# Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises

Chad J. Ashley, DBA, MBA | BlueHalo, Director of Strategy and Innovation

Michelle Preiksaitis, JD, PhD, SPHR, SHRM-SCP | Coastal Organizational Research and Learning Strategies LLC (CORALS LLC)
http://orcid.org/0000-0002-3064-2392

Contact: chadashley.dba@gmail.com

## Abstract

Over the past decade, the number of cyberattacks affecting United States small- and medium-sized enterprises (SMEs) has increased substantially; with an average per-breach loss of $500,000 USD. Cyber-breaches most often result in business closure within 6 months of the breach. A modified Delphi technique used with a 20-member panel of cybersecurity experts was conducted to discover ways SMEs could prevent these breaches. Using four sequential survey rounds sent using confidential SurveyMonkey links, information and cybersecurity experts shared their ideas about forward-looking practices for strategic cybersecurity risk management for SMEs and then, after data analysis reduction occurred, provided expert opinions regarding their level of agreement with and consensus regarding strategic, cybersecurity, risk-management practices for SMEs. The experts were located through the UserInterviews platform, and their credentials were validated using LinkedIn data. Both qualitative and quantitative analyses led to a final list of 20 practices that could protect and secure business information, organized among three previously identified categories: security culture, strategic alignment, and value. After acquiring the list of practices, the final survey round asked the experts to rate the practices for desirability and feasibility. Comments from experts regarding their reasons for their choices and ratings were also documented, analyzed thoroughly, themed and discussed. The identified practices led to a new framework: the Ashley Information Protection Framework (AIPF). SME information professionals could use the AIPF to improve the overall security posture of their businesses and protect business intelligence from cyberattack. Other cybersecurity researchers could use the AIPF for future research on specific practices identified by this study.

**Keywords:** Cybersecurity, Strategic Risk Management, Secure Business Information, Business Intelligence, Security Culture, Strategic Alignment, Value Creation, The Ashley Information Protection Framework, Small And Medium Businesses

# Introduction

The trend towards the use of big data, technology, and business intelligence has grown exponentially over the past decade. Similarly, the threat and reality of cybercrime has increased, especially for small- to medium-sized enterprises (SMEs), which have fewer resources to protect against such attacks. Cyberattacks affected nearly 70% of surveyed owners of SMEs in 2020 (Tharnish, 2020) and over 58% of those surveyed admitted that security breaches occurred because of those attacks. Recent data showed that COVID-19 and the resulting move to more remote work and online data usage created new and unique security challenges for SMEs (Lallie et al., 2021). Bocetta (2019) found that 20% of all SMEs were victimized by cybercriminals and of those who experienced such attacks, nearly 60% of them were driven to close because of financial and reputational damages caused by breaches. IBM (2019) similarly noted that for SMEs, cybercrimes cost, on average, $2.5 million per breach. Since 2019, with unprecedented inflation and the impact of the pandemic, these costs are significantly higher. Connectwise (2022) reported that the changes to types of cybersecurity breaches from 2021 to 2022 will include a move from previous "big game hunting" methods (targeting huge organizations and utility grids) to smaller wins with SMEs, which will give them more targets and less exposure to being caught (p. 19).

The U.S. Small Business Administration's (SBA) chief information officer (CIO) encouraged all SMEs to implement cybersecurity strategies into their business plans (Brands, 2020). Numerous researchers have explained why SMEs ignore this advice, including lack of knowledge (Bada & Nurse, 2019; Scott, 2019; Small Business Administration, 2019; Watad et al., 2018), inadequate resources (Bada & Nurse, 2019; Paulsen & Toth, 2016; Scott, 2019; Small Business Administration, 2019; Watad et al., 2018), lack of appreciation of cybersecurity threats (Foley, 2017; Teymourlouei, 2018), and failure to recognize how human errors lead to breaches (Watad et al., 2018). Connectwise's 2022 report showed that more SMEs will fail to prevent breaches as the cost of talent increases post-pandemic will mean fewer dollars available for cybersecurity. As the war in Ukraine has increased the tensions between Russia and the U.S., Connectwise also warned that SMEs need to be ever vigilant for cyber-breaches. This study sought to find feasible and manageable strategic cyber-protective practices for SMEs to implement.

# Background

Cybercriminals exist in a dark world that is difficult to locate. Most SME leaders focus heavily on their day-to-day and strategic goals related to their service model or product lines and fail to recognize the danger of cyber-vulnerabilities until it is too late. Ghafir et al. (2018) showed how malicious cyberattacks advance in lockstep with technological advances; SME owners must include a dependable information technology (IT) infrastructure to support modern customer requirements and provide access to their services (Watad et al., 2018). Yet, few cybersecurity

strategy studies have focused on the special needs of SMEs, mostly focusing on large organizational needs and product lines. While the cost of IT products can seem steep, the potential for loss due to cybercrime is much greater (Watad et al.).

Many cybersecurity frameworks exist which lead large organizational leaders and CIOs through complex, dense, and expensive processes to protect their business information (Paulsen & Toth, 2016). Wild (2018) found 250 different cyber and information security frameworks in use, and since then, many more have been created. Kaušpadienė et al. (2019) noted that there are no strategies or guidelines for SMEs to use; Scott (2019) warned that most cybersecurity trainings are designed for larger organizations and not SMEs, even though at least 40% of SME data breaches are a result of employee error and human vulnerabilities. Finally, survey and research data continue to highlight the SME owner overall lack of appreciation of their own potential for victimization; a false sense of security in thinking they are too small to be noticed leads them into the traps of cybercriminals (Foley, 2017; McCollum, 2019).

# IT Business Problem and Gap in Practice

The United States (U.S.) SBA (2019) noted that 99% of all companies with employees in the U.S. were considered small businesses, they accounted for 33.3% of all export revenue totaling $429.3 billion and employed nearly half of all U.S. private-sector employees. While the global pandemic due to COVID-19 paused many SBA and government reporting centers, the number of SMEs moving to remote and hybrid worker models during that time has created a heightened problem for SMEs with fewer skilled workers to help create solutions (Connectwise, 2022). Considering the statistical relationship between cyberattack losses and SME closures, the impact to U.S. workers remains a concern and problem to the U.S. economy and SME functionality. The problem of cyberattacks remains a concern for all SME owners.

The literature review section of this article regarding SMEs and vulnerability to cybercrime shows that a gap in practice exists – SMEs simply do not recognize their potential for breach, they do not establish protective practices, and they do not have strategic plans in place to avoid cybertheft of their company and informational assets. This study's goal was the creation of a framework and a list of strategic practices that pertain specifically to SMEs, endorsed and established by knowledgeable SME cybersecurity experts. The practices were geared toward potential losses of five types of data defined by the Council of Economic Advisors (2018): personal identifying data, confidential intellectual property information, digital infrastructure knowledge, financial data, and infrastructure control data.

# Terms and Definitions

This study relied on the following terms and definitions of those terms to assist in a consistent and interpretable set of findings and results. These terms and definitions were shared with the expert panel to ensure that everyone understood the foundation of the problem and meaning of each word or strategic practice.

- ***Cybersecurity*:** Protecting information assets by addressing threats to information processed, stored, and transported by internetworked information systems (ISACA, n.d.).
- ***Information Security*:** Protecting information from unauthorized users, improper modification, and denial of data availability (HITRUST, 2020a; ISACA, n.d.).
- ***Security Culture*:** "A pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things" (ISACA, 2012, p 91).
- ***Small and Medium Enterprise (SME)*:** Independent businesses with fewer than 500 employees (U.S. Small Business Administration, 2019).
- ***Small and Medium Business Leadership*:** The persons who make SMEs' strategic decisions, manage the employees, allocate resources, or shape organizational culture.
- ***Strategic Alignment*:** Information and cybersecurity plans and activities that enable enterprise business strategy and objectives (International Organization for Standardization, 2018; ISACA, 2012).
- ***Value Creation*:** Demonstrating business value by positively contributing to business objectives resulting from information and cybersecurity activities or investments adjusted for risk (ISACA, n.d.; ISACA, 2012).

# Project Questions

Two project questions guided the data collection process of the study and explained the overarching aim of the study.

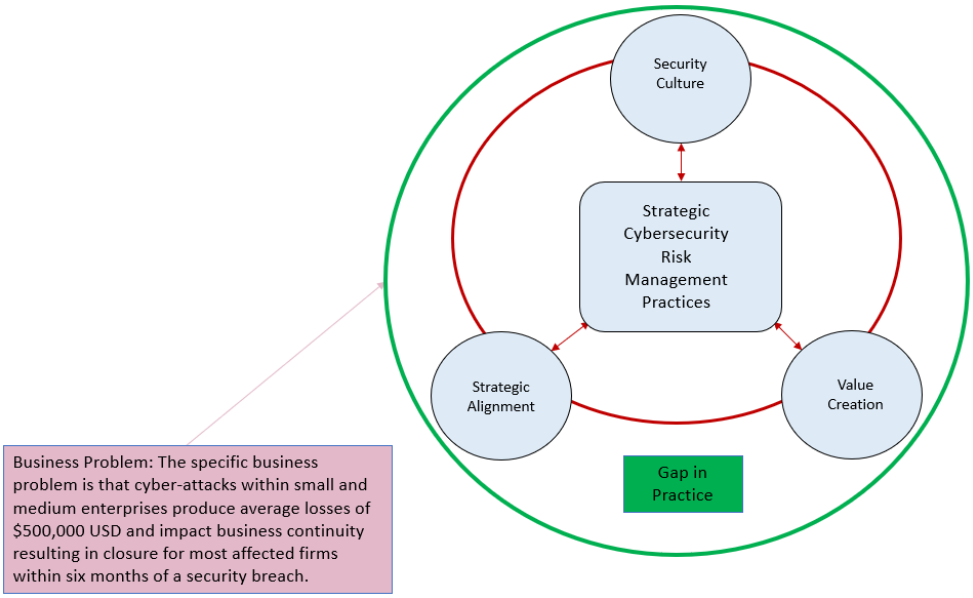
> **Question 1:** What forward-looking practices did a panel of IS strategic experts identify as best fitting the needs of strategic cybersecurity risk management of SME business information?
>
> **Question 2:** On which of the practices were IS strategic experts able to reach consensus as to their desirability and feasibility for strategic cybersecurity risk management of SME business information?

# Applied Framework

This project's initial guiding framework amalgamized 15 information and cybersecurity frameworks into three key business concepts: security culture, business alignment, and value creation (Figure 1 and Table 1).

**Figure 1**

*Applied Framework of Study*




*Note.* Framework pieces adapted from "SBA official: Hacks cost small business average of $500,000," by W. Heilman, *Colorado Springs Gazette*, (https://gazette.com/business/sba-official-hacks-cost-small-business-average-of-500-000/article_dc5e7e0a-f74f-11e9-a5b1-bb5b760b734b.html). "Small and mid-size businesses need to focus on cybersecurity," by M. Chevalier, *Security Magazine*, (https://www.securitymagazine.com/articles/89202-small-and-mid-size-businesses-need-to-focus-on-cybersecurity).

**Table 1**

Information Security Existing Frameworks with their Sources

| Framework | APA Citation |
|---|---|
| COBIT 5 | Information Systems Audit and Control Association. (2012). COBIT 5: A business framework for the governance and management of enterprise IT https://www.isaca.org/bookstore/cobit-5/wcb5 |
| Information Technology Infrastructure Library (ITIL) | Rouse, M. (2020). *Information technology infrastructure library (ITIL)*. https://searchdatacenter.techtarget.com/definition/ITIL |
| NIST Cybersecurity Framework (CSF) | National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. |

| | |
|---|---|
| | https://doi.org/https://doi.org/10.6028/NIST.CSWP.04162018 |
| ISO/IEC 38500 Information technology – Governance of IT for the organization | Holt, A. (2013). *Governance of IT: An executive guide to ISO/IEC 38500*. BCS Learning & Development Limited. http://ebookcentral.proquest.com/lib/capella/detail.action?docID=1213991 |
| ISO 27000 Series | International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://standards.iso.org/ittf/PubliclyAvailableStandards/ |
| NIST SP 800-53 Privacy Framework | National Institute of Standards and Technology. (2020). NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0. https://doi.org/https://doi.org/10.6028/NIST.CSWP.01162020 |
| NIST SP 800-171 | Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). Protecting controlled unclassified information in nonfederal systems and organizations. https://doi.org/https://doi.org/10.6028/NIST.SP.800-171r2 |
| HITRUST CSF | HITRUST. (2020b). HITRUST CSF version 9.4 https://hitrustalliance.net/csf-license-agreement |
| IT governance for SME | Josi, P. (2012). IT governance for SME. http://www.isaca.ch/images/downloads/downloads/diplomarbeiten/IT_Governance_for_SME.pdf |
| NIST NICE Framework | Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf?trackDocs=NIST.SP.800-181.pdf |
| Cyber Security Governance: A Component of MITRE's Cyber Prep Methodology | Bodeau, D., Boyle, S., Fabius, J., & Graubart, R. (2010). *Cyber security governance*. The MITRE Corporation. https://www.mitre.org/publications/technical-papers/cyber-security-governance |
| An Information Security Governance Framework | da Veiga, A., & Eloff, J. H. P. (2007). An Information Security Governance Framework. Information Systems Management, 24(4), 361-372. |

| | |
|---|---|
| Information security governance: Framework and toolset for CISO's and decision-makers | Volchkov, A. (2018). Information security governance: Framework and toolset for CISO's and decision-makers. Auerbach Publications. |
| Full IT Service Management | FITSM. (2016). Part 0: Overview and vocabulary. https://www.fitsm.eu/downloads/#toggle-id-1 |
| The Information Assurance for SMEs (IASME) Governance Standard for Information and Cyber Security | Dresner, D. G. (2018). The IASME governance standard for information and cyber security. (5). https://iasme.co.uk/wp-content/uploads/2019/04/IASMEStandardv5.pdf |
| Enterprise Risk Management | Committee of Sponsoring Organizations [COSO]. (2017). Enterprise risk management: Integrating with strategy and performance. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf |

# Literature Review

A modified Delphi technique relies first on a thorough literature review to identify the practices previously found in research and practice (Stewart et al., 1999). Then, the researcher can use all known practices as a foundation for moving forward and finding new, forward-looking practices or strategies. This section identifies the most pertinent of research used to seed the initial Delphi round.

*The Evolution of Cybersecurity Risk Management Literature*

Practitioners recognized that the information revolution gave firms a strategic and competitive advantage (Porter & Millar, 1985; Rastogi & von Solms, 2005), while the evolution of the personal computer introduced risk into the world of IT (Dlamini et al., 2009). Risks from information loss led to elementary security practices (i.e., passwords, physical locking of storage rooms); most early efforts related to information security focused on the technical aspects of security designed to manage cybersecurity risks (B. von Solms, 2000).

With the expansion of the internet and early e-commerce, firms focused on policy, procedures, standardization, best practices, and security plans (B. von Solms, 2006; S. H. von Solms, 2010). Firm leaders learned that these practices failed to address the human factor (da Veiga & Eloff, 2007). Managers were encouraged to communicate information security importance from top-down, and to lead by example (Corriss, 2010; da Veiga et al., 2020).

Throughout the early 2000s, information security experts and leaders began growing their knowledge and understanding of the need to implement risk management for their IT protections

(Dlamini et al., 2009; Gashgari et al., 2017; Posthumus & von Solms, 2004). Yet, SMEs continued to disregard the dangers of cyberattacks. While many sets of best practices have been created for and by large firms, scaled and appropriate practices for SMEs remain a gap in the body of knowledge and practices. The known practices were organized by the three categories gleaned from the frameworks listed in Table 1.

*Security Culture*

Security culture elements focus on human behavior, ways of working, and heightened security awareness across the organization. Bull (2019) asserted that a robust security culture has more influence on the successful implementation of a security strategy than security professionals' traditional hard skills. Noncompliance and poor enforcement undermine the strategy's goals (Bull, 2019). Companies should make security an everyday occurrence with rewards or reprimand for employee security behavior, creating a culture (Dresner, 2018). Many security experts proposed policy management, awareness, and training and education initiatives that work for larger firms with extensive resources (Santos-Olmo et al., 2016). SMEs, however, could not afford to adopt these initiatives to protect themselves from malicious actors, despite the potential for devastating loss by failing to do so. Research showed that a preventative information security culture mitigates human-related threats in organizations (da Veiga et al., 2020; Parsons et al., 2015).

Finding an appropriate security culture definition for SMEs was difficult since multiple definitions exist. Van Niekerk and von Solms (2010) argued for a four-element definition: artifacts, espoused values, shared tacit assumptions, and knowledge. AlHogail (2015) agreed that artifacts, values, and assumptions make up an IS culture but did not note knowledge as an element. Nel and Drevin (2019) found 24 cultural factors in their study. Nasir et al.'s (2019) meta-analysis of 79 studies identified 12 elements, plus multiple sub-elements. A scouring of the literature resulted in the security culture elements listed in Table 2 which fueled the survey instrument of the Round 1 modified Delphi approach.

**Table 2**

*Literature Review Summary Table for Security Culture*

| Citations | Solutions for Round 1 of Delphi Study |
|---|---|
| (Bull, 2019; ISACA, 2018; Santos-Olmo et al., 2016) | Audit the company culture to establish a set of KPI's to create a baseline security culture. |
| (AlHogail, 2015) | Develop methods to measure employee security competence. |
| (ISACA, 2018; Nel & Drevin, 2019) | Regular training programs create awareness for employees on how to respond to security threats. |

| | |
|---|---|
| (COSO, 2017; da Veiga et al., 2020; International Organization for Standardization [IOS], 2018) | Establish a comprehensive training program to promote information security knowledge among employees. |
| (COSO, 2017; IOS, 2018; Santos-Olmo et al., 2016) | A corporate learning initiative should be enacted to ensure the aspect of information security are communicated to all levels of the organization. |
| (AlHogail, 2015) | All employees should be trained on legal regulations regarding cybersecurity. |
| (Nel & Drevin, 2019) | Companies should invest in the personal needs of the employees to enhance loyalty and reduce the risk of insider threats. |
| (Santos-Olmo et al., 2016) | Security policies and practices tend toward simplicity to ensure employee convenience and easier adherence to information security practices. |
| (AlHogail, 2015; da Veiga et al., 2020; Nel & Drevin, 2019) | A comprehensive employee management system should be enacted that includes good and bad consequences of information security behaviors. |
| (AlGhamdi et al., 2020) | Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, practices, and consequences of protecting business information. |
| (Josi, 2012; Newhouse et al., 2017) | Develop strategies to mitigate insider threats to systems and networks. |
| (Dresner, 2018; Santos-Olmo et al. 2016) | Develop access control plans to control who can access business information with a “need to know” way of working. |
| (da Veiga & Eloff, 2007; Newhouse et al., 2017) | Leadership provides sponsorship for cybersecurity governance. |

*Strategic Alignment*

Multiple researchers have pointed to the need to align business process, services, and practices to ensure a more supportive security-focused culture (Josi (2012; Volchkov, 2018). As with security culture, the literature and existing frameworks were scoured to create the strategic alignment practice lists for the participants to use as a seed to their inputs.

Decision-makers struggle with prioritizing activities and their respective value, making alignment with the larger business difficult (Hayden, 2016). SME resource scarcity means that alignment is even more important for them to ensure resources are available for security activities (AlGhamdi et al., 2020). Pratt (2019) recommended including lower-level employees in the planning process and Petrie (2017) explained that using performance management metrics which included security imperatives would assist with strategic alignment goals. Other researchers warned that all corporate governance activities need to include a component of information security (Schinagl & Shahim, 2020; S.H. von Solms, 2010).

Strategic alignment of information security to business goals is not without its challenges. One-third of firms lacked an alignment between technology strategy and security in 2019 (Pratt, 2019), only 15% of SMEs had a security component in their strategy in 2020 (Lloyd, 2020) and Connectwise (2022) found the numbers for alignment and inclusion were even more dire for SMEs in 2021 and 2022 (finding two-thirds were underprepared for cyberattacks). Table 3 provides the literature-based findings of practices which fed the Round 1 survey for the study.

**Table 3**

*Literature Review for Strategic Alignment Elements*

| Citations | Solutions for Round 1 of Delphi Study |
|---|---|
| (Pratt, 2019) | Create a process where security teams and IT teams, developers, and functional business teams all collaborate early in the development cycle to ensure alignment of security and business goals |
| (Hayden, 2016) | Business leaders and information security teams jointly fill in Osterwalder's Business Model Canvas to understand all facets of the business, security, and customer relationships. |
| (Granneman, 2018; Volchkov, 2018) | Create an aligned business and security strategy and roadmap to span a three3-year period. |
| (Granneman, 2018; Stackpole, 2019) | Create a cross-functional committee to establish a centralized technology budget structure to offer transparency into IT security investments to internal stakeholders. |
| (Petrie, 2017) | Create information security key performance indicators that tie directly to business goals and imperatives. |
| (Bodeau et al., 2010; Josi, 2012; Volchkov, 2018) | Align information security practices with business strategy to support organizational objectives. |

| | |
|---|---|
| (Bodeau et al., 2010; Dresner, 2018; FITSM, 2016) | Leadership must be actively involved and committed to strategic planning related to security services in the organization. |
| (Bodeau et al., 2010; HITRUST, 2020b; National Institute of Standards and Technology, 2018) | Develop an organizational strategy to manage cybersecurity risks that supports business objectives. |
| (National Institute of Standards and Technology, 2020) | Develop appropriate activities (strategy making) to enable the organization to manage data with sufficient granularity to manage privacy risks. |
| (Bodeau et al., 2010; Dresner, 2018; HITRUST, 2020b) | Develop a risk management profile for use in strategy formulation. |

*Value Creation*

As noted in both the strategic alignment and security culture sections, SME resource-limitations mean that value creation for the business is a critical component of a cyber-focused implementation framework. The value creation component of the applied framework was built using elements included in COBIT 5 (ISACA, 2012), ISO 27000 (International Organization for Standardization, 2018), ISO 38500 (Holt, 2013), and Volchkov (2018). Additional customer-focused security strategies recommended by Farshchi and Douglas (2010), Dickson (2019), Boehm et al. (2019), and Wu and Saunders (2016) were also included. A company can create value with cybersecurity by creating a level of cybersecurity threat awareness across the business (Berkman et al., 2018).

Suer (2018) explained that leadership needs proof that information security adds to business value for them to consider it an essential function, while Scala et al., (2019) showed how establishing a set of measures that show the impact of information security on achieving organizational objectives helps provide that value-add proof. Showing the expensive results of cyberbreaches also lends to proving value-creation (Connectwise, 2022). Bailetti and Craigen (2020) and Hepfer and Powell (2020) recommended that the value of cybersecurity practices should be communicated to stakeholders to build confidence and trust that confidential business information is protected. Table 4 provides the value creation items and the literature from which they were derived.

**Table 4**

*Value Creation Items from the Literature*

| Citations | Solutions for Round 1 of Delphi Study |
|---|---|
| (Information Systems Audit and Control Association, 2012) | Ensure value creation is a foundational governance principle. |
| (Holt, 2013) | Develop means to ensure IT services meet current and future business requirements. |
| (Volchkov, 2018) | Develop strategies to optimize IT investments supporting organizational objectives. |
| (International Organization for Standardization, 2018) | Ensure the governance plans answer stakeholder needs by enhancing societal values. |
| (Volchkov, 2018) | Develop a performance measurement strategy to report information security metrics that ensure organizational objectives. |
| (Hepfer & Powell, 2020) | Communicate the firm's cybersecurity practices to customers, to build trust and confidence that critical business information is protected. |
| (Scala et al., 2019) | Develop information security metrics that measure security practices' impact on organizational objectives. |
| (Suer, 2018) | Develop a set of KPI's that measure the value of security investments. |
| (Xu et al., 2019) | Proactively make cybersecurity investments to protect business information that gain a competitive advantage. |
| (Xu et al., 2019) | Cybersecurity investments to protect business information should be made reactively as cyber threat information is made available. |
| (Bailetti & Craigen, 2020) | Communicate to stakeholders the importance the company places on protecting business information. |

# Modified Delphi Technique

This mixed-method study used a modified Delphi technique, rather than a classic Delphi technique. Instead of beginning with interviewing or focus group questioning for Round 1, the modified technique started the data collection with a survey seeded with practices and suggestions from the literature and frameworks, as shown in Tables 2, 3, and 4; it also elicited from the participants updated, future-looking, and additional information about each of those ideas (Stewart et al., 1999). Solomon et al. (2021) noted that the modified Delphi technique is "used in the social sciences as a method for formalizing input from multiple parties, using voting and discussion" (p. 342). In this study, four consecutive rounds of data collection and analysis occurred.

*Participant Recruitment and Requirements*

Purposive, nonprobabilistic sampling was used for this study to take advantage of expert knowledge regarding the study's cybersecurity focus, as recommended by Palinkas et al. (2015) and Skulmoski et al. (2007). Varying opinions exist about the best sample size and homogeneity needed for a Delphi expert panel (Akins et al., 2005; Avella, 2016; Keeney et al., 2001). A typical Delphi panel size is between 10-20 panelists and will see a participation rate of 70% (Akins et al., 2005; Hasson et al., 2000).

In this study, an *a priori* goal of 18 panel members was exceeded; 20 panelists contributed throughout all four rounds of the study. Attrition, which is normal for Delphi studies, was low; in this case, only two out of the 22 (9%) originally identified participants left the study prior to its completion. Based on comments from multiple participants, the low attrition was gained due to the experts' interest in both contributing to the results and learning about the final decisions of the panel.

*Participant Characteristics*

Skulmoski et al. (2007) said to ensure Delphi participants had knowledge relevant to the study topic, a willingness and capacity to participate, time to actively engage, and the ability to effectively communicate. Potential participants found through UserInterviews were provided the following criteria and the required expert qualifications (Keeney et al., 2001) to decide to self-select for the study:

- 3+ years of current experience in the information security, or cybersecurity, or IT management field;an
- bachelor's degree or higher in a related field or demonstrated equivalent experience; and
- experience in strategy formulation or consulting related to small and medium-sized business operations, cybersecurity, or information security activities.

Selected participants' qualifications were then cross-checked using LinkedIn before receiving invitations and informed consents for the study participation. Capella University IRB approval and forms were used to recruit, gain consent, and confirm qualifications of the participants.

# Delphi Data Collection and Analysis

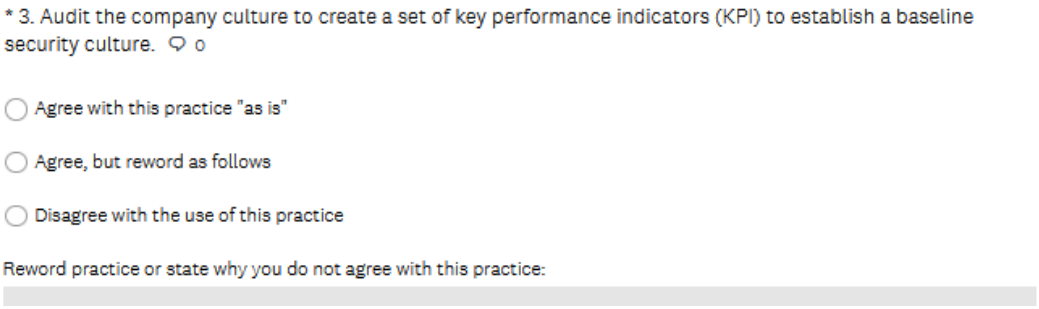
Delphi techniques use rounds of data collection and analysis, and in this study, four rounds were used. The analyses built on each round.

*Round 1 Data Collection*

A survey based on the findings from the literature review was created and reviewed by two Delphi technique experts. Two modifications occurred, including adding expert panel comment options to Round 1 and a ratings section. A sample item of Round 1 is provided in Figure 2.

**Figure 2**

*Sample Instrument Question from Round 1*




Round 1 was opened on June 5, 2021 and closed on June 12th, 2021 with one reminder sent June 10th. A response rate of 95% was achieved with average completion time of 24 minutes over the 20 participants (the one participant who failed to complete the survey was removed from the study). Round 1 included 35 strategic information and cybersecurity solutions organized by security culture, strategic alignment, and value creation (Tables 5, 6, and 7, respectively, with tallied responses). The panelists offered 64 unique comments on security culture, including solution rewording, disagreement explanations, or general unrelated comments (i.e., P9 said "Completed..Very interesting. I'm involved in this activity in my current company...Looking forward to the next survey...best."

**Table 5**

*Round 1 Panelists Responses – Security Culture*

| Solution | Total Number of Occurrences | | | |
|---|---|---|---|---|
| | Agree "as is" | Agree, but reword | Disagree | Comments |
| Audit the company culture to create a set of key performance indicators (KPI) to establish a baseline security culture | 14 | 4 | 2 | 5 |
| Develop methods to measure employee security competence. | 18 | 2 | 0 | 3 |
| Create regular information and cybersecurity training programs to create awareness for employees on how to respond to security threats. | 17 | 3 | 0 | 5 |
| Establish a comprehensive training program to promote information security knowledge among employees. | 18 | 2 | 0 | 3 |
| A corporate learning initiative should be enacted to ensure the aspect of information security are communicated to all levels of the organization. | 12 | 8 | 0 | 9 |
| All employees should be trained on legal regulations regarding cybersecurity. | 12 | 2 | 6 | 9 |
| Companies should invest in the personal needs of the employees to enhance loyalty and reduce the risk of insider threats. | 14 | 2 | 4 | 6 |
| Security policies and practices tend toward simplicity to ensure employee convenience for easier adherence to information security practices. | 12 | 3 | 5 | 6 |
| A comprehensive employee management system should be enacted that includes good and bad consequences of information security behaviors. | 14 | 4 | 2 | 5 |
| Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, practices, and | 17 | 2 | 1 | 3 |

| | | | | |
|---|---|---|---|---|
| consequences of protecting business information. | | | | |
| Develop strategies to mitigate insider threats to systems and networks. | 18 | 2 | 0 | 2 |
| Develop access control plans to control who can access business information with a “need to know” way of working. | 15 | 5 | 0 | 5 |
| Leadership provides sponsorship for cybersecurity governance. | 16 | 3 | 1 | 3 |

**Table 6**

*Round 1 Panelists Responses – Strategic Alignment*

| Solution | Total Number of Occurrences | | | |
|---|---|---|---|---|
| | Agree "as is" | Agree, but reword | Disagree | Comments |
| Create a process where security teams and IT teams, developers, and functional business teams collaborate early in the IT and enterprise software development cycle to ensure alignment of security and business goals. | 17 | 3 | 0 | 5 |
| Business leaders and information security teams joint fill in Osterwalder's Business Model Canvas to understand all facets of the business, security, and customer relationships. | 12 | 4 | 4 | 6 |
| An aligned business and security strategy and roadmap should be created to span a three-year period. | 9 | 7 | 4 | 9 |
| Create a cross-functional committee to establish a centralized technology budget structure to offer transparency into security and IT investments to internal stakeholders. | 14 | 0 | 6 | 4 |
| Create information security key performance indicators that tie directly to business goals and imperatives. | 17 | 1 | 2 | 2 |

| | | | | |
|---|---|---|---|---|
| Align information security practices with business strategy to support organizational objectives. | 18 | 0 | 2 | 1 |
| Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | 18 | 1 | 1 | 2 |
| Leadership active involvement and commitment to in strategic planning related to security services. | 14 | 5 | 1 | 6 |
| Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives. | 18 | 2 | 0 | 2 |
| Develop appropriate activities (strategy making) to enable the organization to manage data with sufficient granularity to manage privacy risks. | 19 | 1 | 0 | 1 |
| Develop a cybersecurity risk management profile for use in strategy formulation. | 20 | 0 | 0 | 0 |

**Table 7**

*Round 1 Panelists Responses – Value Creation*

| Solution | Total Number of Occurrences | | | |
|---|---|---|---|---|
| | Agree "as is" | Agree, but reword | Disagree | Comments |
| Ensure value creation is a foundational governance principle. | 14 | 4 | 2 | 5 |
| Develop means to ensure IT services meet current and future business requirements. | 19 | 1 | 0 | 2 |
| Develop strategies to optimize IT investments to support organizational objectives. | 19 | 1 | 0 | 1 |
| Ensure the information and cybersecurity governance plans answer stakeholder needs by enhancing societal values. | 11 | 0 | 9 | 7 |

| | | | | |
|---|---|---|---|---|
| Develop a performance measurement strategy to report information security metrics to assure the achievement of organizational objectives. | 19 | 1 | 0 | 1 |
| Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | 18 | 0 | 2 | 2 |
| Develop information security metrics that measure security practices' impact on organizational objectives. | 20 | 0 | 0 | 0 |
| Develop a cybersecurity KPI scorecard that reflects measures the value of security investments. | 16 | 4 | 0 | 4 |
| Cybersecurity investments to protect business information should be made proactively to obtain a competitive advantage. | 17 | 3 | 0 | 3 |
| Cybersecurity investments to protect business information should be made reactively as cyber threat information is made available. | 12 | 3 | 5 | 7 |
| Communicate to the stakeholders the importance the company places on protecting business information. | 20 | 0 | 0 | 0 |

*Round 1 Data Analysis*

The Round 1 comments ($N = 134$) included ideas to update, enhance, or reword the original solutions. enhancements to the original solutions. A significant number of changes and updates were made before moving the new list to Round 2. The following shows examples of how the Round 1 qualitative data were analyzed and used.

The original solution "Security policies and practices tend toward simplicity to ensure employee convenience for easier adherence to information security practices" received a comment from P3 that adding "effectiveness" and expanding the solution to include the four "P's" – policies, procedures, processes, and practices was appropriate. Other commenters ignored the term "employee convenience", instead saying "easier adherence," "easily understand and comply," and "easy to understand and comply." Synthesis yielded a more robust solution, "Security policies, procedures, processes, and practices should be kept simple, clear and effective to ensure that employee can easily understand them, making it easier to comply" for Round 2.

While some experts disagreed with solutions, their comments were uncompelling; thus, the solutions advanced to Round 2. However, multiple panelists disagreed with the solution, "An aligned business and security strategy and roadmap should be created to span a 3-year period." The comments showed that while the initial part of the practice was accepted, the period was too long. Round 2's version was, "An aligned business and security strategy and roadmap should be created and updated *annually*." Tables 8 through 10 show the updated solutions that were passed to Round 2 of the study. Overall, 25 original solutions (out of 34) were re-worded and nine new solutions were added (see tables, red comments).

**Table 8**

*Round 1 Synthesized Solutions Passed to Round 2 – Security Culture*

| Original Solution | Synthesized Solution | Justification |
|---|---|---|
| Audit the company culture to create a set of key performance indicators (KPI) to establish a baseline security culture. | Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs. | Completeness – added a time element to indicate the activity should not be a single event. The training and awareness programs were added to ensure the audit is to create actions and the KPI are a measure of progress. |
| Develop methods to measure employee security competence. | Develop methods to measure employee security competence and address any identified gaps**.** | Completeness |
| Create regular information and cybersecurity training programs to create awareness for employees on how to respond to security threats. | Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats. | Completeness – added the time element to ensure that this activity is not a one-time activity. |
| Establish a comprehensive training program to promote information security knowledge among employees. | Establish a comprehensive training program to promote information security knowledge among employees with additional training available depending on the employee role (i.e., secure coding for developers). | Completeness – addition of role specific training as appropriate. |

| | | |
|---|---|---|
| A corporate learning initiative should be enacted to ensure the aspect of information security are communicated to all levels of the organization. | A corporate learning initiative should be enacted or implemented to ensure that all appropriate aspects of information security are communicated to all levels of the organization. | Clarity |
| All employees should be trained on legal regulations regarding cybersecurity. | All employees should be trained on applicable legal regulations regarding cybersecurity. | Clarity |
| Companies should invest in the personal needs of the employees to enhance loyalty and reduce the risk of insider threats. | Companies should evaluate employee needs on a regular basis to identify any potential issues that could lead to the risk of insider threats. | Completeness and clarity – evaluation and identification of employee needs to reduce insider threat are more clearly actionable. |
| Security policies and practices tend toward simplicity to ensure employee convenience for easier adherence to information security practices. | Security policies, procedures, processes, and practices should be kept simple, clear, and effective to ensure that employees can easily understand them making it easier to comply. | Completeness – addition of the two other “P”’s to include practices and procedures and the element of understandability to ease compliance. |
| A comprehensive employee management system should be enacted that includes good and bad consequences of information security behaviors. | A comprehensive employee management system should be enacted that reinforces positive behavior and ensures bad behavior and poor security habits are addressed and corrected appropriately. | Completeness |
| Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, practices, and consequences of protecting business information. | Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, procedures, processes, practices, and the importance of protecting business information. | Completeness – addition of the four “P’s” |

| | | |
|---|---|---|
| Develop strategies to mitigate insider threats to systems and networks. | Develop strategies and plans to understand and mitigate insider threats to systems and networks. | Completeness |
| Develop access control plans to control who can access business information with a "need to know" way of working. | Develop and maintain access control plans to control who can access what business information based on a "need to know" principles. | Clarity |
| Leadership provides sponsorship for cybersecurity governance. | Leadership provides sponsorship, ownership, and direction for cybersecurity governance. | Completeness |
| Develop employee training and reward programs to enhance employee "buy-in". | | New solution. |
| Cybersecurity news and general how-to's should be regularly shared with staff to encourage a sense of security culture normalcy. | | New solution. |
| If a cyber incident occurs, employees should be informed of needed behavioral changes, and training programs should be developed if needed. | | New solution. |
| Educate and enhance awareness of information security as a way of working life. | | New solution. |
| Create an ongoing risk register that can be used to promote information security knowledge among employees. | | New solution. |
| Review program practices to ensure that new procedure has minimal impact on work products. | | New solution. |
| Monitor the network with Security information and event management (SIEM) tools. | | |

*Note:* Additional practices suggested by the panelists are in red.

**Table 9**

*Round 1 Synthesized Solutions Passed to Round 2 – Strategic Alignment*

| Original Solution | Synthesized Solution | Justification |
|---|---|---|
| Create a process where security teams and IT teams, developers, and functional business teams collaborate early in the IT and enterprise software development cycle to ensure alignment of security and business goals. | Create a process where security teams and IT teams, developers, and functional business teams collaborate early in the IT and enterprise software development cycle to ensure alignment of security and business goals with clearly defined objectives. | Completeness |
| Business leaders and information security teams joint fill in Osterwalder's Business Model Canvas to understand all facets of the business, security, and customer relationships. | Business and information security teams document all facets of the business, security, and customer relationships such as the Osterwalder's Business Model Canvas | Appropriateness – reworded to use the BMC as an example tool and not the only tool that can be used. Each business may need to use a different tool. The goal of the study is to find practices that an SME can use - not all will be able to use the BMC. |
| An aligned business and security strategy and roadmap should be created to span a 3-year period. | An aligned business and security strategy and roadmap should be created and updated annually. | Appropriateness – The panelist recommendations were clear that the span of 3 years is too long for this topic because the landscape changes rapidly. All comments that suggest rewording suggested a 1-year period was appropriate. |
| Create a cross-functional committee to establish a centralized technology budget structure to offer transparency into security and IT investments to internal stakeholders. | Create a cross-functional committee to establish a centralized technology budget structure offering transparency into security and IT investments to internal stakeholders. | No Change – the comments were more observational and not recommendations to reword the solution. |

| | | |
|---|---|---|
| Create information security key performance indicators that tie directly to business goals and imperatives. | Create information security key performance indicators that align directly to business goals and imperatives and clearly articulate the risks that are being addressed. | Completeness - The addition of "clearly articulate the risk that are being addressed" more aligns this practice with the key business concept "*Strategic Alignment*". The practice is strengthened by the addition. |
| Align information security practices with business strategy to support organizational objectives. | Align information security practices with business strategy to support organizational objectives. | No Change – the comments were more observational and not recommendations to reword the solution. |
| Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | No Change – the comments were more observational and not recommendations to reword the solution. |
| Leadership active involvement and commitment to in strategic planning related to security services. | Leadership maintains active involvement and commitment to strategic planning related to security services. | Completeness - The addition of maintains to the solution adds a "time element" to the solution and clarifies the ongoing role of SME leadership to address the evolving security threats. |
| Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives. | Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives with clearly defined ownership. | Completeness - The addition of "clearly defined ownership" strengthens the solution. Identification of who will own the implementation of the strategy is critical. |
| Develop appropriate activities (strategy making) to enable the organization to manage data with sufficient granularity to manage privacy risks. | Develop appropriate activities (strategy making) to enable the organization to manage data with sufficient granularity to manage privacy and security risks. | Completeness - The addition is logical and enhances the solution by adding “security risks” to privacy risks. |

| | | |
|---|---|---|
| Develop a cybersecurity risk management profile for use in strategy formulation. | Develop a cybersecurity risk management profile for use in strategy formulation. | No Change – no recommended rewording or comments were provided by the panelists. |

*Note.* No new solutions were proposed.

**Table 10**

*Round 1 Synthesized Solutions Passed to Round 2 – Value Creation*

| Original Solution | Synthesized Solution | Justification |
|---|---|---|
| Ensure value creation is a foundational governance principle. | Ensure value creation is a foundational governance principle. | No Change – comments did not offer rewording. |
| Develop means to ensure IT services meet current and future business requirements. | Develop means to ensure IT services meet current and future business requirements. | The original wording will remain for this practice. A review of the original practice sources from ISO38500 intended to address any IT services are meant to do what is necessary - not over-engineered or under-engineered to meets its purpose. Ensuring any IT service meets requirements required resources. Requirements in technical disciplines are another way to describe how resources are expended (tasks and money are not separable). |
| Develop strategies to optimize IT investments to support organizational objectives. | Develop strategies to optimize IT investments to support organizational objectives including the identification and reduction of risk. | Completeness. |

| | | |
|---|---|---|
| Ensure the information and cybersecurity governance plans answer stakeholder needs by enhancing societal values. | Ensure the information and cybersecurity governance plans answer stakeholder needs by enhancing societal values. | No Change – comments did not offer rewording. |
| Develop a performance measurement strategy to report information security metrics to assure the achievement of organizational objectives. | Develop a performance measurement strategy to report information security metrics to allow for informed decision making in the pursuit of organizational objectives. | Completeness |
| Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | No Change – comments did not offer rewording. |
| Develop information security metrics that measure security practices' impact on organizational objectives. | Develop information security metrics that measure security practices' impact on organizational objectives. | No Change – comments did not offer rewording. |
| Develop a cybersecurity KPI scorecard that reflects measures the value of security investments. | Develop a cybersecurity KPI scorecard that measures the value of security investments. | Clarity |
| Cybersecurity investments to protect business information should be made proactively to obtain a competitive advantage. | Cybersecurity investments should be made to proactively to protect business information. | Clarity |
| Cybersecurity investments to protect business information should be made reactively as cyber threat information is made available. | Cybersecurity threats should be continuously monitored, and new investments should be made as additional threat information becomes available. | The panelist comments state that investments are made based on a "reaction to new information" and aligns with the intent of the original practice. |

| | | |
|---|---|---|
| Communicate to the stakeholders the importance the company places on protecting business information. | Communicate to the stakeholders the importance the company places on protecting business information. | No Change – comments did not offer rewording. |
| Develop additional security planning to support organizational growth objectives. | | New solution. |
| Cybersecurity investments to protect business information should be made to address current and emerging risk to the organization. | | New solution. |

*Note:* Additional practices suggested by the panelists are in red.

*Round 2 Data Collection*

The synthesized and new solutions from Tables 8, 9, and 10 became the foundation of the Round 2 instrument. The goal for Round 2 was to learn whether the experts felt the solutions gleaned from literature from large firm research could also be desirable (useful) and feasible (existing, affordable, *and* manageable) for SMEs. The rating system used Likert-type scales as shown in Table 11.

**Table 11**

*Round 2 Instrument Ratings*

| Rating Level | Desirability | Feasibility |
|---|---|---|
| 5 | Very desirable | Very Feasible |
| 4 | Desirable | Feasible |
| 3 | Neither desirable nor undesirable | Neither feasible nor infeasible |
| 2 | Undesirable | Infeasible |
| 1 | Very undesirable | Very infeasible |

The Round 2 survey was opened from June 15 to 22, 2021, with email reminders sent on June 18th and 20th. The survey achieved a 100% response rate ($N = 20$) and, on average, participants spent 27 minutes completing the survey. The predetermined requirement for earning a "desirable and feasible" final rating was 4 or above for each category.

*Round 2 Data Analysis*

The Round 2 scores for *desirability* and *feasibility* were analyzed using the threshold of 75% for advancing the solution to Round 3. Tables 8 to 10 provide the advanced solutions with their scores.

**Table 8**

*Security Culture Solutions Advanced to Round 3*

| Solution | Desirability | Feasibility |
|---|---|---|
| Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs. | 90% | 75% |
| Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats. | 95% | 95% |
| Establish a comprehensive training program to promote information security knowledge among employees with additional training available depending on the employee role (i.e., secure coding for developers). | 95% | 80% |
| A corporate learning initiative should be enacted or implemented to ensure that all appropriate aspects of information security are communicated to all levels of the organization. | 100% | 75% |
| Security policies, procedures, processes, and practices should be kept simple, clear, and effective to ensure that employees can easily understand them making it easier to comply. | 95% | 75% |
| Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, procedures, processes, practices, and the importance of protecting business information. | 90% | 85% |
| Develop and maintain access control plans to control who can access what business information based on a “need to know” principles. | 100% | 95% |
| Develop employee training and reward programs to enhance employee "buy in". | 85% | 80% |
| Cybersecurity news and general how-to's should be regularly shared with staff to encourage a sense of security culture normalcy. | 90% | 75% |

| | | |
|---|---|---|
| If a cyber incident occurs, employees should be informed of needed behavioral changes, and training programs should be developed if needed. | 95% | 95% |
| Monitor the network with Security information and event management (SIEM) tools. | 100% | 85% |

**Table 9**

*Strategic Alignment Solutions Advanced to Round 3*

| Solution | Desirability | Feasibility |
|---|---|---|
| An aligned business and security strategy and roadmap should be created and updated annually. | 100% | 85% |
| Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | 90% | 85% |
| Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives with clearly defined ownership. | 100% | 75% |

**Table 10**

*Value Creation Solutions Advanced to Round 3*

| Solution | Desirability | Feasibility |
|---|---|---|
| Ensure value creation is a foundational governance principle. | 90% | 75% |
| Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | 85% | 90% |
| Cybersecurity investments should be made to proactively to protect business information. | 95% | 80% |
| Cybersecurity threats should be continuously monitored, and new investments should be made as additional threat information becomes available. | 100% | 75% |
| Communicate to the stakeholders the importance the company places on protecting business information. | 95% | 100% |

| Solution | Desirability | Feasibility |
|---|---|---|
| Cybersecurity investments to protect business information should be made to address current and emerging risk to the organization. | 100% | 75% |

After applying the 75% threshold, 20 solutions moved to Round 3 from a field of 44 (Table 11). The panel rated one solution as undesirable: "Ensure the information and cybersecurity governance plans answer stakeholder needs by enhancing societal values," with a desirability score of 55%. All other omitted solutions were rated infeasible for SMEs, even though they were desirable.

**Table 11**

*Percentage of Solutions Advanced to Round 3*

| Key Business Concept | Total Count | Desirable | Feasible | Advanced to Round 3 |
|---|---|---|---|---|
| Security Culture | 20 | 20 | 11 | 55% |
| Strategic Alignment | 11 | 11 | 3 | 27% |
| Value Creation | 13 | 12 | 6 | 50% |

*Round 2 Themes*

Comments provided by the panelists for each of the solutions presented were qualitatively analyzed to create themes.

**Round 2 Theme 1: Types of Training to Assist with SME Cybersecurity.** P2 thought "departmental" training was appropriate, and P3, P4, and P20 suggested that "role-based training was desirable as a security culture-building practice." However, comments recommended not training people about legal issues. P1 stated, "I can't see a company of my size trying to train everyone on legal regulations of cybersecurity." P9 stated this was desirable "but heavy" and P13 suggested that "This one seems tough because legal regulations regarding cybersecurity is broad. Currently, it is trying to achieve the fact that employees are made aware of cybersecurity trends and actions; applicable regulations may be an unnecessary uplift for 'all employees'". P2 said, "I don't need to have contract knowledge," and P3 said, "few benefit from knowing the legal framework surrounding it all."

**Round 2 Theme 2: Top-Down Solutions for SME Cyber Policies Difficult.** Some commenters were negative about upper-leadership's inputs into policymaking. P6 stated, "Many think they are above the law. In many ways, they are," yet P7 said, "if senior leadership is not driving and leading by example, this all falls apart quickly." P1 said, "my c-suite has zero interest in any sort of security initiatives, let alone taking ownership of any," and P4 warned, "you don't want

someone in leadership that knows nothing about security telling you what you need." Overall, commenters suggested that upper leadership in SMEs may be part of the security problem.

**Other Thoughts from Round 2 to Round 3.** Panelists did comment that the study was useful. P1 offered via the User Interviews internal messaging platform, "Really enjoying the surveys so far! Interesting questions I've never thought about before that I'm going to implement in my own organization." P11 offered, "This was very insightful. Really in-depth questions which really made me think about different possibilities and scenarios." P16 offered,

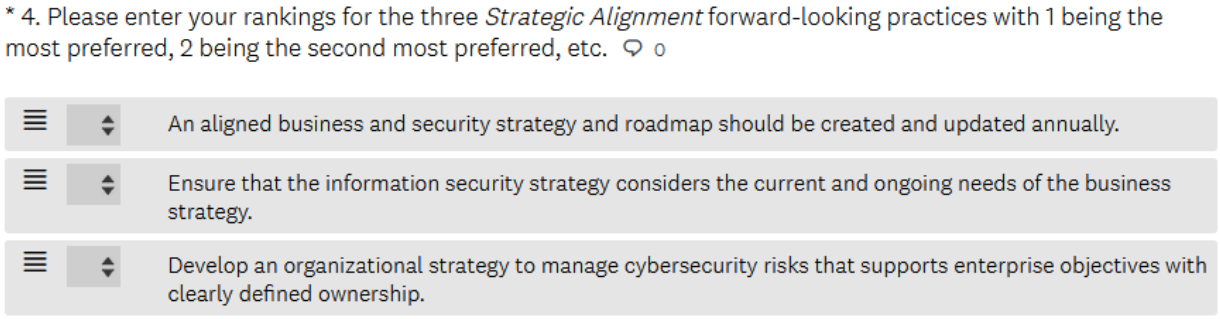
> *I am deeply into Cyber Security, GRC and been managing some large initiatives for FinTech and social media companies. I usually like to stay ahead of the curve and these studies/surveys are one way to know and see how researchers are reinventing the Cybersecurity landscape.*

*Round 3 Data Collection*

The Round 3 survey, consisting of the remaining 20 solutions, was opened to participants from June 23 to 30, 2021, and received a 100% response rate with an average of 8 minutes spent. Panelists rank-ordered the solutions within each category using a scale of 1 = *most important,* 2 = *next most important,* etc. Figure 3 shows a sample survey question.

**Figure 3**

*Round 3 Strategic Alignment Sample Question*




**Round 3 Data Analysis**

The ranking decisions were analyzed using weighted averages, as per the following equation, where $r$ = response count for the answer choice and $w$ = weight of the ranking choice:

$$\frac{r_1 w_1 + r_2 w_2 + \cdots r_n w_n}{number\ of\ responses}$$

Weights were reverse ranked to give the highest ranked item (1) the highest ranked store (i.e., 11 for security culture). Tables 12 to 14 show the weighted average rankings for Round 3, provided from highest ranked item (most important) to lowest ranked item (least important).

**Table 12**

*Security Culture Weighted Average Rankings*

| Solution | Score |
|---|---|
| Develop and maintain access control plans to control who can access what business information based on a “need to know” principles. | 7.80 |
| Monitor the network with security information and event management (SIEM) tools. | 7.25 |
| Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, procedures, processes, practices, and the importance of protecting business information. | 6.65 |
| Security policies, procedures, processes, and practices should be kept simple, clear, and effective to ensure that employees can easily understand them making it easier to comply. | 6.45 |
| Establish a comprehensive training program to promote information security knowledge among employees with additional training available depending on the employee role (i.e., secure coding for developers). | 6.10 |
| Develop employee training and reward programs to enhance employee "buy in". | 6.00 |
| If a cyber incident occurs, employees should be informed of needed behavioral changes, and training programs should be developed if needed. | 5.90 |
| A corporate learning initiative should be enacted or implemented to ensure that all appropriate aspects of information security are communicated to all levels of the organization. | 5.80 |
| Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats. | 5.60 |
| Cybersecurity news and general "how-to's" should be regularly shared with staff to encourage a sense of security culture normalcy. | 4.55 |
| Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs. | 3.90 |

**Table 13**

*Strategic Alignment Solutions Weighted Average Rankings*

| Solution | Score |
|---|---|
| Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives with clearly defined ownership. | 2.45 |
| Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | 1.85 |
| An aligned business and security strategy and roadmap should be created and updated annually. | 1.70 |

**Table 14**

*Value Creation Solutions Weighted Average Rankings*

| Solution | Score |
|---|---|
| Cybersecurity threats should be continuously monitored and new investments should be made as additional threat information becomes available. | 4.50 |
| Cybersecurity investments to protect business information should be made to address current and emerging risk to the organization. | 4.40 |
| Cybersecurity investments should be made to proactively to protect business information. | 3.55 |
| Communicate to the stakeholders the importance the company places on protecting business information. | 2.95 |
| Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | 2.85 |
| Ensure value creation is a foundational governance principle. | 2.75 |

*Round 4 Data Collection*

The Round 4 survey measured the experts' confidence level in the final set of solutions. Open from July 2 to July 7, 2021, it received a 100% response rate with average time spent of 12 minutes. The instrument listed the solutions with the following scale of choices:

5 = *Very Confident (low risk of being wrong),*
4 = *Confident (some risk of being wrong),*
3 = *Neither Confident nor Unconfident (neutral),*
2 = *Unconfident (substantial risk of being wrong),*
1 = *Very Unconfident (great risk of being wrong).*

*Round 4 Data Analysis*

Solutions receiving at least 70% of the panelists rating of 4 or higher were considered credible. Tables 15 to 17 show the confidence rating scores.

**Table 15**

*Security Culture Confidence Rating Scoring Totals*

| Solution | 1 | 2 | 3 | 4 | 5 | Percent |
|---|---|---|---|---|---|---|
| Develop and maintain access control plans to control who can access what business information based on a "need to know" principles. | 1 | 1 | 1 | 5 | 12 | 85 |
| Monitor the network with security information and event management (SIEM) tools. | 1 | 1 | 3 | 5 | 10 | 75 |
| Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, procedures, processes, practices, and the importance of protecting business information. | 0 | 0 | 2 | 9 | 9 | 90 |
| Security policies, procedures, processes, and practices should be kept simple, clear, and effective to ensure that employees can easily understand them making it easier to comply. | 0 | 0 | 2 | 6 | 12 | 90 |
| Establish a comprehensive training program to promote information security knowledge among employees with additional training available depending on the employee role (i.e., secure coding for developers). | 0 | 1 | 9 | 10 | 8 | 95 |
| Develop employee training and reward programs to enhance employee "buy-in". | 1 | 2 | 6 | 4 | 7 | 55 |
| If a cyber incident occurs, employees should be informed of needed behavioral changes, and training programs should be developed if needed. | 0 | 1 | 2 | 7 | 10 | 85 |
| A corporate learning initiative should be enacted or implemented to ensure that all appropriate aspects of information security are communicated to all levels of the organization. | 0 | 1 | 4 | 5 | 10 | 75 |
| Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats. | 0 | 1 | 3 | 4 | 12 | 80 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Cybersecurity news and general "how-to's" should be regularly shared with staff to encourage a sense of security culture normalcy. | 0 | 2 | 2 | 8 | 8 | 80 |
| Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs. | 0 | 1 | 6 | 5 | 8 | 65 |

*Note:* The practices highlighted in red did not meet the 70% confidence threshold.

**Table 16**

*Strategic Alignment Confidence Rating Scoring Totals*

| Solution | 1 | 2 | 3 | 4 | 5 | Percent |
|---|---|---|---|---|---|---|
| Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives with clearly defined ownership. | 0 | 1 | 2 | 7 | 10 | 85 |
| Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | 0 | 2 | 2 | 7 | 9 | 80 |
| An aligned business and security strategy and roadmap should be created and updated annually. | 0 | 0 | 6 | 4 | 10 | 70 |

**Table 17**

*Value Creation Confidence Rating Scoring Totals*

| Solution | 1 | 2 | 3 | 4 | 5 | Percent |
|---|---|---|---|---|---|---|
| Cybersecurity threats should be continuously monitored, and new investments should be made as additional threat information becomes available. | 0 | 0 | 0 | 10 | 10 | 100 |
| Cybersecurity investments to protect business information should be made to address the current and emerging risk to the organization. | 0 | 0 | 1 | 10 | 9 | 95 |
| Cybersecurity investments should be made to proactively to protect business information. | 1 | 1 | 1 | 8 | 9 | 85 |
| Communicate to the stakeholders the importance the company places on protecting business information. | 0 | 2 | 2 | 7 | 9 | 80 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | 0 | 3 | 2 | 6 | 9 | 75 |
| Ensure value creation is a foundational governance principle | 1 | 1 | 6 | 5 | 7 | 60 |

*Note:* The practice highlighted in red did not meet the required 70% confidence threshold.

**Round 4 Reasons for Low Confidence.** The security culture had two low-confidence practices. The reasons for low-confidence ratings seemed somewhat conflicting. While multiple commenters stated that reward programs were unnecessary practices, other comments in the training area stated that certificates (often considered rewards) were important to give out after training. Representative comments included P5's "I don't see the need for reward programs related to training. Employees should be paid competitive wages, and their comp[ensation] will be based on job responsibility which entails the protection of information/security, etc."; P8 stated, "Training is critical, rewards may not be necessary,"; and P6 wrote that the focus should be on operations and not individual's buy-in:

> *I think this should be placed closer to the back of the list. We're talking about small companies, again, so I just don't think we should be focusing so much on the individual's buy-in to the program and more focused on the technical operations of the program. I think this is a valuable item, however. Just not number 6.*

P9 stated,

*Initial training process involves getting the employee a visual certificate for completing levels of training. Management makes it a point to elevate employees who do well in training.*

P20 added,

*Some employees need incentives to peak [*sic*] interest. No harm has ever come from offering rewards.*

P14 offered that developing employee buy-in was a *good practice and should be mandatory*.

These comments suggested that there may not be a consensus among experts on the need to create a reward program to gain employee buy-in as it pertains to developing and building a security culture. P3 stated, *You can't manage what you don't measure.* And P14 stated, *This is a good practice and should be mandatory.*

P6 felt the practice deserved a higher overall ranking,

*This should be much higher up in the list. KPI's need to be established, reviewed, and measured FREQUENTLY.*
P5 expressed,

*Operating effectiveness of existing internal control should be examined on at least an annual basis. External reviews or evaluations are essential for accountability and independence.*

The removal of *Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs* seemed related to SME skepticism. P7 stated, *getting this established is much easier than maintaining it*. P8 offered, *Good practice, but goals need to be set with achievable milestones*. This comment may suggest that achievable milestones are either overlooked or not established properly. P9 stated:

> *This has been driven more by the weight of the damages to the organization instead of regularity...We have had some big hits this year, and our KPIs did not help us get that under control...we are still developing strategies and KPIs.*

The low-confidence value creation practice was *Ensure value creation is a foundational governance principle.* P3 offered, *Sounds like this comes out of LEAN.. if it doesn't create (or have) value, don't do it*. P9 stated, *We review our process based on this key point....it is a fundamental Agile principle*. P14 offered this practice should be mandatory, and P6 stated, *This will help the overall program succeed!* P5 wrote, *Encourage value creation throughout an organization will yield more motivation and a better security culture.* Despite these five positive comments, the item earned lowered confidence due to significant neutral responses.

# Results and Discussion

The results of the study fulfilled its original purpose of discovering strategic cybersecurity risk-management practices for SMEs and learning whether an expert panel agreed on the importance, desirability, feasibility, and confidence level of those practices. Using an applied framework, the study was guided by previous research, the stated problem, and the gap in practice.

Two project questions were answered by the study:

> **Question 1:** Which forward-looking practices did a panel of IS strategic experts identify as best fitting the needs of strategic cybersecurity risk management of SME business information?

Tables 8, 9, and 10 provided the forward-looking practices from the panel participants, while tables 12, 13, and 14 provided the ranked importance levels.

> **Question 2:** Which of the practices were IS strategic experts able to reach consensus on as to their desirability and feasibility for strategic cybersecurity risk management of SME business information?

Tables 15, 16, and 17 provided the panel experts' choices of the solutions and practices they were most confident, as a team of experts, in assisting SMEs with their cybersecurity risk-management choices.

# Discussion

ISACA (2012) defined a security culture as "A pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things" (p. 91). The study results confirmed the ISACA definition. For example, the comments related to *Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats* included P3's, *make it so* and P14's, *This is a good practice and should be mandatory. Adjust to the changing times/environment*. P2 stated, *should be mandatory*, and P9 added, *Yes, we have training to match most recent types of attacks.... this has worked.* The study replicated Nel and Drevin's (2019) suggestion that training and awareness efforts are critical to building a security culture.

Strategic alignment is defined as information and cybersecurity plans and activities that enable enterprise business strategy and objectives (International Organization for Standardization, 2018; ISACA, 2012). The results showed that the three practices suggest that a SME should align the business and security strategy using roadmaps that address current and future needs and risks, which comports with Granneman's (2018) suggestion that a roadmap for both the business and security strategy should be created.

Pratt (2019) had found one-third firms lacked cybersecurity strategies and Connectwise (2022) has increased that estimate to two-thirds post-pandemic. The study panelists commented that SMEs most certainly need a cybersecurity strategy. P6 remarked, *This is a key objective for an SMB. Security has to be seen as an enabler for the organization*. P3 supported P6's assertion, *The whole reason for the security is to support the organization's mission*, and P20 stated, *An aligned strategy is critical in meeting business goals*. P10 added, *My confidence assessment increases to the extent that information security policy is "written" into general business strategic thinking*, One panelist offered his firm is actively engaging in this practice.

Value creation is defined as the demonstration of business value by positively contributing to business objectives resulting from information and cybersecurity activities or investments adjusted for risk (ISACA, n.d.; ISACA, 2012). The concept of value creation is predicated on the premise that information security should advantage the business in some way. The literature showed revenue, profits, innovation, customer retention, and growth are enhanced when robust cybersecurity practices are enacted in SMEs (Lloyd, 2020). A key consideration for any business is the customers they serve. Bailetti and Craigen (2020) and Hepfer and Powell (2020) recommended that the value of cybersecurity practices should be communicated to stakeholders to build confidence and trust that confidential business information is protected. The study showed a theme of communicating the firm's security posture to customers and stakeholders. P5 stated, *This is one of the best things that can be done, assuming there is data to back this up*, and *This is important at all companies. It gets more consideration when it is a public declaration or*

*contractual requirement for a certain level of information security (e.g., encryption of data, etc.).* P20 stated, *Always communicate steps you've taken to harden security* and *effective communication with stakeholders is critical*. P14 offered that communicating with customers and stakeholders is *good practice and should be mandatory*.

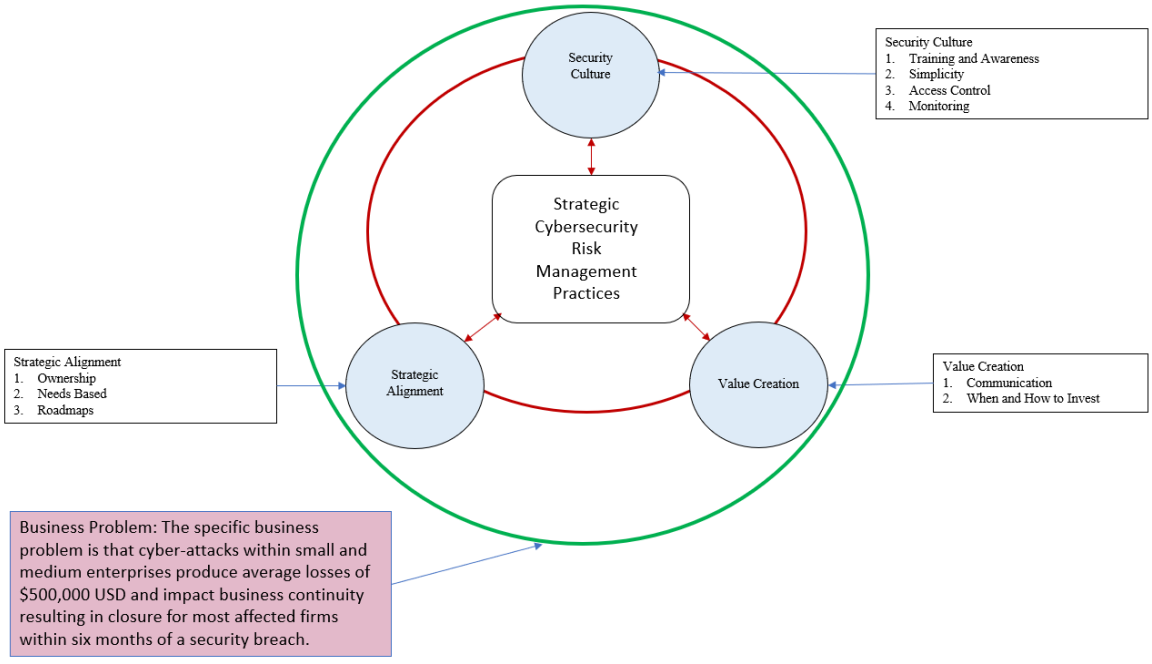
Another theme from the study that emerged centered around when and how to invest in creating value. P10 noted, *Investing in cybersecurity is critical to managing a program and in creating value*. When addressing the practices that suggested investing in current and emerging threats and monitor the environment to uncover new threat information, P3 offered, *match protection to the threat* and *Adapt your security program to meet the threat environment*. P9 supported P5 comments, *I have learned that there are things you may not be able to plan for. You have to adjust across the board when new threats happen*. P10 noted, *Proactive investment is critical to staying ahead in a rapidly evolving sector*. This theme is supported by the findings in the literature review, where it was noted that some scholars suggest investments to protect business information should be made proactively, creating a competitive advantage.

# Application and Recommendations

While the cyber threat continues to increase, SME leaders are unprepared (Connectwise, 2022). This study produced practices that experts found were appropriate and implementable by SMEs which resulted in a new SME-focused cybersecurity risk-management framework (see Figure 4).

**Figure 4**

*The Ashley Information Protection Framework*



*Note:* The themes that emerged from the study results are noted on the original applied framework to create the new framework.

# Practical Application

Information security is a complex evolving issue to address. The AIPF includes roles for all employees. Table 18 shows the practices mapped to a theme and the critical factors in practice. One way to use this framework is to examine the critical factor and then apply the practice. For example, for strategic alignment key business concept, the critical factors are “Define where you are going,” “Define ownership,” and “Only address needs.” The critical factors establish the goal and the practices define how to achieve the goal.

**Table 18**

*Key to Using the Ashley Information Protection Framework*

| Key Business Concept | Theme | Practices | Critical Factor in Practice |
|---|---|---|---|
| Security Culture | | | |
| | Training and Awareness | Develop awareness programs that are "top-down" in the organizations to ensure that all levels understand the policies, procedures, processes, practices, and the importance of protecting business information. | Top to bottom awareness |
| | | Establish a comprehensive training program to promote information security knowledge among employees with additional training available depending on the employee role (i.e., secure coding for developers). | Train everyone based on needs |
| | | If a cyber incident occurs, employees should be informed of needed behavioral changes, and training programs should be developed if needed. | Communicate changing training needs |
| | | Create periodic information and cybersecurity training and awareness programs that educate employees on how to detect and respond to security threats. | Teach employees to recognize issues |

| | | | |
|---|---|---|---|
| | | Cybersecurity news and general "how-to's" should be regularly shared with staff to encourage a sense of security culture normalcy | Make security the “new normal.” |
| | Simplicity | Security policies, procedures, processes, and practices should be kept simple, clear, and effective to ensure that employees can easily understand them, making it easier to comply. | Keep it Simple |
| | Access Control | Develop and maintain access control plans to control who can access what business information based on a “need to know” principles. | Need to know for access |
| | Monitor | Monitor the network with security information and event management (SIEM) tools. | Trust but verify |
| | | Periodically audit any existing company policies and culture to create a set of key performance indicators (KPI) to establish a baseline security culture reinforced with cybersecurity training and awareness programs. | Evolve with the times |
| Strategic Alignment | | | |
| | Ownership | Develop an organizational strategy to manage cybersecurity risks that supports enterprise objectives with clearly defined ownership. | Define ownership |
| | Needs-Based | Ensure that the information security strategy considers the current and ongoing needs of the business strategy. | Only address needs |
| | Roadmaps | An aligned business and security strategy and roadmap should be created and updated annually. | Define where you are going. |
| Value Creation | | | |

| | | | |
|---|---|---|---|
| | Communication | Communicate the firm's cybersecurity practices to build trust and confidence that critical business information is protected in the eyes of the customer. | Gain the trust of the customer |
| | | Communicate to the stakeholders the importance the company places on protecting business information. | Gain the trust of the stakeholder |
| | When and How to Invest | Cybersecurity investments should be made proactively to protect business information. | Be proactive |
| | | Cybersecurity threats should be continuously monitored, and new investments should be made as additional threat information becomes available. | Data-driven investments |
| | | Cybersecurity investments to protect business information should be made to address the current and emerging risks to the organization. | Evolve your investments |

# Area for Additional Studies

Additional studies to assist SMEs in maintaining an adequate security posture are critical. Finding ways of taking large firm practices and scaling them for SMEs is a needed gap in practice that future researchers could fill. For example, while *Develop additional security planning to support organizational growth objectives,* achieved a 95% desirability score but a 60% feasibility score, research on how to increase feasibility is warranted.

The AIPF is future-looking in terms of emerging and evolving threats for current SME business-size, but not with rapid growth. Research which includes a growth-factor of risk is needed. As a firm grows, they tend to hire employees most often from other firms, changing culture, shifting training needs, and incorporating risks from loyalty shifts. A research project within that realm is encouraged.

# Conclusion

A panel of 20 cybersecurity experts agreed that 20 specific strategic practices (Table 18, column *Practices*) could apply to SMEs to assist them with reducing their risk of cyberbreaches. The AIPF 2021 framework was created which extended the existing body of knowledge of business information protection to SMEs. SME owners and principles can take the findings from this study to begin creating and guiding their own cybersecurity strategic planning and practices.

# References

Akins, R. B., Tolson, H., & Cole, B. R. (2005). Stability of response characteristics of a Delphi panel: Application of bootstrap data expansion. *BMC Medical Research Methodology*, *5*(1), 37. https://doi.org/10.1186/1471-2288-5-37

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/10.1016/j.cose.2020.102030

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior*, *49*, 567-575. https://doi.org/10.1016/j.chb.2015.03.054

Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges [Article]. *International Journal of Doctoral Studies*, *11*, 305-321. https://doi.org/10.28945/3561

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information and Computer Security, 27*(3), 393-410. https://doi.org/10.1108/ICS-07-2018-0080

Bailetti, T., & Craigen, D. (2020). Examining the relationship between cybersecurity and scaling value for new companies. *Technology Innovation Management Review*, *10*(2), 62-69. https://doi.org/10.22215/timreview/1329

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508-526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Bocetta, S. (2019). How a small business should respond to a hack. *CSO.* https://www.csoonline.com/article/3437777/how-a-small-business-should-respond-to-a-hack.html

Bodeau, D., Boyle, S., Fabius, J., & Graubart, R. (2010). *Cyber security governance*. The MITRE Corporation. https://www.mitre.org/publications/technical-papers/cyber-security-governance

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stahle, T. (2019). The risk-based approach to cybersecurity. *McKinsey Insights*. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf

Brands, K. C. M. A. (2020). Creating cybersecurity awareness. *Strategic Finance, 101*(7), 60-61. https://sfmagazine.com/post-entry/january-2020-creating-cybersecurity-awareness/

Bull, W. (2019). Enterprise security risk management...Culture eats strategy [Article]. *Security: Solutions for Enterprise Security Leaders*, *56*(4), 26-35. https://www.securitymagazine.com/articles/90062-enterprise-security-risk-managementculture-eats-strategy

Committee of Sponsoring Organizations. (2017). Enterprise risk management: Integrating with strategy and performance. https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

Connectwise. (2022). *2022 MSP Threat Report.* eBook. https://www.connectwise.com/resources/search?types=threat-report

Corriss, L. (2010). *Information security governance: integrating security into the organizational culture* Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, Austin, Texas, USA. https://doi-org.library.capella.edu/10.1145/1920320.1920326

Council of Economic Advisors. (2018). *CEA report: The cost of malicious cyber activity to the U.S. economy*. U.S. National Security and Defense. https://www.whitehouse.gov/articles/cea-report-cost-malicious-cyber-activity-u-s-economy/

da Veiga, A., Astakhova, L. V., Botha, A., & Herselman, M. (2020). Defining organisational information security culture—Perspectives from academia and industry. *Computers & Security, 92*, 101713. https://doi.org/10.1016/j.cose.2020.101713

da Veiga, A., & Eloff, J. H. P. (2007). An information security governance framework. *Information Systems Management*, 24(4), 361-372.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, *28*(3), 189-198. https://doi.org/10.1016/j.cose.2008.11.007

Dresner, D. G. (2018). The IASME governance standard for information and cyber security. (5). https://iasme.co.uk/wp-content/uploads/2019/04/IASMEStandardv5.pdf

Farshchi, J., & Douglas, A. (2010). Information security and balanced score card. *CIO Magazine*. https://www.cio.com/article/2415017/information-security-and-the-balanced-scorecard.html

FITSM. (2016). *Part 0: Overview and vocabulary.* https://www.fitsm.eu/downloads/#toggle-id-1
Foley, T. (2017). *Practical cybersecurity tech for small business [PDF file]*. Florida SBDC http://floridasbdc.org/wp-content/uploads/2017/09/PracticalCybersecurityTech4-2.pdf

Gashgari, G., Walters, R., & Wills, G. (2017). *A proposed best-practice framework for information security governance* [Paper Presentation]. Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security Volume 1: IoTBDS,, Porto, Portugal.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, *74*(10), 4986-5002. https://doi.org/10.1007/s11227-018-2337-2

Granneman, J. (2018). The business guide to improving information security. *The Journal of Equipment Lease Financing (Online)*, *36*(3), 1-9.

Hasson, F., Keeney, S., & McKenna, H. (2000). Research guidelines for the Delphi survey technique. *Journal of Advanced Nursing*, *32*(4), 1008-1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x

Hayden, L. (2016). Three ways to align security programs to enterprise strategy. *CSO Magazine*. https://www.csoonline.com/article/3067733/three-ways-to-align-security-programs-to-enterprise-strategy.html

Hepfer, M., & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. *MIT Sloan Management Review*, *62*(1), 40-45. https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/

HITRUST. (2020a). Glossary of Terms and Acronyms. v.5 [PDF]. https://hitrustalliance.net/csf-rmf-related-documents/
HITRUST. (2020b). *HITRUST CSF version 9.4*. Retrieved from https://hitrustalliance.net/csf-license-agreement

Holt, A. (2013). *Governance of IT: An executive guide to ISO/IEC 38500*. http://ebookcentral.proquest.com/lib/capella/detail.action?docID=1213991

IBM. (2019, July 23). *IBM study shows data breach costs on the rise; Financial impact felt for years*. https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

International Organization for Standardization. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://standards.iso.org/ittf/PubliclyAvailableStandards/

ISACA. (n.d.). Glossary. https://www.isaca.org/resources/glossary

ISACA. (2012). COBIT 5: A business framework for the governance and management of enterprise IT https://www.isaca.org/bookstore/cobit-5/wcb5

ISACA. (2018). *Narrowing the culture gap for better business results*. https://www.isaca.org/-/media/info/cybersecurity-culture-report/index.html

Josi, P. (2012). IT governance for SME. http://www.isaca.ch/images/downloads/downloads/diplomarbeiten/IT_Governance_for_SME.pdf

Kaušpadienė, L., Ramanauskaitė, S., & Čenys, A. (2019). Information security management framework suitability estimation for small and medium enterprise. *Technological and Economic Development of Economy, 25*(5), 979-997. http://dx.doi.org/10.3846/tede.2019.10298

Keeney, S., Hasson, F., & McKenna, H. P. (2001). A critical review of the Delphi technique as a research methodology for nursing. *International journal of nursing studies*, *38*(2), 195-200. https://doi.org/10.1016/s0020-7489(00)00044-4

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/https://doi.org/10.1016/j.cose.2021.102248

Lloyd, G. (2020). The business benefits of cyber security for SMEs. *Computer Fraud & Security*, *2020*(2), 14-17. https://doi.org/10.1016/S1361-3723(20)30019-1

McCollum, J. (2019). Small business owners outsmart cybercriminals. https://www.infosecinstitute.com/newsroom/small-business-owners-outsmart-cybercriminals-heres-how/

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications*, *44*, 12-22. https://doi.org/10.1016/j.jisa.2018.11.003

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity: Cybersecurity framework. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology. (2020). NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0. https://doi.org/10.6028/NIST.CSWP.01162020

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information and Computer Security*, *27*(2), 146-164. https://doi.org/10.1108/ICS-12-2016-0095

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://doi.org/10.6028/nist.sp.800-181

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation

research. *Administration and Policy in Mental Health and Mental Health Services Research*, *42*(5), 533-544. https://doi.org/10.1007/s10488-013-0528-y

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129. https://doi.org/10.1177/1555343415575152

Paulsen, C., & Toth, P. (2016). Small business information security: The fundamentals. https://doi.org/10.6028/NIST.IR.7621r1

Petrie, J. (2017). Aligning security with changing business strategy, goals and objectives. *CSO Magazine*. https://www.csoonline.com/article/3231994/aligning-security-with-changing-business-strategy-goals-and-objectives.html

Porter, M. E., & Millar, V. E. (1985). How information gives you competitive advantage. *Harvard Business Review*, *63*(4), 149-160. https://hbr.org/1985/07/how-information-gives-you-competitive-advantage

Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

Pratt, M. K. (2019). Why security-IT alignment still fails. *CSO Magazine*. https://www.csoonline.com/article/3386999/why-security-it-alignment-still-fails.html

Rastogi, R., & von Solms, R. (2005). *Information security governance - A re-definition*. Security Management, Integrity, and Internal Control in Information Systems, Boston, MA.

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). Protecting controlled unclassified information in nonfederal systems and organizations. https://doi.org/https://doi.org/10.6028/NIST.SP.800-171r2

Rouse, M. (2020). *Information technology infrastructure library (ITIL)*. https://searchdatacenter.techtarget.com/definition/ITIL

Saleem, J., Adebisi, B., Ande, R., & Hammoudeh, M. (2017). *A state of the art survey - Impact of cyber attacks on SME's* [Paper Presentation]. The Proceedings of the International Conference on Future Networks and Distributed Systems, Cambridge, United Kingdom. https://doi-org.library.capella.edu/10.1145/3102304.3109812

Santos-Olmo, A., Sanchez, L. E., Caballero, I., Camacho, S., & Fernandez-Medina, E. (2016). The Importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, *8*(3), 30. https://doi.org/10.3390/fi8030030

Scala, N. M., Reilly, A. C., Goethals, P. L., & Cukier, M. (2019). Risk and the five hard problems of cybersecurity. *Risk Analysis*, *39*(10), 2119-2126. https://doi.org/10.1111/risa.13309

Schinagl, S., & Shahim, A. (2020). What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. *Information & Computer Security*, *28*(2), 261-292. https://doi.org/10.1108/ICS-02-2019-0033

Scott, R. (2019). Small businesses beware: Cyberwar is right around the corner. *SC Magazine*. https://www.scmagazine.com/home/opinion/executive-insight/small-businesses-beware-cyberwar-is-right-around-the-corner/

Selznick, L. F., & LaMacchia, C. (2018). Cybersecurity liability: How technically savvy can we expect small business owners to be? *Journal of Business & Technology Law, 13*(2). http://digitalcommons.law.umaryland.edu/jbtl/vol13/iss2/4

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63-75. https://doi.org/10.3233/efi-2004-22201

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education: Research*, *6*(1), 1-21.

Small Business Administration. (2019). Small business cybersecurity. https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity

Solomon, D. H., Weissman, J. S., Choi, H., Atlas, S. J., Berardinelli, C., Dedier, J., Fischer, M. A., Fitzgerald, J., Hinteregger, E., Johnsen, B., Marini, D. D., Mclean, R., Murray, F., Neogi, T., Oertel, L. B., Pillinger, M. H., Riggs, K. R., Saag, K., Suh, D., . . . & Barry., M. J. (2021). Designing a strategy trial for the management of gout: The use of a modified Delphi panel. *ACR Open Rheumatol, 3*(5), 341-348. https://doi.org/10.1002/acr2.11243

Stackpole, B. (2019). CIO's get strategic. *State of the CIO 2019*, 12-21. https://idgcommunications.lookbookhq.com/ciodigitalmagazine-cradlepoint/01-ciod-winter-2019--1

Steinberg, J. (2017). Small businesses beware: Half of all cyber-attacks target you. *Inc*. https://www.inc.com/joseph-steinberg/small-businesses-beware-half-of-all-cyber-attacks-target-you.html

Stewart, J., O'Halloran, C., Harrigan, P., Spencer, J. A., Barton, J. R., & Singleton, S. J. (1999). Identifying appropriate tasks for the preregistration year: Modified Delphi technique. *BMJ, 319,* 224 – 229. https://doi.org/10.1136/bmj.319.7204.224

Suer, M. (2018). *How CIOs prove business value*. https://www.cio.com/article/3276274/how-cios-prove-business-value.html

SurveyMonkey Inc. (n.d.). *Ranking Question*. https://help.surveymonkey.com/articles/en_US/kb/How-do-I-create-a-Ranking-type-question

SurveyMonkey Inc. (2021). *Security Statement*. https://www.surveymonkey.com/mp/legal/security/

Teymourlouei, H. (2018). Preventative measures in cyber & ransomware attacks for home & small businesses' data. In (pp. 87-93). *Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).*

Tharnish, S. (2020). As cyber attacks become more prevalent, here's why your small business is at risk. *Security Magazine.* https://www.securitymagazine.com/articles/91806-as-cyber-attacks-become-more-prevalent-heres-why-your-small-business-is-at-risk

U.S. Federal Bureau of Investigation. (2019). *2019 Internet Crime Report*. https://pdf.ic3.gov/2019_IC3Report.pdf

U.S. Small Business Administration. (2019). Frequently asked questions [Brochure]. https://cdn.advocacy.sba.gov/wp-content/uploads/2019/09/24153946/Frequently-Asked-Questions-Small-Business-2019-1.pdf

Van Niekerk, J. F., & von Solms, R. (2010). Information security culture: A management perspective. *Computers & Security*, *29*(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

Verizon. (2019). 2019 *Data breach investigations report*. https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Volchkov, A. (2018). *Information security governance: Framework and toolset for CISO's and decision makers*. Auerbach Publications.

von Solms, B. (2000). Information security — The third wave? *Computers & Security*, *19*(7), 615-620. https://doi.org/10.1016/S0167-4048(00)07021-8

von Solms, B. (2006). Information security – The fourth wave. *Computers & Security, 25*(3), 165-168. https://doi.org/10.1016/j.cose.2006.03.004

von Solms, S. H. (2010). *The 5 Waves of Information Security – From Kristian Beckman to the Present* [Paper Presentation]. Security and Privacy – Silver Linings in the Cloud, Berlin, Heidelberg.

Watad, M., Washah, S., & Perez, C. (2018). IT security threats and challenges for small firms: Managers' perceptions. *International Journal of the Academic Business World, 12*(1), 23-30.

Wild, J. (2018). Five most common security frameworks explained. https://originit.co.nz/the-strongroom/five-most-common-security-frameworks-explained/

World Economic Forum. (2019). The global risk report 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

World Economic Forum. (2020). The global risk report 2020. http://reports.weforum.org/global-risks-report-2020/wild-wide-web/#view/fn-20

Wu, Y. A., & Saunders, C. S. (2016). Governing the fiduciary relationship in information security services. *Decision Support Systems*, *92*, 57-67. https://doi.org/10.1016/j.dss.2016.09.008

Xu, F., Luo, X., Zhang, H., Liu, S., & Huang, W. (2019). Do strategy and timing in IT security investments matter? An empirical investigation of the alignment effect. *Information Systems Frontiers*, *21*(5), 1069-1083. https://doi.org/10.1007/s10796-017-9807-6