Georgia State University
ScholarWorks @ Georgia State University

Business Administration Dissertations | Programs in Business Administration

Spring 5-2-2021

An Examination of the Role of vCISO in SMBs: An Information Security Governance Exploration

William Dicker
Georgia State University

Follow this and additional works at: https://scholarworks.gsu.edu/bus_admin_diss

Recommended Citation

Dicker, William, "An Examination of the Role of vCISO in SMBs: An Information Security Governance Exploration." Dissertation, Georgia State University, 2021.
doi: https://doi.org/10.57709/22497964

This Dissertation is brought to you for free and open access by the Programs in Business Administration at ScholarWorks @ Georgia State University. It has been accepted for inclusion in Business Administration Dissertations by an authorized administrator of ScholarWorks @ Georgia State University. For more information, please contact scholarworks@gsu.edu.

PERMISSION TO BORROW

In presenting this dissertation as partial fulfillment of the requirements for an advanced degree from Georgia State University, I agree that the Library of the University shall make it available for inspection and circulation in accordance with its regulations governing materials of this type. I agree that permission to quote from, copy from, or publish this dissertation may be granted by the author or, in her absence, the professor under whose direction it was written or, in his absence, by the Dean of the Robinson College of Business. Such quoting, copying, or publishing must be solely for scholarly purposes and must not involve potential financial gain. It is understood that any copying from or publication of this dissertation that involves potential gain will not be allowed without written permission of the author.

William Charles Dicker

NOTICE TO BORROWERS

All dissertations deposited in the Georgia State University Library must be used only in accordance with the stipulations prescribed by the author in the preceding statement.

The author of this dissertation is:

William Charles Dicker
J. Mack Robinson College of Business
Georgia State University
Towerplace 200, Suite 500
3348 Peachtree Road, NE
Atlanta, GA 30326

The director of this dissertation is:

Dr. Karen Loch
J. Mack Robinson College of Business
Georgia State University
Towerplace 200, Suite 500
3348 Peachtree Road, NE
Atlanta, GA 30326

An Examination of The Role Of vCISO In SMBs: An Information Security Governance Exploration

By

William Charles Dicker

A Dissertation Submitted in Partial Fulfillment of the Requirements for the Degree

Of

Doctorate in Business Administration

In the Robinson College of Business

Of

Georgia State University

GEORGIA STATE UNIVERSITY

ROBINSON COLLEGE OF BUSINESS

2021

Copyright by
William Charles Dicker
2021

ACCEPTANCE

This dissertation was prepared under the direction of WILLIAM CHARLES DICKER Dissertation Committee. It has been APPROVED and accepted by all members of that committee, and it has been accepted in partial fulfillment of the requirements for the degree of Doctoral in Business Administration in the J. Mack Robinson College of Business of Georgia State University.

Richard Phillips, Dean

DISSERTATION COMMITTEE

Dr. Karen Loch (Chair)

Dr. Richard Baskerville

Dr. Aaron Baird

DEDICATION

First, I will begin by giving all credit to my savior, Jesus Christ, for providing me with "footsteps in the sand" that I have followed during our lifelong voyage together. With him, all things are possible.

This research is dedicated to my wife, Candice Dicker, who provided me with the love, support, and encouragement to accomplish all things once deemed impossible. Your constant drive to push me beyond my boundaries and never accepting failure provided me the opportunity to grow, excel and complete my doctoral journey. Without your support, this paper would not exist.

I want to thank my chair, Dr. Karen Loch, and my esteemed committee members, Dr. Aaron Baird and Dr. Richard Baskerville, for your continued support, patience, and guidance as I diligently worked to complete this study. Your expertise is highly praised, and I will always be thankful for the mentorship provided to me.

Finally, for all those that were told you were not smart enough, did not have enough money, or were too old to achieve your dreams, I say enough is enough. Buckle down, listen to your heart, and do what is best for you and your family, regardless of the cynics. Strive for perfection, and your dreams are achievable. Forget those that continue to degrade you and surround yourself with those that offer support. Failure is only an option if you allow it in your life.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

An Examination of the Role of vCISO in SMBs: An Information Security Governance Exploration

By

William Dicker

March 2021

Committee Chair: Karen Loch

Major Academic Unit: Doctorate in Business Administration

Information security threats and their associated breaches are exponentially growing, with millions of records containing personally identified information released to the public each year. Cyber incidents targeting businesses nearly doubled in US past 6 years, with more than 130 large-scale targeted breaches per year in U.S. In the first half of 2020, 36 billion records were exfiltrated by external hackers, with the average cost to recover from a cyber-attack averaging $21.00 per record.

While Small and Mid-sized Businesses (SMBs) attempt to stay ahead of this growing trend and protect organizational data, they have specific behaviors that do not affect larger organizations. The four behaviors (non-strategic executive-level sponsorship, apathetic risk management procedures, constrained resources, and non-existent technical skills) are identified in the literature and recognized within the small to midsized industry. If not correctly identified and remediated, these behaviors may impede the businesses from protecting information assets and achieve a mature level of information security governance. To assist organizations in achieving information security governance, the literature identifies five domains that all organizations should possess for organizational alignment and governance maturity. These governance domains are Strategic Alignment, Value Delivery, Risk Management, Performance Measurement, and Resource Management. However, extant literature does not align the five

governance domains with the small to midsized business behaviors, nor provide a solution to assist SMBs in achieving information security governance.

The literature review focused on four main aspects that are relevant to the study: SMB Characteristics, Virtual Leadership, Information Security Governance, and Information Security program. Previous research identified how similar organizations utilized virtual leadership positions to overcome SMB behaviors to attain organizational business requirements but did not identify virtual positions that can assist SMBs with information security governance. To bridge this gap, this study explored a recent phenomenon, identified as a virtual Chief Information Security Officer (vCISO), that can align the SMB behaviors with the five governance domains and provide a viable solution for SMBs to achieve Information Security Governance within the identified behaviors. Specifically, this qualitative exploratory study interviewed six vCISOs and 14 companies to examine the role the vCISO provided in bridging SMB's organizational behaviors with the five Information Security Governance domains.

Keywords: virtual Chief Information Security Officer, vCISO, small and mid-sized businesses, SMB, information security governance

I INTRODUCTION

I.1: Background for the Study

Organizations are transitioning away from paper records by transforming data into electronic media, with access to digital information more readily available today than in previous years. According to Accenture (2017), a statistical report indicated there are over 130 large-scale, targeted breaches in the U.S. per year, and this figure is increasing by 27 percent each year. Furthermore, current reports indicate that it averages 23 days to recover from a ransomware attack and 50 days to recover from a malicious insider attack (Accenture, 2017). The average cost to recover from a cyber-attack is $21.00 per customer record or $17 million annually (Accenture, 2017), with 95% of all breaches in 2020 caused by human errors (Varonis, 2020). Finally, Statista (2020) indicated cyber incidents targeting businesses nearly doubled, with the number of reported data breaches in the United States equaling 784 (2015), to 1,506 (2019), and 36 billion records were exfiltrated by external hackers in the first half of 2020 (Varonis, 2020).

Unlike larger organizations, many small and mid-sized businesses (SMBs) lack the resources for in-depth tools or in-house information security expertise to harden their systems and networks against potential threats (Bourne, 2019). In its most simplistic form, SMBs have four specific organizational behaviors that inhibit them from maintaining an Information Security Governance program and the protection of organizational data (Berry & Berry, 2018). As paper records become obsolete and digital records' transformation is increasing amongst organizations lack the information security awareness and knowledge about current or future cybersecurity threats is a significant cause of concern for small and mid-sized businesses. In contrast, the 2020 Data Breach Investigation Security Report (Table 1) demonstrated that the number of overall cybersecurity incidents between small and large businesses is narrowing and may be an indication

of various attack vectors, better cybersecurity practices at the organizational level, or the lack of reporting of breaches (Verizon, 2020).

Table 1: 2020 DBIR Report (Verizon, 2020)

	Small (less than 1,000 employees)	**Large (more than 1,000 employees)**
Frequency	• 407 incidents • 221 confirmed data disclosures	• 8,666 incidents • 576 confirmed data disclosure
Threat Actors	• External (74%) • Internal (26%) • Partner (1%) • Multiple (1%)	• External (79%) • Internal (21%) • Partner (1%) • Multiple (1%)
Actor Motives	• Financial (83%) • Espionage (8%) • Fun (3%) • Grudge (3%)	• Financial (79%) • Espionage (14%) • Fun (2%) • Grudge (2%)
Data Compromised	• Credentials (52%) • Personal (30%) • Other (20%) • Internal (14%) • Medical (14%)	• Credentials (64%) • Other (26%) • Personal (19%) • Internal (12%)

Gordas (2014) defines Information Security Governance as a supporting tool to align the business objectives and information security strategies to the information security program by using a collection of tools that enhances the five information security domains. Furthermore, the information security program is a compilation of organizational information security policies, procedures, and standards to ensure the confidentiality, integrity, and availability of client and customer data supported by three foundational information security pillars (Gordas, 2014). However, most small to mid-sized businesses (SMBs) lack the resources required to build an effective information security program (Lewis et al., 2014), which is the foundation for a robust Information Security Governance program, and ultimately, the SMBs becomes an easy target for malicious actors (Ključnikov, et al., 2019).

Another concern for SMBs is a lack of information security expertise, which poses an increased risk to a small business's cybersecurity culture. To expand on the lack of technical information security expertise, One Trust Alliance surveyed security breaches in 2017 and determined that 93% of the reported attacks are preventable with simple cyber hygiene practices, such as regularly updating software, blocking fake email messages, and training employees to recognize phishing attacks (Olmstead, 2019). To further illustrate this point, Karanja and Rosso (2017) highlighted the importance of having a CISO at the information security program's helm. In one example, Karanja and Rosso (2017) reported that Target hired its first CISO after identifying a malware infection in their point-of-sale registers that exfiltrated over 40 million credit and debit card data as well as 70 million customers' personal data. Without the proper information security tools and expertise onboard, Target reported it spent $148 million to mitigate this breach (Karanja & Rosso, 2017); therefore, it is more cost-effective to invest in the proper information security tools and personnel to deter an attack rather than be reactionary post-attack.

Statista (2020), a German-based company that hosts the largest cybersecurity database, performed a 12-year study of information security expenditures for all organizations. In 2005, organizational security expenditures were identified as 7.5% of the overall IT budget regardless of the organization's size. Additionally, the study indicated that expenditures continued to increase annually, culminating in 2017 with 10.6% of the overall IT budget allocated to security initiatives for all sizes of organizations. When viewed as a single entity, an SMB's security expenditure was 5.6% lower than the 2017 expenditures for all organizations and is directly related to the constrained resources of SMBs.

I.2: Motivation for the Study

Working in the Information Security field for more than a decade, I have continuously enhanced or built information security programs for all sizes of organizations. Each strategy depended on the organization's information security culture, risk appetite, available funds for security expenditures, and the information security team's skillset. Despite the approach used, the end goal always remained the same: to build an information security program using expertise in the field, to reduce risks to an acceptable level, and to secure client data with minimal expenditures. However, my experience discovered that information security vendors focus security initiatives on larger organizations with a substantial IT budget but forego the smaller organizations with minimal budgets. Third-party vendors sell the high-priced solution to large organizations to make quarterly sales quotas but forget that even the smallest organizations require similar solutions to meet organizational objectives. Limited by constrained resources, SMBs have minimal options to pursue information security solutions to build an effective Information Security Governance program.

SMB leaders are aware of cybersecurity trends and witness reports of information security breaches within similar-sized organizations. During an evaluation of the 2019 State of SMB Cybersecurity, a survey of 850 SMBs with sizes ranging from 10 to 1,000 employees, 64% of the SMBs indicated they had suffered a security breach (Bourne, 2019). Additionally,

- 89% viewed cybersecurity as a top-five priority for the organization.
- 75% agreed there should be more cybersecurity focus.
- 79% would invest more in cybersecurity initiatives in 2020.
- 62% lacked the skills in-house to deal with security issues.
- 13% would not be able to defend against an attack.
- 52% felt helpless from identifying new forms of attacks.

- 80% are worried that they will be the target of a cyber-attack in the next six months.

With these alarming statistics, it is evident that SMBs face the same threats as large organizations but lack the funding, resources, security infrastructure, and staff available to large organizations (Williams & Manheke, 2010). These limitations place a heavy burden on SMBs attempting to mature while maintaining a level of information security protection needed for brand recognition, stewardship of limited capital, and regulatory behaviors. A recent survey conducted by Continuum revealed that 89% of SMBs view cybersecurity as a top-five project for their organization, with 79% of the respondents indicating a requirement for investing more financial dollars into cybersecurity strategies (Bourne, 2019). However, the challenge for SMBs is the financial price tag of protecting the data (Banham, 2017), and without having the monetary investments available for cybersecurity initiatives, or skilled employees required to manage those investments, small businesses fall behind the cybersecurity trend (Labossiere, 2015).

To help reduce the information security challenges facing SMBs, a new market has emerged that allows SMBs to employ an Information Security Executive for a fraction of a full-time security executive's cost. This emerging market is known as the virtual Chief Information Security Officer (vCISO) and is rapidly gaining traction within the SMB space. The identified SMB gaps motivated research of the vCISO role to explore how a virtual Chief Information Security Officer (vCISO) can overcome the security behaviors identified by researchers and assist SMBs to attain information security governance, protect organizational resources, and add value to the organization.

I.3: Research Approach

The research design approach is provided in Table 2. The remainder of the study is divided into several chapters.

- Chapter II is the literature review and discusses the characteristics of small to mid-sized businesses, SMB information security comportment, information security governance, and the information security program.
- Chapter III outlines the theoretical framing for the research.
- Chapter IV summarizes the research design and methodology.
- Chapter V analyzes the interview observations, including identified themes and propositions.
- Chapter VI examines the discussion of the study, contributions, limitations, and future research.

Table 2: Components of Engaged Scholarship Research (Mathiassen, 2017)

Component	Details
Problem Setting (P)	Small and Medium-size Businesses (SMBs) have four areas of concern that prohibit information security governance: a) lack executive-level sponsorship, b) apathetic risk management procedures, c) constrained resources, and d) non-existent technical skills.
Area of Concern (A)	• SMBs have the same cyber risk that threatens larger organizations. • SMBs are unable to provide the level of security that larger organizations can provide. • SMBs consist of 99% of all businesses in the U.S. • SMBs lack the resources and technical expertise to secure information systems and a mature governance program.
Theoretical Framing (F)	Information Security Governance Domains
Research Method (M)	Exploratory multi-case approach, using qualitative interviews and inductive analysis.
Research Questions (RQ)	• What is the role of the vCISO while addressing the SMB's Information Security Governance maturation? • How does an SMB receive value from a vCISO while attempting to achieve a mature Information Security Governance program? • How can a vCISO utilize their experience and mentorship to modify the SMB's information security behavior?
Contribution	• C(a): this study explores how a vCISO can utilize their technical experience and expertise to assist SMB leadership teams in achieving a mature governance platform that protects confidentiality, integrity, and data availability. • C(a): the study explores the extent to which a vCISO adds value to an SMB from actualized benefits derived from a vCISO engagement.

	• C(a): Provides a proposed vCISO process model for an SMB client engagement. • C(p): the study will provide evidence to practitioners that vCISOs assist SMBs by achieving governance with minimal cost to the SMB. • C(p): explores how the vCISO assists SMBs to improve their security posture while providing value to the organization. • C(p): provides evidence of how the vCISO delivers mentorship to SMBs in the governance maturation process.

II LITERATURE REVIEW

The literature review focused on identifying foundational constructs to further the exploratory study of the vCISO utilization within an SMB. Expressly, the research indicated three primary constructs: SMB Characteristics, Virtual Leadership, and Information Security Governance. Each construct is further divided into specific streams that were deemed essential to the study. The research utilized a "building blocks method" where specific keywords, using Boolean operators, were entered into the search field to reveal substantial articles that required further investigation. Each of the identified literature streams was methodically reviewed using results obtained from EBSCO, ABI/INFORM, ProQuest, where 58 peer-reviewed scholarly articles were selected for inclusion in the literature review. To ensure the most updated information was included in the study, further research of practitioner articles, information security trends and reports, government documents, and other journals utilizing Google Scholar and publicly available information were selected for inclusion in the literature review.

II.1: SMB Characteristics

II.1.1: Designation as a Small and Mid-sized Businesses (SMB)

The Small and Mid-sized Businesses (SMB) market represents a very diverse, fragmented collection of businesses, from solopreneurs running home-based lifestyle businesses, fast-growth startups, and midmarket firms who have been in business for 30-plus years. Definitions identified in the literature vary between annual revenue or number of employees, creating confusion and disarray with financial loans, process deployment, and technology implementations. JP Morgan Chase (2014) classifies over 99 percent of America's 28.7 million firms as small or medium businesses, with 88 percent having fewer than 20 employees and nearly 40 percent of all enterprises grossing less than $100k in revenue. Additional research indicates that other financial institutions struggle to identify a collective definition of small- and mid-sized businesses, which

tends to provide negative financial reviews due to the lack of profit and high risk of failure (Crassula, 2019).

In 2019, The Small Business Administration (SBA) identified that small businesses in the United States employ over 59.9 million employees or 47.3% of the total workforce, with these numbers increasing each year. To further complicate SMB designations, the Small Business Administration will qualify an organization as a small business in some industries by recognizing the organizational revenue instead of its number of employees. In other industries, the employee count is the most relevant component over gross revenue. For example, the SBA identifies Pharmacies and Drug Stores as having a maximum income of 27.5 million dollars but does not specify a maximum number of employees to be considered a small business. In contrast, the SBA recognizes Direct Property and Casualty Insurance Carriers with a maximum of 1,500 employees to qualify as a small business, regardless of the maximum revenue (U. S. Small Business Administration, 2019).

Gartner (2020) has an international standard to define small and mid-sized businesses and uses both revenue and employee count as quantifiers., Unlike the SBA analysis, Gartner does not separate SMBs based on industry. Organizations that contain fewer than 100 employees or less than $50 million in annual revenue are designated as a small business, and organizations with 100 to 999 employees or more than $50 million but less than $1 billion in annual revenue as mid-sized companies (Gartner, 2020).

Continuing with the inconsistency of contrasting definitions, international organizations employ the term Small and Mid-sized Enterprises (SMEs) to delineate the difference in organizational size and revenue. SMEs are a more globally used term than SMB with a more extensive range of operational activities (Crassula, 2019), and account for 90% of firms and

employ 63% of the world's workforce (Munro, 2013). Internationally based enterprises, such as the United Nations, World Bank, World Trade Organization, and the European Union, designates SMEs as their official market phrase instead of using SMB (Sangoma, 2020)

An SME usually employs a full-time workforce of fewer than 500 employees with a revenue of more than 50 million dollars, but less than 100 million dollars (Berisha & Pula, 2015). Other countries have similar statutes to differentiate between small and mid-sized businesses. In South Africa, SMEs have fewer than 200 employees, an annual turnover of fewer than 64 million Rands (around 3.5 million dollars), assets of less than 10 million Rands ($541,000.00) and must include direct managerial involvement by owners (South African Government, 2004). The European Union identifies medium businesses with fewer than 250 employees, a turnover of fewer than 50 million euros, and a balance sheet total of fewer than 43 million euros, and small-sized enterprises with less than 50 employees, turnover less than 10 million euros, and a balance sheet total of fewer than ten (10) million euros (European Commission, 2020). Canada defines a small business as having less than 100 employees and a mid-sized company that employs at least 100 and fewer than 500 employees and designates 98.2 percent of all Canadian businesses (Government of Canada, 2013).

SME's and SMB's have recognition worldwide based on the industry, the number of employees assigned, revenue, and country of origin. For this study, the identifiers for an SMB and SME are interchangeable and considered the same entity. Being the most consistent of all definitions and serving as a foundational base for this study, the Gartner (2020) definition will be utilized for SMB identification.

- Small Businesses: organizations that contain fewer than 100 employees or less than $50 million in annual revenue.

- Mid-sized Businesses: organizations with 100 to 999 employees or more than $50 million but less than $1 billion in annual revenue are classified as mid-sized businesses.

II.1.2: SMB Information Security Behavior

Information security is a critical business function for all organizations, and SMBs are no exception. As organizational demands continue to grow and data storage has evolved into electronic medium rather than storage in paper format, SMB weaknesses are more readily identifiable to hostile actors and provide lucrative alternatives, such as using the SMB as a pivot point for broader, more large-scale attacks. SMB information security behaviors are a shared characteristic throughout the SMB industry (Rohn et al., 2015), usually involving behaviors that larger companies do not possess. SMBs have a smaller workforce than larger organizations; hence, they are more heavily dependent on digitally enabled products, thus increasing the risk of breaches (Hibbert, 2012). Consequently, past studies indicate that SMBs are far behind larger companies in data protection and governance because they lack:

- the financial resources to invest in security initiatives or hire skilled employees (Lee & Larsen, 2009)
- the technical skills required to prevent attacks (Labodi & Michelberger, 2010),
- a formalized risk assessment process (Gupta & Hammond, 2005)
- executives that are cognizant of information security emerging trends and threat vectors (Mitchell et al., 1999)

As indicated in the introduction, SMB's have specific behaviors that negatively affect the information security posture and are generalized into four main categories: executive-level sponsorship, apathetic risk management procedures, constrained resources, and non-existent technical skills.

II.1.2.1: Non-strategic Executive-level Sponsorship.

Senior executives are the foundation for any organization and set the climate, direction, and goals for its employees. This foundational concept ensures that all business initiatives, including the Information Security Governance program, provide executive-level sponsorship with the tools, funding, and processes to successfully integrate each initiative into the business functions. Addressing information security challenges is not isolated as only technical problems; management support and the organization's behavioral aspects (culture) are often overlooked by smaller organizations (Singh et al., 2013). Senior management and information security executives must treat information security as another business investment rather than a technical expenditure (Kayworth & Whitten, 2010; Goles et al., 2005), and should receive the same importance as other ventures, with decisions made in the board room instead of server rooms.

SMBs are focused on growing the business, and the senior leaders are viewed as the ones that will guide the company's direction. As a result, senior management's attitude towards information security directly impacts employees' attitudes, which indirectly affects an organization's information security culture and the overall maturity of the Information Security Governance of the SMB (Alhogail & Mirza, 2014). Executive management is accountable for ensuring the organization has a safe and secure environment for implementing, operating, and maintaining information assets (Whitman & Mattord, 2012; Kwon & Wang, 2012). Security executives have a difficult decision with providing employee usability of information assets to balance the organization's business requirements to the stricter compliance requirements required to secure information assets (Moon et al., 2018). However, during an analysis of the worst security breaches reported in 2012, seven percent of the breaches revealed that senior management did not provide an adequate priority for security investments (Houngbo & Hounsou, 2015). Additionally,

in a 2012 survey released by Price Waterhouse Coopers (PWC), 57% of small organizations breaches directly resulted from insider actors, with 36% of the reported breaches created unintentional human error (culture) (Alhogail & Mirza, 2014).

Typically, SMB owners lower the importance of network security issues in favor of more pressing matters (Nijnik, 2005), such as obtaining clients, operational constraints, and revenue generation. As suggested by Gordas (2014), SMBs must change the mentality regarding information security, and it must become a top priority to ensure SMB survival. SMB leadership teams will take a more proactive role in Information Security Governance if they feel their organizations are vulnerable (Barlette et al., 2015), but the problem is that most SMBs feel they are not susceptible to external attackers due to a false sense of security (Banham, 2017). Alongside management's attitude, the SMB's senior leaders must recognize they are targets, just like the more prominent companies (Banham, 2017). Small business attacks usually do not make national headlines (Labossiere, 2015), such as the Equifax breach. The lack of national coverage enhances a false sense of security, and many SMBs will disregard their organization's fundamental security requirements (Gordas, 2014) or lower the importance of security initiatives. As summarized by Nijnik (2005), one of the greatest threats to small businesses is the owners' false sense of security in protecting their networks.

II.1.2.2: Apathetic Risk Management Procedures.

Risk management is a holistic view of the entire organization's risk and should not be siloed only to information technology. However, most SMBs do not take risk management seriously or fail to manage risk at all (Joshi and Singh, 2017). Risk is a business initiative associated with the context of an organization's use, ownership, operation, involvement, influence, and adoption of controls within an enterprise (ISACA, 2010). Organizations that address risk as a

subordinate business function will inherently do less to protect themselves, thereby increasing the risk of a catastrophic breach (ISACA, 2010). Therefore, SMB leadership should strive for Information Security Governance by investing in information security procedures proportionate to the level of organizational risk to the SMB (Hibbert, 2012). In its most simplistic form, the identified risk is a business problem, with a clear line of accountability to the owner of the risk, or the individual who is ultimately accountable for managing the risk, as directed by the organization (ISACA, 2010; Stanford University, 2020). Business leaders must understand that risk management is not a one-and-done task but is an ongoing concept that should remain on the business owner's minds with all business activities (Labossiere, 2015). Furthermore, research indicates that most SMBs lack the knowledge to assess risk accurately and to identify the specific business risk to mitigate (Labossiere, 2015). Outsourcing risk management functions to third-party vendors is feasible if business owners understand that they remain accountable for risk management and continuous risk monitoring (Gordas, 2014).

The most significant risk that SMB faces is an environment where the employees are unaware of the information security threats that exist to the organization, known as the information security culture. To properly enforce information security governance, senior leaders must ensure that their organization has an information security culture that recognizes suspicious threats and reacts appropriately. Employees' information security awareness and behavior, accompanied by their compliance or non-compliance with information security policies, is identified as one of the most critical vulnerabilities in any organizational security strategy (Guhr et al., 2017). Mishra and Dhillon (2006) identify that an organization that punishes those who fail to follow the rules (deviant behavior) serves as a deterrent for others and is the cornerstone of behavioral information security governance. Typically, employees are hired with specific skill sets to perform their

primary duties but lack the requisite knowledge of security threats to enhance the security culture (Van Niekerk & Von Solms, 2010). Education, awareness, and proactive monitoring are essential components of a productive information security culture where employees are enabled and equipped to behave and mitigate the organizational risk to the organization's security of information assets (Martins & Eloff, 2002).

Risk management is a daunting task for novice executives and can become overwhelming if not properly managed. Enterprise Risk Management (ERM) systems provide organizations with a systematic methodology and processes to manage risks and facilitate Information Security Governance (Wu & Olsen, 2009). However, for a novice executive, selecting the correct Enterprise Risk Management framework is essential for a successful risk management program. Some ERM's are provided with a negligible cost to the organization, while other frameworks are commercial products requiring annual subscriptions for full-use products. Regardless of the chosen structure, all enterprises need to adopt a risk management strategy and methodology to identify, assess, and treat risks (Ključnikov et al., 2019). Table 3 provides an overview of some of the most common ERM frameworks SMBs can employ within the organization (Joshi & Singh, 2017).

Table 3: Risk Management Frameworks (extended from Joshi & Singh, 2017)

Risk Management Framework	Governing Body	Description
OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)	Cert	A model for risk-based infosec strategic assessment and planning.
FAIR (Factor Analysis of Information Risk)	RiskLens	Allows organizations to standardize the risk, apply risk assessment, view in total organizational risk, defend risk determination using advanced analysis and understand how time and money will affect the organization's security profile
RMF (Risk Management Framework)	NIST	A six-step risk management framework: Categorize, Select,

		Implement, Assess, Authorize, and Monitor
TARA (Threat Agent Risk Assessment)	Intel	Assists companies to manage risk by distilling the possible information about security attacks.
COSO Enterprise Risk Management Framework	Committee of Sponsoring Organizations (COSO) of the Treadway Commission	It contains five significant components: Governance and Culture, Strategy & Objective-Setting, Performance, Review and Revision, and Information, Communication, and Reporting
ISO 31000, and ISO 27005	International Organization for Standardization	ISO is an international standard that provides principles and guidelines for effective risk management. It outlines a generic approach to risk management, which can be applied to different risks (financial, safety, project risks) and used by any organization.

II.1.2.3. Constrained Resources.

Resource management refers to the availability of capital, personnel, and time (Cholez & Girard, 2013). As previously discussed, an SMBs focus is on obtaining clients, operational constraints, and revenue generation. During the early formation years, SMB resources are limited and sparse, and in some cases, non-existent for non-revenue generating events. It is widely understood that larger companies have resources to address cybersecurity issues; small companies often do not (Berry & Berry, 2018). Deploying security initiatives and the cost of protecting the data is an additional business expense for SMBs (Banham, 2017), and security initiatives should not solely depend on price but should be evaluated based on the mitigation of identified risks (Hibbert, 2012). Considering only a few essential items required for an adequate information security program, SMBs could expect to initially spend at least $50,000 to $100,000 on infrastructure components and an additional $10,000 to $25,000 annually for maintenance, which is considered overly expensive for many SMBs. For example,

- A basic 24-port managed firewall designed to block unwanted traffic will cost an SMB between $3,000.00 and $4,300.00 for the device and an additional $800.00 to &1,000.00 annually for maintenance and support.
- A Security Incident and Monitoring System (SIEM) designed to alert security incidents in real-time, averages $55,000 for the basic SIEM, plus an annual $10,000 for maintenance and support.
- Annual security training and email phishing programs average about $12.00 per user.
- Third-party risk assessments vary depending on the organization's size, but an enterprise risk assessment is about $5,000.00 per location.
- Anti-virus (AV) solutions vary by product, but the most basic AV subscription is about $14.99 per user per year.

In addition to the monetary costs associated with an information security and governance program, SMBs also experience difficulties managing other resources, such as time and personnel. For most businesses, resources are constrained, and there may be no budget to hire a dedicated security professional. This assertion holds factual for employing a senior-level information security executive and a cybersecurity team (Cholez & Girard, 2013; Gordas, 2014). On average, a full-time Chief Information Security Officer's (CISO) salary averages $181,160 annually, and a security analyst's salary averages about $76,410 annually (Glassdoor, 2020). To properly employ a security team, SMB executives are required to understand the level of protection required for the organization, such as cloud hosting security specialists, network specialists, or web application specialists. However, when faced with spending vital resources on hiring an internal security team or outsourcing to a Managed Service Provider (MSP), most SMBs will outsource vital security functions to an MSP that may not have security specialists in-house. As the data indicates, SMB

leaders lack the monetary resources to secure the infrastructure by purchasing essential network equipment or hiring someone to secure the infrastructure. In some cases, neither option is feasible.

II.1.2.4: Non-existent Technical Skills.

When people rely on the technology without understanding it, even the more obvious security weaknesses are often overlooked (ISACA, 2010). The final area of concern that threatens SMB operations is the lack of security experts' technical skills. SMBs lack the technical expertise to understand the cybersecurity strategies to implement or how to protect organizational data, which yields the temptation to cut corners (Gupta & Hammond, 2004). The lack of technical expertise creates an opportunity to lull SMB executives into believing a false sense of protection by purchasing specific products, particular tools, unvetted managed security services, or inexperienced consultants (Hibbert, 2012). Simultaneously, SMB leadership teams may desire to implement Information Security Governance but lack availability because of overwhelming daily operations (Gupta & Hammond, 2004) or become confused by the astounding number of Information Security Governance standards (Hibbert, 2012). From a business perspective, when an organization does not develop or implement cybersecurity strategies, the effects of a breach could create unplanned costs that may bankrupt the business and knowing the corners not to cut can spell the difference between security success or disaster (Gupta & Hammond, 2004).

The senior information security officer title varies between organizations, but the consensus from academics and practitioners is that the senior information security officer will serve as the subject matter expert on all information security issues (NIST 800-55, 2008). For this study, the senior information security officer is referred to as the Chief Information Security Officer (CISO).

The Chief Information Security Officer (CISO) is an executive-level position with a particular skill set responsible for implementing the organizational security strategy and managing organizational security issues. To build an effective Information Security Governance program, CISOs are required to have excellent communication, collaboration, and essential skills to work with other business leaders (Maynard et al., 2018). As a C-level position, Chief Information Security Officers should have the ability to report the security program's effectiveness directly to the CEO or Board of Directors. However, this is not the case in most organizations. As reported by Shayo and Lin (2019), the Ponemon Institute discovered that the CISO reporting structure differed among all the surveyed organizations, where fifty percent (50%) reported to the CIO, nine percent (9%) reported to the Chief Technology Officer, nine percent (9%) reported to the Chief Financial Officer (CFO), six percent (6%) reported to the Chief Operating Officer (COO), and four percent (4%) reported to the Chief Executive Officer (COO). The remaining twenty-two percent (22%) reported to other non-C-level executives. This myriad of reporting structures has considerable variance across industries, which contributes to an unorganized Information Security Governance program by 1) minimizing the influence the CISO has on senior leadership when addressing information security gaps of people, processes, and technology, 2) minimizes the importance of information security, and 3) creates a higher security risk for SMBs.

From an implementation perspective, the CISO must be the technical subject matter expert for all security issues. A survey of CISO responsibilities indicated that seventy percent (70%) of the CISOs were responsible for the information security policies and procedures, infrastructure management, and security education (Whitten, 2008). Additional skill sets identified include security of the network infrastructure, strict adherence to regulatory requirements, and ensuring the confidentiality, integrity, and availability (CIA Triad) of organizational data (Karanja & Rosso,

2017). More importantly, a CISO must understand the industry in which they operate (Whitten, 2008).

From a strategist perspective, the CISO position has evolved from a technical expert to a business executive with a presence in the boardroom and more significant input into the strategic business measures (Alexander & Cummings, 2016; Dawson et al. 2010). As a strategist, the CISO develops and drives the information security and governance strategies that enable the SMBs to achieve their goals and objectives (Dillen et al., 2018). With some organizations, the CISO faces challenges being accepted as an executive and gaining credibility with their peers (Maynard et al., 2018), which impacts the credibility of the CISO role for the organization.

Likewise, a senior-level information security executive (CISO) or information security analysts are difficult to afford on the SMB's limited budget. As a result, SMB leaders may be forced to fill those roles, even if on a part-time basis without the expertise or required requisite knowledge. The security landscape is continually changing, and attackers know that smaller organizations lack the employee depth and skills needed to develop a defensive security strategy (Banham, 2017) or the capacity to react promptly to security incidents (Gordas, 2014). This evolving security landscape requires an information security executive that a) understand the importance of a security posture from a business perspective, b) can evaluate and mitigate risks to the organization, and c) keeps current on information security practices, which is an added burden on businesses that are already overly busy, short-staffed, and display risky information security behaviors (Williams & Manheke, 2010). Knowing this void exists, SMBs are forced to seek information security advice and information (Renaud, 2016) from publicly available sources, such as the internet or information security discussion groups.

II.2: Virtual Leadership

The virtual leader concept identified in the literature focuses on the successes and failures in a virtual leadership environment, especially when managing virtual teams. As the vCISO serves as an individual information security executive and a virtual team member, both concepts were reviewed during the literature review.

In organizations where the traditional leadership style is face-to-face interactions with an organizational employee, the primary challenge for a virtual leader is creating an environment where the virtual leader can influence the organization, like the traditional leader, without the requirements of the face-to-face interactions (Kerfoot, 2010). Virtual leadership has many forms, but each definition posits that virtual leaders are not bound by traditional leadership conditions but have options to manage people, processes, and technology through electronic media communications. Direct leadership is the most conventional form of leadership in typical working environments, but a more practical approach with virtual leaders and teams is accomplished through empowerment and delegating managerial functions to the virtual members (Hertel et al., 2005). Moreover, Williams (2002) generalizes virtual leadership as one that leads in any environment other than in a physical environment. Finally, virtual leaders are described as managers who inspire people in geographically separated locations from the primary working environment (Fisher & Fisher, 2001).

Virtual leaders can work in varying environments that are identified based on the parameters of different time zones, geographical locations, and cultures (Kerfoot, 2010; Schmidt, 2014). SMBs have numerous types of cultures, each with different approaches to information security development. When organizational culture and norms vary across industries, establishing common goals and expectations is challenging. The virtual leader must explore processes to

address cultural challenges (Kayworth & Leidner, 2002) to further mature the organizational Information Security Governance initiative. The most important factor when working with virtual leaders and virtual teams are the assurances of information and timely communications (Schmidt, 2014). Providing relevant and timely data is essential for SMB's survival, and a proper communication medium is a success criterion for alleviating virtual leadership concerns. The virtual team leader's communication quality is a critical element of the virtual team's success or failure (Nixon, et al., 2012). The awareness of developing and utilizing high-performing virtual leaders may create a competitive advantage for firms operating in a competitive market (McCann & Kohntopp, 2019).

II.2.1: Virtual Executives

As businesses continue to trim high payroll costs and benefit savings, virtual executives become a popular alternative for outsourcing specific business functions. Organizations employ a virtual executive to direct people from a distance to complete required work that accomplishes the organization's mission and objectives (Renu, 2014) and requires a broader skillset than managers working on traditional teams (Meyer, 2010). Traditional leadership environments may not require formalization of specific roles and responsibilities, but the virtual leader must ensure functionality is clearly articulated from the organization (Meyer, 2010). Virtual leaders encompass a wide range of experience and have business knowledge of all types of industries. The most important asset that a virtual executive can provide an organization is the broad depth of experience at a fraction of the cost for in-house senior-level executives. Furthermore, virtual leaders often have a team of industry specialists at their disposal to assist executives on behalf of the organization.

III.2.1.1: Virtual Chief Financial Officer (vCFO).

The most referenced virtual executive in the literature is the virtual Chief Financial Officer (vCFO). vCFOs offers solutions from necessary bookkeeping skills to expert financial advice from a senior-level perspective with associated payroll costs about one-eighth to one-tenth the fee of their full-time counterparts (Adhikari, 2012). Colin Wright, the President and founding member of the Virtual CFO Association, asserted that a "trustworthy virtual CFO business would provide a level of service equivalent to that provided by a CFO/Financial Controller who is a part of the client's team" (Ozolins, 2018). Succinctly stated, Wright credits the success of vCFO's as an integral part of the team, focused on successfully building SMB strategies and managing performance through accountability (Ozolins, 2018). A virtual CFO's primary goal is to help small and mid-sized businesses build a sustainable business model, introduce robust controls, ensure regulatory compliance, and raise resources for emerging businesses (Adhikari, 2012).

III.2.1.2: Virtual Chief Operating Officer (vCOO).

Another type of virtual executive is the virtual Chief Operating Officer (COO). The vCOO is typically considered the visionary for the organization and is second in command to the Chief Executive Officer (CEO). A competent COO allows other executives the opportunity to focus on more pressing issues, such as organizational growth and revenue generation. Like other virtual executive positions, the vCOO allows for seamless management of shared team services and permits the organization to utilize their broad experiences and resources for minimal costs. vCOOs provide growing SMBs experience in both regulated and non-regulated environments and can provide best-practice recommendations from previous client interactions.

III.2.1.3: Virtual Chief Information Security Officer (vCISO).

Like the Chief Information Security Officer (CISO), the virtual Chief Information Security Officer (vCISO) serves as an executive-level position responsible for protecting the organization's data and assisting with information security governance. As the concept of using a virtual Chief Information Security Officer (vCISO) is relatively new, extant literature of the vCISOs successes and failures is obsolete, but practitioner articles reporting on successful engagements of the vCISO are paving a path forward for academic research.

vCISOs provide SMBs with a wealth of knowledge and experience with industry information security frameworks, Information Security Governance and stay abreast of the most current threat vectors and information security breaches. Furthermore, a vCISO has an equivalent skillset of a CISO, with a team approach's flexibility to meet the SMB's individual requirements. Virtual CISO services help companies concentrate their resources to make the most difference in protecting them against this growing threat. Finally, vCISOs can serve as stand-alone consultants or part of a larger group of virtual security services known as Managed Security Service Providers (MSSP).

II.2.2: Virtual Security Services

The act of outsourcing information technology and information security to virtual team members using third-party vendors is well-studied (Gupta & Zhdanov, 2012; Cezar et al., 2017) and provides illustrative examples of specific successes and failures for organizations employing virtual security services. Gordas (2014) acknowledges a rise in SMBs outsourcing the business's security functions to managed security service providers (MSSPs), and the lack of expertise, staff, resources, and time to handle information security issues has resulted in an evolution of the managed security services (MSS) industry. Managed security services will secure a client

company's infrastructure (Andress, 2001; Weiss & Muegge, 2019), but advanced skills, such as Information Security Governance and strategy development, may not be a managed security services focus. Furthermore, Amaladoss (2001) asserts that an organization should select an MSSP that provides various services to support information security governance's overarching business objective.

Outsourcing information security is not without risks. As MSSPs work with an extensive client population, security services will inevitably not meet every client's demands (Masuda, 2006). Outsourced information security services occur in two separate categories: prevention services and detection services (Cezar et al., 2013). Prevention services involve the deployment of infrastructure control mechanisms with the sole intent of preventing or deterring intrusions. In fact, to provide a cost-effective solution to the organizations, most MSSPs apply a baseline control mitigation plan to all clients, regardless of the client's industry, culture, or business goals (Masuda, 2006). In contrast, detection services utilize an intrusion detection system, such as a Security Incident and Event Monitoring (SIEM) system, to proactively monitor the network for active intrusions or block intrusions, if applicable. However, both services offer benefits as well as additional organizational risks. Furthermore, studies indicate that some security experts have advocated outsourcing prevention and detection to different MSSPs (Cezar et al., 2013) to prevent a single point of failure and minimize insider threats. Additional studies indicate that MSSPs offer various security products and solutions to their clients to achieve the comprehensive protection of their information assets and can be grouped into three main categories: device management, security training, and assessment services (Feng et al., 2019). Moreover, studies indicate that most organizations receive maximum benefits for their information security endeavors if they outsource information security services as part of their overall information security strategy (Gupta &

Zhdanov, 2012). Managed services provide clients with a cost-saving mechanism to overcome constrained budgets and minimal resources. However, the savings are not without the risk of third-party breaches, cookie-cutter solutions, and out-of-the-box information security solutions designed to protect data but not directed toward advancing organizational information governance maturity.

II.3: Information Security Governance

Organization governance is a broad concept where executive management provides strategic direction to the organization while achieving its objectives, mitigating organizational risks, and managing constrained resources effectively and efficiently (Johnston & Hale, 2009). As a subset of organizational governance, Information Security Governance (ISG) is an executive responsibility designed to protect organizational assets from unauthorized access, data loss or destruction, exfiltration, modification, or misuse (Yaokumah & Brown, 2014). Information Security Governance is focused on securing assets through strategic direction and alignment of business practices, with the responsibility solely residing on the Board of Directors and Executive Management (Allen & Westby, 2007). The Information Technology Governance Institute asserts that Information Security Governance provides strategic direction, measures the achievement of objectives, employs risk management practices, responsibly utilizes organizational resources, and monitors the corporate security program (ITGI, 2006). An effective Information Security Governance program's critical factors include executive-level sponsorship and support (Johnston & Hale, 2009), continuous reviews of organizational processes and procedures, and the facilitation of organizational changes to meet new challenges (Ezingeard & Bowen-Schrire, 2007).

Posthumus and Von Solms (2004), identifies two sides of Information Security Governance that contribute to an effective information security strategy. First, the governance component (executive management and the Board of Directors) identifies how executive leaders

focus on information security direction and strategy. This strategic alignment occurs through an information security executive's advice, such as a Chief Information Security Officer (CISO) or a virtual Chief Information Security Officer (vCISO). Next, the management side identifies the procedures required to implement an organization's security strategy, and usually occurs through an information security program's development. The governance program provides SMBs with measurable objectives, employs risk management practices, and manages organizational resources to facilitate an information security program (ITGI, 2006). Similarly, Weill and Ross (2004) indicated that IT governance's goal is to ensure IT investments have an optimal return on investment, ensure progress is measurable, and long-term stakeholder value is achieved, with this concept being vitally crucial for SMBs with constrained resources. Although Information Security Governance responsibilities can be delegated to individuals outside of the C-suite or Board of Directors' purview, information security governance's overall accountability resides with the organization's senior leadership (ISACA, 2010).

II.3.1: Top-down Approach

The information security governance's alignment (ISG) requires three core components (Information Security Strategy, Business Objectives, and Information Security Program) (ITGI, 2006) and requires a top-down approach for a successful Information Security Governance program. A top-down approach begins with the program's executive-level sponsorship and indicates the senior leadership's influence in the Information Security Governance program (Albrechtsen & Hovden, 2010). The International Standards Organization (ISO) asserts that implementing an organizational-wide Information Security Management System (ISMS) to support the governance program requires a top-down approach to enhance the organizations' Information Security Governance program (Humphreys 2016; Gordas, 2012). As identified during

the SMB information security behavior review, SMBs executives focus on growing the business and less on non-revenue generating events. This behavior is detrimental to the success of an Information Security Governance program, and the engagement of virtual leaders will facilitate SMB executives with the opportunity to focus more on revenue-generating events.

II.3.2: Information Security Governance Definitions

ISG definitions vary amongst scholars and practitioners, but the most common attributes, regardless of industry or business size, include a) information security strategy aligned with the business, b) the inclusion of organizational business objectives, and c) the development of an information security program. From an academic perspective, four main definitions identify closely with Information Security Governance within an SMB:

- Gordas (2014) defines governance as the primary supporting tool for aligning business objectives with information security strategies and can be set globally as business management activities in various organizations.
- Moulton and Cole (2003) identifies ISG as the establishment and maintenance of the control environment to manage the risks relating to the confidentiality, integrity, and availability of information and its supporting processes and systems.
- ISG is intended to govern the relationships between the leadership, shareholders, and stakeholders (Ching et al., 2006).
- Governance includes established policies and procedures to assure the IT system of an organization sustains its business strategies (Haes & Grembergen 2004)

From a practitioner's perspective, leading information security organizations have identified several definitions of Information Security Governance that apply directly toward small to midsized businesses.

- The Information Technology Governance Institute (ITGI) defines an Information Security Governance program as one where people, processes, and technology facilitate the strategic alignment of the business objectives and the information security program (ITGI, 2006)
- The process of establishing and maintaining a framework to assure that information security strategies are aligned with and support business objectives and provide an assignment of responsibility (NIST, 2003).
- IT governance is the business's strategic alignment with the business to maximize business value by developing and maintaining effective IT control and accountability, performance management, and risk management (Le, 2013).

Summarizing the definitions into one focus, the underlying intent is that senior leaders must provide direction and strategic alignment for the Information Security Governance program using information security domains as part of the Information Security Governance framework (ITGI, 2006). However, the variance of the definitions on Information Security Governance leads SMB leaders to misinterpret cybersecurity professionals' roles and responsibilities of the organization.

II.3.3: Industry-specific Requirements

Organizations generally fall into two categories: Regulated and non-regulated industries. The primary difference between the two categories is the process of implementing information security governance. Regulated environments must implement a minimum-security protection level using approved Information Security Governance frameworks, whereas non-regulated environments are highly encouraged to adopt information security frameworks. According to Ula, et al., (2011), the most economical method for organizations to achieve a mature Information Security Governance level is to commit to an established Information Security Governance framework. However, Information Security Governance does not recognize universally accepted

models (Williams et al., 2013). Instead, organizations should select a model that enhances and adequately aligns with their industry, business objectives and meets the organization's requirements (Whitman & Mattord, 2013), and should be comprehensive enough to help organizations create an all-inclusive plan for information security (Ula et al., 2011). A correctly selected Information Security Governance framework should facilitate directing and controlling strategic level management directives (Von Solms et al, 2011), both in regulated and non-regulated environments (Abdullah & Valentine, 2009).

Regulated organizations are required to follow specific laws or industry standards to attain information security governance. If a breach occurs in a regulated industry, and a subsequent investigation proves the organization did not follow the required governance frameworks, the offending organization could be fined, regardless of the attack originating from internal or external actors. There are three primary types of regulated environments, and associated frameworks are: healthcare organizations, payment card industry, and federal government systems.

Healthcare organizations are legally required to comply with three Health Insurance Portability and Accountability Act (HIPAA) laws (Privacy Rule, Security Rule, and Breach Notification Rule). Each subsection of the law identifies generalized requirements but is considered vague for SMBs that lack the technical knowledge to understand the requirements. The payment card industry requires organizations to follow industry-specific criteria (PCI/DSS) to be authorized to process payment card data. Unlike the HIPAA law, PCI/DSS is not a law but is an industry-standard created by three prominent credit card vendors (Master Card, Visa, and American Express) and does not include monetary fines for non-compliance. However, the impact of failing to follow the PCI/DSS framework allows payment card organizations the right to refuse the processing of payments and negatively impacts the business goals of SMBs and their associated

business objectives. The final Information Security Governance framework applies only to federal systems but can be used by other industries as a best practice for securing data. The National Institute of Standards and Technology (NIST) provides a series of technical documents, identified as the 800 series, to help federal systems attain Information Security Governance and control mitigation standards. The most common NIST document utilized by industry experts is NIST 800-53 (2003), which identifies 17 control families and provides guidance on implementing control mitigation strategies based on risk identification levels. Although these Information Security Governance frameworks are required for regulated environments, information security organizations provide information security frameworks that can be utilized for regulated and non-regulated organizations.

Non-regulated organizations are not required to follow specific Information Security Governance frameworks, although certain practitioner organizations provide documentation for non-regulated organizations to attain information security governance. Non-regulated organizations have the flexibility to select an Information Security Governance framework that best fits their organizational requirements, as suggested by practitioner organizations, or they can do nothing to protect organizational data.

One practitioner organization, Information Systems Audit and Control Association (ISACA) produced the Control Objectives for Information Technology (COBIT 5) that defines a set of generic IT management processes for all organizations. Each process is defined together with inputs and outputs, significant activities, objectives, performance measures, and an elementary maturity model. A second practitioner organization, International Organization for Standardization (ISO), published ISO 27002, which establishes guidelines and general principles for "initiating, implementing, maintaining, and improving information security management

within an organization. ISO 27002 is an international standard and is recognized worldwide, especially in European countries. Finally, the Information Systems Security Association (ISSA) created the Generally Accepted Information Security Principles (GIASC) to assist with implementing governance from the boardroom (top-down) to the information security professional (bottom-up). The GAISP promotes best practices that will ensure the confidentiality, integrity, and availability of organizational information assets that serve as a primary input into the information security program.

II.4: Information Security Program

The information security program serves as the primary supporting tool for the Information Security Governance program and is required for regulated environments. Technology is a core component of information security program development, but alone, it is not enough to protect an organization from the rising risks of increased cybersecurity attacks (Dutton, 2017). Like the Information Security Governance definitions and frameworks described earlier, information security program's definitions vary slightly, but the program's focus is relatively similar.

- CISOShare (2020) states the information security program describes the foundation as having the intent to define a clear set of repeatable requirements that align program objectives with the organization's business objectives to ensure the protection of confidentiality, integrity, and availability of client and customer data.
- NIST provides documentation for federal systems aimed at improving their cybersecurity posture. The framework provides a common taxonomy and mechanism for organizations to a) describe their current cybersecurity posture; b) describe their target state for cybersecurity; c) identify and prioritize opportunities for improvement within the context

of a continuous and repeatable process; d) assess progress toward the target state; e) communicate among internal and external stakeholders about cybersecurity risks.

- Information Systems Audit and Control Association (COBIT5) identifies three vital objectives for an effective information security program: a) cost of mitigation controls should never exceed the cost of replacing the data or the equipment, b) executive management support is essential, and c) the importance of the IS program aligning with the organization's business objectives (ISACA, 2019). COBIT5 is an industry-accepted framework that provides a methodical approach for organizations to achieve their governance business objectives while managing enterprise IT.
- The Committee of Sponsoring Organizations of the Treadway Commission (COSO) identified a combined method for evaluating an internal control system that management designs intending to achieve reasonable assurance of the fundamental business objectives (Mishra, 2015). COSO describes five domains and 17 subdomains, each focused on internal control appliances (COSO, 2020).

Schneier (2013) pioneered the concept that information security was more than a technology-based mindset but is a combination of information security pillars described as People, Process, and Technology (PPT). Additionally, Dutton (2017) reverberated Schneir's assertation that an information security program is built using the three information security pillars, with ISO 27001, an international standard for information security programs, echoing the same sentiment (ISO, 2013). ISO 27001 further clarifies that an organization must balance all three pillars for a successful information security program (Dutton, 2017; ISO, 2020). Furthermore, Zamman and Razali (2016) identified three factors for a successful information security management program: people, process, and organization. Finally, successful organizations have long-established

investments in people, processes, and technology to combat threats to their corporate assets (Hibbert, 2012). However, most small to midsized businesses only have certain aspects of the three pillars deployed within their infrastructure, if any at all.

II.4.1: People

As discussed earlier, information security is no longer a technical application but affects all organizational components. The pillar "people" is the cornerstone for any organization and refers to any human resource, internal or external, available at the firm's disposal (Khanduri, 2020). Some scholars will argue that people are classified as the weakest link in any information security program (Martins & Eloff, 2006). Nevertheless, organizations cannot survive without people, hence introducing a significant weakness to any information security program (Andress, 2001). Senior leaders must ensure people are a) adequately trained and aware of the security threats to the organization, b) possess the professional skills and qualifications to execute the job for which they were hired, and c) are provided with available resources to complete the assignments provided.

As identified in earlier sections of the literature review, the most significant threat to an SMB is a weak information security culture, where employees are unaware of the information security threats to the organization or the senior leadership's false sense of security in protecting their networks (Nijnik, 2005). Senior leader's attitudes and employee's personal beliefs regarding information security initiatives will generate a positive or negative information security culture within the SMB. Typically, an organization will hire and train employees for a specific skill set to perform their duties but fail to provide additional security awareness training directed towards information security threats (Van Niekerk & Von Solms, 2010), which serve as a critical mitigating factor to threats and vulnerabilities. People are empowered through proper training, and senior

leadership within the SMB structure is accountable for protecting the data the organization hosts (Khanduri, 2020).

Employees possessing unique qualifications should be employed in the organization, especially in SMBs with limited resources. At times, some employees will perform numerous duties, including performing part-time information security functions. At other times, SMBs will outsource daily tasks to third-party providers, such as managed service providers or managed security service providers (Crassula, 2019). Employees, either internal or external, should have clear roles to eliminate wasted SMB resources on duplicating functionalities. Many businesses fall into the trap of concentrating too heavily on processes and technology while ignoring the people who manage them (Khanduri, 2020). The information security principle least privilege and separation of duties are an industry-standard in information security (NIST 800-53, 2003). Employees should only have the minimum level of access to perform their duties (least privilege) and separate individual roles in minimizing internal collusion (separation of duties). Stakeholders must provide proper oversight and resources to ensure that people are adequately prepared to accomplish the positions they were hired to perform, and leaders must enable junior managers to enforce sanctions for policy violations. People are assets and can become an organizational enhancer or detriment, depending on their information security culture.

Finally, SMB leaders must provide the proper resources required to perform their jobs, with skilled people being the scarcest resource for SMBs. Most small to mid-sized businesses (SMBs) lack the people resources needed to build an effective information security program (Lewis et al., 2014) and ultimately become a target for malicious actors (Ključnikov et al., 2019). As summarized by Williams and Manheke (2010), SMBs face the same threats as large organizations but lack the people resources available to large organizations. As the larger

companies can address cybersecurity issues by allocating resources to the information security department (Berry & Berry, 2018), SMBs lack the same opportunity. They must be creative and invest in other measures to achieve the same information security protection level.

II.4.2: Processes

The second information security pillar identified by Dutton (2017) is the organizational processes implemented by the SMB. When viewed holistically as one entire framework, processes are the glue that combines "people" (the who) and "technology" (the what) to assist the SMB with "how" they expect to achieve the business plan's desired results (Khanduri, 2020). Once considered secure, preventative processes are no longer sufficient since cybersecurity threats are continually evolving, and the threat landscape is a moving target (Baskerville, et al., 2014). Processes should define the organization's activities, roles, and documentation used to mitigate information security risks, threats, and activities while mitigating the risk of cyber threats when appropriate. If processes are loosely integrated into the workflow, the possibility of security breaches is enhanced.

Information Security Governance begins with creating policies and procedures (P & P), and organizational processes result from those policies and procedures. Policies are high-level strategic governance documents with executive sponsorship, and procedures are the operational processes required to implement policies. All regulated industries are required to have information security policies and procedures distributed throughout the organization. NIST 800-53, (2003), has seventeen control families that necessitate policy and procedure development to achieve a baseline compliance level. Non-regulated industries are not required by regulated bodies to create policies and procedures. However, the stakeholders can make this a requirement to ensure due diligence is applied within the organization. Regardless of the justification for creating policies and procedures, small and mid-sized businesses must develop and institutionally implement them to

protect data and develop a mature Information Security Governance model that includes repeatable and sustainable processes.

It is difficult for processes to be classified as repeatable and sustainable within the organization without implementing the appropriate policies and procedures. The Project Management Institute (PMI) identifies repeatable processes as ones that produce a set of duplicated actions by numerous employees (PMI, 2020). Furthermore, processes are sustainable if those repeatable actions can be maintained over time (PMI, 2020). The Cybersecurity Maturity Model Certification requires repeatable and sustainable processes, accompanied by metrics to measure improvement or declination (CMMC, 2020). When an organization applies the appropriate processes in its daily workflow, progress is considered measurable and repeatable. Processes that are not repeatable and sustainable are considered ad-hoc and may fail to measure Information Security Governance progress correctly (CMMC, 2020).

When a process is repeatable and sustainable, the SMB has a favorable opportunity to obtain continual improvement within the organizational structure. The concept of continuous improvement is a term used by many to achieve a specific business objective. Continual improvement is an ongoing improvement of products, services, or processes through incremental and breakthrough improvements. Operationally, continuous improvement involves the concept that there are always methods to improve processes to meet the needs, stakeholders, and industry requirements (DOD, 2006).

II.4.3: Technology

The final pillar discussed is the concept of implementing the correct technology within the organization. Technology is a crucial component for information security governance, but technology alone will not solve the issue while attempting to secure data and achieve Information

Security Governance (Rodriguez & Edwards, 2010). Often, organizations will invest in technology first and attempt to mold the people and process pillars to match the technology. Instead, organizational leaders should consider each pillar with equal weight, ensuring people and processes are available to support costly technological investments. Companies that spend a significant amount of money on technology and lack the people and processes to manage or implement the technology correctly cannot visualize the return on investment (ROI), hence minimizing future governance maturity (Rodriguez & Edwards, 2010).

The technology pillar is an equal component in the PPT framework and a subordinate to other pillars at the same time. To properly invest in technological innovations, the SMB must have the skilled staff available to understand and manage the investment. As discussed earlier, SMBs lack the skilled information security employees, technical knowledge, and monetary resources available at larger organizations. Aware of these behaviors, some SMB leaders will still attempt to protect their data by contacting information security technology resellers to acquire technology that may not be prudent to the organization's business goals. Third-party vendors strive to ensure SMB executives become smitten with the latest and greatest information security technology despite the cost, only for the leaders to discover that it does not fit the SMBs needs and business objectives. Finally, implementing technology into an organization without trained personnel, internal or external, can create more harm by exposing the organization to unsuspecting vulnerabilities.

Comparable to the people pillar, SMBs should implement technology that supports the current processes of the SMB. When the implementation of technology occurs before process identification, the organization's changes may negatively affect its workforce. Process designs ensure that technology serves as the cohesive bond to ensure the process works as expected. When

the process is built around the technology, gaps in controls may exist, and maturity growth may be limited. Technologies are implemented after the risk assessment to reduce the cyber threat and effects. The most common technology implemented within an environment is control management (NIST 800-53, 2003). Controls are recommended in all compliance documentation and required for regulated industries and should only be applied when the risk outweighs the control cost.

II.5: Literature Review Summary

The literature review identified four SMB information security behaviors that specifically affect small to mid-sized businesses more than larger organizations within the same industry. First, SMBs lack an executive to sponsor information security governance. The lack of sponsorship is not due to the indifference to information security breaches but relates to the desire of the senior leadership interested in growing the business and generating revenue for future growth. A second SMB behavior was inadequate risk management procedures. Small to mid-sized businesses lack the experience to adequately analyze the risks to their organizations and apply proper risk mitigation procedures to identified risks. The third SMB behavior is the lack of resources that an SMB has available to secure information assets and attain a mature level of information security governance. Finally, SMBs lack the organizational technical skills required to secure organizational requirements and protect data from unauthorized access.

The literature review identified a phenomenon known as virtual executives that can help SMBs mitigate the identified information security behaviors through virtual executives' previous successes and failures. The most referenced virtual executive was the virtual Chief Financial Officer (vCFO), that can perform financial services as an independent consultant, or as a team of accounting professional. Next, the literature identified the virtual Chief Operations Officer (vCOO) as second in command to the CEO. The vCOO has experience within the SMBs industry

and can alleviate time-consuming tasks that senior executives require to grow the businesses. The final virtual executive is the virtual Chief Information Security Officer (vCISO). This information security executive is a recent phenomenon that was not identified in the literature. Although the literature did not indicate the successes and failures of a vCISO working within an SMB, the literature did identify virtual security services, such as a Managed Security Service Provider (MSSP), to solve information security management concerns for the SMB. Information security management is different from information security governance. It focuses more on implementing the information security program and less on the Information Security Governance program's strategic alignment to the organization's business objectives.

Academic research indicates that a successful governance program derives from an information security program that focuses on people, processes, and technology (Dutton, 2017). Furthermore, Information Security Governance is a subset of organizational governance and is an executive responsibility designed to protect organizational assets through strategic direction and business practices. Information Security Governance utilizes a top-down approach with the responsibility solely residing on the Board of Directors and Executive Management. The Information Security Governance program provides SMBs with measurable objectives, employs risk management practices, and manages organizational resources to facilitate an information security program. Moreover, its goal is to ensure IT investments have an optimal return on investment, ensure progress is measurable, and long-term stakeholder value is achieved, with this concept being vitally crucial for SMBs with constrained resources. Finally, Information Security Governance must be utilized in regulated environments and is highly encouraged in non-regulated environments.

The final section of the literature review focused on the development of an information security program. The information security program is the foundation that supports the Information Security Governance program. The program focuses on the proper employment and training of people, deployed organizational processes to measure successes or failures, and technology investment to support the organizational processes. Each component is inter-related and supports each other in a cyclic cycle.

II.6: Research Questions

After an extensive review of published literature and searching the following keywords/phrases (Virtual Chief Information Security Officer, vCISO, Fractional Chief Information Security Officer, or fCISO), the results did not yield academic research utilizing a vCISO within an SMB. As a result of the recent vCISO phenomenon, this study will use an exploratory qualitative, multi-case study research method, with an inductive approach to explore the following:

- What is the role of the vCISO in the SMB?
- How are vCISOs utilized in the SMB?
- Why an SMB employ a vCISO?

After reflecting on the identified concepts reviewed in the literature, the following specific research questions were derived:

1) ***What is the role of the vCISO while addressing the SMB's Information Security Governance maturation.***

2) ***How does an SMB receive value from a vCISO while attempting to achieve a mature Information Security Governance program?***

3) ***How can a vCISO utilize their experience and mentorship to modify the SMB's information security behavior?***

III THEORETICAL FRAMING

III.1: Information Security Governance Domains

To facilitate a more definitive organizational alignment, the Information Technology Governance Institute (2006) introduced five Information Security Governance domains designed to assist executives with a process to maintain alignment of information security governance, organizational business objectives, and the information security program. Boards and executive management must extend governance to information security and provide the leadership, organizational structures, and processes that ensure the SMB sustains and extends its strategies and objectives (ITGI, 2006). By incorporating the five Information Security Governance domains (Strategic Alignment, Value Delivery, Risk Management, Performance Measurement, and Resource Management), SMBs are more likely to achieve organizational objectives, be resilient enough to learn and adapt to emerging threats, judiciously manage the risks it faces, and recognize opportunities that require immediate attention (Yaokumah & Brown, 2014; ITGI, 2006). However, during the initial stages of the information security program development, not all domains may be impacted but will become more defined as the governance matures (NIST 800-171).

III.1.1: Strategic Alignment

Security strategies are used to implement governance and compliance practices, but a strategy developed only to satisfy compliance requirements hinders the security posture's maturation (Le & Hoang, 2017). Strategic alignment is the first information security domain described by Yaokumah & Brown, (2014) and is defined by the organizational business objectives and mission. The relationship between strategic alignment and the four other governance domains were empirically tested, with strategic alignment significantly related to all other domains (Yaokumah & Brown, 2014). According to ISO/IEC 38500, information technology’s strategic alignment with the business achieves maximum value by developing and maintaining adequate controls and

accountability, performance management, and risk management (Lee, 2013). Moreover, the General Strategic Alignment Theory (Henderson & Venkatraman, 1993) advocates that strategic alignment is achieved when the organization coordinates business objectives, values, and needs according to the business strategy (Rocha et al., 2014). Information security is the gatekeeper of protecting data, and governance cannot be achieved without proper strategic alignment of the information security program and business objectives (ISACA, 2010). To ensure organizational activities are strategically aligned and practically attainable for the organization, the security strategy should encompass current information security capabilities, future security initiatives and include the people and technology to meet business needs (Yaokumah & Brown, 2014). Before implementing a security strategy or security program, leaders must understand how information security benefits the organization's strategic alignment (ITGI, 2006). ITGI (2006) further identifies four principles in the strategic alignment domain.

- Ensure all information security program expenditures align with business objectives. The actualization of program expenditures is challenging to value when the allocated security initiatives are not aligned to the business objectives.
- The information security program should align directly with the enterprise's operational focus, supporting the business processes and information security initiatives to function as one cohesive unit.
- The alignment of the information security strategy and the enterprise strategy is essential for governance maturity. The information security strategy is the foundation from which the information security program is built, and alignment at the enterprise/department levels is required for seamless interoperability.

- Ensure that all activities' alignment (department-level and enterprise-level) function as one cohesive unit to provide a competitive advantage over peer organizations within the respective industry.

III.1.2: Value Delivery

Value delivery focuses on the value that the information security program provides to the organization. The term value can assume many forms, but for this study, value occurs when security investments are adequately managed (Hardy, 2006). Moreover, executive leaders must invest in information security investments that demonstrate value for the investment, decrease wasteful spending, improve services, and enhance the stakeholders' confidence level for protecting data (Gregor et al., 2006; Kobelsky et al., 2008; Yaokumah & Brown, 2014). ITGI (2006) identifies four principles in the value delivery domain. First, the information security program must provide measurable feedback to the organization. Second, the program must achieve the desired results as outlined in the information security strategic plan. Next, the program should provide quality output, which is essential to measure progress. Finally, the program should provide the desired output on time and within budget constraints. Value delivery within the organization will continue to evolve as the information security program and governance matures. Changes in value require executive leaders to continuously monitor value metrics to ensure value creation and business effectiveness are sustained (Damianides, 2005). Value delivery is complex because the value obtained by one stakeholder may not always be of value to another. However, existing, and future information security investments must provide value for effective Information Security Governance (Parker, 2005). For this study, value is determined from the actualized benefits described by SMBs during a vCISO engagement.

III.1.3: Risk Management

Risk management is the foundation of any Information Security Governance program. By not correctly identifying the risks associated with the business objectives, leaders will not know what data to protect or how to protect them, resulting in allocating funds without clear direction (Banham, 2017). According to the NIST 800 series technical publications, risk management's primary objective is to ensure that risks are identified and mitigated according to the organization's risk appetite. A risk appetite is defined as the level of risk that an organization is prepared to accept to pursue its objectives before action is deemed necessary to reduce the risk (NIST 800-39, 2011). Furthermore, risk identification and mitigation influence organizations to make conscious efforts to minimize anticipated risks (managing risks) or face the agent's possible failure (Yaokumah & Brown, 2014). Risk management aims to mitigate identified risks to reduce adverse impacts on the organization at a satisfactory level (risk appetite) acceptable to executive leaders (Bonabeau, 2007) and when it meets an organization’s security expectations and defined objectives (ITGI, 2006).

According to NIST 800-39, a risk analysis can be performed qualitatively by using data to determine the impact of the risk versus a likelihood of occurrence, or quantitatively, by using numbers to calculate the annual loss expectancy (ALE) of an incident. A qualitative risk analysis is subjective, meaning the risk analysis is based on an educated guess, focusing on identifying risks to measure both the likelihood of a specific risk event and its impact on the overall organization. Results are then recorded in a risk assessment matrix to communicate risks to stakeholders. Alternatively, a quantitative risk analysis is objective and uses verifiable data to analyze the effects of risk in terms of monetary value. Quantitative risk analysis assigns a numerical value to risks and is entirely dependent upon the data's quantity and accuracy. The risk analysis's end state

determines a risk approach for identified risks, intending to reduce the risk to an acceptable level (NIST 800-39, 2011).

ITGI (2006) identifies three possible options for identified risks. First, the organization can accept the risk and take no further action. Acceptance of risk is to identify and acknowledge the risk and monitor it for changes. Next, the organization can mitigate the risk, which is a significant component of the information security program. After identifying the organization's information security threats, the organization must have plans to mitigate those threats. Different techniques and methods are deployed to face threats and reduce the impact of information security risk. Risk mitigation can assume many forms, but the most popular mitigation plan is implementing an information technology control framework, such as NIST 800-53. The final risk approach is to transfer the risk. Some organizations will identify risks as too costly to mitigate or too necessary to accept; in this case, an organization may decide to transfer the risk, as in purchase cyber insurance, to defer costs associated with a cybersecurity breach.

III.1.4: Performance Measurement

Performance management, also known as continuous monitoring, focuses on measuring the adequacy of security controls, policies and procedures, and the security investments within an information security program, and facilitates executive decision-making and improve performance and accountability through the collection, analysis, and reporting of performance-related data (NIST 800-55, 2008). Performance is measured in various ways, but consistently improving performance measurements by evaluating key performance indicators (KPIs) indicates a positive correlation between the Information Security Governance and the organizational business objectives (Lee, 2013). ITGI (2003) defines performance measurement as organizational set goals and benchmarks that can measure the Information Security Governance and the impact on business

objectives. Furthermore, NIST identifies four essential factors of performance measurement (NIST 800-55).

- The measure must yield quantifiable information.
- Data that supports the measurement must be easily obtainable.
- Only repeatable information security processes should be considered for measurement.
- Measures must be valid for tracking performance and directing resources.

NIST 800-55 identifies four benefits for performance measurement. First is an increase in accountability for employee actions and security technology investments. Next, performance measurement improves the effectiveness of information security by quantifying progress in strategic goals and objectives. Thirdly, it helps to demonstrate compliance by the implementation and maintenance of an information security measurement program. Finally, performance management can serve as quantifiable data for recommending resource allocations for the organization.

Accurate data collection must be a priority with stakeholders and users if the collected data is meaningful in improving the overall information security program and evaluated by the degree by which results are achieved (NIST 800-55, 2008). As the information security program matures, policies become more detailed and documented, processes are more standardized and repeatable, and produces reliable performance measurement data (NIST 800-55, 2008). Without measurable statistics for the information security program, SMBs may not visualize the actualized return on investment of their security expenditures.

III.1.5: Resource Management

Resource management appropriately allocates resources to business units to assist with the adherence of business goals and the subsequent management of those resources to ensure value is

delivered. Resource management has four principles identified by ITGI (2003). The first principle is to ensure the organization identifies, prioritizes, and allocates resources to ensure the information security program correctly supports the business objectives. Next is the adherence to a strict lifecycle processing plan that manages the lifecycle of hardware, software contracts, and permanent and contracted human resources. Lifecycle maintenance is a crucial component of resource management to optimize resources and avoid unnecessary costs. Thirdly is the organization of resources. Properly organizing the resources prevent waste and ensure budgets are appropriately allocated for replacement or repair. Finally, SMBs must monitor and evaluate internal and outsourced IT services to maximize the use and validity of the resource charges to the organization. The monitoring of outsourced IT services usually occurs through a service level agreement (SLA), a contractually binding agreement identifying the services provided by a third-party. This principle is overly vital to SMBs that do not employ an "in-house" IT department but decide to outsource these requirements to a Managed Service Provider (MSP). Resource management is applied to organization activities where executive leaders appropriate a balanced number of resources and employees with trained skills to manage information security projects and activities (Hardy, 2006). As discussed during the threats to SMBs, resources are limited in SMBs, and having funds or employees to invest in Information Security Governance properly is a vital component for success.

III.2: Theoretical Framing Summary

Ensuring Information Security Governance alignment to the five ISG domains is crucial for a small to mid-sized business's success. If the alignment does not occur, information security behaviors may not be modified, and valuable resources could be wasted. Strategic alignment coordinates the business goals derived from executive leadership with the Information Security

Governance goals. This strategic alignment produces value delivery for the organization by appropriately measuring the information security investments, ensuring resources are appropriately allocated, and measuring critical business functions' performance. Risk management is an Information Security Governance domain and an SMB security behavior. For governance to be successful and mature over time, risk management must be foremost in the business owner's mind. When risk management is an ad-hoc process and not part of the daily operations, risks can be quickly introduced into the environment without sufficient controls to mitigate unanticipated risks due to new business processes. If organizations maintain a risk-averse posture, unanticipated risks are minimized because new business processes are carefully evaluated before being deployed in the environment. As discovered during the synthesis of the available literature, the SMB information security behaviors and information security domains are not aligned by previous studies. SMB’s that are focused on ensuring Information Security Governance must have a proper alignment to ensure their behaviors positively relate to the five information security domains.

IV RESEARCH DESIGN AND METHODOLOGY

IV.1: Exploratory, Qualitative, and Multi-case Approach

An exploratory case study seeks to find answers to the questions “who” or “what” and is used when the set of outcomes has numerous possibilities (Dudovskiy, 2019). Additionally, Myers (2013) identified an exploratory research method as appropriate when the primary motivation is to discover and explore a recent phenomenon and accompanies additional data collection methods, such as interviews, questionnaires, experiments, and historical records (Dudovskiy, 2019). The case study is appropriate because a case study is an empirical method investigating the phenomenon in-depth and within a real-world context (Yin, 2018).

The advantages of using a case study are a) the ability to collect robust data, b) the analysis is specifically focused on the phenomenon, c) the integration of qualitative and quantitative data in the analysis, e) and the ability to capture intricacies of real-life situations to obtain a deeper understanding of the phenomenon (Dudovskiy, 2019). Yin (2018) defined three conditions for the proper use of a case study. First, the purpose of the research question must be to determine how or why a phenomenon exists. Next, the researcher does not have control over the events that have taken place. Finally, the focus of the research must be on a current phenomenon within a real-life context.

This qualitative study utilizes two approaches. First, in-depth interviews were conducted with six virtual Chief Information Security Officers (vCISOs) to explore the perceived advantages of using a vCISO to assist SMBs while protecting their data, assets, and intellectual property while attempting to achieve an Information Security Governance maturity level acceptable to the organization. Next, in-depth interviews were conducted with fourteen SMB leaders that used a vCISO for at least one year to explore the actualized value received from the vCISO. This approach

allowed study participants the opportunity to articulate the advantages or disadvantages of using a vCISO within their respective environments.

Inductive research begins with the observation of a phenomenon (more specific) and culminates with a theory (more general) based on those observations (Miessler, 2020). Inductive approaches are generally used for theory building (Glaser & Strauss, 1967), but is also relevant for exploratory case studies since it supports conceptual thinking and theory building rather than empirical testing of the theory (Kahn, 2014). Gray (2009) suggested that deductive reasoning aims for hypothesis testing based on empirical data, whereas inductive reasoning constructs generalizations, relationships, and theories by analyzing the data collected. Finally, inductive reasoning does not prove a conclusion but instead predicts an outcome; it does not create a definite answer for the phenomenon but demonstrates that the outcome is the most probable one given the phenomenon. Based on the above pragmatic points, an exploratory case study using inductive reasoning is valid for this research.

IV.2: Cases and Participants Selection Strategy

The unit of analysis is the individual, and the SMB cases included participants from small and mid-sized businesses, regulated and non-regulated environments (Table 4). The research participant selection schematics' goal was to ensure that the population representativeness of all interview participants was generalizable across several industries. Specifically, vCISO recruitment occurred from professional networking sites, such as LinkedIn, information security groups, active vCISO organizations, and personal information security contacts. SMB case recruitment occurred similarly as the vCISO recruitment, except that SMB study participants had a more definitive scope to meet specific qualifying criteria: a) the SMB must have used a vCISO or be currently using a vCISO for at least one year; b) the study participants must have direct knowledge and involvement

in the vCISO recruitment and subsequent management of vCISO services; c) the study participant must be an employee of the organization before and after the vCISO engagement; d) the SMB must have the criteria as defined by Gartner (2020) to be classified as a small or mid-sized business. A total of 450 recruitment emails/phone invitations were sent to possible SMB participants requesting participation in the study. In total, 80% (360) of the respondents indicated that they did not require information security services, 12% (54) indicated they did not use virtual information security services but relied on internal or external IT technicians to secure their data, and 8% (36) indicated they would be interested in participating in the study. Of the 36 interviewed participants, 15 did not use vCISO services but outsourced to a third-party security provider. Of the remaining 21 participants, four did not use a vCISO for at least one year, one was not an employee before vCISO services were engaged, and two were not involved in the vCISO selection and engagement services. Finally, 14 SMB participants met the identified study requirements and were selected for the study.

Table 4: Interview Matrix

Firm Size	Regulated	Non-regulated
Small	3	2
Medium	6	3

IV.3: Development of the Interview Protocol

There were two interview protocols used in the study (Appendix A), with the question development based on the analysis of the literature review. The first interview, SMB Interview Protocol, was focused on four sections: Background, Motivation for the Selection (Why), Patterns and Processes (How), and Benefits (Outcome). The second interview, vCISO Interview Protocol, was focused on four sections: Background, vCISO Employment, vCISO Services, and

Benefits (Outcome). Both sets of questions were open-ended to allow for the participants to fully explain the vCISO engagement process.

IV.4: Study Participant Demographics

Study participants were provided with a de-identified six-digit number to protect the participant's identity and interview notes. The first two digits represented the case number, followed by two digits to indicate the type of organization (regulatory, non-regulatory, or vCISO service), and the final two digits were to identify the level of responsibility of the employee (Table 5). The study participants' demographics are distinguished by two categories: vCISO and SMBs (Tables 6 and 7).

Table 5: Participant Assignment Numbers

Identification Number	Explanation
First two digits	• Represents case number • 01 for case 1; 02 for case 2; 03 for case 3.
Second two digits	• 01 SMBs with regulatory requirements • 02 SMBs without regulatory requirements • 03 vCISOs with regulatory experience • 04 vCISOs without regulatory experience
Third two digits	• 01 for C-level employee • 02 for mid-level managers • 03 vCISO employee

Table 6: vCISO Demographics

Participant Number	Role	CISO Experience	vCISO Experience	Regulatory Experience	Advanced Certifications	vCISO Engagements
02	vCISO	8 years	5 years	Yes	CISSP	30-40
03	vCISO	20 year	4 years	Yes	CISSP	6
05	vCISO	10 years	1.5 years	Yes	CISSP	40

06	vCISO	25 years	6 years	Yes	CISSP, CISM	25
09	vCISO	20 years	10 years	Yes	CISSP, GPEN	80-90
13	vCISO	20 years	5 years	Yes	CISSP	50+

After compiling the six vCISOs demographics, the interviewees had 17.6 average years of experience as a CISO and 103 years of combined CISO experience. The vCISO with the fewest years of experience as a CISO was eight years. However, although this interviewee did not have a decade or more as a CISO, they had more than 20 years of information security experience while serving in the military. Overall, the interviewees averaged 5.25 years of experience as a vCISO and a combination of 251 engagements over ten years. Each vCISO had at least one senior-level information security certification, and all contained experience working in heavily regulated environments.

Table 7: SMB Demographics

Participant Number	Role	Business Size	Regulated	vCISO Utilization	Industry
01	HIPAA Privacy Officer	Mid	Yes	4 years	Healthcare
04	CEO	Mid	Yes	5 years	Government
07	Director of Information Technology	Mid	Yes	2 years	Education
11	Chief Strategy Officer	Mid	Yes	2 years	Business Process Outsourcing
12	Chief Operations Officer	Mid	Yes	3 years	Healthcare
16	Director of Technology Services	Mid	Yes	2 years	Healthcare
10	Business Development Manager	Mid	No	3 years	Information Technology

15	Managed Services Executive	Mid	No	5 years	Information Technology
20	Chief Information Officer	Mid	No	6 years	Real Estate
08	Senior Director of IT	Small	Yes	4 years	Sports Entertainment
14	Senior Auditor	Small	Yes	3 years	Financial Accounting
19	Director of Accounting	Small	Yes	4 years	Financial Accounting
17	Senior Attorney	Small	No	3 years	Law
18	President/CEO	Small	No	3 years	Business Development

The SMB interviewees consisted of numerous industries, both regulated and non-regulated environments. In total, there were 14 SMB interviews completed. Of the 14, six were regulated mid-sized companies; three were non-regulated mid-sized companies; three were regulated small companies, and two were non-regulated small companies. Cumulatively, the 14 SMBs have a total of 49 years of vCISO utilization, with one SMB utilizing more than one vCISO.

IV.5: Data Collection

Information provided in the interviews was kept confidential, and data identifying an individual source during the analysis did not occur. The interview protocol was a semi-structured interview but resembled guided conversations. This approach is more suitable for case studies (Yin, 2018) and yielded flexibility for the study participants' exploration of the topic. vCISO interviews averaged 45 minutes and focused on the engagement process with the SMB and the engagement deliverables. The SMB interviews lasted about one hour and began by discussing the

SMB's security behaviors pre-vCISO employment, culminating with the role of the vCISO during the client engagement.

To ensure the individual's privacy and protect the vCISO and SMB participants' confidentiality, the researcher conducted each interview remotely using secured third-party software with the interviewer and interviewee as individual participants. All interviews were digitally transcribed, and audio and written transcripts were saved to a secure network drive, password-protected, and secured by a firewall. Information regarding the research and interview procedure was communicated through a generic email address explicitly for this study. Before conducting the interview, each participant was requested to consent, both verbally and in written format, that the interviewee read and agreed to the informed consent form.

IV.6: Data Analysis

Information security requirements vary across industries, regulatory requirements, and organizational mandates. Although these varying requirements exist, SMBs continually strive to protect organizational assets and data while increasing the Information Security Governance program's maturity. The data analysis from this study did not occur from a single methodology but employed a qualitative analytical process to analyze the data using NVIVO 12 for Windows. The qualitative research approach provides the tools required to interact directly with industry experts allowing the researcher to gain new insights into the role (Yin, 2016).

Meyers (2013) describes a bottom-up approach when analyzing data that has an inductive research approach. A bottom-up approach is a method to analyze the data from the bottom without the use of preconceived coding schematics or propositions (Meyers, 2013, pg. 166). Since previous research on the SMB utilization of vCISOs was sparse, the bottom-up approach will allow concepts to emerge from the data.

The study was also designed using a multi-case approach to facilitate a cross-case synthesis and a within-case analysis (Yin, 2018). To ensure themes were captured appropriately, the interviews were analyzed in different phases beginning with the vCISO participants followed by the SMB participants. The first phase included the first-level analysis to identify chunks of data that were coded into NVIVO nodes. The second phase included a higher-level analysis to group the first-level nodes into categories and develop a coding scheme. The final phase was to identify themes based on the second-level coding, where theme creation was easily attainable. Due to the limited availability of secondary or historical data, the data analysis only included participant interviews.

The analysis was conducted using Meyers's (2013) analytical approach to verify the data's literal or theoretical replication. As defined by Yin, 2018, a literal replication predicts similar results, and a theoretical replication predicts contrasting results but for anticipatable reasons (Yin, 2018, pg. 55). Each analysis phase implemented the three concurrent flows of activity (1) data condensation, (2) data display, and (3) concluding/verification., as defined by Miles et al., (2014). Data condensation refers to the process of selecting, focusing, simplifying, abstracting, and transforming the data that appear in the full corpus (body) of written-up field notes, interview transcripts, documents, and other empirical materials (Miles et al., 2014). Condensing the data is designed to make the data clearer so that conclusions can be drawn and verified (Miles et al., 2014: 12). Upon completing each phase, the data was condensed and displayed in an excel table that permitted conclusion drawing and theme development (Miles et al., 2014). Finally, drawing and verifying conclusions involved identifying and noting patterns, explanations, causal flows, and propositions (Miles et al., 2014). The conclusions were verified for validity, testing for plausibility, sturdiness, and confirmability (Miles et al., 2014).

Miles (2014) indicates that consistency in coding is achieved when the inter-rater reliability (IRR) check is 85% to 90% of the coded data. The inter-rater reliability check was completed after the second-level coding (phase 2) and before theme development (phase 3), with three random transcripts and the coding scheme provided to two additional qualitative coders. Each interview was coded independently using NVIVO 12 and analyzed using the coding comparison function in NVIVO. Upon completion of the inter-rater reliability checks, themes were developed based on the second-level analysis. The identified themes and inter-rater reliability results are identified in Tables 8 (vCISO analysis) and 9 (SMB analysis).

Table 8: Inter-rater Reliability Results for vCISO interviews

vCISO Themes	Codes Identified	Codes Matched	Percentage Matched
1. vCISOs are equipped to identify information security as a business problem and provides a business solution.	18	16	88%
2. Active SMB leadership involvement is the key to a successful engagement.	14	14	100%
3. vCISOs provide a depth of knowledge on information security threats.	27	26	96%
4. vCISOs offer SMBs a cost-effective, experienced, and flexible team approach to information security governance.	22	19	86%
5. vCISOs provide a framework for continual process improvement, growth, and Information Security Governance maturity.	5	5	100%
6. Information security program development is the key to protecting data.	10	10	100%
Inter-rater Reliability (IRR)	**96**	**90**	**93.75%**

Table 9: Inter-rater Reliability Results for SMB interviews

SMB Themes	Codes Identified	Codes Matched	Percentage Matched
1. vCISOs provide value to the organization by the services offered.	31	29	93%
2. SMBs are more aware of the risks to the organization.	8	8	100%

3. Information security program refinement or development is enhanced by the utilization of a vCISO.	13	12	99%
4. SMBs have a long-term information security officer with strategic and technical abilities.	7	5	86%
5. vCISOs provided an information security and governance program that is realistic, attainable and aligned with its business goals.	14	13	92%
6. vCISOs experience serves as a mentor to SMB leaders and employees.	9	8	88%
Inter-rater Reliability (IRR)	**82**	**75**	**91.4%**

V EMPIRICAL OBSERVATIONS

V.1: vCISO Thematic Overview

The detailed analysis produced several themes from the perspective of the vCISO and the actualized gains from SMB leadership teams. The six vCISO interviews identified 92 categories in the first level coding, defined as nodes in NVIVO. The second-level coding grouped the first-level nodes into nine different categories, from which six themes related to the three research questions were derived (Table 10).

Table 10: vCISO Themes

vCISO Themes
1. vCISOs are equipped to identify information security as a business problem and provide a business solution.
2. Active SMB leadership involvement is the key to a successful engagement.
3. vCISOs provide a depth of knowledge on information security threats.
4. vCISOs offer SMBs a cost-effective, experienced, and flexible team approach to information security governance.
5. vCISOs provide a framework for continual process improvement, growth, and Information Security Governance maturity.
6. Information security program development is the key to protecting data.

V.2: vCISO Theme Analysis

1: vCISOs are equipped to identify information security as a business problem and provide a business solution.

Environments, where information security was isolated to information technology, is an idea of the past. Security is a business problem that affects the entire organization. The interviewees discussed that SMBs are at a tipping point where the vCISOs witness a clear-cut business reason why SMB leaders want to improve their cybersecurity capabilities. One possible reason identified by the interviewees was that SMBs have business partnerships with third-party

entities. When third-party business processing is a vital component of an SMBs success, one must ensure that they protect a business partner's data and their own. According to one vCISO,

> Our goal is to start turning their heads away from just looking at technology and start looking at the business because the business aspect of what they are doing will inform and drive what they buy for technologies and not the other way around (vCISO 2)

As the interviewees' conversation developed, numerous vCISOs indicated that the ability to speak to clients in the business language is the key to a successful relationship. One vCISO stated, "To fully understand information security and how it affects the business, we must include language that is meaningful to executives" (vCISO 13). Similarly, another vCISO indicated, "Because of the approach that we are using, we use business language, a business approach, and business documentation, which is getting the attention of the C level and the Board of Directors" (vCISO 5). Furthermore, articulating the integration of technology with the business is essential. "I have done quite a few board-level presentations, and one of the things I learned was that if you want the business to be involved, you need to speak in business language" (vCISO 6). Finally, another vCISO interviewee succinctly summarized the importance of information security as a business focus. "If you do not speak in business language, they are not going to listen to you" (vCISO 9).

1.1: Brand reputation is at stake. SMBs strive hard to maintain brand recognition in their desired industry. By not aligning the business with information security, catastrophic results can occur during an information security breach. When organizations view information security as a business problem that requires a business solution, stakeholders view information security initiatives as a business necessity instead of a business indulgence. In contrast, when information security is an isolated function of IT, a breach may be magnified and affect the organization's

brand, customer confidence, and trustworthiness. Succinctly stated, “It takes 20 years to build a reputation and a few minutes to destroy it” (vCISO 5).

2: Active SMB leadership involvement is the key to a successful engagement.

During the interviews, all six vCISOs discussed the importance of senior leadership involvement as key to a successful engagement. Senior leadership involvement in information security decisions is significant, as leaders can delegate the tasks, but the accountability and responsibility remain within their realm as leadership teams. Several vCISOs went one step further and stated for the protection of themselves and the organization, the initial sales call and expectation discussion would only occur with the executive leadership teams. As one vCISO discussed regarding leadership involvement:

> Our initial interactions primarily involve stakeholders, [the business owner, the CEO, CFO COO], someone where cybersecurity falls on their shoulders or their responsibility. From there, we will work with the local IT team or managed service provider to determine if gaps exist in the security matrix (vCISO 3)

2.1: Leader involvement in successful and unsuccessful engagements. To further understand the leadership involvement in a vCISO engagement, the interviewees were asked to differentiate between a successful engagement and an unsuccessful engagement. A successful engagement generated an in-depth discussion with each of the vCISOs. Similarities amongst the interviewees described a successful engagement as one where all parties know the criteria for success and where the SMBs understand that success is best viewed from the eyes of the SMB. Additionally, another vCISO discussed a successful experience when the senior leaders are wholly engaged in the process and involved from the start. Finally, a vCSIO with over 20-years in the industry recalled a successful engagement as one where leadership teams show an interest in

protecting information assets because they “want to do it, instead of having to do it.” Succinctly stated from another interviewee:

> One of the most successful experiences I have seen over the past ten years as a vCISO are the leaders that come forward to us after having attended a conference and realized that they need to get a handle on this security stuff (vCISO 9)

As with successful engagements, there are those projects that were not viewed favorably in the eyes of the vCISOs. The most prevalent type of negative engagement discussed was when the leadership is not fully invested and only wants a “check the block” assessment or accreditation for a business venture with a larger company. The interviewees are invested in the mindset that security is an essential function of the operational business activities and should be treated with as much respect as any other business initiative. The following reflects three sentiments from study participants about unsuccessful vCISO engagements:

> Unfortunately, dealing with these earlier stage startups in our business, some customers do not actually care about security. They have got a deal with Target or NASCAR or Disney or some large corporation. That corporation is putting them through a due diligence process on security and business practice, and they want to check the boxes and get through the thing. They have not achieved buy-in or understanding of the importance of security (vCISO 2)

Likewise, another vCISO stated, “There have certainly been cases where customers come back to me and say, Oh, this is a lot of stuff. I thought you guys were the easy way” (vCISO 3).

Finally,

> We conducted a penetration test on an organization because they needed that as part of their security proof. The SMBs customer wanted to see a clean bill of health for a

> penetration test conducted within the last six months. We found several vulnerabilities, and those were met with a bit of disdain. The following email received is that the SMB has fixed that already and would like us to take that off the report (vCISO 13)

2.2: Leader involvement in organizational change management. The final section discussed with the vCISOs is the senior leadership involvement is how an organization reacts to changes brought forth by the vCISO. Changes to the organization's infrastructure, including security enhancements, require employees to accept the changes (known as receiving buy-in from the employees). When a vCISO engages with a client, changes must occur to ensure the proper growth in Information Security Governance maturity. The interviewees discussed the importance of organizational leadership and how it can positively or negatively influence an organization's information security culture. According to one interviewee:

> Effective leadership is a top-down approach, and the employee's attitude towards information security is directly related to the leadership's disposition. Suppose a leader integrates security into their daily business processes and refers to it as a business function. In that case, employees will believe that it is an integral part of their daily operations (vCISO 9)

3: vCISOs provide a depth of knowledge on information security threats.

A familiar premise indicates that some SMB leaders have a sense of urgency to protect organizational data because they fear that external actors will attack them. Simultaneously, others do not believe their businesses offer anything to attackers, and larger businesses are more lucrative for hostile actors. Unethical hackers and malicious insiders are aware of this mentality and attempt to exploit this false sense of security for their advancement. To further complicate the risk that SMBs face, attackers know that limited resources will prevent the SMB from adequately protecting

the data and maintain a mature level of Information Security Governance required by the industry. Numerous vCISOs discussed several instances where a hostile actor used the SMB as a pivot point to attack a larger organization, based on the trust relationship between the SMB and the larger entity. The goal of a vCISO is to educate the SMB leadership teams on the risks that, if exploited, could be detrimental to the organization's survival. The education process begins during the SMB expectation discussion to identify SMB resources available to secure the infrastructure and attain the desired governance maturity level. As annotated by one vCISO,

> SMBs that are positioned in the business-to-business space [they] are stepping stones into these larger organizations. This compelling business reason is why we see many SMBs starting to realize that they need to improve their security leadership capabilities. These larger organizations are saying you need to be able to prove to us that you have a cybersecurity program place; you need to be able to prove to us that you have someone in a leadership position that is taking care of this and owning this (vCISO 2)

However, when viewed holistically, SMB threats are not marginalized based on their size. In fact, many vCISOs felt the SMB size was more detrimental to securing the data than larger organizations because the information security landscape changes daily, and SMBs do not have the wherewithal to maintain a defensive posture against new threats. When queried about the limited resources of SMBs, the interviewees concurred that information security is an expensive investment but is one of necessity rather than convenience. The overwhelming sentiment towards SMB resources was that “In smaller organizations, [they] generally lack the budget, technical knowledge, sophistication, and governance to protect themselves from attackers” (vCISO 5). Additionally, another vCISO interviewee indicated that “The small business attribute that makes it attractive from the hackers' perspective is that large organizations have more resources in

security" (vCISO 3). Finally, some vCISOs indicated that, during discussions with SMB leaders, a false sense of security is expressed. Some SMBs are willing to accept the risk of being breached based on their organization's idea that an attacker would not desire to obtain their data. Spending valuable resources to protect something that is not desirable to others is futile. This idea could not be farther from the truth, and as indicated by one vCISO, "When leaders do not prioritize information security, this same attitude will persist throughout the organizations. It is our job as vCISOs to ensure that the idea of why they would hack me is stopped" (vCISO 13). The virtual CISOs works with all types of organizations, from small to large, regulated, and non-regulated. They are involved in designing security programs, both small and big, while staying abreast of the constant security landscape changes. This wealth of knowledge, vast industry experience, and subject matter expertise provide the vCISO with the skills necessary to assist SMB leadership teams in making informed security investment decisions.

4: vCISOs offer SMBs a cost-effective, experienced, and flexible team approach to information security governance.

Virtual CISOs are more than just ad-hoc, temporary employees to serve as an SMB consultant. Instead, vCISOs offer many years of experience, both in a regulated and non-regulated environment, within various industries, both small and large organizations. The interviewees discussed how a vCISO could provide cost-effective security advice for a fraction of the cost of a full-time CISO. Additionally, some vCISOs offer a flexible, multi-tiered approach accompanied by industry expert teams to meet all information technology and security requirements as a one-stop-shop. When viewed holistically, the six vCISOs interviewed agreed that vCISO services support industry-recognized frameworks, with their vast experience facilitating the ability to tailor information security initiatives to the SMB's individual, organizational requirements.

Categorizing the average for the six interviewees, the breadth of knowledge and experience the vCISOs presents is unequivocally years beyond what an SMB can afford with minimal resources. As one vCISO stated,

> We work with several clients simultaneously, many in different industries. Hiring a vCISO with five years of experience but supporting clients from various industries is similar to hiring a CISO with 30 years of experience, assuming they change industries every few years (vCISO 9)

4.1: Flexible team approach. However, no two vCISOs had the same approach to managing client engagements. Some virtual CISOs worked independently and provided consultation and strategic support for SMBs with their local IT teams. In contrast, other virtual CISOs were part of a larger information technology team, known as a Managed Services Provider (MSP), and provided vCISO services as part of an MSP support package. One virtual CISO focused strictly on risk management and control mitigation to address identified risks, while another focused on network and application-level security. Another virtual CISO focused on vulnerability management and penetration testing, while another specialized in governance, risk, and compliance (GRC). Each vCISO identified as having access to a team of specialists to help mitigate urgent issues occurring within the SMB. Sometimes, this team of specialists worked internally in the same vCISO organization or externally through shared MSP connections. The point identified by the interviewees is that SMBs have flexibility in selecting a vCISO that specializes most closely with their organizational requirements. When requested to elaborate on the meaning of the team approach for SMBs, one vCISO responded,

> I work as a team of tier professionals. I work as part of a team and oversee what the team is doing compared to what the customer requires. The customer has an extended security

team using our services, and I provide that oversight for the combined set of teams that we have with the customer (vCISO 2)

4.2: Cost-effective approach. The final section of this theme was the cost-effectiveness of using a vCISO rather than employing a full-time CISO and security team. The team of professionals involved in the vCISO experience has individual and team specialties that most individuals cannot obtain by themselves. Not only are SMBs engaging with an experienced CISO, but the SMB also has a team of specialized professionals at their disposal. As one vCISO responded, "It is like hiring a Chief Information Security Officer and an entire team of specialists, which will cost at least $500,000 in pay and benefits" (vCISO 13).

The interviewees discussed utilizing a tiered approach to services offered. SMB leadership teams could purchase individual security options à la carte (services that SMBs could afford on a limited budget) or engage in multi-year full-spectrum information security services. One interviewee stated that an individual risk management/risk mitigation service started at $3,000 per location, while another interviewee offered full-spectrum information security services for $10,000 a month. Some vCISO services provide a monthly amount of consulting hours, identified as buckets, per month at a set price, with each vCISO identifying a different number of hours per bucket, but generally, they were separated into three basic categories: 20 hours a month, 40 hours a month, and 70 hours a month. However, there is always a break-even point where it is more cost-effective for an SMB to hire an internal CISO to manage their systems. When calculating the cost-effectiveness of hiring a virtual or in-house CISO, one interviewee indicated that if an SMB requires vCISO services for more than 70 hours a month, the SMB should invest in hiring an in-house CISO. Regardless of the approach selected by the SMB, the benefit of an experienced team

of virtual security professionals available to engage with the organization far outweighs the cost of employing a full-time security team with limited budget and resources.

5: vCISOs provide a framework for continual process improvement, growth, and Information Security Governance maturity.

As described by the interviewees, Information Security Governance is not a one-and-done task. It is an organizational growth process of hiring the right people, developing the right processes, and investing in the right technology. Governance requires an organization to follow regulatory requirements or industry best practices. It is measured by a five-level maturity model that projects organizational maturity throughout a lifecycle of maturity and program development. To achieve a mature Information Security Governance program, [an organization] "must understand the requirements and fully invest in a path where governance aligns with the organizational business objectives, or future efforts will be futile." (vCISO 13). Without governance, the proper tools, and security management, SMBs will introduce a wide variety of sporadic vulnerabilities and a lack of organizational consistency.

Governance programs rely heavily on requirements by which organizations must abide. While non-regulated SMBs are not required to follow legal, regulatory requirements, such as HIPAA and PCI/DSS, they still have a fiduciary responsibility to protect information assets and data to better the organization, the customers, and its stakeholders. Regulatory requirements can be troublesome for immature governance programs. As one vCISO stated,

> I think it is the mammoth of regulation that's coming down on them. It is outside of their control, and if SMBs do not have a realistic plan to meet that compliance within their financial boundaries, it could bankrupt and put these people out of business (vCISO 5)

Virtual CISOs are equipped with the knowledge and experience to help guide the SMB through the regulated restrictions, government oversight, and numerous reporting requirements required to have a mature governance program. As a program begins to mature, SMB leadership teams, through the assistance of the vCISO mentorship process, can fully understand the stringent requirements of operating within a regulated industry. Furthermore, during initial vCISO engagements, SMBs are encouraged to achieve attainable maturity levels through industry-recognized frameworks instead of maturity maximization.

5.1: Information Security Governance frameworks. Governance is measured using industry-approved frameworks and is essential to measure growth and demonstrate sustained progress. The vCISOs interviewed use numerous frameworks for their clients, but the frameworks identified are based on best practices of the five-level maturity model known as the Capability Maturity Model (CMM). The CMM was developed in 1986 to manage software developments, with the term maturity focusing on the degree of formality and optimization of processes and procedures. Maturity models utilize well-known control frameworks to measure maturity from level 1 (ad-hoc processes) to level 5 (optimized processes). The vCISOs discussed that 95% of SMBs will always begin with a level 1 maturity unless they had previous information security expertise within the organization. The interviewees agreed that an SMBs goal is to obtain a maturity level 3 (defined) within the organization's budgetary constraints. However, this maturity progress does not occur overnight. Maturity is a methodical, deliberate process that is a component of the security strategy defined in a compliance roadmap. As one vCISO indicated,

> After the initial assessment, if an SMB is at a maturity level of 1.6, we define the steps required for advancement to a possible 2.8 in 12 months. The steps are projects with subtasks that need to be completed. We provide oversight, resources, and guidance to

> achieve the desired result. For some SMBs, they want to jump right in and purchase the Ferrari. Instead, we help focus them on getting their Toyota Corrola up and running. Moving towards the Ferrari is all part of the maturity process. As crucial as it is, governance maturity can also be overly quantified, especially when the SMB is new to cybersecurity. We do not want to scare them off; we want to start with the basics and not over-complicate stuff (vCISO 2)

5.2: Security strategy alignment. The starting point of any governance program is to define the desired goal or security strategy for the organization. If a strategy is not clearly defined, SMBs can be easily lost in the overwhelming requirements, and motivation will quickly decline. Each vCISO interviewed had a different opinion on the most optimal length of a security strategy. For the SMBs that engaged with vCISOs on more extended contracts (2-5 years), strategies developed were long-term and encompassed annual milestones. For shorter vCISO engagements or project-based engagements, SMBs were placed on quarterly strategies, also known as a roadmap to compliance. However, before diving directly into strategy development, all six interviewees confirmed that a gap assessment must be created as a baseline document to determine the current maturity level and identify compliance concerns. As one vCISO emphasized, “The gap analysis analyzes the network’s infrastructure, information system assets, policies/procedures, and risk management process” (vCISO 13). Likewise, another vCISO classified their gap assessment as phase one of any engagement project. “It is our baseline assessment because SMBs have never measured their cybersecurity maturity capabilities against an industry framework” (vCISO 6).

Upon identifying the organizational gaps, the interviewees stated they met with the executive team to define its short-term or long-term security strategy. According to one vCISO, “this is not our strategy. This is part of the organization’s mission, and they must be an integral

part of the development process and fully invest in the strategy for it to be successful." (vCISO 5). The strategy is a focused document that identifies the current maturity level, identified gaps, and guides future information security initiatives to reduce gaps and increase governance maturity. Although the strategy is an essential component of a governance program, it only serves as a guide to help the SMBs attain the desired Information Security Governance level. The security strategy must be hardwired to the information security program, which is the foundation for achieving an organization's desired level of governance maturity.

6: Information security program development is the key to protecting data

With the excessive amount of frameworks available to measure growth and maturity, Information Security Governance is only a title without an information security program, and it must align with organizational business objectives to be successful. When any organizational program misaligns with the business objectives, it is a recipe for disaster. The organization grows based on the business objectives, and the information security program is designed to support those business objectives. However, after discussing the importance of business objectives with the vCISOs, numerous interviewees indicated that SMBs lacked robust business objectives. In fact, no interviewees indicated that previous engagements contained information security objectives that were aligned to the business objectives. The high importance placed on the business objectives alignment was further described by one vCISO, "As part of our intake process. Before we even talk about security, we spend part of the first hour or two understanding their business acumen and objectives" (vCISO 3). Also, another vCISO had a similar perspective.

> We need to understand the business vertical itself and where they see themselves sitting within that vertical. We want to understand whom the SMB considers their nearest competitors and what differentiates them from the others. We look at the objectives to

> determine the business drivers and map that to the risks they perceive from a cybersecurity perspective. The initial engagement is more around their business risks than specific cybersecurity controls (vCISO 9)

The business objectives are the primary driver for the security strategy and information program development, but the risk management process guides the information security program's direction.

6.1: Holistic risk management. A risk management plan is a subset of the information security program and is applied throughout the organization. Risk management consists of two main deliverables: risk analysis and risk mitigation. The risk analysis holistically views the entire environment and identifies anticipated risks to the organization. A deliverable from the risk analysis, the risk management plan is designed to mitigate identified risks and monitor risk reduction in the organization. This approach, known as a risk-based approach, was emphasized during all the vCISO interviews. As discussed, one primary focus during a client engagement is to mentor SMB leadership teams on utilizing a risk-based approach in their daily business functions. As one vCISO identified, “If an organization does not know what risks they face, how will they know what to protect?” (vCISO 9).

This comment was echoed through the interviews, with all vCISOs indicating that the risk-based approach was the most appropriate action item in developing the information security program. However, some interviewees also suggested implementing a risk-based approach was the most challenging part of a client engagement. When queried further, the interviewees indicated that during the earlier stages of the client relationship, SMB leadership teams display difficulties accepting that risk management should be viewed holistically throughout the organization and is not siloed within information technology. As one vCISO stated,

> Initially, some of our clients think of risks as only affecting the bottom-line profits. If the risk is listed as possibly occurring, it is not worth spending money on. We spend much time ensuring that clients understand risks come in all shapes and sizes, and some risks are difficult to quantify numerically. It is our job to change this mentality (vCISO 2)

The vCISOs indicated that the two main deliverables used to develop the information security program are the security strategy and the gap assessment. Like governance, the interviewees indicated they utilize several control frameworks to develop an information security program, depending on the organization's size, respective industry, and business objectives. Each framework has a specific purpose, and with consultation from the vCISOs, SMB leaders can make an educated decision on the control framework utilized the build the information security program. The most common type of risk mitigation is through the deployment of controls. Control mitigation allows an organization to mitigate identified risks through industry-recognized frameworks. A strong sentiment from a vCISO interviewed was, “SMBs should adopt one framework and allow the organization to mature through that framework” (vCISO 9). All control frameworks begin with creating policies and procedures (P and P) as the starting point for any information security program. Policies are the big picture statement and include formal guidance to coordinate and execute activity throughout the institution. They are high-level strategic governance documents with executive sponsorship. Procedures are the operational processes required to implement institutional policy. Policies and procedures are the cornerstone of the information security program and help define its governance maturity level. According to another interviewee, “Without one, the other will never be successful.” (vCISO 13).

6.2: People, processes, and technology. Finally, an information security program cannot fully mature without having the correct people employed, defined processes in place, and

investments in technology (PPT) to enhance the organization's security posture. According to our interviewees, PPT is the foundation of the information security program and subsequent governance maturity. It is practically impossible to build a program without first ensuring PPT is adequately addressed. Generally speaking, the interviewees agreed that enhancing the organization's PPT is their responsibility but buy-in from the organization's leaders and employees is crucial for the proper implementation. Executive leaders must employ adequate people resources (either internally or externally), enforce documented procedures, especially those that enhance governance maturity, and invest in technology that will adequately secure organizational assets and protect data from malicious actors. Summarized by numerous vCISOs,

> Information security program development is a set of mini projects. We analyze the business objectives, strategy, and gaps. We assign a maturity level and begin a project plan by defining milestones and objectives. We walk the SMB through the entire process. It is a very hands-on approach. (vCISO 2)

V.3: SMB Thematic Overview

The detailed analysis produced several themes from the perspective of the SMB, as indicated by the actualized gains from SMB leadership teams. The 14 SMB interviews identified 82 categories in the first level coding, defined as nodes in NVIVO. The second-level coding grouped the first-level nodes into 12 separate categories, from which six themes related to the three research questions were derived (Table 11).

Table 111: SMB Themes

SMB Themes
1. vCISOs provide value to the organization by the services offered.
2. vCISOs ensure the SMB is more aware of the risks to the organization.
3. The utilization of a vCISO enhances an information security program's refinement or development.
4. vCISOs provide SMBs with a long-term information security officer with strategic and technical abilities.
5. vCISOs provided an information security and governance program that is realistic, attainable and aligned with its business goals.
6. vCISOs experience serves as a mentor to SMB leaders and employees.

V.4: SMB Theme Analysis

1: vCISOs provide value to the organization by the services offered.

The receiver's reality defines what one considers value, and each SMB leader interviewed discussed the value received through the utilization of a vCISO. Every benefit described by the interviewees adds value to the organization. However, one category quickly surpassed all other values discussed, and that was the monetary value saved while utilizing the vCISO services. Every interviewee provided examples of the cost of hiring a CISO or a security team. These examples were followed with the SMB not having available capital to fill those positions or settle for someone with less experience at a lower salary. One example provided by an interviewee stated, "I was able to get an entire security team, and an experienced CISO for less than 100k a year through the vCISO company" (SMB 17). Likewise, another SMB executive stated, "I think outsourcing security oversight through a virtual or fractional Chief Information Security Officer is wonderful. You get the same capabilities as a full-time, experienced CISO, but less cost." (SMB 12).

A security team cost to the organization can be exorbitant, depending on the regulatory requirements the organization must maintain. Another interviewee indicated the lack of skilled individuals available for the salary they could afford. “We tried for six months to hire a senior security analyst or a CISO. We found two individuals we liked but only had $86,000 for an annual salary. Neither one accepted the job offer.” (SMB 1).

Additionally, some interviewees suggested they went without hiring a CISO because the cost was over the allocated budget or decided to do the job themselves to save money. According to one interviewee:

> I have seen many organizations look at the cost and the expense of hiring a CISO and then make their decision, the unfortunate decision to go without it, instead of leveraging the services like a vCISO service. We regretfully were one of those companies (SMB 15)

Also, another SMB executive stated:

> We decided the cost was too much to hire a security person, so I temporarily performed the job. It worked out well for the short-term, but I became overwhelmed, and it fell to the lower rung of priorities. We hired a junior analyst and provided a salary that was within our budget constraints. A year later, we were hit with ransomware, and it cost us a ton of money in regulatory fines, and all our data was lost. Hindsight being 20/20, we would have saved money by going with vCISO services from the start (SMB 20)

Likewise, another SMB leader stated, “The challenge for an organization like ours, the cost associated with having a full-time CISO is very cost-prohibitive.” (SMB 7).

Hiring an internal security team might affect the IT department’s overall budget and hinder future security initiatives or upgrades to the infrastructure. Summarized succinctly by an interviewee,

> If I had to bring those skillsets in-house, it would be costly, and that is a cost that the organization does not want to carry right now. Organizations would have to pay the cost for the benefits, those ancillary costs right along with salary. If it is being outsourced or not a part of the organization, those costs are not a factor. If you bring those costs in-house, it tilts the view of the IT expenditures differently (SMB 8)

Finally, hiring an internal security employee has indirect costs of which some SMB leaders are not aware. Publicly available sites, such as Indeed, charge a fee to post positions on its job board. Conducting on-site interviews requires the interview panel to take time away from their regular duties. Conducting reference and background checks has a fee for the service. The unanticipated costs are alleviated when an organization hires a vCISO. One interview stated they saved several hundred dollars in background checks by hiring a vCISO team instead of an internal security team. To summarize the value obtained by selecting a vCISO service to manage the organization's security requirements, one SMB executive summarized, "When budgets are stretched, a penny saved is a penny earned." (SMB 4).

2: vCISOs ensure the SMB is more aware of the risks to the organization.

Another issue identified during the literature synthesis was that SMBs were unaware of the organization's information security risks. However, when this topic was discussed during the interviews, it was evident that SMB leadership understood the risks to the business risks better after the vCISO engagement. Interviewees were adamant that the vCISO services helped them and their employees be more self-aware about security risks and threats directed to the organization. As one interviewee stated,

> Before the vCISO started, we did not understand how vulnerable we are to technology. Now, we understand that we have the same threats as anyone else. Just because we are a

> mid-sized business does not mean our data is less critical. We have phishing emails, attacks from foreign countries, theft of equipment, and so forth. You name it, we face it (SMB 10)

Furthermore, another SMB director stated:

> I am more educated now than before. We face breaches originating from phishing emails, hostile actors trying to access our internal network, SQL server breaches, stuff like that. I do not see that we have any more or fewer threats than larger organizations. Our data is still important, and if released into the wrong hands, it could be detrimental. When you talk about security threats, I think they can be grouped into two categories: internal and external. We have both kinds, and it is crucial to remain vigilant (SMB 20)

2.1. Training and awareness to reduce risks. During the interviews, a predominant discussion was phishing emails, designed to trick users into providing authentication information (username and passwords). As indicated by one interviewee, "We have had phishing incidences where emails have been hacked, like our CEO's email was hacked once, and started sending out emails to people under his name" (SMB 1). Although the interviewees understood phishing emails' intent, it appeared essential to the interviewees that phishing awareness and awareness of other security threats were vital for business success.

During a discussion of awareness training, respondents indicated that security awareness training was a part of the vCISO services. For the most part, the interviewees identified that all employees receive awareness training on an annual basis. Furthermore, in conjunction with the vCISO, one interviewee went further and required role-based training for their employees.

> We started with the same annual training for our employees. Our vCISO recommended we conduct training based on specific roles in the organization. We modified our approach, and our regular employees now receive basic awareness training; IT people receive

> technical training, and leadership receives targeted executive training. Each program is different and has a more targeted focus. It works out really well (SMB 16)

Another SMB leader mentioned that his vCISO conducts live training and provides the SMB with a quarterly newsletter highlighting security trends. Finally, to remain vigilant in the threat landscape, interviewees agreed that it was essential to maintain a proactive security culture instead of a reactive approach to incidents. One interviewee stated,

> One thing the vCISO did was to partner with the high trust cyber threat exchange program. They share all the threats coming to the healthcare industry, and we wanted to participate in that. The forum showed some spyware and configuration issues and ransomware that were new threats. We were prepared to react to new threats, which is very important (SMB 16)

3: The utilization of a vCISO enhances an information security program's refinement or development.

The SMBs interviewed were obtained from a variety of industries with varying levels of Information Security Governance requirements. Some interviewees (10) did not have a security program before the vCISO employment, and others (4) required refinement of a current security program. The information security programs ranged from creating a complete program, including all control recommendations from the CIS Top 20, to implementing specific action items to enhance the program's security posture. As one interviewee stated about the creation of a new program. "We did not have a program in place before the vCISO came aboard. That was part of the contract, was for the vCISO to help us establish a program" (SMB 17). Moreover, another SMB leader discussed the refinement of an existing program in progress when their security manager left the organization.

> Our previous security and compliance manager created a basic program. But he was only one person, and the program was pretty basic. The virtual CISO took our program to a whole new level and created a roadmap for us to be more compliant. He took our program and expanded it to meet our growing needs (SMB 16)

Other programs originated from the gap analysis results by providing recommended improvements to the SMB leadership teams.

> They began by reviewing the HIPAA security rule and the CIS Top 20 controls. Any gaps identified were implemented, and we followed up to make sure it was completed. For example, we had annual security training. The HIPAA Security Rule says everyone must have annual security training, even management. That was a gap. So, we had to revamp the training to include managers." (SMB 12)

The interviewees discussed that the program development or refinement was a conversation, with each party being an active participant in the program's creation. According to one SMB executive, "We never felt like the vCISO was dictating to us. Instead, we felt like part of a team, with input being bi-directional" (SMB 19).

Finally, the interviewees discussed that the process was continual with quarterly updates and reassessments. Some interviewees discussed how the implementation was a slow, gradual process, which was more comfortable for the employees to digest. In contrast, other interviewees characterized program development as many small projects. Both approaches received high approval ratings from the leaders and staff, eager to continue maturing the program. Summarizing program development by one SMB executive,

> We used an iterative process that evaluated all components of the organization, and it is still an ongoing process. We began by looking at compliance frameworks and evaluating

> our current maturity level. Our vCISO used the CIS security controls and evaluated our systems using three buckets: people, processes, and technology. First, we evaluated the people involved in our organization, including other third-party providers. We wanted to ensure that we had the right people in the right places. Unfortunately, we had to move on from one MSP because we found systems that had not been patched in over two years, and we had employee resources not adequately utilized. As a result, we revamped the individuals involved with our IT team and third-party vendors, saving us enough funds to cover 60% of the vCISO services. From there, we reviewed all the processes in place to determine what we were and were not doing. I have over 20 years of IT experience and am very confident in my knowledge. However, when viewed from the lens of a security professional, our processes were lacking. Finally, we evaluated our technology and determined that we had much work to secure our technology. As I said, this was an iterative process. As something changed, we re-evaluated the other buckets to ensure we did not have unexpected reactions to the changes. Once the initial evaluation was complete, and we knew our maturity level, we began revising our policies and procedures, implementing security awareness training and strategic operations, such as roadmaps and strategic planning (SMB 7)

4: vCISOs provide SMBs with a long-term information security officer with strategic and technical abilities.

A concern indicated by the interviewees was the lack of qualified security personnel available within the confines of an SMBs limited budget or the high turnover of security employees. However, during the interviews, the SMB leaders discussed how this concern was

alleviated with the engagement of a vCISO. When queried about the selection process of a vCISO, the SMB leader stated:

> We interview the vCISO, just like they were a regular employee. If we did not like them or think there could be an issue with personality or experience, we would interview another vCISO. It is our money, and we prioritize our selection that best fits our organization (SMB 4)

SMBs do not consider vCISOs as an outside entity. In fact, over 75% of the SMB leaders considered a vCISO an integral part of the team and a senior strategic leader for the organization. When further queried about the perception of the vCISO from the employees outside of the executive team, the respondents indicated that most employees consider the vCISO part of the organization. As discussed during the interviews, the senior information security leader should possess the organization's required technical skills but have the business knowledge to represent information security as a business initiative. As indicated by one SMB leader, “We were looking for the resources, skill set, but the requirement was specifically construed as a senior position or a senior leadership position within the organization” (SMB 4). Likewise, another SMB executive indicated, “Our vCISO provided us with quarterly status presentations and briefed the board of directors at our annual meeting. His business knowledge about the industry and our organization impressed the board and the CEO.” (SMB 16). Finally, another SMB executive identified his interactions with the vCISO as neo-strategic, where external partners assist with strategic organizational solutions.

> Virtual CISO is neo-strategic, where you can have strategic solutions but use external partners that can help make decisions. The SMB does not have to commit to many

> resources to accomplish the strategic goals. This changes the scope of the business by using virtual security officers and MSPs (SMB 11)

4.1: High-turnover rate minimized. A final consideration within this theme was the high-turnover rate of internal security team members. Information security has a negative employment rate, meaning there are not enough skilled personnel to meet the growing demand. Interviewees discussed that it could take up to a year to hire and inculcate a new information security leader into the organization, only to see them leave after 18 months for a higher paying job. This high turnover can prove deadly for some organizations fighting to stay afloat in a competitive industry. As stated by one SMB Director,

> It took us eight months to hire a skilled Information Security Manager, but she left after a few years for a higher paying job. As the only security employee in the company, we were left unprotected with unmanaged devices (SMB 16)

The issue of high turnover is alleviated with security organizations that offer vCISO services. The depth of vCISOs within some larger security organizations offer a long-term option for SMBs and provides flexibility for SMB leaders to select a security leader that fits well with the organizational culture. On occasion, a vCISO does not match the organization's culture, and organizations must consider alternative options. A sentiment from one SMB executive indicated the contracted security organization efficiently resolved a cultural mismatch.

> We had a vCISO that worked for a security organization. The vCISO left the company, and after a reasonable transition period, we were assigned a new vCISO. However, the new relationship was not easy to forge, and the replacement vCISO did not work out as we expected. The security firm provided the SMB with a list of available vCISOs, and the

> SMB was allowed to select a new vCISO that best fit the mission, requirements, and culture (SMB 4)

A similar example from another SMB leader indicated that their vCISO left the security organization to start a vCISO company. After attempting to work with other vCISOs of the larger security organization, the SMB decided to discontinue the contract and re-contract with the original vCISO, as the bond they built was indispensable. As summarized by this interviewee, "We had options, and we decided to stay with the old vCISO at his new company" (SMB 14).

5: vCISOs provided an information security and governance program that is realistic, attainable, and aligned with its business goals.

Information Security Governance and compliance is not something an organization is but a concept of something an organization has. Furthermore, Information Security Governance is not attainable without implementing an information security program in conjunction with organizational business objectives. However, the myriad of regulatory requirements, stakeholder mandates, limited resources, and customer concerns create an environment where some SMBs selectively decide to forego achieving governance and focus on revenue generation. These sentiments were similar to the SMB interviewed for the study pre-vCISO engagement but utterly contrary to post-vCISO engagement. The most ubiquitous discissions yielded how the information security program and governance adapted from becoming a nuisance to a manageable and desirable state of being. The vCISO ensured the SMB teams were aware of the requirements and implemented a roadmap utilizing small projects with associated milestones. SMBs indicated they were receptive to the change and excited about the opportunity. Directly relating this success to the vCISO's ability to frame the idea of program development and governance maturity in a positive light. According to one SMB leader,

> After the first meeting, I was running for the hills. I thought there was no way we could ever achieve governance. To my surprise, the vCISO divided the security program requirements into small chunks. Before I knew it, we went from a maturity score of 1.3 to 2.1 (SMB 17)

As noted by another SMB leader, "We were doing the right things; we just lacked formalization." (SMB 18).

5.1: Information security program development. Often, information security programs were more challenging to develop. Most SMBs interviewed discussed that they did not have an existing program in place. Creating an information security program and subsequent governance maturity was a slow, methodical process for those ten interviewees. This process began with mitigating high-risk areas while planning additional mitigations in future quarters using a roadmap as a guideline for budgetary purposes. As indicated by one interviewee,

> It is an ongoing program. When we partnered with the vCISO, we developed a speedy basic program focused on protecting our business and customers. We continue to develop that and continue to integrate that into our overall program. For us, it is an ongoing evolution as we continue to move up the value chain with our vCISO (SMB 12)

A similar perspective from another SMB leader concurred that a program is not a single document but is a set of documents, processes, and procedures that continuously evolves.

> We continue to evolve. From our perspective, we see evolution and integration as a larger MSP would have. We see ourselves as evolving into a single managed service provider that provides security, and that is with the help of vCISO (SMB 15)

Another interviewee discussed how implementing technology into a non-existent program revealed vulnerabilities not previously discovered.

> We lacked technology, so our initial goal was to provide visibility into our network. This approach identified additional risks that we did not know existed. The virtual CISO had to re-do the strategy and make some changes. Keeping the organization aligned strategically and balancing risk were among the benefits of that engagement (SMB 18)

Finally, interviewees described instances where the vCISO did not approach the engagement with a list of tools that the SMB must purchase. Instead, the vCISO enhanced the organization's current processes and technology and, with input from the SMBs, created a roadmap with designated goals to strengthen weak areas. According to one respondent, "We, the vCISO and myself, did a fairly exhaustive job of setting forward our goals, expected outcomes, and measurable success criteria" (SMB 20).

6: vCISOs experience serves as a mentor to SMB leaders and employees.

The final theme identified in the SMB interviews was the mentorship provided by the vCISO. The interviewees discussed the desire to learn more to manage information security as part of the long-term organizational plans. When queried about the mentorship received during an engagement, 100% of the interviewees responded favorably that the vCISOs spent a considerable amount of time mentoring SMB leaders. Definitions of mentoring contained varying meanings from the interviewees, but a standard idea was imparting knowledge and experience to leave the organization with a more focused security posture. One interviewee is a Managed Service Provider (MSP) and receives vCISO services to enhance his organizational security and provides vCISO services as part of a package to clients. This interviewee stated, "The vCISO service is mentoring me as a client but is also mentoring our clients as well. It is a tiered effect where everyone receives enhanced services" (SMB 15). Moreover, another vCISO indicated that his company has grown from the interactions with the vCISO.

> The level of respect our employees have for the vCISO is impressive. He treats us like people and not as another client providing a paycheck. He speaks to the employees like they have known each other for years, attends our monthly lunches, and conducts live training. He has taught us so much in 18 months (SMB 17)

Finally, another SMB executive discussed a situation where he utilized vCISO services more than 70 hours a month, and the vCISO recommended they hire an internal CISO. According to the interviewee, “The vCISO helped us create a job description, calculate compensation, and participated in the first-level interviews. We do not consider our vCISO to be a third-party provider. We have a lifelong friendship” (SMB 12).

V.5: Summary of Findings

The interviews produced findings that supported the research questions identified for the study and yielded numerous propositions for further discussion and possible future research.

V.5.1: Proposed Process Model and Propositions

Client engagements are individually crafted to fit the specialized requirements and constraints of each SMB. However, based on the vCISOs and SMB executives' interviews, most client engagements follow a similar process from start to finish. (see Figure 1). The client engagement process model includes seven stages and is designed to provide practitioners and vCISOs a model to attain Information Security Governance within the SMB domain.

Proposition 1: vCISOs have the experience to understand the SMB's business acumen and transform Information Security Governance into a business solution for the entire organization.

The first stage of the process model is the expectations stage and is the most crucial stage in the client engagement process. During this stage, the SMB leadership teams and vCISOs meet

to discuss the stakeholder requirements, SMB constraints, length of the engagement, perceived benefits of the engagement, and the identified objectives (expectations). As discussed during the interviews, information security is not a technical issue but is a business investment that must be managed as a business focus. To accurately manage a business solution, vCISOs must convey information security in business terminology that the board of directors, executives, and employees will understand. Moreover, vCISOs can produce executive-level reports on a scheduled basis or ad-hoc as needed for the SMB.

Proposition 2: vCISOs possess a substantial amount of experience in differing industries, organizational sizes, and governance frameworks to assist SMBs with organizational strategic alignment.

The second phase of the process model is the alignment of the organizational strategies with the business operations. This phase is the most comprehensive stage of the client engagement process and aligns all business elements to best support the fulfillment of the SMBs long-term goals. As direct input from the expectations meeting, the SMB and vCISOs, align the business objectives and the engagement expectations to form an overall strategic focus for the organization. As identified during the analysis, vCISOs have experience developing information security and governance programs in numerous industries, regardless of the organization's size. Furthermore, vCISOs provide a wealth of knowledge on the different governance frameworks and facilitate a strategic information security plan with executive leadership teams. Finally, vCISOs have the mutual respect with their clients to facilitate a conversation on organization maturity and concern areas that may require future mitigation.

Proposition 3: vCISOs employ a risk-based approach to solving information security problems.

The third phase of the process model is the development of the security strategy. The security strategy receives direct input from the organizational strategic alignment and forms the basis of the information security program. During this phase, vCISOs employ a risk-based approach to solve information security issues by conducting a holistic risk assessment and gap analysis against an identified framework. The risk-based approach provides the SMB leadership teams with the requisite knowledge to decide current and future security investments and is inclusive of all anticipated risks to the organization. Furthermore, the risk-based approach enables the SMB culture to be more information security conscious and proactive to threats instead of reactive. The gap assessment recognizes areas of weakness from the selected framework identified during the second phase of the model. The gap analysis, in conjunction with the risk analysis are used as an input into the security strategy geared towards the development of the information security program.

Proposition 4: vCISOs provide the SMB with strategic and technical abilities, a team approach, and flexible services that are adjustable based on the requirements of the SMB.

The fourth phase of the process model is the creation and deployment of an iterative information security program based on the SMB's security strategy utilizing the strategic and technical abilities of the vCISO. The information security program receives guidance from the information security strategy and is used as the foundation to measure the organization's Information Security Governance maturation. The information security program focuses on ensuring that the proper people are assigned to the SMB, processes are in place to measure performance and maturity, and technology is implemented to managed identified weaknesses. SMBs discussed the importance of working with the vCISO to ensure value is achieved from the view of the SMB. This value was attributed to the vCISO possessing strategic and technical skills,

the option to employ a team of specialists, as needed, and services that are flexible and adjusted to the SMB's requirements and budget constraints.

Proposition 5: vCISOs can provide SMBs with sustained cost-savings by aligning the Information Security Governance domains to the Organizational Strategic Objectives and Information Security Program.

The fifth phase of the process model aligns the Information Security Governance domains in the model to provide sustained cost-saving benefits for the SMB. Upon deployment of the information security program, a process of governance maturity and performance measurability utilizing the five Information Security Governance domains is undertaken. As identified by Yakomah and Brown (2014), strategic alignment is the foundation to which all other domains are related. The alignment is between information security governance, the information security program, and the Organizational Strategic Alignment. As maturity progresses, each item is updated to reflect the most current maturity level of the organization. Value is achieved individually at the firm level, with the vCISOs and SMBs indicating monetary cost-savings were during the client engagement. During the interviews, the most prominent value discussed was the monetary savings the SMBs achieved by outsourcing the organization's security function through the vCISO.

The sixth proposition provides a measurable return on investment for information security initiatives Value, identified as actualized benefits in the process model, can be identified as monetary or non-monetary, and was discovered during numerous phases of the study.

Proposition 6: vCISOs provide a measurable return on investment for all information security investments.

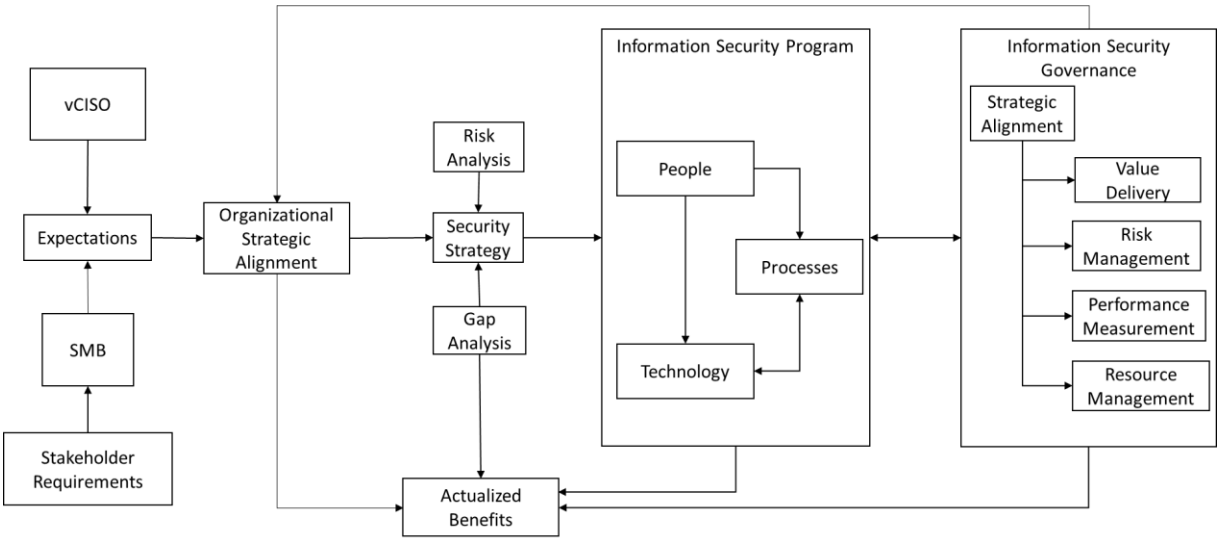
The sixth phase of the process model creates sustained value, either monetary or non-monetary, throughout the model. Security investments are problematic expenditures for SMBs on a constrained budget. vCISOs and SMBs indicated several examples of how squandered funds, poorly managed security investments, and wasted people resources attributed to a decline in the

information security posture. SMB leadership teams acknowledged that vCISOs are an information security executive that provides long-term sustainability for each organization. The Organizational Strategic Alignment creates non-monetary value by the alignment of the organizational business objectives to the information security goals. The security strategy provides both types of value as unnecessary resources are identified and eliminated, and risks are identified and mitigated. The information security program provides value by implementing a governance framework that properly implements people, processes and technology. Finally, Information Security Governance provides many forms of value through each of the five domains, with some domains providing interrelated value to others.

Proposition 7: vCISOs provide SMBs with a proven methodology to measure governance maturity and a process to assist the SMB with governance maturation within the confines of the SMB's allocated resources.

The final phase of the process model provides a vCISO methodology that works in all industries, regardless of size or regulatory requirements. However, no two engagements are always the same. The methodology is designed from the lessons learned throughout numerous vCISO engagements and validated by the SMB’s experiences identified during the interviews. vCISOs execute a governance methodology that is proven to be successful during other engagements. Additionally, vCISOs provide lessons learned, positive or negative, to their clients on other organizations' information security initiatives. SMBs verbalized that the approach used by the vCISO was project-based and contained governance roadmaps for planning and budgeting purposes. Finally, SMBs can further the governance process with the mentorship of the vCISO and measure sustained governance progress and maturity.

Figure 1: Proposed vCISO Engagement Process Model



VI DISCUSSION, CONTRIBUTIONS, LIMITATIONS, FUTURE RESEARCH, AND CONCLUSION

As discussed during the literature review, small and mid-sized businesses (SMBs) have the same types of information security threats as large companies. Some scholars argue that smaller companies have a more considerable disadvantage in protecting information assets and achieving information security governance. Research indicates that SMBs have four primary concerns (senior management role, risk management, resource management, and technical skills) that present major security concerns for their organizations and hinder the opportunity to appropriately protect information assets. These concerns create an opportunity for hostile actors to expose the vulnerabilities of an SMB and steal vital data or serve as a pivot point for larger-scale attacks. Without immediate attention to mitigate threats and secure the infrastructure, a successful attack on an SMB could be detrimental to the organization's survival.

Information Security Governance (ISG) aims to protect data from unauthorized access, loss, destruction, disclosure, modification, or misuse (Tassabehji, 2005). Furthermore, Gordas (2014) defines governance as the primary supporting tool for aligning business objectives with information security strategies in regulated and non-regulated industries (Abdullah & Valentine, 2009). Alternatively, the Information Technology Governance Institute (ITGI) defines an Information Security Governance program as one where people, processes, and technology facilitate the strategic alignment of the business objectives and the information security program (ITGI, 2006) and is intended to govern the relationships between the leadership, shareholders, and stakeholders (Ching, et al., 2006). However, Information Security Governance within the SMB is not easily forged, and research does not provide a solution for SMBs to achieve governance while working within the SMB's budget and time constraints.

The purpose of this research was to explore how a virtual Chief Information Security Officer (vCISO) can overcome the security behaviors identified by researchers and assist SMBs to attain information security governance, protect organizational resources, and add value to the organization. The discussion chapter closes the gap by aligning the four SMB areas of concern identified in the literature (executive-level sponsorship, apathetic risk management procedures, constrained resources, and non-existent technical skills) with the five Information Security Governance domains identified by ITGI (2006) (strategic alignment, value delivery, risk management, performance measurement, and resource management) and answers the following three research questions:

1) What is the role of the vCISO while addressing the SMB's Information Security Governance maturation.

2) How does an SMB receive value from a vCISO while attempting to achieve a mature Information Security Governance program?

3) How can a vCISO utilize their experience and mentorship to modify the SMB's information security behavior?

VI.1: Discussion

The Information Security Governance domains are designed to streamline the governance process for organizations with little experience. The vCISO helps the SMB identify deficiencies related to the domains and select a path to correct each deficiency. Moreover, the vCISO provides a strategic direction for the SMB to align current business processes with the governance domains to mature the entire organization. The final proposition asserts that vCISOs have the experience to align the five Information Security Governance domains with the SMB security behaviors to

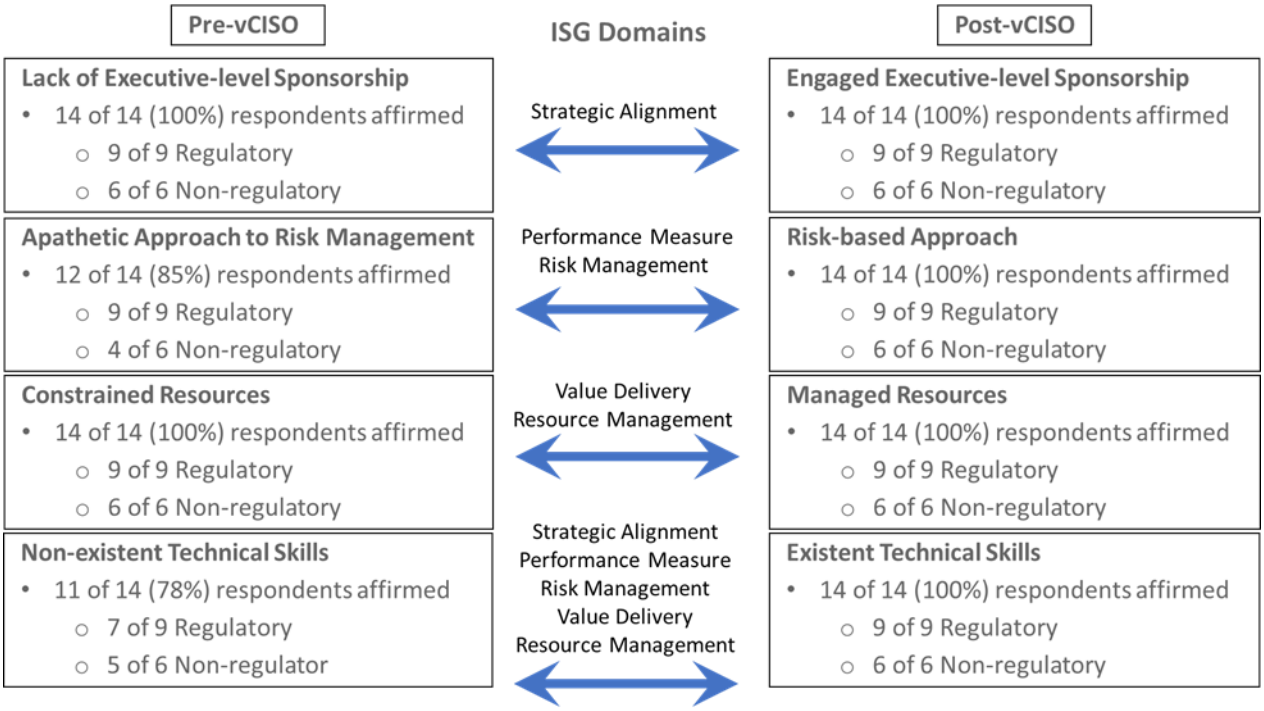
functionally support technology and has the strategic capabilities to modify the SMB security behaviors.

As identified throughout this study, the SMB information security behaviors were significantly affected when compared from the pre-vCISO posture to the post-vCISO posture. As the numbers tell the story, the maturity of the information security behaviors improved for the betterment of the respective organization (Figure 2). The behavior that drives the organization is executive-level sponsorship. Executive-level sponsorship was modified from non-strategic to strategic by the alignment of the business units into one organization strategic focus. Senior leaders were more involved in non-revenue generating events and employed a top-down approach to information security. Having matured due to the vCISO engagement, apathetic risk management became risk-centric, with individual business units included in the risk management process. Prior to the vCISO engagement, SMBs noted that if conducted at all, risk management focused on business risks or was outsourced to third-party IT vendors without information security expertise. Upon completion of the vCISO engagement, risk identification and mitigation are a priority, with individual business units involved in risk management process. Finally, risk is considered a business problem, and vCISOs were able to provide measurable metrics for risk improvement to the organizations. SMBs still have constrained resources, and the vCISOs were unable to eliminate this reality. However, vCISO engagements modified the resource management capabilities from constrained to optimized by identifying wasteful spending on unnecessary expenditures and providing measurable value-delivery to SMBs. Additionally, the cost-effective, and flexible team approach to Information Security Governance and information security program development enhanced the SMB security posture for a fraction of the cost of a full-time information security executive. Finally, the SMBs did not have skilled information security employees, or the

information security tools required to protect organizational data and assets. These non-existent technical skills are a direct result of SMBs' constrained resources but are now classified as accessible with a vCISO engagement. The vCISOs provided a team of information security experts to solve information security problems, identify, and mitigate risks more efficiently, and provided SMBs with strategic and technical abilities to solve information security problems with business solutions.

While the experiences described by the SMB leaders were overwhelmingly positive, they expressed two main concerns with employing a vCISO over a full-time CISO. First, some SMB leaders expressed concern that the vCISO did not permanently reside in the organization. This concern was prevalent when SMB leaders discussed hot issue items that had to be addressed immediately, instead of waiting for an email response or phone call to resolve the concern. A second concern noted by the SMB interviewees was the immersion into the business culture and organizational dynamics. Some interviewees discussed aspects of the information security program development where specific information security initiatives may be difficult to implement. For example, one SMB participant discussed a situation where the vCISO recommended an email encryption program with encryption occurring after the employee selected the encrypt button. The SMB leader expressed a concern that some of his employees were not very technical, and this change would be difficult to implement. To mitigate the SMB leader's concern, the vCISO and SMB leader worked on a solution that would automatically encrypt emails based on identified rules, instead of user actions. Although this concern was not widespread amongst the study participants, advice was provided that the vCISO should immerse themselves into the organization before making recommended changes that may impact the employees' business operations.

Figure 2: Strategic Alignment of the ISG Domains and the Information Security Behaviors



VI.1.1: Executive-level Sponsorship

During the early formation years, SMBs are focused on growing the business, and the senior leaders are viewed as the ones that will guide the company's direction. Senior leaders must guide the organization to ensure security is a business initiative rather than siloed as a technical concern. Senior management's information security mindset directly impacts the employees' attitudes (culture) and guides the Information Security Governance program for the SMB. However, research indicates that most SMB leaders feel they are not susceptible to internal or external hostile attackers and display a "false sense of security" to their employees.

As the key driver for the organization, the SMB executives interviewed understood the vulnerabilities to which SMBs are exposed and took a more proactive role in Information Security Governance and program development. However, this was not always the case. Numerous

interviewees indicated that they once displayed a false sense of security until the vCISO highlighted the security landscape that challenges SMB organizations.

SMBs lack technical expertise or internal staff to comprehend which cybersecurity strategies to implement or the governance models to follow. Some SMB leaders expressed the desire to implement Information Security Governance as a part-time duty or hire external Managed Service Providers (MSPs) to secure networks. As described by a vCISO, the concern with these approaches is that senior management becomes overwhelmed with daily operations, and information security falls to the lower rungs of priorities, or the MSPs lack the security foundation to understand the overwhelming compliance requirements or security best practices. In essence, the lack of domain knowledge leaves the organization vulnerable to large-scale attacks.

As discussed during the study, both the vCISO and SMB participants identified senior leader involvement as the key to a successful client engagement. One interviewee went one step further and described the initial engagement call as only involving senior leaders of the organization and the vCISO. The senior leaders' involvement ensures that SMBs are committed to change, information security development, and define a roadmap to success. When queried further about senior leader involvement in a vCISO engagement, several vCISOs described a negative engagement as a "check the block" scenario where leaders only sought an engagement to provide information security assurance to third-party business associates. These negative engagements reflect poorly on the SMBs leaders' commitment to information security improvements and the vCISO that assists with the engagement.

Contrasting the negative engagements, several vCISOs, and SMB leaders expressed that a positive engagement is where the senior leaders and vCISO have mutual respect and trust for the other, with each party exhibiting the internal motivation to enhance the business and information

security profession. Moreover, numerous vCISOs and SMB leaders described the "mutual respect" phenomena as solidified with a lifelong friendship well past the engagement window. Several interviewees described instances where the vCISO morphed from a third-party security provider to a mentor for the SMB and its employees. One example of this mentorship program identified during the study was when a vCISO assisted a SMB in providing a position description for hiring an internal security team, participated in interviews to ensure the best candidates were selected, and formulated a pay scale beneficial to the SMB and employee. Lifelong friendships are hard to acquire in the business world. However, the trust and respect earned during positive engagements directly resulted from a committed senior leader and organization. Governance responsibilities lie on the shoulders of executives. Information security tasks can be delegated, but the overall accountability and responsibility remain within the executive leadership realm. SMB leaders should strive to serve as ambassadors for information security and inculcate the same stewardship in their employees.

The emergence of executive level sponsorship does not come as a surprise. The importance of executive leadership as a critical success factor in organizations is not new. Hambrick and Mason's seminal article (1984) reported a study on top management teams (TMT) and how leader engagements impact the outcome of the organization while influencing employee behaviors. The authors posited that the organization is a reflection of its top managers. (Hambrick & Mason, 1984: 193). Menz (2012) found that research on TMTs is one of the more prominent, well-researched areas in the management field. His extensive review and synthesis of the literature on functional TMT members spanning almost 30 years (1984-2012) affirms Hambrick and Mason's statement, basically, as goes top management, so goes the organization. Menz further reports that there is in fact a consensus across the research, regardless of significant differences of the various functional

TMT members' roles, because they all share a strategic leadership role in the organization. The expressed need for executive-level sponsorship in SMBs is that top management teams must be strategically involved in all business decisions for continued growth and maturity within their respective industries.

VI.1.1.1: Strategic Alignment. The first step in any vCISO engagement strategically aligns the information security goals to the organization's business elements. Information security is designed to support the business units and is defined by the organization's business objectives and mission. Information security is the gatekeeper of protecting data, and governance cannot be achieved without proper strategic alignment of the information security program and business objectives (ISACA, 2010). According to ISO/IEC 38500, information technology's strategic alignment with the business achieves maximum value by developing and maintaining adequate controls and accountability, performance management, and risk management (Lee, 2013). The security strategy ensures that organizational activities are strategically aligned, practical and should encompass current information security capabilities, future security initiatives, and the people and technology to meet business needs (Yaokumah & Brown, 2014). However, before implementing a security strategy or security program, leaders must understand how information security benefits the organization's strategic alignment (ITGI, 2006).

As discussed by the participants, the strategic alignment is a small project conducted during the engagement's initial stages to define and deliver an organizational security strategy. The strategy development project begins with an expectation call, where senior leaders and the vCISO meet to identify the desired goals of the engagement, business objective analysis, budgetary constraints, timelines for the engagement, and current security posture (gap analysis and risk assessment). As discussed by numerous interview participants, the strategy's goal is to ensure that

the information security and governance program is realistic, attainable, and aligned with its business goals. If the strategy is not aligned to the specific business, the information security program's maturity will be minimal, if at all. As envisioned by some SMB leaders, the participants believed it was best for the businesses if the vCISO spent a week onsite to fully engage with the business units and understand aspects of the business before developing an information security strategy. This thought was also echoed by several vCISOs, with one participant indicating they would add this development to future engagements. The strategic alignment project culminates with a security strategy that includes security initiatives and roadmap short-term or long-term model for governance maturity.

VI.1.2: Risk Management

Risk management is a vital function of any organization, regardless of size. This concept is so essential that the literature defines risk management as a security concern for SMBs and an Information Security Governance domain. Risk management is a business function, and vCISOs encourage SMBs not to address risk as a subordinate function. The study indicated that most SMBs lack the foundational knowledge to accurately assess risk and identify the specific business risk to mitigate without assistance from a security expert. Interview participants acknowledged that risk management could not be avoided and implementing Information Security Governance without a risk management program is impossible. As identified by the vCISO participants, the client engagement ensures SMBs understand how risk management facilitates the organization to identify and mitigate risks and provides insights on the development of risk analysis plans and a risk mitigation plan. Furthermore, all interview participants acknowledged that risks are not limited because SMBs are not as well-known as larger organizations.

The risk analysis identifies risks across the organization and is not isolated to only information technology. However, during the study, several SMB leaders indicated they considered the risk analysis as an IT function pre-vCISO engagement. At the same time, vCISOs indicate that one of the more difficult tasks during an engagement is to assist SMBs with viewing risks at the business level and not be isolated to information technology. vCISOs indicated that leaders involved in vCISO engagements are more aware of the organization's risks, but awareness of a changing threat landscape is a concept that must be continually reinforced. Moreover, SMB leaders confirmed that they are more aware of the risks post-vCISO engagement than pre-vCISO engagement. When questioned about changes in attitudes towards risk at the senior leader and business level, SMBs indicated it was due to a gradual transition from IT risk management to business risk identification.

Risk management aims to correctly identify and mitigate risks outside of the organization's risk tolerance level. The mitigation of risks is completed using a risk mitigation plan and works in conjunction with the security strategy's roadmap developed during the strategic alignment. SMB interviewees identified risk mitigation as a primary element that forms the information security program. Additionally, those same participants positively acknowledged the role the vCISO performed in creating the risk mitigation plan and the subsequent validation of the information security program. When requested to elaborate on the vCISO role, participants detailed several examples of risk mitigation items and their associated mitigating controls in the program. Moreover, as identified during the interviews, SMBs appear to be more aware of the risks, measures to address risks, and have a risk-aware culture that enhances the best security controls available.

VI.1.2.1: Performance Measurement. Performance measurement is a governance domain used to measure the risk management progress in the organization. All regulated industries must use performance measurements to validate risks to ensure they are identified and mitigated within a timely fashion. During the interviews, the respondents had varying views on the timeframes for risk mitigation. However, most interviewees agreed that high risks should be mitigated within 30 days, medium risks within 180 days, and low risks within a year. The vCISOs interviewed discussed the importance of having key risk indicators to measure progress but failed to suggest useful measurements for specific organizations. However, they insisted that the individual business leaders decide the metric of measurement and not an external entity. The interviewees understood that lead indicators provide meaningful metrics for senior executives and board members to quantify the monetary funds expended on security investments.

The SMBs were more detailed than the vCISOs in their descriptions of risk mitigation measurements. In this study, 82% of the senior leaders encouraged performance measurement tools to verify risks are addressed as annotated in the risk management plan, and the risk management framework applies to the business as it continues to grow. Metrics are essential for business leaders, but extreme caution was shown when deciding which metric to present to the stakeholders or the board of directors. Each metric described by the interviewees was purposefully selected to provide concrete improvement with security investments and provide monetary value to the organization. Some examples provided by the SMB interviewees include:

- the percentage of mitigation for high/medium/low risks completed.
- the percentage of the risk mitigation identified in the risk management plan.
- employees trained compared to the base target goal.
- the number of third-party vendor contracts evaluated for risks.

- the number of root cause analysis conducted to learn from successes and failures.
- the number of control self-assessments conducted.

VI.1.3: Resource Management

Resource management is one of the most significant security issues identified in the literature and identified as an SMB short-coming during the study. Additionally, resource management is a governance domain that must be adequately managed for governance to be successful. The literature identifies resources as the availability of capital, personnel, and time (Cholez & Girard, 2013), with each component limited in small and mid-sized businesses. As previously discussed during the study, an SMBs focus is on obtaining clients, operational constraints, and revenue generation. During the early formation years, SMB resources are limited and sparse, and in some cases, non-existent for non-revenue generating events. Berry and Berry (2018) acknowledge that larger companies have resources to address cybersecurity issues, but small companies often do not. This assumption provides the opportunity for this study to explore how the virtual Chief Information Security Officer (vCISO) can provide SMBs a cost-effective, professional, and flexible team approach to information security governance.

SMBs acknowledged that they lack the monetary capital to hire an internal Chief Information Security Officer (CISO) or an internal security team. In fact, over 60% of the SMB interviewees acknowledged that information security was not a priority during the business's formation years. Additionally, another 12 of the 14 SMBs interviewed identified monetary limitations as the driving force behind selecting a vCISO over an internal CISO. Further exploration of the driving force for the two remaining interviewees that did not select the vCISO based on monetary savings indicated the selection was based on a low population of available information security candidates (theoretical replication). Glassdoor (2020) confirmed that a full-

time Chief Information Security Officer's (CISO) salary averaged $181,160 annually; a security analyst's salary averages about $76,410 annually, not including benefits and administrative costs associated with hiring an internal security team. The SMB and vCISO participants in the study indicated that the average cost of vCISO services, depending upon the engagement's hours and scope, ranged from $5,000 to $8,000 a month. An exception to this average was one SMB that indicated their organization vCISO costs exceeded $100,000 annually. However, this estimate was scoped for complete information security services, including penetration and vulnerability testing and 24/7 continuous monitoring for 40 remote locations and 3,000 endpoints. It is evident from the study that a vCISO engagement is lower than the Glassdoor average of an internal CISO and provides services that provide value to the organization's governance program. However, an unanticipated discussion during the vCISOs indicated that at 70 hours of monthly consulting time, it might be more beneficial for an SMB to hire an internal CISO but maintain the information security services provided by a managed security services provider (MSSP).

Secondary to the cost savings on personnel, another topic of discussion during the participant's interviews included the indirect savings of time management. Staying abreast of the changing threat landscape can be a full-time job, even for the most knowledgeable information security professionals. As time availability is identified as a critical resource for SMBs, executives have little time to maintain the current threat landscape and stay abreast of the changing trends of information security threats. As an internal asset, an information security officer would maintain a security posture that protects organizational assets, freeing up SMB executives' time to perform other critical functions. Nevertheless, when accompanied by the cost savings of hiring an internal team and executives with more time available for business-related functions, the vCISO is an invaluable alternative for SMBs with limited resources.

VI.3.1.1: Value Delivery. ITGI (2006) identified four measurements for the value delivery, but the generalizing of value is complex because the value obtained by one stakeholder may not always be of value to another.

- the program must provide measurable feedback to the organization.
- the program must achieve the desired results as outlined in the strategic plan.
- the program should provide quality output.
- the program should provide the desired output on time and within budget constraints.

When requested to provide the top three value delivery possibilities, the SMB participants rated value delivery differently within their specific organization or industry. When generalized into categories, from the most important to the least significant, the vCISO engagement value identified by the SMB executives were monetary savings (79%), time savings (14%), and vCISO stabilization (7%). When the vCISO participants were provided with an identical question, the overwhelming majority of participants identified measurable progress for stakeholders as the most significant value delivery attribute for SMBs. This contrasting view was anticipated (theoretical replication) because vCISOs are more concerned with information security programs and governance maturation over other value delivery characteristics.

VI.1.4: Technical Skills

The final SMB weakness identified in the literature was the lack of internal technical skills within the organization. As indicated throughout the study, most SMBs lack the financial resources to hire an information security executive or an internal security team. Throughout the interviews, this concept was reverberated and served as a foundation. An astounding 79% of SMB executives identified monetary constraints as the driving force behind engaging with a vCISO for security functions. The monetary constraint limits the SMB's ability to recruit experienced CISOs or

security teams. Furthermore, the SMB participants identified that information security currently has a negative unemployment rate, meaning there are not enough qualified candidates to fill the available positions. Executives displayed concern with the amount of time involved in hiring the right individual and inculcating the new hire with the business would not return positive results if the employee leaves for a higher paying position within the first 24 months. With the monetary constraint removed, SMB executives were still concerned about the current workforce's amount of experience and technical abilities for their respective industries. To compound this issue, interviewees added that technological advancements, the movement toward cloud hosting, and complex regulated requirements further diminish the pool's qualified candidates. This conundrum experienced by SMB executives provides the vCISO with the opportunity to exploit an industry weakness and tailor services to meet a specific niche's demands.

VI.1.4.1: Strategic Alignment. A vCISOs engagement allows the SMB to strategically align its business functions with organizational business units to meet its growing demands. To assist in the strategic alignment of the information security program to the business, the vCISOs and their staff rely on their technical expertise, specific information security specializations, and industry-recognized certifications, accompanied by decades of combined experience. The vCISO and SMB executives, through a technical discussion, will chart the most appropriate path to Information Security Governance through the creation of an information security program and the development of a compliance roadmap. The roadmap will enhance the governance maturation by working with business leaders to identify compliance gaps, implement a holistic risk management program, and provide an attainable methodology to achieve the desired compliance.

VI.1.4.2: Risk Management. Business leaders must understand that risk management is not a one-and-done task but an ongoing concept that should be a priority for all business activities

(Labossiere, 2015). Nevertheless, most SMB leaders lack the knowledge to assess risk accurately and to identify the specific business risk to address (Labossiere, 2015). The technical expertise of the vCISO provides SMB leaders the opportunity to holistically analyze risks by employing risk management frameworks and compliance guidelines while conducting a thorough and accurate assessment of all anticipated risks to the organization. Performed during the initial phases of a vCISO engagement, the risk management plan and risk assessment serve as documentation to guide the security strategy, information security program development, and compliance roadmap. The vCISOs interviewed discussed numerous approaches to conducting risk management for SMBs, with most interviewees (80%) preferring to use a qualitative approach over the more complicated quantitative approach. However, the consensus among all vCISOs was that the risk assessment was the organization's product, and the approach utilized was determined from the business leaders' input and guidance from the vCISO. Upon completion of the risk assessment, and in conjunction with the risk management plan, the business leaders and vCISOs will categorize risks and implement a risk mitigation plan, also known as a Plan of Action and Milestones (PO&M). All documents produced in the risk management process will help formulate a compliance roadmap to measure governance maturation in the SMB.

VI.1.4.3: Performance Measurement. Performance measurement is the key to success when evaluating governance maturity. Additionally, metrics are useful in demonstrating the organization's due diligence with auditing agencies, provide a return on investment to stakeholders, and the continuous monitoring of weaker areas that require further strengthening. The SMB participants indicated that performance measurement is essential when making informed business decisions on future security investments or providing quarterly updates to the Board of Directors. However, SMB executives indicated that before the vCISO engagement, they lacked

the processes and procedures to measure the organization's security posture accurately. vCISOs provide executive-level and technical dashboards to help SMB executives demonstrate compliance with federally regulated requirements and validate improved governance maturity throughout the organization. Nevertheless, before dashboards are beneficial to the organization, vCISOs must work with SMB business leaders to develop current processes and procedures that measure performance in near real-time mode. As summarized during the VCISO interviews, performance measurement is vital, but SMBs must identify the assets to protect and how they will be protected before they can measure success or failure, or crucial resources will be wasted.

VI.1.4.4: Resource Management. Resources are limited in SMBs, and resource maximization is a priority for organizations in today's competitive market. vCISOs provide a cost-effective solution for SMBs that lack resources to hire internal information security staff members. Additionally, the vCISOs expertise allows an outside entity to evaluate SMB resource expenditures and recommend a cost-saving plan for leadership to consider. Moreover, due to the size of most SMBs, a full-time CISO may not be warranted to achieve the SMB's business goals. VCISOs provide flexibility by providing a specific amount of consulting hours that SMB leaders can utilize for specific information security initiatives.

Although vCISOs could save an SMB in annual salary costs, SMB executives indicated that resource management was more crucial when outsourcing business functions. Numerous interviewees provided examples where the contract's statement of work and scope continued to expand with some external services. If not correctly managed, scope creep will cost the SMB more money than initially budgeted, and monetary savings will quickly evaporate. Likewise, SMB participants signaled that it was more important to manage third-party providers' resource usage than internal staff resource usage. During a discussion of resource management with vCISO

participants, interviewees discussed the importance of organizational goal setting and mutual involvement during all contract negotiations. Additionally, vCISOs agreed that contract scope creep could be problematic for third-party service providers. However, they indicated this could be assuaged by following the compliance roadmap developed by the vCISO and SMBs business leaders.

VI.1.4.5: Value Delivery. The study intended to provide small to mid-sized businesses options to protect data and attain Information Security Governance when budgetary constraints limited hiring internal security teams. The study delivers definitive proof that the experience (strategic and technical) far outweighs the internal candidates' availability on an SMBs constrained budget. The study evaluated value from two distinct viewpoints:

- vCISO participants identified the perceived value provided to an SMB from the perspective of a vCISO.
- SMB participants identified actualized value derived from a vCISO engagement.

To summarize the study from a communal view, each SMB executive was asked to rate the vCISO value delivery on a scale of 1-7, with seven identified as the most significant value. The average value delivery score was 6.7, with 10 out of 14 respondents maximizing value delivery from the vCISO engagement. Finally, the vCISO is unequivocally the most cost-effective, attainable, and value-driven alternative for SMBs with limited resources and the intrinsic desire to achieve a mature level of Information Security Governance and data protection for their clients, customers, and stakeholders.

IV.1.5: Regulated and Non-regulated Industries

SMBs with regulatory requirements, such as HIPAA or PCI/DSS have specific rules that they must follow to be considered compliant. Two-thirds of the SMB interviewees worked in a

heavily regulated environment, that drove the Information Security Governance and compliance requirements. Regulated SMB participants discussed the exemplar performance of the vCISOs providing guidance on the regulatory requirements and mentorship throughout the Information Security Governance process.

At the same time, one-third of the interviewees were not regulated and had the option to institute Information Security Governance within the confines of organizational business objectives. During the interviews, all non-regulated SMB participants expressed the intrinsic motivation to enhance Information Security Governance but were clear that all modifications must align with their business goals. An SMB participant described a driver for his organization was the opportunity for organizational growth by becoming a business associate for larger companies.

VI.3: Contribution to Academics

This study offers three main academic contributions. First, academic research yielded numerous studies on SMB security concerns, Information Security Governance models, and information security management. However, the research did not generate results exploring opportunities for SMBs to attain Information Security Governance with limited resources. Specifically speaking, when the following keywords/phrases were entered: Virtual Chief Information Security Officer (vCISO), Fractional Chief Information Security Officer (fCISO), no academic results returned. As the concept of using a vCISO is relatively new, only one practitioner journal returned results. However, these results were selling vCISO services instead of exploring value obtained through the SMB's utilization of vCISO services. The study provided evidence of how a vCISO provides value to the organization through a perceived value construct and supports the actualized benefits derived from a vCISO engagement as indicated by SMB executives.

Specifically, the first contribution to academics explores the extent to which a vCISO adds value to an SMB from actualized benefits derived from a vCISO engagement.

Second, academic studies indicate that SMBs have four consistent information security behaviors (non-strategic executive-level sponsorship, apathetic risk management procedures, constrained resources, and non-existent technical skills) that further weakens an SMB's security posture (Rohn et al., 2015). Furthermore, academic and practitioner literature identifies five Information Security Governance domains that organizations should align with to attain a mature Information Security Governance level. However, academic literature does not integrate the SMB information security behaviors with the Information Security Governance domains. This research proposes that vCISOs can help integrate the identified SMB information security behaviors with the five information security domains to result in the maturation of information security governance, data protection, and value delivery to the SMB. Likewise, this study provides empirical evidence on how the vCISO utilized their technical experience and industry expertise to help SMB leadership teams achieve a mature governance platform that protects the confidentiality, integrity, and availability of data without the internal CISO or security team expenditure. The second contribution to academics explores how a vCISO can utilize their technical experience and expertise to assist SMB leadership teams in achieving a mature governance platform that protects confidentiality, integrity, and data availability.

Third, past research does not provide a process model that will enhance SMBs on a limited budget to secure assets and attain information security governance. The completed research contributes a proposed process model focused on a vCISO client engagement designed to provide governance maturity and assist SMBs with governance maturation within the constraint limitations of the SMB's allocated resources.

VI.4: Contribution to Practice

With the SMB security breach statistics discussed throughout the study, it is evident that SMB executives desire to protect organizational data but are limited due to resource availability. The contribution to practice includes three areas identified during the research. Based on the identified gaps from the research, the study explores how SMBs can overcome the information security behaviors identified by researchers to attain information security governance, protect organizational resources, and add value to the organization.

The first contribution is the empirical evidence to practitioners that vCISOs can help SMBs achieve governance with minimal cost to the SMB. As noted throughout the study, hiring a full-time CISO, or security analysts, accompanied by the expenditures of security implementations are overwhelming for many SMBs, so they selectively decide to ignore their information systems' risk by not taking action, which was identified as a mistake by numerous SMB interviewees. As indicated by the SMB interviewees, there was a significant cost savings of employing a vCISO over hiring a full-time information security executive. Additionally, 12 of the 14 SMBs interviewed identified monetary limitations as the driving force behind selecting a vCISO over an internal CISO. Furthermore, all interviewees indicated that the flexibility in vCISO services and the availability of a team of security professionals provided additional monetary savings to an organization with constrained resources. Finally, SMB and vCISO interviewees discussed how the alignment of the information security strategy to the business processes helped the SMB identify specific business processes that should allocate more robust mitigating controls and other areas where controls are not required. This alignment resulted in reduced wasteful spending or unneeded resources as additional savings to the overall IT budget.

The second contribution to practitioners explored how the vCISO helped the SMBs improve their security posture while providing value to the organization. As indicated during the study, SMBs have four shared information security behaviors that increase the likelihood of a catastrophic breach to the organization. The study included an analysis of the organization's security behaviors before the vCISO employment and changes to the security behaviors after the vCISO employment. The vCISO's strategic and technical experience provided the SMB leaders with a renewed perspective of the intricacies of information security and how an intrinsic modification of information security behaviors will enhance the SMB information security posture upon completing the vCISO engagement. Finally, every SMB interviewee discussed actualized value received during the vCISO engagement. Although each interviewee defined the actualized value differently, the consensus among the SMB interviewees was that the value received enhanced the organization's information security knowledge, senior leader involvement, and modifications to the organization's overall culture. The discussion on the value delivery during and after a vCISO engagement in similar-sized organizations will solidify the discussion and provide a way for SMBs to achieve compliance and data protection for a fraction of the cost of hiring a full-time CISO.

The final contribution identified during the study was that the vCISO delivered mentorship to SMBs in the governance maturation process. Numerous SMB interviewees discussed the importance of the vCISO role in modifying employees' attitudes towards information security. SMB interviewees discussed how the vCISO mentored the leadership teams to understand the advantages of including information security as part of the long-term organizational plans. When queried about the mentorship received during an engagement, 100% of the interviewees responded favorably that the vCISOs spent a considerable amount of time mentoring SMB leaders. The

mentorship program generated a standard that the vCISO imparted their knowledge and experience to leave the organization with a more focused security posture than before the engagement. The interaction and organizational involvement from the vCISOs showed SMBs continue to learn and grow from the interactions with the vCISO. Finally, SMB leaders expressed gratitude to vCISOs and the work completed on behalf of the SMB. SMB leaders viewed the vCISOs as developing a lifelong friendship with a security expert.

VI.5: Limitations and Future Research

This study attempted to generalize the vCISO engagement in as many industries as possible. However, the study did not represent all industries, and an even participant distribution was not attained. The study attempted to uniformly distribute the interviews based on regulated or non-regulated environments to determine if peculiarities existed between the two environments. Regulated environments have specific reporting and control mitigation directives as identified by industry standards and federal laws. Non-regulated SMBs do not have federally regulated reporting requirements or control mitigation directives. During the data analysis, specific intricacies between regulated and non-regulated environments did not evolve. Additional research should include an in-depth analysis of benefits earned by an SMB in a heavily regulated environment, such as the healthcare or payment card industry. Additionally, future studies that include non-regulated environments should focus on the driving force behind allocating essential resources to secure an environment when security is not legally required, and data protection is at the behest of the SMB leadership.

This study focused on how a vCISO assist SMBs with constrained resources to attain a mature Information Security Governance program. As the information security program is part of the governance program, the study did not evaluate specific program development instances,

known as information security management. Information Security Governance and information security management are two distinct domains and should be studied separately. Further studies should evaluate the information security management progress (new or refined programs) concerning Information Security Governance maturity through a vCISO engagement. Future studies should also include the quantitative evaluation of information security management investments and the potential monetary savings using vCISO services in developing information security programs.

This study focused on the vCISO engagement as a snapshot in time during a specific timeframe. It did not account for data collected over time, including historical records. The long-term effects of using a vCISO could positively or negatively impact the organization or information security culture. Future studies should include a longitudinal study for a more in-depth analysis of the benefits of utilizing a vCISO for security functions over a more extended period. The analysis could be quantitative or qualitative and should include examining an information security and governance program's historical records.

REFERENCES

134 Cybersecurity Statistics and Trends for 2021. (2020). Varonis. Retrieved from https://www.varonis.com/blog/cybersecurity-statistics/

Abdullah, H., & Valentine, B. (2009) Fundamental and Ethics Theories of Corporate Governance. *Middle Eastern Finance and Economics, 4*, 88-96.

Adhikari, A. (2012). The Virtual CFO. *Business Today*, 62-66.

Albrechtsen, E., & Hovden, J. (2010). Improving Information Security Awareness and Behaviour through Dialogue, Participation and Collective Reflection. An Intervention Study. *Computers and Security, 29*(2010), 432-445.

Alexander, A., & Cummings, J. (2016). The Rise of the Chief Information Security Officer. *People & Strategy, 39*(1), 10-13.

Alhogail, A., & Mirza, A. (2014). A Framework of Information Security Culture Change. *Journal of Theoretical and Applied Information Technology, 64*(2), 540-549.

Alhogail, A., & Mirza, A. (2014). A Proposal of an Organizational Information Security Culture Framework. *2014 International Conference on Information, Communication Technology and System*. 243-249.

Allen, J. & Westby, J. (2007). Characteristics of Effective Security Governance. *EDPAC: The EDP Audit, Control, and Security Newsletter, 35*(5), 1-17. doi:10.1080/07366980701394229.

Amaladoss, B. (2001, March). Managed Security Services: An Evolving Security Solution!. Sans Institute.

Accenture. (2017). Cost of Cyber Crime Study. Retrieved from https://www.accenture.com/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf

Andress, A. (2001). *Surviving Security: How to Integrate People, Process, and Technology, 2nd ed*. Boca Raton, FL:CRC Press.

Banham, R. (2017). Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accounting*.

Barlette, Y., Gundolf, K., & Jaouen, A. (2015). Toward a Better Understanding of SMB CEOs' Information Security Behavior: Insights from Threat or Coping Appraisal. *Journal of Intelligence Studies in Business, 5*(1), 5-17.

Baskerville, R., Spagnoletti, P., and Kim, J. (2014). Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response. *Information and Management, 51*(1) 138-151.

Berry, T., & Berry R. (2018). An Initial Assessment of Small Business Risk Management Approaches for Cyber Security Threats. *International Journal Business Continuity and Risk Management, 8*(1), 1-10. https://doi.org/10.1504/IJBCRM.2018.090580

Berisha, G., & Pula, J. (2015). Defining Small and Medium Enterprises: A Critical Review. *Academic Journal of Business, Administration, Law and Social Sciences, 1*(1), 17-28.

Bonabeau, E. (2007). Understanding and Managing Complexity Risk. *MIT Sloan Management Review, 48*(4), 62–68.

Bourne, V. (2019). Underserved and Unprepared: The State of SMB Cyber Security in 2019. Retrieved from http://info.continuum.net/rs/011-QRO-

092/images/Underserved%20and%20Unprepared_%20The%20State%20of%20SMB%20Cyber%20Security%20in%202019.pdf?hsCtaTracking=912e901a-d33c-4893-afc4-6155565fde54%7C9e2dc862-075a-4df2-990f-e491d1e15135

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2017). Sourcing Information Security Operations: The Role of Risk Interdependency and Competitive Externality in Outsourcing Decisions. *Production and Operations Management, 26*(5), 860-879. https://doi.org/10.1111/poms.12681

Ching, K. W., Tan, J. S., & Ching, C. R. G. (2006). *Corporate Governance in East Asia: The Road Ahead*. Upper Saddle River: Pearson Prentice Hall.

Cholez, H., & Girard, F. (2013). Maturity Assessment and Process Improvement for Information Security Management in Small and Medium Enterprises. *Journal of Software: Evolution and Process. 26*, 496-503.

CISOShare (2020). Security Program Explained. Retrieved from https://cisoshare.com/security-program-explained

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). Guidance on Internal Control. Retrieved from https://www.coso.org/Pages/ic.aspx

Control Objectives for Information Technology (COBIT) (2019) ISACA. Framework Introduction and Methodology.

Crassula. (2019) SMBs & SMEs — Definition and Approach Retrieved from https://medium.com/@Crassula/smbs-smes-definition-and-approach-65bd883f88de

Damianides, M. (2005). Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance. *Information Systems Management. 22*(2005). 77-85.

Dawson, M., Burrell, D.N., Rahim, E., & Brewster, S. (2010). Examining the Role of the Chief Information Security Officer (CISO) & Security Plan. *Journal of Information Systems Technology & Planning, 3*(6), 1-5.

Department of Defense (2006). Continuous Process Improvement Transformation Guidebook. Retrieved from https://www.dau.edu/cop/se/DAU%20Sponsored%20Documents/DoD%20Continuous%20Process%20Improvement%20CPI%20Guidebook%20May%202006.pdf

Dillen, Y., Laveren, E., Rudy Marten, Vocht, S.D., & Imschoot, E.V. (2018). From Manager to Strategist: An Examination of the Evolving Role of Persistent High-Growth Entrepreneurs. *International Journal of Entrepreneurial Behavior & Research, 25*(1) 1-27. doi:10.1108/IJEBR-01-2017-0010

Dudovskiy, J. (2019). Retrieved from https://research-methodology.net/research-methods/qualitative-research/case-studies/

Dutton, J. (2017). Three pillars of cyber security. Retrieved from https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security

European Commission. (2020). Public consultation on the review of the SME definition. Retrieved from https://ec.europa.eu/info/consultations/public-consultation-review-sme-definition_en

Ezingeard, J., & Bowen-Schrire, M. (2007). Triggers of Change in Information Security Management Practices. *Journal of General Management, 32*(4), 53–72.

Feng, N., Wanga, M., Lia, M., & Li, D. (2019). Effect of Security Investment Strategy on the Business Value of Managed Security Service Providers. *Electronic Commerce Research and Applications*. 35. https://doi.org/10.1016/j.elerap.2019.100843

Fisher, K., & Fisher, M.D. (2001). *The Distance Manager: A Hands-on Guide to Managing Off-site Employees and Virtual Teams*. New York: McGraw-Hill.

Gartner Glossary. (2020). Small and Midsize Business (SMB). Retrieved from https://www.gartner.com/en/information-technology/glossary/smbs-small-and-midsize-businesses

Glaser, B. G., & Strauss, A. (1967). *The Discovery Grounded Theory: Strategies for Qualitative Inquiry*. Milton Park: Abingdon.

Glassdoor. (2020). Retrieved from https://www.glassdoor.com/Salaries/ciso-salary-SRCH_KO0,4.htm

Goles, T., White, G. B., & Dietrich, G. (2005). Dark screen: An Exercise in Cybersecurity. *MIS Quarterly Executive, 4*(2), 303–318.

Gordas, V. (2014). *Implementing Information Security Management System in SMEs and Ensuring Effectiveness in its Governance* (RHUL–MA–2014– 6). Information Security Group.

Government of Canada (2013). Key Small Business Statistics. Retrieved from http://www.ic.gc.ca/eic/site/061.nsf/eng/h_02800.html

Gray, D. E. (2009). Doing Research in the Real World (2nd ed.). SAGE Publications.

Gregor, S., Martin, M., Fernandez, W., Stern, S. and Vitale, M. (2006), The Transformational Dimension in the Realization of Business Value from Information Technology. *The Journal of Strategic Information Systems, 15*(3), 249-270.

Guhr, N., Lebek, B., & Breitner, M. (2017). The Impact of Leadership on Employees' Intended Information Security Behavior: An Examination of the Full-range Leadership Theory. Information Systems and Management Institute, 29, 340-362. doi: 10.1111/isj.12202.

Gupta, A., & Hammond, R. (2004). Information Systems Security Issues and Decisions for Small Businesses. *Information Management and Computer Security*, *13*(4), 297-310. doi:10.1108/09685220510614425.

Gupta, A., & Zhdanov, D. (2012). Growth and Sustainability of Managed Security Services Networks: An Economic Perspective. *MIS Quarterly*, *36*(4), 1109-1130.

Haes, S.D., & Grembergen, W.V. (2004). IT Governance and its Mechanisms. *Information Systems Control Journal*, *1*, 27–33.

Hambrick, D. C., & Mason, P. A. (1984). Upper Echelons: The Organization as a Reflection of its Top Managers. Academy of Management Review, 9(1984),193-206.

Hardy, G. (2006). Using IT Governance and COBIT to Deliver Value with IT and Respond to Legal, Regulatory and Compliance Challenges. *Information Security Technical Report*, *11*(1), 55-61.

Henderson J.C., & Venkatraman N. (1993). Strategic Alignment: Leveraging Information Technology for Transforming Organizations. *IBM Systems Journal*, *32*(1), 4–16.

Hertel, G., Geister, S., & Konradt, U. (2005). Managing Virtual Teams: A Review of Current Empirical Research. *Human Resource Management Review, 15*(1), 69-65.

Hibbert, R. (2012). SMBs and the Struggle for Compliance. *Computer Fraud & Security*, 2012(11), 5-7. https://doi.org/10.1016/S1361-3723(12)70112-4.

Houngbo, P. & Hounsou, J. (2015). Measuring Information Security: Understanding and Selecting Appropriate Metrics. *International Journal of Computer Science and Security 9*(2), 108-120.

Humphreys, E. (2016). Chapter 2: ISO/IEC 27001 ISMS Family. Implementing the ISO/IEC 27001:2013 ISMS Standard. Artech House. 11–26.

Information Security Management (2013). ISO 27000 Series. International Standards for Organization.

Information Security Governance: Guidance for Boards of Directors and Executive Management. (2006). Information Technology Governance Institute.

Johnston, A. C., & Hale, R. (2009). Improved Security Through Information Security Governance. *Communications of the ACM, 52*(1), 126–129.

Joshi, C., Singh, U. (2017). Information Security Risks Management Framework – A Step Towards Mitigating Security Risks in University Network. *Journal of Information Security and Applications, 35*, 128-137. http://dx.doi.org/10.1016/j.jisa.2017.06.006

JP Morgan Chase. (2014). Small businesses are an anchor of the US economy. Retrieved from https://www.jpmorganchase.com/corporate/institute/small-business-economic.htm

Kahn, S. (2014). Qualitative Research Method: Grounded Theory. *International Journal of Business and Management, 9*(11), 224-233.

Kayworth, T. and Leidner, D. (2002) Leadership Effectiveness in Global Virtual Teams. *Journal of Management Information Systems, 18*(3), 7-40, doi:10.1080/07421222.2002.11045697.

Kayworth, T., & Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive, 9*(3), 163–175

Karanja, E., & Rosso, M. (2017). The Chief Information Security Officer: An Exploratory Study. *Journal of International Technology and Information Management*, *26*(2), 23-47.

Kerfoot, K. (2010). Listening to See: The Key to Virtual Leadership. *Nursing Economics, 28*(2), 114-118.

Khanduri, A. (2020). People, Process, Technology: The PPT Framework, Explained. Retrieved from https://www.plutora.com/blog/people-process-technology-ppt-framework-explained

Ključnikov, A., Mura, L., & Sklenár, D. (2019). Information Security Management in SMEs: Factors of Success. *Entrepreneurship and Sustainability Issues, 6*(4), 2081-2094. doi: 10.9770/jesi.2019.6.4(37).

Kobelsky, K., Hunter, S. and Richardson, V. J. (2008). Information Technology, Contextual Factors and the Volatility of Firm Performance. *International Journal of Accounting Information Systems, 9*(3), 154-174.

Kwon, J., Ulmer, J. R., & Wang, T. (2012). The Association Between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems, 27*(1), 219–236. https://doi.org/10.2308/isys-50339.

Labodi, C. & Michelberger, P. (2010). Necessity or Challenge – Information Security for Small and Medium Enterprises. *Annals of the University of Petrosani, Economics, 10*(3), 207-216.

Labossiere, D. (2015). *A Matrix For Small Business Owners to Better Protect Their Network* (Doctoral Dissertation). Retrieved from ProQuest. (1605731)

Le, N.T., & Hoang, D. B. (2017). Capability Maturity Model and Metrics Framework for Cyber Cloud Security. *Scalable Computing: Practice and Experience, 8*(4), 277-290.

Lee, M. (2013). IT Governance Implementation Framework in Small and Medium Enterprise. *International Journal of Management and Enterprise Development, 12*(4), 425-441.

Lee, Y. & Larsen, K. R. (2009). Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software. *European Journal of Information Systems, 18*(2), 177-187. https://doi.org/10.1057/ejis.2009.11

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). Cybersecurity Information Sharing: A Framework for Information Security Management in the UK SME Supply Chains. *Twenty-Second European Conference on Information Systems.*

Martins A., Elofe J. (2002). *Information Security Culture. In: Ghonaimy* M.A., El-Hadidi M.T., Aslan H.K. (eds) Security in the Information Society. *IFIP Advances in Information and Communication Technology, 86*. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35586-3_16

Masuda, B. (2006). Managing the Risk of Managed Security Services. *Information Systems Security. 15*(1). 35-42.

Maynard, S., Onibere, M. & Ahmad, A. (2018). Defining the Strategic Role of the Chief Information Security Officer. *Pacific Asia Journal of the Association for Information Systems, 10*(3), 61-86. doi: 10.17705/1PAIS.10303.

McCann, J., and Kohntopp, T. (2019). Virtual Leadership in Organizations: Potential Competitive Advantage? *SAM Advanced Management Journal, 84*(3). 26-39.

Menz, M. (2012). Functional Top Management Team Members: A Review, Synthesis, and Research Agenda. *Journal of Management, 38*(1). 45-80.

Miessler, D. (2020). Retrieved from https://danielmiessler.com/blog/the-difference-between-deductive-and-inductive-reasoning/

Miles, M., Huberman, A.M., & Saldaña, J. 2014. Qualitative Data Analysis: A Methods Sourcebook (3rd ed.). Thousand Oaks, CA: SAGE Publications.

Mishra, S. (2015). Organizational Objectives for Information Security Governance: A Value Focused Assessment. *Information and Computer Security, 23*(2), 122-144. doi: 10.1108/ICS-02-2014-0016.

Mishra S., & Dhillon, G. (2006). Information System Security Governance Research: A Behavioral Perspective. *Information Assurance Symposium*, 18-26.

Mitchell, R.C., Marcella, R. and Baxter, G. (1999). Corporate Information Security Management. *New Library World, 100*(5), 213-227. https://doi.org/10.1108/03074809910285888

Moon, Y., Choi, M., & Armstrong, D. (2018). The Impact of Relational Leadership and Social Alignment on Information Security System Effectiveness in Korean Governmental Organizations. *International Journal of Information Management 40*, 54-66.

Moulton, R & Coles, R. S. (2003). Applying Information Security Governance. *Computers & Security 22*(7), 580-584.

Munro, D. (2013). *A Guide to Financing SMEs*. New York: Palgrave Macmillan.

Meyer, E. (2010). The Four Keys to Success with Virtual Teams. Retrieved from https://www.forbes.com/2010/08/19/virtual-teams-meetings-leadership-managing-cooperation.html?sh=149f34c930cc

Myers, M. (2013). *Qualitative Research in Business Management*. New York: Sage Publishing.

Nijnik, I. (2005) Small Business Network Security 101. Retrieved from https://www.madersystems.com/Small_Business_Network_Security_101.pdf

National Institute of Standards and Technology. (2011). *Managing Information Security Risk* (Special Publication 800-39). Washington, DC: U.S. Government Printing Office.

National Institute of Standards and Technology. (2003). *Security and Privacy Controls for Federal Information Systems and Organizations* (Special Publication 800-53, Rev. 4). Washington, DC: U.S. Government Printing Office.

National Institute of Standards and Technology. (2008). *Performance Measurement Guide for Information Security* (Special Publication 800-55, Rev. 1). Washington, DC: U.S. Government Printing Office.

National Institute of Standards and Transportation. (2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (Special Publication 800-171, Rev 2). Washington, DC: U.S. Government Printing Office.

Nixon, P., Harrington, M., and Parker, D. (2012). Leadership Performance is Significant to Project Success or Failure: A Critical Analysis. *International Journal of Productivity and Performance Management 61*, 204-216.

Office of Advocacy. (2019). Small Business Administration. Retrieved from https://cdn.advocacy.sba.gov/wp-content/uploads/2019/04/23142719/2019-Small-Business-Profiles-US.pdf

Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification (CMMC). (2020). Retrieved from https://www.acq.osd.mil/cmmc/

Olmstead, K. (2019, July 9). Internet Society's Online Trust Alliance 2018 Cyber Incidents & Breach Trends Report. Internet Society. https://www.internetsociety.org/blog/2019/07/internet-societys-online-trust-alliance-2019-cyber-incidents-breach-trends-report/

Ozolins, H. (2018). Rise of the Virtual CFO. Business CFO. *Acuity*.

Parker, B. (2005) Study Reveals Extracting Value is Top IT Governance Imperative. *Manufacturing Business Technology, 23*(10), 44.

Posthumus, S., & Von Solms, R. (2004). A Framework for the Governance of Information. *Security. Computers and Security, 23*(8), 638-646.

Project Management Institute. (2020). Retrieved from https://www.pmi.org/

Renaud, K. (2016). *How Smaller Businesses Struggle with Security Advice*. Computer Fraud and Security, 2016(8), 10-18. https://doi.org/10.1016/S1361-3723(16)30062-8

Renu, A. (2014). E-Leadership- A New and Modern Style of Leadership. *International Journal of Advances in Management and Economics, 3*(5), 88-93.

Rocha, F., Antonsen, E., Ekstedt, M. (2014). Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. *Computers & Security, 43*, 90-110. http://dx.doi.org/10.1016/j.cose.2014.03.004.

Rodriguez, E & Edwards, J. (2010). People, Technology, Processes and Risk Knowledge Sharing. *Electronic Journal of Knowledge Management 8*(1), 139- 150.

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining Small Business InfoSec Posture Using Social Theories. *Information and Computer Security, 24*(5), 534-556. doi: 10.1108/ICS-09-2015-0041

Sangoma Success Team. (2020). SMB, SME, and Large Enterprise: Why Your Business Size Classification Matters. Retrieved from https://www.sangoma.com/articles/smb-sme-large-enterprise-size-business-matters/

Schmidt, G. (2014). Virtual Leadership: An Important Leadership Context. Industrial and Organizational Psychology, 7(2), 182-186. doi:10.1111/iops.12129

Schneier, B. (2013). Schneier on Security: People, Process, and Technology. Retrieved from https://www.schneier.com/blog/archives/2013/01/people_process.html

Singh, A., Gupta, M. P., & Ojha, A. (2013). Identifying Factors of Organizational Information Security Management. *Journal of Enterprise Information Management, 27*(5). doi:10.1108/JEIM-07-2013-0052

Shayo, C. & Lin, F. (2019). An Exploration of the Evolving Reporting Organizational Structure for the Chief Information Security Officer (CISO) Function. *Journal of Computer Science and Information Technology, 7*(1) 1-20. doi: 10.15640/jcsit.v6n2a1

South African Government. (2004). National Small Business Amendment Act 29 of 2004. Retrieved from https://www.gov.za/documents/national-small-business-amendment-act

Stanford University. (2020). Office of the Chief Risk Officer. Retrieved from https://ocro.stanford.edu/erm/risk-owner#:~:text=Risk%20Owner%3A%20The%20individual%20who,his%2Fher%20risk%20management%20efforts.

Statista (2020). Cyber security trends and expenditures. Retrieved from https://www.statista.com/statistics/536764/worldwide-it-security-budgets-as-share-of-it-budgets/

Statista (2020). Annual number of data breaches and exposed records in the United States from 2005 to 1st half 2020. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

The Business Model for Information Security. (2010). Information Systems Audit and Control Association (ISACA).

Tassabehji, R. (2005), Information Security Threats: From Evolution to Prominence. In Encyclopedia of Multimedia Technology and Networking. Idea Group Inc., ISBN: 1-59140-496-6, 404-410

The Risk IT Framework (2020). Information Systems Audit and Control Association (ISACA).

Ula, M., Ismail, Z., & Sidek, Z. (2011). A Framework for the Governance of Information Security in Banking System. *Journal of Information Assurance & Cybersecurity, 2011*. doi: 10.5171/2011.726196.

U. S. Small Business Administration Table of Small Business Size Standards, (2019). Retrieved from https://www.sba.gov/sites/default/files/files/Size_Standards_Table.pdf

Van Niekerk, J., & Von Solms, R. (2010). Information Security Culture: A Management Perspective. *Computer and Security 29*(4), 476–486. doi:10.1016/j.cose.2009.10.005

Verizon. (2020). Data Breach Investigation Security Report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/2020/smb-data-breaches-deep-dive/

Von Solms, R., Thomson, K., and Maninjwa, M. (2011). Information Security Governance Control Through Comprehensive Policy Architectures. Information Security for South Africa, Johannesburg, 2011, pp. 1-6, doi: 10.1109/ISSA.2011.6027522.

Wang, H., Tsui, H., Xin, K. (2011). CEO Leadership Behaviors, Organizational Performance, and Employees' Attitudes. *The Leadership Quarterly 22*(2011), 92–105

Weill, P. & Ross, J.W. (2004) *IT Governance: How Top Performers Manage IT Decision Right for Superior Results*. Watertown, MA: Harvard Business School Press.

Weiss, M. & Muegge, S. (2019). Conceptualizing a New Domain Using Topic Modeling and Concept Mapping: A Case study of Managed Security Services for Small Businesses. *Technology Innovation Management Review, 9*(8): 55-64. doi: 10.22215/timreview/1261

Whitman, M., & Mattord, H. (2013). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education, 11*(1), 97-111.

Whitten, D. (2008). The Chief Information Security Officer: An Analysis of the Skills Required for Success. *Journal of Computer Information Systems, 48*(3), 15-19. doi:10.1080/08874417.2008.11646017

Williams, S., Hardy, C., & Holgate, J. (2013). Information Security Governance Practices in Critical Infrastructure Organizations: A Socio-technical and Institutional Logic Perspective. *Institute of Information Management, 23*, 341–354. doi:10.1007/s12525-013-0137-3.

Williams, P., & Manheke, R. (2010). Small Business - A Cyber Resilience Vulnerability. *1st International Cyber Resilience Conference*.

Williams, V. (2002). *Virtual Leadership*. Edison, NJ: Shadowbrook Publishing.

Wu, D., & Olson, D. (2009). Enterprise Risk Management: Small Business Scorecard Analysis. *Production Planning & Control, 20*(4), 362-369. doi:10.1080/09537280902843706

Yaokumah, W., & Brown, S. (2014) An Empirical Examination of the Relationship Information Security/Business Strategic Alignment and Information Security Governance Domain Areas. *Journal of Business Systems, Governance, and Ethics, 9*(2), 50-65. https://doi.org/10.15209/jbsge.v9i2.718

Yin, R. (2018). *Case Study Research and Applications*. New York, NY: Sage Publishing.

Zamman, M., & Razali, R. (2016). An Empirical Study of Information Security Management Success Factors. *International Journal on Advanced Science, Engineering and Information Technology, 6*(6), 904-913.

APPENDIX: SMB INTERVIEW PROTOCOL

This exploratory research uses interviews to examine the importance of a virtual Chief Information Security Officer (vCISO) in Small to Midsize Businesses (SMBs). It includes interviews with two to three employees representing SMBs, and four vCISOs representing the virtual Chief Information Security Officer industry. All interviewees are professionals and range from mid- to senior- executive levels.

Interview guidelines

1. The interviews are being carried out by William Dicker.
2. At the beginning of the interview, the participant will be reminded about the purpose of the study.
3. Informed consent of the participant will be verified before asking any questions.
4. The participant will be asked to confirm they are ok being digitally recorded. The interview will be approximately 60-90 minutes.
5. A follow-up 30-minute interview may be scheduled to confirm expressed views.

Background		
1.	What is your job title, and how long have you held this position?	
2.	How many employees are in the organization?	
3.	What is the primary function of the business?	
4.	What regulatory oversight requirements, does your business have to comply (HIPAA, PCI/DSS, CMS)?	
5.	What type of proprietary or customer data do you want to protect?	
6.	How many information security employees do you have in your organization? What are those positions? If not, elaborate on the reasons for the absence of security employees.	
Motivation for the Selection (Why)		
1.	Did you ever have a full-time CISO or security team in your organization? ***If so, probe the answer more to include a job description, why the CISO left, why they did not hire a new CISO, responsibilities of the CISO, etc.*	
2.	In your own words, can you describe what you think a virtual Chief Information Security Officer (vCISO) is and what functions they perform?	
3.	What occurred that drove the decision for your organization to employ a vCISO? Explain your part in the hiring process. What was your goal when hiring a vCISO?	
4.	Explain your selection criteria for a vCISO? Did you hire an individual vCISO or a company that offers vCISO services? ***Probe the selection criteria to include experience and certifications, and number of organizations interviewed?*	
5.	Did you interview the vCISO before the employment contract was signed or did the company provide you a vCISO without your input? If you interviewed, who was involved and what items were discussed?	

6.	Was there a background check conducted? If so, what type, and by whom?	
7.	Did you verify references? If not, did you ask the company to verify references? ***Probe more*	
8.	How would you evaluate your vCISO selection? Please explain?	
9.	Describe the information security threats your organization faces?	
10.	What level of functionality did you want from the vCISO? Was it a **strategic-level employee, a technical employee or both**? What were your reasons for this decision? How did you determine this selection based on the functionality?	
11.	Can you describe any suspected or actual security breaches/incidents that your organization has encountered? Can you describe the most recent breach/incident? Type? Magnitude? How did you discover the breach?	
12.	Can you describe your information security culture and what is needed to improve it?	
13.	How do your employees react to information security threats to your organization? How do they support the implementation of security controls?	
Patterns and Processes (How)		
1.	Did you provide the vCISO with a mission statement or objectives of duties to be performed? If so, can you explain?	
2.	How long did the vCISO work for you? Was there a time limit on the contract?	
3.	Did the vCISO work an established set of hours or were they on call after hours? Please explain.	
4.	Were the vCISO services "project" based or "long-term" support? Explain in detail.	
5.	How long did you use vCISO services? How did you determine the length of the contract?	
6.	Did you use vCISO services more than one time?	
7.	Explain the contract (scope, time, and pricing) requirements of the vCISO service.	
8.	Explain the agreed upon services of the vCISO? Were these items negotiated or were they part of a package of services?	
9.	Are you currently using a vCISO? If so, can you explain the contract?	
10.	Did you introduce the vCISO to your employees? If so, how did the introduction occur? What title did you give for the vCISO?	
11.	Did you have employees reporting to the vCISO? If so, how does it work? Are they a direct report or dotted line? How do you evaluate the success of that reporting relationship?	
12.	What was the reporting structure of the vCISO? Please explain.	

13.	Was the vCISO on-site or did they work from a remote office? If they were onsite, did they have daily interactions with employees or leadership teams?	
14.	Do you currently have an information security program in place? If so, can you describe the program and how it came to be? Who was involved in the program design? How is it maintained? Is the protection designed for protection of data, compliance or both?	
15.	Do you have organizational business objectives concerning information security? If so, how are they connected?	
16.	Do you have an information security compliance program? If so, can you explain the process used in evaluating your compliance?	
Questions to be asked only if an information security program exists (Q 14).		
	Do you have information security policy and procedure manual developed? If so, how was it developed?	
	Do you track employee awareness of the manual? Do all employees receive the written manual or is it in electronic form? How is it disseminated? How frequently is it updated and by whom? How are the policies enforced and by whom?	
	Do you have a sanction policy? Explain the process for sanctioning an employee for policy violations?	
	Can you explain your infrastructure (workstations, hosted email, controls implemented, measurement of those controls)?	
	Do you have adequate funds to support the infrastructure?	
	Do you think your infrastructure is capable of growing alongside your projected growth plan?	
	Do you have security awareness training implemented? If so, explain the type of training and delivery method.	
	Do you conduct email phishing campaigns? If so, what were the results? What happens if an employee fails?	
	Do you have anti-virus installed on your machines? If so, how does it work for you? Are you satisfied with the product?	
	Explain your real-time alerting for security breaches? Who would your organization contact? How soon would the activation tree alert?	
	Has your organization completed any risk assessments? If so, were they conducted in-house or by a third party? Explain the process and results.	
	Did you have an auditing program? If so, what events were being audited.	
Benefits (Outcome)		
1.	How would you describe the services received from the vCISO hire? ***Probe deeper based on the answer.*	
2.	Did the vCISO services meet your expectations? ***Probe deeper based on the answer.*	
3.	Explain how your information security culture changed after you used the vCISO services.	

4.	Are there any additional information security areas you wish to strengthen?	
5.	How was the vCISO perceived by your employees/management?	
6.	What benefit do you perceive the employment of a vCISO provided to your organization?	
7.	Would you hire a vCISO again? Why?	
8.	Would you recommend a vCISO to another SMB? Why?	
9.	What would you do different internally to enhance/improve the value of the vCISO.	
10.	What would you do different internally to foster a stronger, more aware, info sec culture?	
11.	Is anything more do add? Are there sections that you would like to readdress?	
12.	On a scale of 1-7, 1 no value and 7 extremely valuable how would you evaluate the value of using a vCISO in their organization? Why do you give them this rating? What could be done by the vCISO to improve the score?	

vCISO Interview Protocol

This exploratory research uses interviews to examine the importance of a virtual Chief Information Security Officer (vCISO) in Small to Midsize Businesses (SMBs). It includes interviews with two to three employees representing SMBs, and four vCISOs representing the virtual Chief Information Security Officer industry. All interviewees are professionals and range from mid- to senior- executive levels.

Interview guidelines

1. The interviews are being carried out by William Dicker.
2. At the beginning of the interview, the participant will be reminded about the purpose of the study.
3. Informed consent of the participant will be verified before asking any questions.
4. The participant will be asked to confirm they are ok being digitally recorded. The interview will be approximately 60-90 minutes.
5. A follow-up 30-minute interview may be scheduled to confirm expressed views.

Background		
1.	What is your job title, and how long have you held this position?	
2.	How many years' experience as an actual CISO do you possess?	
3.	How many years' experience as a vCISO do you possess?	
4.	What information security certification do you possess?	
5.	What experience with regulatory requirements do you possess?	
6.	How many client engagements have you performed?	
7.	What is the typical duration of an engagement?	
8.	What is the motivation for SMBs to hire a vCISO over a full-time CISO?	

9.	Describe your perceptions of the threats that SMBs face?	
10.	In your own words, describe a typical client engagement, including services provided.	
11.	In your own words, describe a negative client engagement, including services provided.	
12.	In your own words, describe a positive client engagement, including services provided.	
13.	What are different between the three types of engagements? Do similarities exist? Are there anomalies?	
vCISO Employment		
1.	Do you work alone or as a team of vCISOs?	
2.	Explain the timeframe of client engagements. ***Probe*	
3.	On a typical engagement, do you work selected hours or are you on call as needed? Explain?	
4.	How did contract negotiations with clients requesting services work? Are you involved in the contract negotiations? **Probe*	
5.	Explain the level of functions you perform at client engagements. Strategic, Technical or both? ***Probe*	
6.	Explain the difference between project-based engagements and long-term engagements. Which do you prefer and why?	
7.	Do you work on more than one engagement at a time? If so, explain how this is managed.	
8.	Do your engagements require you to go to the SMBs work location? ***Probe*	
9.	Do you meet leadership teams during an engagement? If so, with whom did you meet? What discussion occurred during the meeting?	
10.	Did you meet with employees during the engagement? If so, with whom did you meet? What discussion occurred during the meeting? How were you introduced? What was the reactions of the employees?	
11.	Do you prepare executive-level briefings? If so, please elaborate.	
12.	Do you have SMB employees reporting to you during an engagement? If so, please elaborate.	
13.	Who do you report to during a client engagement?	
14.	What kind of support did you receive from your client during the engagement? Can you provide examples? If you did not receive support, can you provide examples?	
15.	What kind of obstacles did you encounter during the client engagement? Can you provide examples? How did you overcome these obstacles?	
vCISO Services		
1.	What would you consider a completed client engagement contract? ***Probe deeper based on answer*	
2.	How are goals determined between you and the client before the engagement begins?	

3.	Explain the client engagement kick-off call?	
4.	Did you receive a mission statement or scope of work before you begin the client engagement?	
5.	Does the client provide you with a security landscape before the engagement begins?	
6.	What additional information would you normally request from a client to better determine if the engagement is appropriate?	
7.	What information would you normally request from a client during an engagement to better meet the needs of the client?	
8.	Can you explain a situation where you declined a client engagement? Please provide an example.	
9.	Explain in detail the services you/your company offer? ***Probe services offered in detail*	
10.	Do your services require a single engagement, or do you work as a service retainer? Can you provide examples of both services, if applicable?	
Benefits (Outcome)		
1.	Explain the perceived benefits an SMB receives upon a completed client engagement?	
2.	How would you determine if a client has achieved Information Security Governance post client engagement? Please provide an example.	
3.	How was the vCISO perceived by the SMB/employees?	
4.	Can you describe a typical information security culture of a client before an engagement begins? Is this discussed during a kick-off call or as part of the contract?	
5.	To what extent did the information security culture change during a client engagement.	
6.	Please provide examples where you have returned to a client for repeated engagements? Can you provide examples of how a subsequent engagement continued to enhance the Information Security Governance of the organization?	
7.	Are there other areas that you recommended an SMB enhance/improve their information security and they refused? If so, please explain.	
8.	Are there any SMBs or types of SMBs that you would not work for again? If so, please explain.	
9.	What is the upside/downside to for a SMB to work with a vCISO?	
10.	Is anything more do add? Are there sections that you would like to readdress?	

VITA

William C. Dicker hails from Charleston, South Carolina, and is recognized for developing solid relationships with strategic partners and building consensus across multiple organizational levels. He is an accomplished leader with a proven track record of success in managing all aspects of information security operations.

William's strengths lie in leading, training, and motivating cross-functional teams to improve overall performance and develop and implement strategic plans to streamline business operations to achieve bottom-line results and continuous progress. Through his motivational and inspirational leadership style, William focuses on team building, ensuring each team member can perform at optimum levels.

William holds a Master of Science in Information Security from the University of Maryland University College (UMUC), and has attained numerous information security and compliance certifications, including the prestigious Certified Information Security Manager (CISM).