, 15(3), pp. 398-405

Verizon (2020) 2019 Data Breach Investigations Report, Available at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

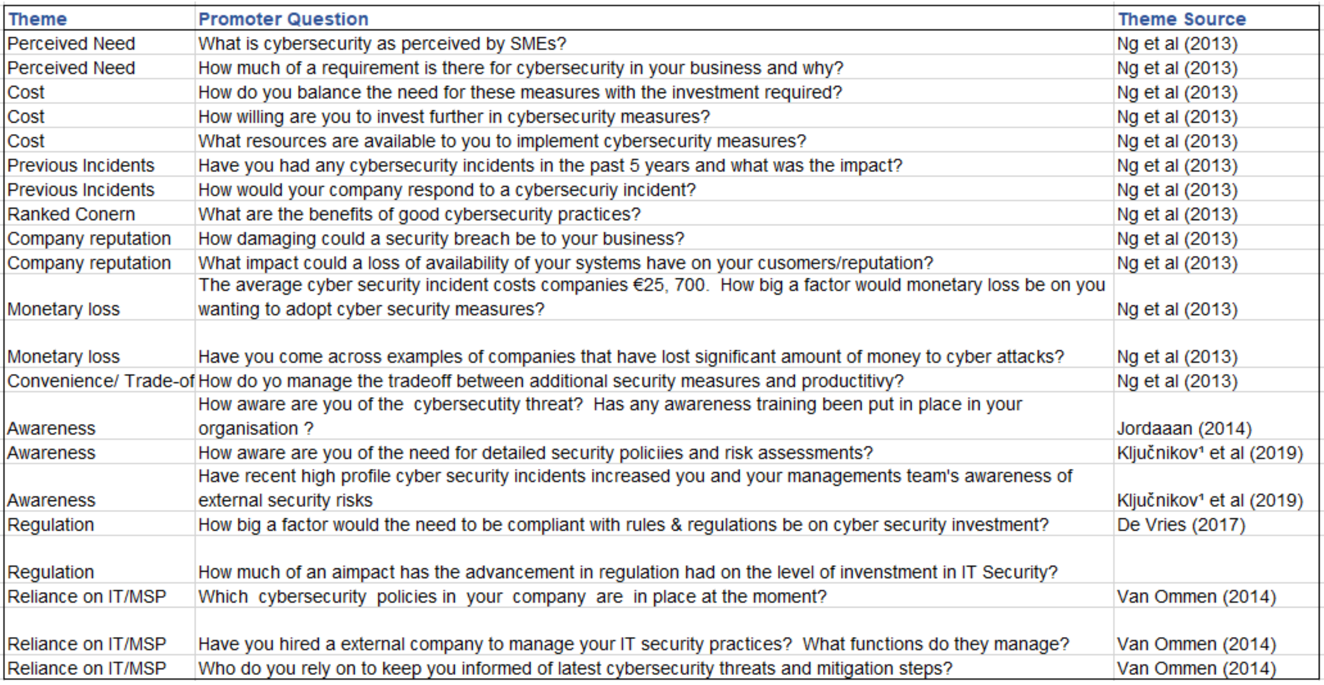
Weber, R. (2004) ‘The Rhetoric of Positivism Versus Interpretivism: A Personal View 1’. MIS Quarterly. 28(1): pp. iii – xi

Willig, C., (2013). Introducing Qualitative Research in Psychology. 3rd ed. Berkshire: Open University Press.

Yaşin, Bahar. (2012). Corporate Reputation and its consequences: Evidence from Turkey. Marketing: Catching the Technology Wave

Yin, R. K. (2016) Qualitative Research from Start to Finish, (2nd ed(, New York: The Guilford Press

Appendix 1 - Interview Questions



Theme	Promoter Question	Theme Source
Perceived Need	What is cybersecurity as perceived by SMEs?	Ng et al (2013)
Perceived Need	How much of a requirement is there for cybersecurity in your business and why?	Ng et al (2013)
Cost	How do you balance the need for these measures with the investment required?	Ng et al (2013)
Cost	How willing are you to invest further in cybersecurity measures?	Ng et al (2013)
Cost	What resources are available to you to implement cybersecurity measures?	Ng et al (2013)
Previous Incidents	Have you had any cybersecurity incidents in the past 5 years and what was the impact?	Ng et al (2013)
Previous Incidents	How would your company respond to a cybersecuriy incident?	Ng et al (2013)
Ranked Conern	What are the benefits of good cybersecurity practices?	Ng et al (2013)
Company reputation	How damaging could a security breach be to your business?	Ng et al (2013)
Company reputation	What impact could a loss of availability of your systems have on your cusomers/reputation?	Ng et al (2013)
Monetary loss	The average cyber security incident costs companies €25, 700. How big a factor would monetary loss be on you wanting to adopt cyber security measures?	Ng et al (2013)
Monetary loss	Have you come across examples of companies that have lost significant amount of money to cyber attacks?	Ng et al (2013)
Convenience/ Trade-of	How do yo manage the tradeoff between additional security measures and productitivy?	Ng et al (2013)
Awareness	How aware are you of the cybersecutity threat? Has any awareness training been put in place in your organisation ?	Jordaaan (2014)
Awareness	How aware are you of the need for detailed security policiies and risk assessments?	Ključnikov¹ et al (2019)
Awareness	Have recent high profile cyber security incidents increased you and your managements team's awareness of external security risks	Ključnikov¹ et al (2019)
Regulation	How big a factor would the need to be compliant with rules & regulations be on cyber security investment?	De Vries (2017)
Regulation	How much of an aimpact has the advancement in regulation had on the level of invenstment in IT Security?	
Reliance on IT/MSP	Which cybersecurity policies in your company are in place at the moment?	Van Ommen (2014)
Reliance on IT/MSP	Have you hired a external company to manage your IT security practices? What functions do they manage?	Van Ommen (2014)
Reliance on IT/MSP	Who do you rely on to keep you informed of latest cybersecurity threats and mitigation steps?	Van Ommen (2014)

Appendix 2 - Interview Consent Form

Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior managers/owner perspective.

Consent to take part in research

- I……………………………………… voluntarily agree to participate in this research study.

- I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind.

- I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted.

- I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study.

- I understand that participation involves a online interview lasting 45-60 minutes discussing cybersecurity within your organisation.

- I understand that I will not benefit directly from participating in this research.

- I agree to my interview being video-recorded.

- I understand that all information I provide for this study will be treated confidentially.

- I understand that in any report on the results of this research my identity will remain anonymous. This will be done by changing my name and disguising any details of my interview which may reveal my identity or the identity of people I speak about.

- I understand that if I inform the researcher that myself or someone else is at risk of harm they may have to report this to the relevant authorities - they will discuss this with me first but may be required to report with or without my permission.

- I understand that disguised extracts from my interview may be quoted in a *dissertation* that will be publicly available on NCI dissertation database

- I understand that signed consent forms and original audio recordings will be retained on encrypted USB drive accessible only to the researcher *until the exam board confirms the results of their dissertation*.

- I understand that a transcript of my interview in which all identifying information has been removed will be retained until September 2022

- I understand that under freedom of information legalisation I am entitled to access the information I have provided at any time while it is in storage as specified above.

- I understand that I am free to contact any of the people involved in the research to seek further clarification and information.

Gerard Whitehead – Masters of Business Administration
National College of Ireland
Phone: 0877681900
Email: X18133215@student.ncirl.ie

Signature of research participant *Date*

-- ----------------

I believe the participant is giving informed consent to participate in this study

Signature of researcher Date

--- ---------------------