2020

An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses

Darrell Eilts
Nova Southeastern University, eiltsdl@gmail.com

An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses

by

Darrell Eilts

A dissertation report submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Computing and Engineering
Nova Southeastern University

2020

We hereby certify that this dissertation, submitted by Darrell Eilts conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Yair Levy, Ph.D.
Chairperson of Dissertation Committee

3/26/2020
Date

Martha M. Snyder

Martha M. Snyder, Ph.D.
Dissertation Committee Member

3/26/2020
Date

Ruti Gafni, Ph.D.
Dissertation Committee Member

3/26/2020
Date

Approved:

Meline Kevorkian

Meline Kevorkian, Ed.D.
Dean, College of Computing and Engineering

3/26/2020
Date

College of Computing and Engineering
Nova Southeastern University

2020

An Abstract of a Dissertation Report Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses

by
Darrell Eilts
February 2020

A cyber-attack can become costly if small businesses are not prepared to protect their information systems or lack the ability to recover from a cybersecurity incident. Small businesses that are not ready to deal with cyber threats are risking significant disruption and loss. In many cases the small business decision makers, owners or managers, do not have a strategy to improve their cybersecurity posture despite the known risk to their business. This research study focused on the relationship between two constructs that are associated with readiness and resilience of small businesses based on their cybersecurity planning, implementation, as well as response and recovery activities. An empirical assessment was conducted on small businesses' level of cybersecurity preparedness relative to their decision makers' perceived risk of cyber-attack (perceived likelihood x perceived impact).

Subject matter experts (SMEs) were used to validate a set of cybersecurity preparedness activities for the construct of cybersecurity preparedness. The SMEs approved 70 cybersecurity preparedness activities among the five functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework to assess the level of cybersecurity preparedness of small businesses. The SMEs then assigned weights to the validated preparedness activities to enable an aggregated benchmark cybersecurity preparedness score (CPS). The construct of the decision maker's perceived risk of cyber-attack (DMPRCA) was updated with a set of common cyber threat vectors and using simple definitions from the SMEs.

A Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) was then developed using the theoretical foundation of prospect theory and status quo bias. The four quadrants of cybersecurity risk postures were defined as indifference, susceptible, aversive, and strategic. The aggregated scores of CPSs and DMPRCA were positioned on the CyPRisT for each of the 216 small businesses who participated in this study. Statistical differences were found in the CPSs and DMPRCA by demographics industry, size (number of employees), and Information Technology (IT) budget (%). The findings of the quantitative analysis are presented along with the position on the CyPRisT for each demographic indicator of the businesses.

The Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) program for small businesses was developed as a cybersecurity strategy planning guide and collection of resources. The cyberARMoRR program was administered to 50 small business decision makers. The CPSs and DMPRCA were evaluated before and after participation in cyberARMoRR program and positioned on the CyPRisT to assess differences in the small businesses’ cybersecurity posture. The results of the paired sample t-test showed no significant differences between the pretest and posttest groups. However, there was an observed increase in both the CPSs and DMPRCA that moved the position toward the risk-aversive quadrant of the CyPRisT.

An analysis of the empirical data was conducted on the cybersecurity preparedness activities that participants identified as most challenging to implement and their explanations of why. Data were collected from 15 semi-structured interviews and 50 surveys with five open-ended questions, one per each function of the NIST Cybersecurity Framework. A two-cycle thematic analysis was performed using the responses that described the challenges of cybersecurity preparedness activities. The results of the qualitative analysis suggest that small business decision makers are more likely to improve their ability to mitigate cyber threats when the applicable technologies are uncomplicated, technical expertise is accessible, and cybersecurity educational material is easy to understand. The small business owners and managers also indicated that the cybersecurity preparedness activities are more attainable when the demand of their time did not change their focus away from business operations. Conversely, the small businesses that were able to improve their cybersecurity posture had committed to incorporating many of the cybersecurity preparedness activities into their routine business processes, such as allocating a budget for cybersecurity and performing vulnerability assessments. The effects of prospect theory and status quo bias are discussed in the context of the CyPRisT positions for the small businesses.

Acknowledgements

I was fortunate to receive amazing support throughout the process of completing my coursework and dissertation. The pursuit of earning a doctorate degree demands an incredible amount of time and concentration. The past six years have been a challenge of perseverance. On many occasions I felt my goal was somewhat selfish because I had missed out on evenings, or weekends, with family and friends. Nevertheless, they stood by my side to offer inspiration and encouragement. There is not enough space here to express my gratitude for their support. I also wish I were able to acknowledge all that positively influenced my life towards achieving this goal. Although, I would like to recognize those that I am especially grateful, and to whom this work is dedicated:

To my wife, Kara Eilts, my greatest appreciation belongs to you. I cannot thank you enough for all the sacrifices you made while I was focused on studies. More than anything, thank you for filling my life with love and fun.

To my stepchildren, Daniel Elfert and Rachel Elfert, I am extremely proud of you for your own accomplishments. You are both brilliant, kind-hearted, full of talent, and have so much to offer the world. I wish you happiness and success in achieving your dreams.

To my mom, Earlene Eilts, you taught me how important it is to have a strong work ethic, and to face difficulties with courage. Thank you for your unwavering confidence in me.

To my dad, Don Eilts Sr., I learned from you the virtues of honor and selfless determination. I wish you were here to see your youngest son graduate with a doctoral degree. I know this moment would have made you very proud.

To my friends and colleagues that helped along the way, I appreciate your backing as well as your constructive critique, opinions, and advice that has led to my personal growth. In particular; Osborne Obeng, Fernando Lopez, Jim Furstenberg, Molly Cooper, Tommy Pollock, Daniel Elliot, Celia Paulsen, Heidi Crouch, Dr. Angel Hueca, Dr. Melissa Carlton, Dr. Karla Clark, Dr. Daniel Long, Dr. Steven McElwee, Dr. Patrick Offor, Dr. Herb Mattord, Dr. Michael Whitman, Dr. Zareef Mohammed, Dr. Gurvirender Tejay, Dr. Scott Overmyer, Dr. Gerry Stahl, Raymond Thombs, and Colonel Bill Davis.

To the research participants and subject matter experts, as well as the associates of NIST, NCSA, InfraGard, and ISACA; I sincerely thank you for your contributions. Your input has been extremely beneficial to this research study.

To my dissertation committee members, Dr. Ruti Gafni and Dr. Marti Snyder, thank you very much for taking the time to review my work. Your comments were instrumental to the progress and added immeasurably to the quality of this work. Also, thank you Dr. Ling Wang for your excellent course and assistance with IRB process.

To my dissertation chair, Dr. Yair Levy, this accomplishment would not have been possible without your guidance, wisdom, and rigor. I also appreciate your patience and humor when times were tough. It has been an honor to work with you. I am forever grateful for your leadership and counsel throughout the dissertation process.

Table of Contents

Appendices

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Cybercriminals are targeting small businesses with weak cybersecurity postures because it is easy to exploit the businesses' vulnerabilities (Symantec Corporation, 2016). Data from the Ponemon Institute (2016, 2017, 2018) showed an alarming trend in the significant rise of small businesses experiencing cyber-attacks over a period of 3 years. In a report from Verizon Enterprise (2018), the majority of victims were small businesses involving data breaches with confirmed disclosure to an unauthorized party. Yet, according to the Better Business Bureau (BBB) (2017), most small businesses are less likely to take comprehensive measures to improve their cybersecurity postures, identifying barriers of resources, time, and knowledge. If small businesses are not adequately prepared, they risk substantial losses caused by the inevitable cyber-attack (Paulsen & Toth, 2016). A single cybersecurity incident can result in financial loss, damage to credibility, legal recourse, and disruption of business (Bulgurcu, Cavusoglu, & Benbasat, 2010; Chittister & Haimes, 2011; Hovav & Gray, 2014). Consequently, the impact of a cyber-incident is disproportionately high for the smallest companies because they typically have fewer resources to prepare and deal with cyber-attacks (Hiscox, 2017). Even when cyber threats are imminent, most small businesses are underprepared to deal with the risk (Hiscox, 2017; Rohn, Sabari, & Leshem, 2016). The ability of the small business to achieve an appropriate cyber posture has been associated with the disposition of the decision makers' (i.e., owners or managers) cyber threat concerns and risk perception (Bhattacharya, 2011; Rohn et al., 2016). This research study addressed the limited ability of small businesses to mitigate cyber threats, which leads businesses to significant losses from cyber-attacks or data breaches (Berry & Berry, 2018; Paulsen, 2016; Rohn et al., 2016).

The remainder of this dissertation is organized as follows. Chapter 1 includes a statement of the specific research problem and the main dissertation goal, followed by research questions, as well as the relevance and significance of this research. Next, specific barriers and issues were identified as well as assumptions, limitations, and delimitations for conducting this research study. Finally, definitions are provided to help the reader remove ambiguities that may exist with key terms that were used in this research study. Chapter 2 comprises a literature review of related research on each of the relevant topic areas: cybersecurity risk management, common cyber threats to small businesses, cybersecurity readiness, cybersecurity resilience, cybersecurity preparedness, decision makers' perceived risk of cyber-attack, as well as prospect theory and status quo bias. Chapter 3 presents methodology for this research study with the specific data collection and analysis techniques that were used to assess the taxonomy of cybersecurity preparedness and decision makers' perceived risk. Furthermore, Chapter 3 outlines the developmental research methods, including sequential exploratory design and quasi-experimental design, that were used to develop the taxonomy as well as the program for the participants.

Problem Statement

The research problem which this study addressed was the limited ability of small businesses to mitigate cyber threats, which leads to significant losses from cyber-attacks or data breaches (Berry & Berry, 2018; Paulsen, 2016; Rohn et al., 2016). Information security standards as well as cybersecurity frameworks provide guidelines of activities, with processes and procedures for organizations to follow when establishing a cybersecurity program (National Institute of Standards and Technology [NIST], 2014, 2018; Paulsen & Toth, 2016). The key components of a successful program consist of preparedness activities to manage cyber risk and activities to ensure business continuity when an event occurs (Cerullo & Cerullo, 2004; Fisher, Norman, & Klett, 2017). A cyber-attack or data breach becomes a cybersecurity incident if the event "has been determined to have an impact on the organization prompting the need for response and recovery" (NIST, 2018, p. 45).

Information systems (IS) researchers have recommended strategies that take into consideration a balanced approach of two cybersecurity paradigms: prevention and response (Baskerville, Spagnoletti, & Kim, 2014). A business's level of readiness is an evaluation of how 'well-prepared' it is to prevent and protect from cyber threats (Hiscox, 2017; Peiro, Cook, & Beydoun, 2005; Sumner, 2009). *Resilience* is having the ability to respond properly by adapting to changing conditions, to recover from a cybersecurity incident, and then to assume close-to-normal operations within an acceptable time and total cost (Chittister & Haimes, 2011; Department of Homeland Security, 2017). Therefore, a strategically balanced cybersecurity posture considers both readiness and resilience. *Cybersecurity readiness* is being prepared to minimize and manage risk

(Hurley, McGibbon, & Everetts, 2014), while *cybersecurity resilience* is the ability to maintain business continuity during as well as after a cybersecurity incident (Bodeau & Graubart, 2017).

The smallest companies, such as those without dedicated IT support, are among the most vulnerable because they are less likely to have a well-established cybersecurity preparedness strategy (Hiscox, 2017; Sumner, 2009). Cyber-attacks against small businesses have recently become more targeted with a higher level of sophistication, resulting in severe consequences and negative financial impacts (Ponemon Institute, 2017). According to Verizon Enterprise (2018), 58% of data breach victims are small businesses likely due to their lack of cybersecurity controls or risk mitigation processes. Cyber threats to IS and data come from an assortment of common attack vectors, including deliberate threats (e.g., ransomware attacks) as well as accidental acts (e.g., unintentional disclosure by an employee). Over the 5-year period from 2014 to 2018, the top patterns of cyber incidents have involved some form of hacking, malware, social engineering, physical loss, misuse, or error (Verizon Enterprise, 2018).

The BBB (2017) emphasized small businesses are an essential part of the cybersecurity economic ecosystem since they can be exploited by cybercriminals seeking a gateway into partnering larger organizations when part of their supply chain. For example, one of the largest consumer data breaches occurred in late 2013 after hackers exploited the network access of a small heating, ventilation, and air-conditioning (HVAC) system supplier (Symantec Corporation, 2017). Stakes can also be high for small businesses, potentially affecting their livelihoods if decisions toward security countermeasures result in loss (Kumar, Park, & Subramaniam, 2017). The smallest businesses suffer a disproportionately higher financial impact from a cyber-attack when their losses are adjusted to organizational size and revenue (Hiscox, 2017; Itai & Onwubiko, 2018). More than 99% of all businesses registered in the United States (U.S.) have fewer than 100 employees, and 97% fewer than 20 employees (U.S. Census Bureau, 2015; U.S. Small Business & Entrepreneurship Council, n.d.). These small businesses face unique challenges when managing cybersecurity risk due to constraints such as financial resources and technical expertise (Hess & Cottrell, 2015). Small businesses with fewer employees have been found to be more exposed to cyber-attacks but less likely to take comprehensive measures toward improving their cybersecurity postures (BBB, 2017). A medium or large company may have sustainable resources for dealing with cyber-attacks, whereas the relatively low net income of a small business generally equates to fewer resources allocated toward cyber defense strategies (Hovav & Gray, 2014; Jang-Jaccard & Nepal, 2014).

The three main challenges faced by small businesses are not having the in-house expertise to mitigate cyber risk, IT budget constraints, and a general lack of understanding of how to protect against cyber-attacks (Ponemon Institute, 2018). In response to the growing number of cybersecurity challenges in the small business community, government agencies have published guidance based on standards and best practices for mitigating risk that have been used in larger businesses as well as federal agencies. Examples include the U.S. Computing Emergency Readiness Team (US-CERT) Resources for Small and Medium Businesses, the Federal Communication Commission (FCC) Small Biz Cyber Planner, and the NIST Interagency Report 7621 (Paulsen & Toth, 2016). A limited number of researchers have examined guidance for cybersecurity preparedness as well as the relation between cyber threat concerns, risk management, and the cybersecurity postures of small businesses. Select examples include Rohn et al.'s (2016) study of small business security posture as well as Berry and Berry's (2018) assessment of small business risk management approaches to cybersecurity risk.

Many small businesses lack cybersecurity incident prevention and response plans because their decision makers (i.e., owners or managers) either do not believe they are at risk or do not consider cybersecurity among their top concerns for the business (Experian-CSID, 2016). Alternatively, the BBB (2017) found most small businesses are very concerned about cybersecurity but are still less likely to have a plan in place to mitigate risk and respond to cyber threats. Rohn et al. (2016) found small business owners often have the tendency to underestimate cybersecurity risk, suggesting social theories may help to explain business owners' inaccurate perception of risk as well as the "lack of commensurate action" (p. 549). Berry and Berry (2018) found small business owners struggle with risk management approaches for mitigating cyber threats due to the rapid pace of advancement in technologies. This evidence is supported by other research illustrating the ability of small businesses to mitigate cyber threats is limited by the resources needed to update technologies or expertise continuously to develop a preparedness strategy (Cragg, Caldeira, & Ward, 2011; Sumner, 2009).

Cybersecurity practitioners and IS scholars have suggested small businesses are at high risk for systems compromise because they do not know what to protect (Osborn and Simpson, 2018; Paulsen, 2016). For example, Osborn and Simpson (2017) argued small businesses are struggling with the complex demands of risk assessment practices and how to assimilate cybersecurity advice into their organizations. Renaud (2016) found small businesses are inconsistent in their implementation of security measures based on their appraisal of threat and ability to implement risk controls. Key findings from recent cybersecurity benchmark reports also showed small businesses are challenged with cybersecurity initiatives to ensure a quick response to emerging cyber threats (Hiscox, 2017). Therefore, additional research is required to examine empirically small business cybersecurity activities for preparedness, decision makers' perceptions of risk, and approaches to improve small businesses' cybersecurity postures (Berry & Berry, 2018; Rohn et al., 2016).

Dissertation Goal

The main goal of this research study was to develop and validate a small business Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) to assess empirically small businesses' cybersecurity postures (readiness & and resilience), and then to develop a strategy program for small businesses to improve their cybersecurity risk management. The Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) for small businesses is a strategy planning program that was developed consisting of cybersecurity preparedness activities, outcomes, resources, and references following a recommended implementation schedule (e.g., week, month, quarter, year). The need for this work has been demonstrated in the work of Sumner (2009), Chittister and Haimes (2011), as well as Baskerville et al. (2014). Sumner (2009) examined risk in both small and mid-sized businesses based upon the perceived impact as well as perceived probability of various threat vectors, finding high levels of preparedness were not always aligned with high levels of risk. Chittister and Haimes

(2011) studied critical factors in cybersecurity preparedness and resilience, including the tradeoffs organizations make in their quest to mitigate threats (i.e., associated costs, benefits, and risk). Baskerville et al. (2014) evaluated security frameworks and the dynamic nature of threats to business IS, finding a balance of prevention and response strategies is critical in implementing an effective information security program.

This work builds on the prior research by proposing a taxonomy to assist small businesses to evaluate their cybersecurity postures through an assessment of their readiness and resilience against cyber-attacks. The CyPRisT, applied to the context of small business cybersecurity, was similar to the development of the mobile cyberslacking-commitment taxonomy (MCCT) by Alharthi, Levy, Wang, and Hur (2019). Nussbaum and Lewis (2017) differentiated the cybersecurity challenges based on an organization's size.

There is clearly a wide array of small business definitions applied in business and IS literature as well as the cybersecurity benchmark reports. For example, per government tax laws, small businesses vary by classification of industry, annual revenue, fixed assets, or employee count (Dilger, 2019). Because there is no generally accepted definition of small businesses, this research study focused on the most vulnerable small business enterprises, those with 10–50 employees (Rohn et al., 2016). Berry and Berry (2018) suggested more research is needed to understand small businesses' approaches to risk management and their responses to cybersecurity threats. Similarly, the industry focus of small business varies greatly. This industry categories for this research study was based on the North American Industry Classification Codes System (BBB, 2017, Romanosky, 2016; U.S. Census Bureau, 2015).

The approach for this research follows Carlton and Levy (2017), who leveraged the NIST Cybersecurity Framework as the basis for developing a cybersecurity risk and mitigation tool, including a cybersecurity skills index. The NIST Interagency Report 7621 Revision 1 is the small business fundamentals guideline for organizing cybersecurity risk management process and procedure (Paulsen & Toth, 2016). To evaluate the level of preparedness for a small business, the measures of cybersecurity preparedness activities were identified and validated using a panel of cybersecurity Subject Matter Experts (SMEs), that were derived from the recommended cybersecurity activities in the NIST Cybersecurity Framework (NIST, 2018; Paulsen & Toth, 2016).

Perceived cybersecurity risk is based on the impact and probability (likelihood) of common cyber-attack vectors identified in cybersecurity benchmark reports, such as the Ponemon Institute (2016, 2017, 2018), Symantec Corporation (2016, 2017, 2018), and Verizon Enterprise (2016, 2017, 2018). When considering risk perceptions, Boss (2007) stated the "probability assessment at the individual level is composed of individual appraisal regarding the likelihood that the unfavorable experience will happen, and the impact of that experience were it to happen" (p. 27). In this context, small business owners must often make cybersecurity risk decisions with uncertainty of threats and likelihood of attacks as well as the impacts to their business (Hayes, Tanner, & Schmidt, 2012; Kahneman & Tversky, 1979; Rees, Deane, Rakes, & Baker, 2011). For example, Rohn et al. (2016) suggested small business decision makers are bias in their risk perception based on a lack of experience in cybersecurity risk management, leading them to underestimate the probability of cyber-attacks. Thus, decision makers of a small business may be susceptible to common cyber-attacks, risk averse, or risk neutral based on their concern for minimizing downtime and expected losses (Chen, Kataria, & Krishnan, 2011; Tversky & Kahneman, 1992). This assessment of cybersecurity preparedness activities in relation to the decision maker's perceived risk of cyber-attacks provides insight into the status of small business cybersecurity posture (Lee & Joshi, 2016; Osborn & Simpson, 2017).

To achieve the main goal, this research study addressed eight specific goals. The first specific goal was to identify and validate by SMEs the cybersecurity preparedness activities from each of the five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, & Recover) that can be used to measure the level of preparedness for a small business (an inventory-based measure following the recommendations of the five functions of NIST Cybersecurity Framework). Cybersecurity measures vary in complexity, expertise, and financial investment to minimize vulnerabilities (NIST, 2018; Osborn & Simpson, 2017). The prioritization and importance of cybersecurity preparedness activities were considered in the context of smaller businesses, such as those with less than 50 employees, because they are among the most vulnerable (BBB, 2017; Hiscox, 2017; Rohn et al., 2016).

The second specific goal of this research study was to have SMEs assign weights to the small business cybersecurity preparedness activities in order to aggregate the measures so they may be used as a benchmarking tool for scoring small business cybersecurity preparedness. The approach of identifying mathematical weights for the SME-approved cybersecurity preparedness activities is useful when computing composite scores and establishing content validity in assessments (Bobko, Roth, & Buster, 2007).

The third specific goal of this research study was to identify and validate by SMEs the measure for small business decision makers' perceived risk of cyber threats to small businesses. The cyber threat vectors were categorized by the most common cyber-attack types small businesses experience: hacking (e.g., stolen credentials), malware (e.g., ransomware), social engineering (e.g., phishing), misuse (e.g., malicious insider), and web-based attacks (Hayes et al., 2012; Jang-Jaccard & Nepal, 2014; Ponemon Institute, 2018; Verizon Enterprise, 2018). Risk analysis techniques typically include a prioritization of cybersecurity activities that rely on judgment of threats. This judgement of uncertainty is an assessment of threat including the potential impact it may have on the business and the likelihood of an attack (Osiyevskyy & Dewald, 2015; Paulsen & Toth, 2016). Thus, the decision makers' perceived risk of cyber-attack measure included an assessment of potential impact and probability of occurrence for the cybersecurity threats to their small business (Sumner, 2009).

The fourth specific goal of this research study was to measure cybersecurity preparedness as well as decision makers' perceived risk of cyber-attack for a sample of small businesses in the U.S. This research study empirically positioned the sample of small businesses' cybersecurity preparedness and decision makers' perceived risk of cyber-attack scores by classifying them in the CyPRisT to indicate their cybersecurity postures for business continuity. As shown in Figure 1, there are four dimensions for the CyPRisT: indifference (Q1), susceptible (Q2), aversive (Q3), and strategic (Q4) to represent the benchmark scores of cybersecurity preparedness and the measure of small business decision makers' perceived risk of cyber-attack. The taxonomy quadrants are based on the theoretical foundations of status quo bias and advances in prospect theory, threat appraisal, indifference, susceptibility to losses and aversion, and strategic decision making as affected by risk perceptions (Kahneman, Knetsch, & Thaler, 1991; Lee & Joshi, 2016; Liang & Xue, 2009; Tversky & Kahneman, 1992).

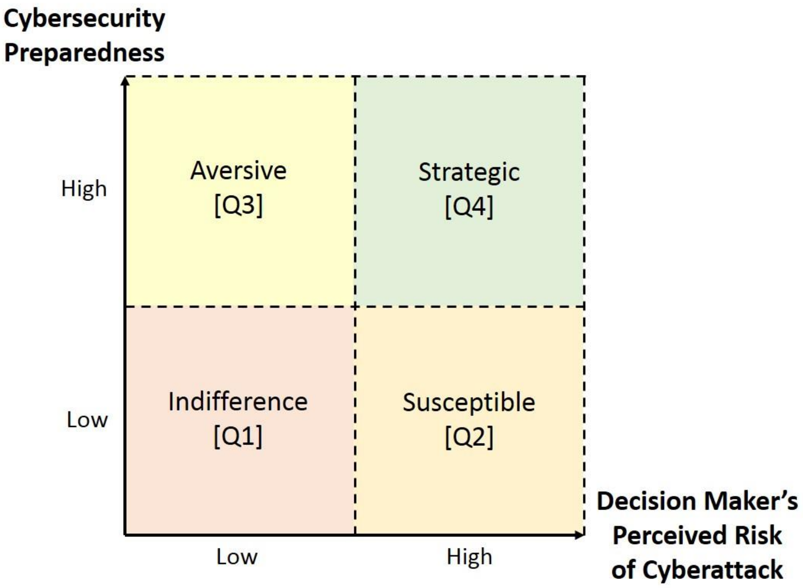


Figure 1. Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)**.**

The fifth specific goal of this research study was to identify statistically significant differences in the cybersecurity preparedness scores and decision makers' perceived risk of cyber-attack when controlled for: (a) industry, (b) number of employees, (c) years in operation, (d) annual revenue, and (e) IT budget. The sixth specific goal was to identify the differences between the levels of small business cybersecurity preparedness as well as the decision makers' perceived risk of cyber-attack before and after the cyberARMoRR program for small businesses. Thus, for small businesses willing to participate in further phases of the research, the cyberARMoRR program was offered to help improve their risk mitigation strategy. Cybersecurity SMEs validated the topics and alignment of program content to the validated measures of cybersecurity preparedness activities and common cyber-attack vectors to small businesses approved in the first and third specific goals, respectively.

The seventh specific goal of this research study was to determine which cybersecurity preparedness activities were implemented by the small business after participation in the cyberARMoRR program for small businesses. Finally, the eighth specific goal of this research study was to identify which of the cybersecurity preparedness activities were most challenging for the small business participants to implement and why they decided not to mitigate certain risk. As described, the eight specific goals supported the main goal of this research study through a set of eight corresponding research questions. The following research questions thus formed the basis of the research and approach.

Research Questions

The main research question that this research study addressed was: what cybersecurity preparedness activities may be used to develop a small business cybersecurity preparedness-risk taxonomy (CyPRisT) to assess small businesses' cybersecurity postures (readiness & resilience) empirically, then benchmark for a cybersecurity strategy planning program to improve risk management in small businesses? The eight research questions this research study addressed were:

RQ1. What is the SME-approved set of cybersecurity preparedness activities from the five functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, & Recover), which need to be measured to assess the level of cybersecurity preparedness for a small business?

RQ2. What are the SME-identified weights of the cybersecurity preparedness activities that enable an aggregation score to benchmark the level of preparedness for a small business?

RQ3. What is the SME-approved set of cyber-attack vectors, which address the most common cyber threats to a small business?

RQ4. How are the sample small businesses positioned on the Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) using the cybersecurity preparedness scores and the decision makers' perceived risk of cyber-attack?

RQ5. Do statistically significant differences exist in cybersecurity preparedness scores and decision makers' perceived risk of cyber-attack based on: (a) industry, (b) number of employees, (c) years in operation, (d) annual revenue, and (e) IT budget?

RQ6. Do statistically significant differences exist in the cybersecurity preparedness scores as well as the decision makers' perceived risk of cyber-attack before and after participation in the Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) program for small businesses?

RQ7. What cybersecurity preparedness activities were implemented after participation in the Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) program for small businesses?

RQ8. What cybersecurity preparedness activities were most challenging for small businesses to implement and why?

Relevance and Significance

This research study was relevant because it provided insight into an area with a limited number of research studies empirically assessing the implementation of the recommended cybersecurity activities in small businesses (Gafni & Pavel, 2019). This research study was significant because it contributed to the knowledge base on IS risk management, cybersecurity posture, and business continuity for small businesses. Gupta and Hammond (2005) reported many small business owners are not adept at implementing appropriate cybersecurity measures. Recent cybersecurity surveys have revealed small business owners know they are at risk of cybersecurity incidents, but do not know what activities will protect their businesses (BBB, 2017; Paulsen, 2016). Recent cybersecurity benchmark reports have indicated most small business owners are concerned about cyber threats and the impacts of cyber-attacks, but do not believe they use data worth being targeted. In other words, small business owners are concerned about cybersecurity risk mitigation and response but are “doing little to proactively prepare for such attacks” (Experian-CSID, 2016, p. 6).

Verizon Enterprise (2018) reported small businesses accounted for 58% of the cybersecurity incidents where the data breach was confirmed disclosure to an unauthored party. Year after year, hackers breached more than half the small businesses in the U.S. (Ponemon Institute, 2016, 2017, 2018). Over three-quarters of the hacking victims involved small businesses with compromised web applications or business systems with malware introduced through phishing emails as part of a multifaceted attack method (Verizon Enterprise, 2017). Most importantly, according to the BBB (2017), more than half of small businesses do not survive more than 2 months after suffering a major data loss. Small businesses typically lack the expertise or resources to invest in cybersecurity, and thus need to consider an improvement to their business strategy process by implementing a prioritized cybersecurity program to help protect from theft, disclosure, and misuse (Paulsen & Toth, 2016). A voluntary framework adopted by small businesses will help to guide the cybersecurity strategy by aligning cybersecurity activities with business processes and enabling business owners to better manage their risk (NIST, 2018). Thus, an empirical assessment of the relationship between cybersecurity preparedness activities and decision makers' perceived risk of cyber-attack may be beneficial in making decisions to improve the cybersecurity postures of small businesses.

Relevance

The relevance of this research study is that small businesses continue to struggle with cybersecurity risk management as well as the strategic balance of prevention and response paradigms (Baskerville et al., 2014; Hiscox, 2017). Consequently, hackers and cybercriminals target small businesses due their inability to implement essential cybersecurity safeguards (Ponemon Institute, 2017). These inadequacies as well as the underprioritizing of cybersecurity preparedness in small businesses puts many of them at high risk of negative financial impacts and severe consequences when subjected to a cyber-attack (Experian-CISD, 2016; Ponemon Institute, 2016, 2017, 2018). The financial impact of a cyber incident is disproportionately high for the smallest companies (Hiscox, 2017). The BBB (2017) confirmed smaller businesses "are less likely to have taken comprehensive measures in regard to cybersecurity, businesses with fewer employees are more exposed to potential breaches and, thereby, the financial losses that can accompany such an attack" (p. 15).

Some IS researchers addressing this problem have reported incomplete or contradictory findings because attention has been focused on a few specific cybersecurity procedures, practices, and policies (Berry & Berry, 2018). Thus, a more comprehensive measure for assessing cybersecurity preparedness must consider an inventory of the cybersecurity activities from all five functions of the NIST Cybersecurity Framework (NIST, 2018). Small business owners' perception of risk is an important component to the small business cybersecurity posture (Rohn et al., 2016). Previous research (e.g., Sumner, 2009) has taken into consideration the perceived risk as it relates to impact and probability of threats. When small business decision makers lack concern toward cybersecurity problems, they are more likely to be ill-prepared to deal with cybersecurity threats (Bhattacharya, 2011). As such, if small business decision makers are aware of the common cyber threats and perform strategic planning of cybersecurity preparedness activities, their risk perception may become better aligned with their cybersecurity postures and the ability to maintain business continuity when a cyber-attack or data breach occurs.

Significance

This study advanced current research in the areas of cybersecurity and business continuity. As a result, the findings and artifacts contributed to the body of knowledge in the fields of cybersecurity, risk management, and small business management. The business continuity of a small business in event of a cyber-attack or data breach is dependent on its ability to achieve an adequate posture of cybersecurity readiness and resilience. Although considerable risk management literature has been published focusing on improvements in cybersecurity for small and medium businesses, a gap exists with respect to the instruments needed to assess cybersecurity preparedness and perceived risk of cyber-attack with a focus on small businesses (Renaud, 2016; Rohn et al., 2016). Prior research has not accurately or consistently assessed the cybersecurity postures of small businesses in relation to cybersecurity preparedness activities and decision makers' risk perceptions (Berry & Berry, 2018). Thus, this research study provided a benchmarking tool and taxonomy enabling small business decision makers to assess their current cybersecurity postures. Additionally, this research study offered a cybersecurity planning program that may be used as a strategic guide for small businesses to manage their risk through prioritized cybersecurity preparedness activities to mitigate cyber-attacks and maintain business continuity (Cerullo & Cerullo, 2004; Paulsen, 2016).

Barriers and Issues

This research study had several potential barriers and issues that were addressed. The first challenge was developing a valid survey instrument to measure cybersecurity preparedness activities and assign weights. Straub (1989) recommended using the Delphi method to evaluate the measurement instrument and improve instrument validity. Accordingly, during the first phase, the Delphi method was used to collect data from SMEs to validate measures for the survey instrument (Ramim & Lichvar, 2014). The same SMEs also approved a set of cyber-attack vectors representing the common cyber threats to small businesses in order to measure decision makers’ perceived risk. The SME consensus of approved cybersecurity preparedness activities and common cyber-attacks was then used to align topics of the cyberARMoRR program for small businesses.

The second challenge was vetting the experience of SMEs. To mitigate this concern, the selection for the panel included only qualified cybersecurity experts with an appropriate level of cybersecurity experience and education as well as professional certification credentials. Third, there was the potential for a low response rate from the SMEs, especially considering the multiple rounds required during the first phase. According to Skinner, Nelson, Chin, and Land (2015), an expert panel size ranges from 10–30 SMEs. To control the possibility of a low response rate as well as nonresponses, 35 SMEs were contacted for participation. This research study received feedback from 22 SMEs using the Delphi method. Finally, permission from the Institutional Review Board (IRB) is needed to conduct a study when human subjects are involved. Therefore, IRB approval was obtained prior to conducting this study.

Another potential challenge for this research study was the communication of the survey instrument and solicitation to attain the target sample of small business decision makers. Kotulic and Clark (2004) observed a lack of empirical research within the discipline of information security risk management and concluded that businesses were reluctant to participate in research due to a general mistrust in disclosing their IS vulnerabilities to an “outsider” without prior support from executive management. To address this issue, data were collected from individual decision makers. The *small business decision maker* is either an owner or manager responsible for the risk and rewards of his or her business decisions. The survey instrument was kept concise, minimizing wording in questions that may prompt adverse reaction, in order to encourage further participation in the next phase of this research study. The survey instrument was structured in a manner that was easy for participants to submit responses (i.e., Yes or No for each of the cybersecurity preparedness activities) and avoided collecting confidential details about their business environment. However, soliciting participants was still a challenge due to the length of the survey. To encourage participation further, the researcher provided participants access to a voluntary, no-commitment, and no-cost cyberARMoRR program with resources and references to improve their cybersecurity postures. Thus, the appeal for participation stemmed from a focus on improving their cybersecurity postures through an assessment of cybersecurity preparedness activities and the decision makers’ perceived risk that will not impose on the business.

Assumptions, Limitations, and Delimitations

The purpose of assumptions, limitations, and delimitations are to determine the scope while considering potential difficulties and controls for making this research study relevant (Simon, 2011). Assumptions are plausible beliefs that are accepted without proof and assumed to be true within the context of a research study (Simon & Goes, 2013). Limitations are weaknesses beyond the control of the researcher that may potentially impact the generalizability, reliability, or validity of a research study (Leedy & Ormrod, 2016). Delimitations are intentional boundaries imposed by the researcher to manage the scope of a research study (Simon, 2011). The following assumptions, limitations, and delimitations were identified.

Assumptions

1. The SMEs were ethical and honest in their responses.
2. The same SMEs participated in multiple Delphi rounds of data collection for instrument development, instrument revisions, and CyberARMoRR program content alignment.
3. The small business decision makers who participated in this research study wanted to improve the cybersecurity postures of their businesses.
4. The participants were honest in their responses.
5. The participants had the authority to make decisions for their small businesses (i.e., owner or manager).
6. Participants were willing to provide responses about their cybersecurity preparedness activities with reasonable assurance of anonymity and privacy; identifiable information was not collected in the surveys.

Limitations

Regardless of the type of study, there are factors associated with the methods employed that may limit a research study (Ellis & Levy, 2010). For example, a weakness of a quantitative approach may be the lack of contextual meaning, while a weakness of a qualitative approach is sometimes generalizability of the findings (Creswell & Clark, 2017). This research study offset methodological weaknesses by drawing on the strengths of mixing both quantitative and qualitative data collection methods in the research design.

A known limitation of this research study was associated with expert opinions of the participating SMEs. This research study necessitated a commitment from the SMEs to provide informed judgment using the Delphi method for the development of the survey instrument and program topics (Ramim & Lichvar, 2014). According to Ellis and Levy (2010), SME opinions are limited by those participating and may not represent the only set of requirements during the developmental research process. Voluntary experts may withdraw from participation in a study at any time (Ellis & Levy, 2010). To mitigate these limitations and preserve validity, this research study combined the Delphi method with review of literature and cybersecurity benchmark reports. The NIST Cybersecurity Framework (NIST, 2018) was used as a reference to identify a preliminary set of cybersecurity preparedness activities for the SMEs to prioritize and approve. This research study utilized SMEs on a voluntary basis. SMEs with requisite qualifications were recruited to obtain consensus for the constructs, instrument, and program topics (Ramim & Lichvar, 2014; Skinner et al., 2015). Consensus and approval were calculated through average scoring of the SME responses. The SMEs were sourced through a network of information security and cybersecurity professionals; the majority had an affiliation with higher education and interests in cybersecurity for small businesses. The researcher made reasonable attempts to solicit SMEs with diverse small business experience along with cybersecurity qualifications. The researcher and SMEs did not provide consulting services to the SMEs or participants if they decided to implement or improve any cybersecurity activities during this research study.

Another limitation was that the respondent population of small business decision makers may not be evenly distributed to represent the complete range of business demographics (e.g., industry, number of employees, years in operation, annual revenue, IT budget). As with many small business studies, a limited sample size may decrease the generalizability of the findings. To mitigate this limitation, the sample population targeted a diverse range of small business owners and managers for each of the demographic indicators. Any outliers, or participants responding for businesses not meeting the small business criteria of less than 10–50 employees, were filtered through pre-screening data analysis. Nevertheless, reasonable efforts were made to reach a wide array of small business demographics through the communication and solicitation of participation to ensure that each small business demographic is appropriately represented. The participants were solicited through various professional business network associations and social media channels. Lastly, self-reported data from the participants were limited by the fact that they rarely can be independently verified and may have contained bias (Chan, 2009). To address the validity limitations, the survey instrument consisted of short and clearly written questions and was validated by the SMEs to encourage honest responses from the participants.

Delimitations

A delimitation is that the scope only consisted of the two constructs: cybersecurity preparedness and small businesses decision makers' perceived risk of cyber-attack. As with any complex problem domain, it is likely additional factors affect a small business decision maker's ability to mitigate cyber threats. For example, cost of security technologies and levels of proficiency will vary greatly (Romanosky, 2016). Small business decision makers may be constrained by resource cost factors in their ability to implement cybersecurity controls. Although an economic-based theoretical lens was adopted as the foundation for this research study, actual cost considerations of specific activities were intentionally excluded from scope due to the wide variety of technology options and skilled labor compensation. The cybersecurity preparedness activities were derived from the NIST Cybersecurity Framework because of its comparatively higher adoption rate among small businesses and the cost-neutral perspective for mitigating cybersecurity risk (BBB, 2017; NIST, 2018). The series of open-ended interview questions was focused purposefully on the SME-approved cybersecurity preparedness activities. Although some open questions may have solicited feedback on the cyberARMoRR program for future enhancements, the intent of the questions was to collect information about the challenges of cybersecurity preparedness activities.

Definition of Terms

The following represents the definitions of key terms used in this research study.

Cyber-attack. "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.” (NIST, 2011, p. B-3).

Cybersecurity. “Computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries” (Association for Computer Machinery [ACM] Joint Task Force on Cybersecurity Education, 2017, p. 16).

Cybersecurity event. “A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation)” (NIST, 2018, p. 45).

Cybersecurity incident. “An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences” (National Initiative for Cybersecurity Careers and Studies [NICCS], 2017, n.p.).

Cybersecurity preparedness. “The activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents” (NICCS, 2017, n.p.).

Cybersecurity preparedness activities. A prioritized set of actions, goals, objectives, and outcomes, as well as informative references for managing cybersecurity risk that are aligned to the high-level functions of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover (NIST, 2018; Sumner, 2009).

Cybersecurity posture. The overall strength of an organization’s cybersecurity controls and how effectively it can mitigate risk as a function of cybersecurity readiness and resilience (Bodeau & Graubart, 2017; Hurley et al., 2014; Rohn et al., 2016).

Cybersecurity readiness. Having situational awareness and being sufficiently prepared to deal with potential cyber threats to business operations, priorities, as well as mission by detecting and protecting against any cyber-attacks or data breach (Hurley et al., 2014).

Cybersecurity resilience. “The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources” (Bodeau & Graubart, 2017, p. 1).

Cybersecurity strategy (planning). The direction, activities, and actions needed to enable or improve cybersecurity in an organization (ACM Joint Task Force on Cybersecurity Education, 2017).

Delphi method. “An iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback” (Skulmoski, Hartman, & Krahn, 2007, p. 1).

Data breach. “The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information” (NICCS, 2017, n.p.).

Information system. A “work system whose processes and activities are devoted to processing information, that is, capturing, transmitting, storing, retrieving, manipulating, and displaying information” (Alter, 2008, p. 453).

Malware. "Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code" (Committee on National Security Systems [CNSS], 2015, p. 79).

Perceived risk. At the individual level, the probability assessment "composed of individual judgments regarding the likelihood that the unfavorable experience will happen, and the impact of that experience were it to happen" (Boss, 2007, p. 27).

Program. A plan or system under which action may be taken toward a goal; a set of related measures or activities with a particular long-term aim (Merriam-Webster, n.d.; Oxford Dictionary, n.d.).

Readiness. A degree of preparedness in the ability to assess cybersecurity posture proactively, gauge threats, and secure IS through a program or framework for managing risk (Peiro et al., 2005; Sumner, 2009; Sun, Ahluwalia, & Koong, 2011).

Resilience. "The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner" (NICCS, 2017, n.p.).

Risk. "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would rise if the circumstance or event occurs; and (ii) the likelihood of occurrence" (NIST, 2018, p. 46).

Risk management. "The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken" (NICCS, 2017, n.p.).

Risk mitigation. "Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process" (CNSS, 2015, p. 105).

Small business. A privately owned and operated business enterprise. Small businesses typically have a small number of employees (e.g., less than 50) (Rohn et al., 2016).

Small business decision maker. An owner or manager of a small business who is responsible for all the risks and rewards of his or her business decisions (Gupta & Hammond, 2005; Hayes et al., 2012).

Threat. "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" (CNSS, 2015, p. 122).

Summary

The purpose of this chapter was to provide an introduction of the research-worthy problem by presenting the background, goals, questions, relevance and significance, as well as assumptions, limitations, and delimitations for this research study. The dissertation goal identified what this research study accomplished; the specific research questions helped shape the literature review and methods; the relevance and significance section supported the problem statement and goal; the barriers and issues identified how to overcome any known and potential problems related to the success of this study; the assumptions, limitations, and delimitations that were beyond the researcher's control, as well as the factors for managing the scope of this research study; and the definition of terms removed ambiguity of key terminology used in this dissertation.

The research problem this research study addressed was the limited ability of small businesses to mitigate cyber threats, which leads to significant losses after a cyber-attack or data breach. The main dissertation goal was to develop and validate the CyPRisT then administer the cyberARMoRR program for small businesses. The eight specific goals of this research study were also discussed. The dissertation work required multiple rounds of collaboration with SMEs to develop the construct *cybersecurity preparedness activities* and update the construct *decision makers' perceived risk*. These constructs were used in the survey instrument, which was applied to the context of small businesses (i.e., those with 10–50 employees). The SME responses assisted in validating the survey instrument and aligning the cyberARMoRR program topics. Data were collected from 216 small business decision makers. The participants were invited to proceed in a quasi-experiment that led to an empirical assessment of cybersecurity readiness and resilience in small businesses. Chapter 2 comprises a comprehensive review of relevant literature. Chapter 3 then details the methodology and research design. Chapter 4 presents the results of this research study. Chapter 5 provides conclusions, implications, recommendations, and future research.

Chapter 2

Review of the Literature

Introduction

This chapter comprises a review of the relevant research studies pertaining to cybersecurity readiness and resilience in small businesses. The purpose of this literature review is to develop support for an exploratory study and quasi-experiment using the constructs of cybersecurity preparedness and small business decision makers' perceived risk of cyber-attack. The analysis of the literature begins with broad discussion on the topics of cybersecurity risk management, cybersecurity frameworks used for risk management, and common cyber threats to small businesses. A review of cybersecurity posture, cybersecurity readiness, and cybersecurity resilience literature leads to the development of the first construct of cybersecurity preparedness. The relevant literature is reviewed for the second construct, small business decision makers' perceived risk of cyber-attack. Next is a review of the literature for the theoretical foundation of this research study, prospect theory and status quo bias (Kahneman et al., 1991; Kahneman & Tversky, 1979; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992), as it relates to decision making under risk and uncertainty in the context of small businesses. This chapter concludes with a section summarizing what is known and unknown as presented by the review of relevant literature to distinguish the expected contributions of this research study.

Cybersecurity Risk Management

The aim of risk management, for any size business, is to reduce risk exposure by minimizing the likelihood of negative outcomes through a process of risk analysis as well as informed decision making (Rees et al., 2011; Straub & Welke, 1998). The process of information security risk management typically includes the key steps of identifying risk, appraising assets, reducing vulnerabilities, assessing and controlling threats, as well as preparing responses to events and planning recovery from incidents (NIST, 2018). *Cybersecurity risk* is "the extent to which an entity is threatened by a potential circumstance or event" based on the potential of an adverse impact and the likelihood of the occurrence (NIST, 2018, p. 46). As a strategy to mitigate cyber threats, the BBB (2017) recommended small businesses adopt a cybersecurity management approach, such as the NIST Cybersecurity Framework, as first step toward a comprehensive cybersecurity solution (NIST, 2014).

In general, cybersecurity risk management frameworks provide guidance for conducting a systematic and structured approach to mitigating vulnerabilities as well as dealing with cyber-attacks that may lead to substantial loss. Although the overall adoption rate is still relatively low, the BBB (2017) showed that the most popular framework used by small businesses is the NIST Cybersecurity Framework. Other reputable security frameworks include the International Organization for Standardizing International Electrotechnical Commission (ISO/IEC) 27000 series and the Control Objectives for Information and Related Technologies (COBIT) framework, especially for international (non-U.S.) organizations.

Many approaches to risk management have been developed and evaluated in IS literature. For example, a taxonomy of Information Security Risk Assessment (ISRA) provided a comparison of prevalent approaches used between 1995 and 2014 (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). The work of Shameli-Sendi et al. (2016), while comprehensive and informative, also highlights the challenges organizations face when attempting to make proper risk management decisions. Innovative advancements as well as the proliferation of emerging technologies utilized by businesses (e.g., mobile computing, social media, and cloud computing) have further complicated the process of assessing cyber risk (Mejias & Balthazard, 2014). Rohn et al. (2016) evaluated the COBIT framework adopted by small businesses and found the tendencies of the organizations with weak cybersecurity postures were due to low levels of threat awareness and decision makers' commitment to mitigate risk. Rohn et al. hypothesized that vulnerabilities were a manifestation of bias toward underestimating risk or the likelihood of an occurrence of an event, which then led to a "lack of urgency" for risk mitigating controls. This study was well founded using social theories but limited in the consideration of using risk perception as a measure in the decision makers' appraisal of threats and commensurate activities toward mitigating risk (Rohn et al., 2016).

In an earlier study, Gupta and Hammond (2005) found small businesses were challenged by cybersecurity strategies because the owners were not as adept at selecting appropriate security technologies. The effectiveness of their cybersecurity controls was affected by the small business decision makers' beliefs that running the business was more important than counteracting security threats with new security technologies, as well as implementing policies and procedures. Bhattacharya (2011) later examined the relation of small business owners' level of concern and the leadership styles that were most effective in preventing cyber-attacks and data breaches. The empirical data showed a significant correlation between the leadership styles of small business owners taking proactive approaches to prepare against common cyber threats. However, further research was advised given the evolving nature of cybercrime and information security best practices as well as the ability of small businesses to mitigate risk. Berry and Berry (2018) recently conducted a study to assess small businesses' cyber risk management tools and techniques. This assessment focused on password protection as well as the success of having cybersecurity policies in place. In the discussion of the problem, Berry and Berry acknowledged differences in perception related to common cyber threats but did not explore specific concerns beyond the questions of basic security activities. Table 1 provides a summary of the pertinent research studies regarding cybersecurity risk management in small businesses.

Table 1

Summary of Cybersecurity Risk Management in Small Businesses.

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Berry & Berry, 2018	Field research – interviews conducted by students	370 assessments collected from small business owners	Questionnaire consisting of various risk management approaches	Small businesses are likely to lack tools for risk mitigation (e.g., policies, procedures, training, and strong passwords)

Table 1

Summary of Cybersecurity Risk Management Studies in Small Businesses (continued)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Bhattacharya, 2011	Empirical study via survey	122 small business owners	Multifactor leadership questionnaire and small business security survey instrument	A significant correlation between small business leadership and levels of concern towards information security
Gupta & Hammond, 2005	Empirical study via survey	138 small businesses	Questionnaire with level of security concerns, competencies, and experiences	Small businesses IS security strategies differ from medium or large business; small businesses are less effective when owners are not adept at selecting appropriate technologies
Hayes et al., 2012	Empirical study, pretest of confidence and posttest actual knowledge of security threats	48 small business owners and managers in the Arkansas region	Knowledge of computer security threats the ability to understand and identify four main types: viruses, trojans, spyware, and phishing attacks	Small business owners and managers were less confident, and lacking knowledge, this led to potential losses from security breaches

Table 1

Summary of Cybersecurity Risk Management Studies in Small Businesses (continued)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Lee & Larsen, 2009	Empirical study via survey	239 small and medium-sized business executives	Constructs of perceived severity, perceived vulnerability, response efficacy, and social influence	Threat appraisals significantly affected security software adoption; this implied that decisions were made based on the negative consequences from cyber-attack as well as the ability to apply countermeasures
Rohn et al., 2016	Field research	17 small businesses and non-profits	Certified IT audit of 67 COBIT controls and 206 related tests.	Less than 1/3 of the controls were correctly implemented, inherent bias may explain tendencies to incorrectly asses risk.
Spillan, 2003	Empirical study via survey	162 responses from the HR or executive offices of small and medium-sized businesses	Crisis events, degree of concern for each event, whether the crisis had actually occurred at the respondent’s organization within the last 3 years, and if they had a crisis management team	The lack of planning among owners and managers of small businesses is a function of their concern for worst-case scenario as well as the actual occurrence of an unexpected crisis event

Cybersecurity Framework for Managing Risk.

Cybersecurity risk management is the process of evaluating business operations and planning risk-related activities including assessing risk, responding to a risk once determined, and monitoring risk over time (Paulsen & Toth, 2016). The NIST Cybersecurity Framework provides a set of guidance to public as well as private sector organizations to improve their ability to identify, prevent, detect, respond, and recover from cyber-attacks (NIST, 2014, 2018). The NIST Cybersecurity Framework was initiated in February 2013 by Executive Order 13636 (NIST, n.d.-a). The Executive Order tasked the development of a set of cybersecurity guidelines and standards for all sectors of critical infrastructure as a framework to reduce risk. After a series of five major workshops and comments from 15,000 cybersecurity experts and stakeholders, the NIST released the Cybersecurity Framework version 1.0 in 2014.

The Cybersecurity Enhancement Act of 2014 (CEA) officially formalized the role of the NIST to facilitate the continued development of the voluntary Cybersecurity Framework through public–private collaboration. Specifically, the CEA public law (P.L. 113-274 S. 1353) set forth a national cybersecurity awareness and education program with widespread effort to make cybersecurity best practices usable by individuals, small to medium-sized businesses, as well as educational institutions. The CEA expanded the role of NIST's development of the voluntary framework in order to identify "a prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cyber threats (NIST, n.p.). The NIST Cybersecurity Framework continued to evolve through a series of workshops, engagement with stakeholders in government and academia, as well as feedback from industry.

The NIST released the Cybersecurity Framework version 1.1 in 2018, which was more adaptable to small businesses as well as a greater variety of industry sectors and nonprofit communities (NIST, n.d.-a). The new version focuses on enabling the framework for any organization “regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving security and resilience” (NIST, 2018, p. v). According the NIST (n.d.-a), the new version of the NIST Cybersecurity Framework was developed to be implemented by first-time users and is fully compatible with the original version if already in use. Organizations currently using version 1.0 may incorporate the additional content and functionality from version 1.1 (NIST, n.d.-a). Figure 2 shows the NIST Cybersecurity Framework development timeline and update process from inception through release of versions 1.0 and 1.1.

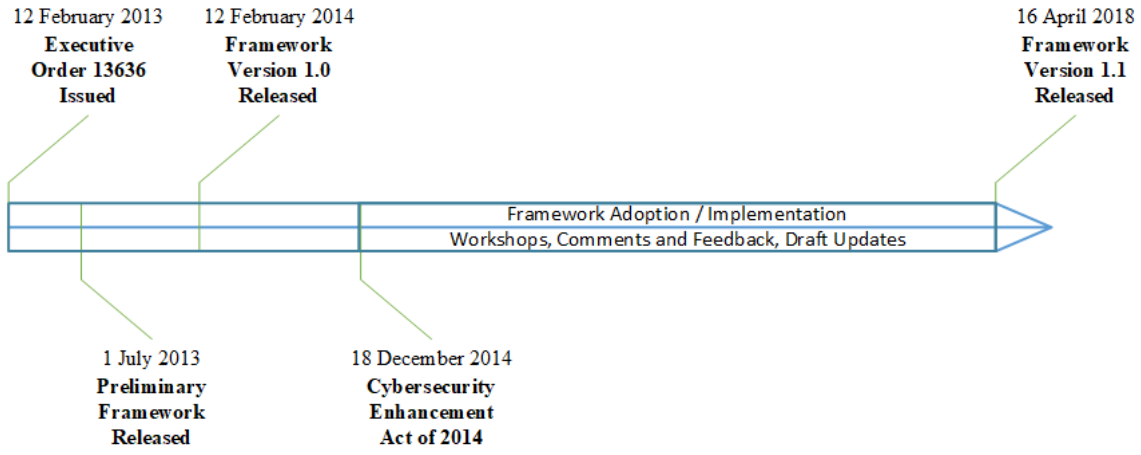

12 February 2013
Executive Order 13636 Issued
12 February 2014
Framework Version 1.0 Released
16 April 2018
Framework Version 1.1 Released
Framework Adoption / Implementation
Workshops, Comments and Feedback, Draft Updates
1 July 2013
Preliminary Framework Released
18 December 2014
Cybersecurity Enhancement Act of 2014

Figure 2. The NIST Cybersecurity Framework Update Process (NIST, n.d.-a).

Recognizing the benefits of the NIST Cybersecurity Framework for small businesses, the U.S. Small Business Administration and Federal Bureau of Investigation

InfraGard partnered with the NIST in conducting research as well as development of outreach programs for small businesses to improve their cybersecurity postures (Paulsen & Toth, 2016). The NIST Interagency Report 7621 Revision 1 was recommended as a 'starter kit' because it provides guidance to understand better the fundamentals of information security as well as the "information needed by small businesses to implement a program to help them understand and manage their information and cybersecurity risk" (Paulsen & Toth, 2016, p. 1). The 'Framework Core' consists of five functions to organizations' risk management portfolio (NIST, 2018): Identify, Protect, Detect, Respond, and Recover. As described by NIST (2018), the functions are a set of cybersecurity activities that "provide a high-level strategic view of the lifecycle of an organization's management of cybersecurity risk" (p. 3). The functions may be performed concurrently or continuously as part of a cybersecurity program to establish and improve cybersecurity. The continuous process of five core functions are represented in Figure 3.

Per the NIST (2018), the five core functions of the Cybersecurity Framework are defined as follows:

1. *Identify* – "Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enable an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs" (NIST, 2018, p. 7).

2. *Protect* – “Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event” (NIST, 2018, p. 7).
3. *Detect* – “Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events” (NIST, 2018, p. 7).
4. *Respond* – “Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident” (NIST, 2018, p. 8).
5. *Recover* – “Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident” (NIST, 2018, p. 8).

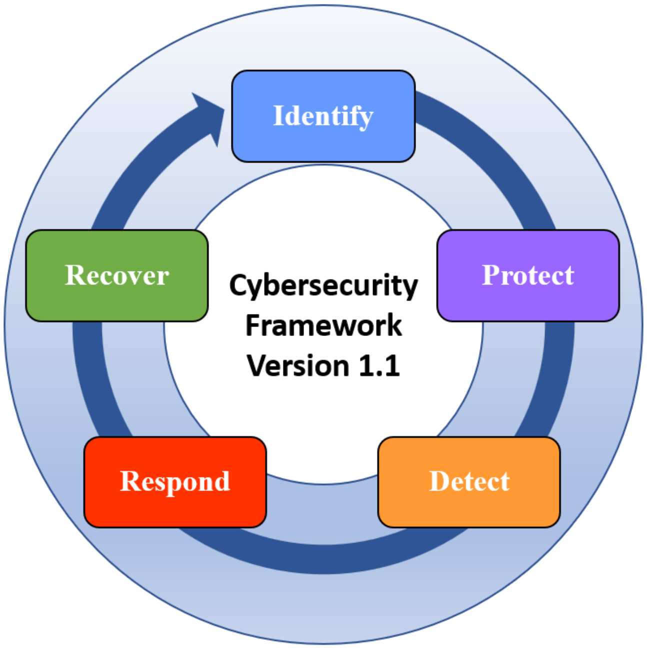


Figure 3. The five functions of the NIST Cybersecurity Framework version 1.1 (NIST, 2018).

Common Cyber Threats and Cyber-attacks

A risk management approach for small businesses involves identification of the common cyber threats and cyber-attacks (Berry & Berry, 2018). In broad terms, a *threat* is the likelihood that a vulnerability may be exploited to cause a security breach, and an *attack* is the actual attempt of unauthorized action. There is inevitably a wide range of cyber threats with the potential to impact any organization negatively, regardless of industry or business size (Symantec Corporation, 2018). Classifications of cyber-attack vectors as well as the vulnerabilities exploited vary within the IS literature and cybersecurity benchmark reports. Cybersecurity benchmark reports provide readers valuable information to gauge trends of threats, cyber-attacks, and data breaches across various demographics. For example, Verizon Enterprise publishes an annual Data Breach Investigation Report (DBIR) that provides statistical summaries by incident and data breach. An *incident* is a "security event that compromises the integrity, confidentiality, or availability of information assets," whereas a b*reach* "is an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party" (Verizon Enterprise, 2018, p. 2). This information is then classified by threat action (i.e., threat actor's tactic or mode of attack).

A *threat vector* (also called an attack vector) refers to the means by which an attack action may occur, such as the tool, technique, or path via which an unauthorized actor gains access. Cyber-attacks often exploit multiple vulnerabilities or combine threat vectors to gain entry to a network or system, such as malware introduced through an email phishing attack. According to the Ponemon Institute (2017, 2018), the most frequent cyber-attacks causing severe financial consequences to small businesses are from phishing/social engineering, web-based attacks, malware, stolen devices, and denial of service attacks. The most frequent data breaches causing severe financial consequences to small businesses are from negligent employees or contractors, third-party mistakes, errors in operating processes, and hacker attacks (Ponemon Institute, 2017, 2018). The top claims of cybersecurity incidents reported to Hiscox (2018a) include ransomware, hacker attacks, and loss or misuse of data. These examples are just a few of many, all with varying threat vectors and vulnerabilities exploited. Nevertheless, the scenarios fundamentally underscore the complexity of problems that face small businesses as threat actors become increasingly sophisticated in their attack techniques. Table 2 provides a summary of the cybersecurity benchmark reports and findings relevant to risk management in small businesses.

Table 2

Summary of Cybersecurity Benchmark Reports

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
BBB, 2017	Empirical study	Over 1500 businesses in the U.S. and Canada	Survey written by Council of BBB Research and conducted using Google consumer surveys	The key barriers for small business are lack of cyber education, lack of resources, and lack of time. Suggests efforts focused on smaller businesses are necessary
Cisco, 2018	Empirical study conducted with technology partners (e.g., Qualys, Saint Corporation)	Over 3600 respondents across 26 countries (all business sizes and industries)	Reporting select data specific to small/midmarket businesses from the Cisco 2018 Security Capabilities Benchmark Study	Unprepared small/midmarket business are less resilient and struggle to survive cyber-attacks
Hiscox, 2018b	Empirical study	Over 4,100 executives, departmental heads, IT managers and other key professionals in the UK, US, Germany, Spain and the Netherlands	Reporting select data specific to small businesses from the Hiscox Cyber Readiness Report	47% of small businesses had at least one cyber-attack in the past year, 44% had two to four cyber-attacks, average costs of a cyber-attack ranged from $24K-$63K for business with fewer than 100 employees

Table 2

Summary of Cybersecurity Benchmark Reports (continued)

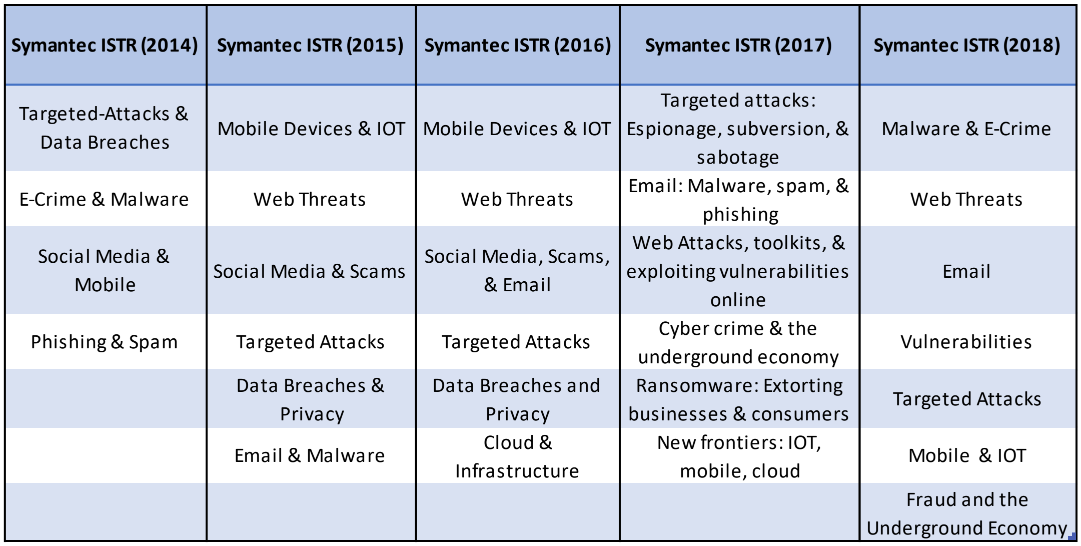
Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Ponemon Institute, 2017	Empirical study	1040 IT security practitioners, managers, owners as well as consultants in small and medium-sized companies located in the UK and US	Security posture, prioritization of IT security, compliance with guidelines or standards, experiences with cyber-attacks	Cyber-attacks rising from 55% to 61% of affected respondents, Phishing/social engineering and web-based attacks were most prevalent. Ransomware rose from 2% to 52% affected (mostly through phishing attack), 54% of breaches contained sensitive information, cyber-attacks were most costly
Ponemon Institute, 2018	Empirical study	1045 IT security practitioners, managers, owners as well as consultants in small and medium-sized companies located in the UK and US	Security posture, prioritization of IT security, compliance with guidelines or standards, experiences with cyber-attacks	Cyber-attacks rising from 61% to 67%, Phishing/social engineering and web-based attacks were most prevalent. Ransomware rose from 52% to 61% affected (mostly through phishing attack), 58% of breaches contained sensitive information.

Table 2

Summary of Cybersecurity Benchmark Reports (continued)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Symantec Corporation, 2018	Empirical study from the largest civilian network of monitored sensors and threat activities	Over 175 million endpoints located in 157 countries, 126.5 million attack sensors, recording thousands of threat events every second, over five petabytes of security threat data	Emerging trends of cybercrime threat landscape, vulnerabilities, targeted attacks (malicious code activity, ransomware, phishing, and spam as well as mobile threats)	Small business (1-250) were largely affected malware and spam. Across the board the threat landscape has become more diverse with spike in supply chain attacks and ransomware.
Verizon Enterprise, 2018	Empirical study from multiple security vendors	Over 333K reported incidents and over 16K reported data breaches using the Vocabulary for Event Recording and Incident Sharing (VERIS) framework	Incident and data breach patterns and figures reported through the global VERIS Community Database (VCDB)	58% of data breach victims were small businesses, malware and point of sale breaches is an on-going major problem for small businesses

Since 2014, Verizon Enterprise has classified the patterns of cybersecurity incidents and breaches into nine categories of commonality: (a) crimeware, (b) cyberespionage, (c) lost/stolen assets, (d) miscellaneous errors, (e) payment card skimmer, (f) point of sale, (g) privilege misuse, (h) web applications, and (i) everything else. The cyber threat actions that are leveraged to carry out an attack or data breach are then classified into seven categories: (a) error, (b) environmental, (c) hacking, (d) malware, (e) misuse, (f) physical, and (g) social (Verizon Enterprise, 2018). Similarly, the Symantec Corporation reports the top categories of cyber threats. Figure 4 presents a summary of major topics representing the shifting threat landscape between 2014 and 2018. The topics are organized by the major categories each year. Because the reporting structure and cybersecurity topics vary, it is difficult to determine trends from the relevant facts and figures. A strong framework, using a simple and consistent classification of cyber-attacks, is recommended for assessing the cybersecurity posture of a small business in their ability to defend against common threats (Rohn et al., 2016).



Symantec ISTR (2014)	Symantec ISTR (2015)	Symantec ISTR (2016)	Symantec ISTR (2017)	Symantec ISTR (2018)
Targeted-Attacks & Data Breaches	Mobile Devices & IOT	Mobile Devices & IOT	Targeted attacks: Espionage, subversion, & sabotage	Malware & E-Crime
E-Crime & Malware	Web Threats	Web Threats	Email: Malware, spam, & phishing	Web Threats
Social Media & Mobile	Social Media & Scams	Social Media, Scams, & Email	Web Attacks, toolkits, & exploiting vulnerabilities online	Email
Phishing & Spam	Targeted Attacks	Targeted Attacks	Cyber crime & the underground economy	Vulnerabilities
	Data Breaches & Privacy	Data Breaches and Privacy	Ransomware: Extorting businesses & consumers	Targeted Attacks
	Email & Malware	Cloud & Infrastructure	New frontiers: IOT, mobile, cloud	Mobile & IOT
				Fraud and the Underground Economy

Figure 4. The Internet Security Threat Report (ISTR) major topics over a 5-year period (Symantec Corporation, 2014, 2015, 2016, 2017, 2018).

Cybersecurity Posture

Social theories may be useful for IS researchers to address the lack of sufficient security controls among small businesses and their limited ability to improve their cybersecurity postures (Rohn et al., 2016). Broadening the problem is the limited availability of cybersecurity product materials as well as risk management programs that are tailored to meet the needs of small business owners (Berry & Berry, 2018). Cybersecurity and IS researchers have argued there is not enough comprehensible information for small business owners to make informed decisions about mitigating cyber threats and combatting cyber-attacks (Gafni & Pavel, 2019; Osborn & Simpson, 2018). For example, small businesses struggle in this area due to a lack of ability to understand what security controls to implement and how to react when there is an incident (Osborn & Simpson, 2018; Ponemon Institute, 2018).

Osborn and Simpson (2018) posited the ‘knowledge problem’ is related to the decision maker having a general lack of cybersecurity awareness. Similarly, Berry and Berry (2018) found there is a lack of ability in many small businesses to understand their information security needs and the use of risk management tools. For example, having full situation awareness of cyber threats can be an onerous process of classifying techniques and impacts. This process includes identifying cyber-attack methods and ranking dimensions based on the origin (inside/outside the company; human/nonhuman) and intent (deliberate/unintentional) as well as the varying degrees of consequences and disruptions (Jouini, Rabai, & Aissa, 2014; Loch, Carr, & Warkentin, 1992). Arguably, this ability is outside small business owners’ primary concern, which is naturally focused on “sales and revenues, in order to survive and stay in business” (Bhattacharya, 2015, p.

11). However, since the CEA of 2014, organizations such as the National CyberSecurity Alliance (NCSA) and the BBB have taken a proactive approach to offer free and easy to understand materials targeted for the small business community. These programs apply core NIST Cybersecurity Framework functions and activities to learning curricula. However, few empirical studies have assessed the levels of preparedness small businesses achieve as a result of participating in these programs or adoption of the framework.

Cybersecurity Readiness

It can be difficult for small business decision makers to assess their level of cybersecurity posture without first establishing a qualified reference point of recommended best practices and cybersecurity preparedness activities. The immersion of Internet-related technologies has led organizations toward evaluating the strategic balance of IS benefits against managing business risk based on a perspective of readiness (Martinsons, Davison, & Tse, 1999). The measure of this perspective is generally at the individual level. For example, Sun et al. (2011) measured users' attitudes toward security measures by developing a model that differentiates risk propensity with IT proficiency and levels of data criticality. Sun et al. (2011) found a higher level of data criticality has a positive impact on information security readiness, but only up to the point perceived as important by the participants. Sun et al. suggested information security preparedness activities are dependent on the business decision makers' feelings and beliefs about protecting data as well as their personal risk propensity. Sun et al. (2011) also suggested tradeoffs occur between the utility of IS and the enhancements of security countermeasures based on a degree of readiness. Sun et al. (2011) defined the term *readiness* as the “degree of preparedness and inclination to use a method, rather than the decision whether not to use it” (p. 573). This can be interpreted as a binary decision to implement a control based on the decision makers’ perceptions of risk (i.e., perceived likelihood and perceived impact of a negative outcome).

Researchers have also applied frameworks to organizational settings to evaluate levels of preparedness. For example, Susanto, Almunawar, and Tuan (2012) proposed a ‘novelty approach’ for an integrated solution framework based on the ISO27000 series standards. Susanto et al. had encountered obstacles with the actual implementation of controls used to support the organization’s processes, particularly in cases of small businesses that had low adoption of ISO standards. Hurley et al. (2014) addressed some of the challenges of metrics and measures for the concept of cybersecurity readiness, suggesting a broader view that includes the key activities and milestones of a cyber profile. However, the perspectives of Hurley et al. (2014) predated the version 1.0 release of the NIST Cybersecurity Framework (2014) and its adoption among small businesses. Although Hurley et al. (2014) examined the concept and quality of cyber-readiness efforts, they did not propose a measure for assessing the level of preparedness.

Cybersecurity Resilience

Cybersecurity resilience often addresses challenges for analyzing resilience at the national strategic level and is rooted in crisis and emergency management literature (Chittister & Haimes, 2011; Harrop & Matteson, 2015; Zobel & Khansa, 2012). For example, Kahan, Allen, and George (2009) presented a structed operational policy framework as building blocks for understanding the parameters of resilience. However, cybersecurity resilience is also useful in the analysis of organizational IS by evaluating the actionable items and threats through the risk assessment process (Linkov et al., 2013). At the organizational level, cybersecurity resilience complements cybersecurity readiness in the function of establishing a strong cybersecurity posture by establishing a framework for business continuity and reducing impacts from major disruptions (Rohn et al., 2016).

Cybersecurity resilience is an area of growing importance for businesses. In risk analysis, Haimes (2009) described the relationship between preparedness, vulnerabilities, and resilience as a manifestation of states in IS. In other words, resilience is a focus on the system's ability to recover from an adverse event. In IS literature, resilience is often associated with the recovery of systems. Williams and Manheke (2010) defined *cybersecurity resilience* for small businesses as "the ability to recover and return to an original state, after some event has occurred to disrupt the original state" (p. 112). Conversely, Bodeau and Graubart (2017) considered the concept of cybersecurity resilience beyond the recovery paradigm to include the ability to anticipate, withstand, and adapt to adverse conditions as well as attacks and compromises on cyber resources. This can be interpreted as having the ability to call to action the level of readiness to ensure business continuity during and after a cybersecurity event. Accordingly, there is strategic significance in the ability for small businesses to achieve a resilient cybersecurity posture. Another perspective is that resilience consists of the cybersecurity principles with an objective to protect systems and ensure business continuity as an intended outcome of activities (Björck, Henkel, Stirna, & Zdravkovic, 2015). As such, many of the cybersecurity preparedness activities can be mapped to the five functions of the NIST Cybersecurity Framework to provide an organization with the ability to withstand and recover from adverse events (NIST, 2014, 2018).

The Construct of Cybersecurity Preparedness

The concept of preparedness is a fundamental aspect of risk management that includes both cybersecurity readiness and resilience. Yet, it appears the conceptual construct of cybersecurity preparedness has not been proposed or empirically validated in IS research. Therefore, this research study used the aforementioned literature as the foundation to propose and validate empirically the construct of cybersecurity preparedness. To measure the level of preparedness in small businesses, the cybersecurity preparedness activities were based on the five functions of the NIST Cybersecurity Framework, then presented, approved, and prioritized by cybersecurity SMEs, as further described in Chapter 3.

Perceived Risk of Cyber-attack

Perceived risk has been evaluated through various theoretical lens and contexts. For example, Bettman (1973), in the field of marketing, empirically examined risk handling and inherent risk reduction techniques in consumer decision-making processes using an additive model for calculating overall risk. Bettman (1973) found consumer decisions were influenced by perceived risk. Goodhue and Straub (1991) are among the seminal IS researchers who investigated the construct of perceived risk in the context of information security. They examined issues with IS departments and the end-users' perceptions about security concerns with their systems. Protection of data as a security concern is dependent on the relationship between risk perceptions and the protective actions to reduce risk (Goodhue & Straub, 1991). Featherman and Pavlou (2003) conducted a review of perceived risk in literature in order to merge the construct into a technology acceptance model with facets of perceived risk as a second-order variable. In the context of e-services adoption, this research model incorporated the likelihood of interacting with unknown people, products or services by measuring various dimensions of perceived risk. Stewart (2004) used risk compensation theory to address concept of perceived risk in security problems when making key business decisions suggesting “reaction to risk is most influenced by the severity of the possible outcome” (p. 367). This viewpoint is congruent with the notion that small business decision makers are likely to improve their security postures if there is a possibility of loss or higher likelihood of significant impact.

Dinev and Hart (2006) investigated security and privacy choices through a theoretical calculus model that individuals use to assess risk. Dinev and Hart (2006) described risk beliefs as the “possibility of loss” and related perception to levels of risk uncertainty (p. 63). Sumner (2009) established that risk mitigation strategies, specifically among small and medium businesses, are often aligned with the decision makers’ perceived risk based on their level of preparedness to deal with common threats.

Sun et al. (2011) proposed a psychological construct of Information Security Readiness (ISR) to describe attitudes toward security measures. The ISR differs from security awareness in that it evaluates both proficiency (knowledge and skill/expertise) and risk propensity. Thus, the term *readiness* denotes the “degree of preparedness and inclination to use a [cybersecurity] method, rather than the decision whether or not to use it" (Sun et al., 2011, p. 573). However, the findings of Sun et al. (2011) are limited in generalizability because the sample population consisted of university students who were familiar with IT security systems rather than the business environment.

Sangani and Vijayakumar (2012) provided an overview of cyber threats as well as examples of controls that small and medium sized businesses could easily implement with minimal costs and without disruption to service to address some of the major cybersecurity threats. However, the suggestion did not follow a structured framework that could be incorporated as part of the business strategy and operations. The strategy of a well-balanced cybersecurity posture for small businesses depends on the cybersecurity preparedness activities to mitigate the most common and potentially harmful types of cyber-attacks (Baskerville et al., 2014).

Baskerville et al. (2014) investigated the risk–safeguard relationship in several businesses when factoring risk assumptions. The perspectives of cybersecurity prevention and response paradigms provide valuable insight about cybersecurity strategic posture and the decision-making process. In essence, how assumptions and perceptions affect the relationship between risk and safeguards through the balance of prevention and response strategy. In this research study, this relationship between risk and cybersecurity activities refers to the level of preparedness given the ability to assess cybersecurity threats and vulnerabilities (Sumner, 2009; Sun et al., 2011). Thus, this research study considered both the cybersecurity readiness and resilience of small businesses as an indicator of their cybersecurity postures. Table 3 provides a summary of select research studies specific to risk analysis in relation to cybersecurity posture and preparedness decision making.

Table 3

Summary of Perceived Risk in IS Literature

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Baskerville et al., 2014	Comparative case studies	3 large organizations	Prevention and Response paradigms	Strategic posture regarding balancing efforts of prevention and response is related to risk assumptions (perceptions)
Dinev & Hart, 2006	Empirical via survey	369 students at a university in Southeastern U.S.	Perceived privacy risk, Internet privacy concerns, Internet trust, personal interest.	The risk decision making process by individuals to conduct transactions involved weighing costs, convenience, reputation, and other factors the security calculus of perceived risk and privacy concerns.
Lee & Larsen, 2009	Empirical study via survey	239 U.S. small and medium-sized business executives	Threat and coping appraisals; perceived severity, perceived vulnerability, response efficacy, and social influence	Threat and coping appraisal predicted anti-malware software adoption intention; the decision was influenced by perceived severity of consequences from malware attacks and the perceived vulnerability to the attacks

Table 3

Summary of Perceived Risk (continued)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Osborn & Simpson, 2018	Empirical study and qualitative meta-study	33 responses to the initial questionnaire from small and medium-sized companies in the UK, spanning 19 different industry sectors; 20 detailed unstructured interviews	Decision-making and risk assessment practices of small-scale IT users and businesses to compare the processes implemented with common corporate cyber security practices	Decision makers focused on easy measures leads to a disconnect between the security implemented and any risks identified; available resources, knowledge, prioritization of business processes, reduced system control and a lack of threat intelligence all combine to limit the ability to make cybersecurity decisions
Sumner, 2009	Empirical study	102 IT professional in 10 organizations	Risk assessment based on the perceived impact and perceived probability of threats, risk mitigation based on perceived level of preparedness, as well as the extent of occurrence and the impact of threats relate to the level of preparedness	Most high-impact and high probability threats were aligned but the levels of preparedness were not aligned with perceived risk

Table 3

Summary of Perceived Risk (continued)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Sun et al., 2011	Pilot study and laboratory experiment	109 students enrolled in computer IS courses	IT proficiency, risk propensity, Information Security Readiness (affective, cognitive, & behavioral)	Proposed the ISR construct as well as measures to capture user cognitive, affective, and behavioral attitudes towards security levels (data criticality)

The Construct of Decision Makers' Perceived Risk of Cyber-attack

According to Mejias and Balthazard (2014), common cyber threats include, but are not limited to, "viruses, network worms, trojan horses, denial of service (DoS) attacks, SQL injection, botnets, DNS attacks, virus hoaxes, steganography, cross-site scripting, and SCADA attacks" (p. 164). To measure small business decision makers' perceived risk of common cyber-attacks effectively, this research study proposes using the classification types from the Ponemen Institute's cybersecurity benchmark reports (Ponemon Institute, 2016, 2017, 2018). Sumner (2009) used cyber threat classifications in a similar manner following Whitman's (2003) research, Sumner assessed risk by measuring the perceived impact and probability of threats. However, even the most recent threat categories, such as those identified by Whitman and Mattord (2015), are broadly focused on shifting threat types and do not specifically address the context of common cyber-attacks from a decision maker's risk perception. This research study proposed adopting the classifications of cyber-attacks so the data may be evaluated against actual reported incidents and trends. The important distinction between cyber threat and cyber-attack is the materialization of a cyber threat (Mejias & Balthazard, 2014). Therefore, the classification types of cyber-attacks from the Ponemon Institute (2016, 2017, 2018) were used to provide familiarity to the small business decision maker as a frame of reference to the common cyber threats with the potential to cause severe financial consequences. The following 10 cyber-attack categories were briefly defined for the small business participants from the IS literature and presented to SMEs for approval.

1. *General malware* – A wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs) (Hayes et al., 2012).
2. *Advanced malware/zero-day attack* – Sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats – the intruder establishes a discrete presence to mine data). A zero-day attack targets newly discovered system vulnerabilities when a patch has not yet been developed (Hurley et al., 2014).
3. *Compromised/stolen devices* – Theft of equipment or information. Stolen devices contain information of value that is stored locally. Compromised credentials allow further access into an organization’s IS or networks (Romanosky, 2016).

4. *Cross-site scripting* – Placement of scripts into attacker-controlled, trusted and typically high-traffic websites in order to inject malicious client-side code on the visitor's computers (Jang-Jaccard & Nepal, 2014).
5. *Denial of services* – Flooding the targeted network with traffic until it cannot respond or crashes, preventing access from legitimate users. In a distributed denial of service attack (DDoS), the incoming traffic flooding the victim originates from many different sources (Zobel & Khansa, 2012).
6. *Malicious insider* – A malicious attack perpetrated by a person within the organization, such as an employee, former employee, contractor or business associate, who has privileged information concerning the organization's security practices, data, and computer systems (Hunker & Probst, 2011; Pfleeger, Predd, Hunker, & Bulford, 2010).
7. *Phishing/social engineering* – The use of human interaction to obtain information about a user, organization, or its computer systems to gain unauthorized access. Phishing is a type of social engineering to obtain sensitive information from individuals, usually by posing as a trustworthy entity (Hong, 2012).
8. *SQL injection* – Targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database and then extract content.
9. *Web-based attack* – Sabotaging websites, probing vulnerabilities through web-connected resources, and exploiting Internet-connected devices to gain unauthorized access to a system or network.

10. *Other* – Any other cyber-attack not listed above (e.g., cyber extortion/espionage, miscellaneous errors, and payment skimmers).

Boss (2007) measured perceived risk as a simple formula of perceived likelihood multiplied by perceived impact using a 5-point Likert scale. This method drew from Barki, Rivard, and Talbot (2001) by using their process to calculate the overall risk by multiplying the likelihood and impact scores together for each threat. The scale was defined as very low–moderate–very high for both impact and likelihood. In this research study, the scales for perceived likelihood used a 7-point Likert range from extremely low likelihood to extremely high likelihood. Likewise, the scales for perceived impact used a 7-point Likert range from extremely low impact to extremely high impact. Both perceived likelihood and perceived impact was collected and multiplied for each of the cyber-attack types. The measurement of small business decision makers' perceived risk of cyber-attack were calculated by multiplying the likelihood of the 10 common cyber-attacks to small businesses listed above. The definitions for common cyber-attacks were presented and approved by the cybersecurity SMEs, as further discussed in Chapter 3.

Prospect Theory and Status Quo Bias

Kahneman and Tversky (1979) developed prospect theory as an alternative to then-popular expected utility theory. Prospect theory challenged the axiom violations of utility theory to describe better how decisions are made under conditions of risk. This theory offered new insight into why nonoptimal decisions are made because they are framed in different ways. For example, when probabilities of a certain outcome are low, a decision is often made on a cognitive weighting function from the derived choices; the “low probabilities are generally overweighed” (Kahneman & Tversky, 1979, p. 281). The inverse is an underweighting of moderate and high probabilities—this is more pronounced in the decision weights of chance events and treating the prospect of highly unlikely events as impossible (Tversky & Kahneman, 1981). The *framing effect* is a perceptive bias in a decision maker’s evaluation of options when presented with positive or negative semantics (Kahneman & Tversky, 1984). Bazerman (1984) examined the core assumptions of prospect theory, including the effects of framing for individuals and organizational decision making. Bazerman (1984) found tendencies “to be risk averse in positively framed situations, while being risk seeking in negatively framed situations” (p. 12). As Whyte (1986) pointed out, prospect theory provided a psychological explanation of this decision-making phenomena because it can be applied to the context of both failure and success, such as justifying a losing course of action through an escalation of commitment. Decisions based on framed circumstances, such as committing to a risk adverse outcome, also have potential for negative consequences if the decision maker justifies maintaining a current state of affair (status quo) when knowing of a significant problem or imminent threat. Figure 5 illustrates prospect theory in the decision-making process where the reference point is the intersect between the subjective value of the perceived gain or loss (Kahneman & Tversky, 1979, 1984).

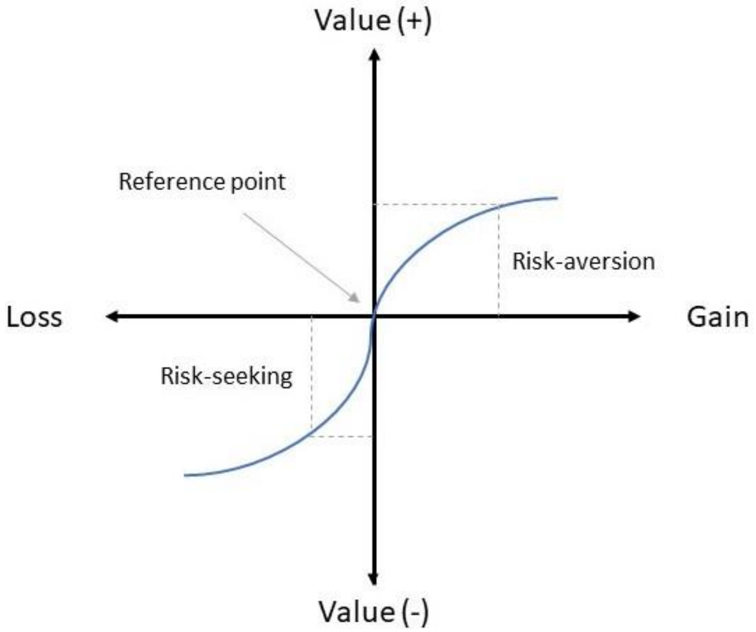


Figure 5. Prospect Theory in the Decision-Making Process (Kahneman & Tversky, 1979, 1984).

Samuelson and Zeckhauser (1988) introduced the framing effect of status quo bias to describe cognitive dissonance in the decision-making process. Tversky and Kahneman (1991) recognized the relation between status quo bias and loss aversion, a significant feature associated with the value function in prospect theory that losses loom larger than gains. The alternative option of status quo implied that the decision maker would be indifferent between choices when presented with positive or negative outcomes. Tversky and Kahneman (1992) later developed a new version of prospect theory to explain the patterns of risk aversion and thereby extended the theory in several respects. Cumulative prospect theory added a weighting to the probability function of outcomes. The contributions of Tversky and Kahneman, particularly in the areas of cognitive bias, have provided a theoretical foundation for scientific advancement as well as a philosophical framework to explain decision-making under risk (Barberis, 2013; Shefrin

& Statman, 2003). Cumulative prospect theory and status quo bias, as well as many other heuristics and biases associated with prospect theory, have been widely adopted as a theoretical perspective in academic literature across disciplines (Lee & Joshi, 2016; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992).

In IS literature, scholars have utilized the theoretical lens of prospect theory and status quo bias to describe many aspects of risk, including making decisions with conditions of uncertainty. For example, Kim and Kankanhalli (2009) examined the psychological commitment of status quo bias as the primary driver for users' resistance to change during a new implementation of IS. This study examined the cognitive misperception of loss aversion for the evaluation and opposition of change as it related to perceived value of the expected outcomes. Kim and Kankanhalli (2009) used prospect theory to outline the levels of resistance from covert passive (ignoring or indifference) to overt active behaviors. From an economic perspective of IS security investments, Gordon and Loeb (2002) described a decision maker's level of indifference as a risk-neutral, value-based proposition used in weighing "the probability of a threat occurring, and the vulnerability, defined in the model as the probability that a threat once realized (i.e., an attack) would be successful" (p. 440). Polites and Karahanna (2012) adopted status quo bias as the theoretical lens to study the habits associated with behavior-based inertia, influence perceptions, and intentions related to using a new system as well as resistance. Polites and Karahanna posited that switching costs, in terms of time and effort, impacts the rationalization to change from an incumbent system to a new system. One of their central arguments was that status quo bias could be used to explain the psychological commitment in the decision-making process when evaluating transition and sunk costs -

whether perceived or real (Polites & Karahanna, 2012). Polites and Karahanna explained perceived costs as a reluctance to switch based on skills and learned IS usage habits. Inertia was described as the "unwillingness to abandon the status quo irrespective of present alternatives or alternatives that may potentially become available in the future" (Polites & Karahanna, 2012, p. 24). Therefore, the first quadrant of the CyPRisT represents the decision maker's level of indifference due to an unwillingness to abandon the status quo based on perceived or real switching costs.

Liang and Xue (2009) applied cumulative prospect theory to explain the judgements that influence a decision of threat avoidance by examining the individual's perceived level of threat severity. They referred to the value function for gains and losses, suggesting humans will approach avoidance behaviors through different evaluation processes and the assessment of undesirable end states. Liang and Xue (2009) also described the relationship between perceived susceptibility and perceived threat as a function of perceived severity. *Perceived severity* was defined as the "extent to which an individual perceives that negative consequences [are] caused by the malicious IT" (Liang & Xue, 2009, p. 80). For the context of this research study, perceived severity is interpreted as potential for loss or the *perceived impac*t of risk. The concept represented in the second quadrant of the CyPRisT is a representation of the susceptibility–threat relationship. This also infers a risk-seeking behavior that is in contract to the third quadrant of risk aversion when considering the decision making of the cybersecurity preparedness activities.

Osiyevskyy and Dewald (2015) investigated the judgement and critical strategic decisions of small business managers. They found strong support of biases in small business managers' decisions and their 'need to act'. These strategic actions were intended to mitigate both noncritical threats of anticipated losses in revenue and critical threats "related to enormous losses that can lead to going out of business" (Osiyevskyy & Dewald, 2015, p. 1015). The cognitive framing effects were both impediments and inducement in the decision makers' strategic choices. Small business managers relied on their judgment and heuristics when making strategic decisions. This was demonstrated when the choice to become risk averse is based on the perceived point of reference for cyber risk and loss aversion.

Li, Liu, and Liu (2016) used the status quo bias framework along with other factors related to prospect theory to investigate loss aversion in the failures of knowledge management initiatives. Loss aversion had the highest influence in the relation between resistance behaviors over rational decision making (e.g., cost–benefit analysis of transition costs) and psychological commitment (i.e., social norms). Li et al. (2016) suggested status quo bias may explain why individuals are less likely to initiate changes voluntarily toward an improved system. Lee and Joshi's (2016) comprehensive review of status quo bias perspective in IS literature further identified additional studies examining specific constructs such as cognitive bias and loss aversion. They argued an individual's bias toward status quo is influenced by rational decision making (e.g., cost–benefit analysis), in addition to other psychological factors, but found weakness in the literature focusing mainly on cost–benefit analysis. Lee and Joshi (2016) recommended further examination of cognitive bias limitations that lead to bounded rational decisions based on the prospect theory constructs of loss aversion, resistance to change, framing and anchoring effects. Goel, Williams, and Dincelli (2017) applied framing of potential gains or losses to evaluate human vulnerabilities (i.e., susceptibility to deceive). One of their hypotheses used prospect theory to explain decision making under uncertainty, suggesting people attach subjective values to weigh losses and gains.

Overall, the review of prospect theory and status quo bias literature provides a theoretical foundation for the taxonomy quadrants of the CyPRisT. For example, the notions of threat appraisal, indifference, susceptibility to losses, and aversion, as well as strategic decision making may provide evidence of decision making affected by the heuristics of risk perceptions (Kahneman et al., 1991; Lee & Joshi, 2016; Liang & Xue, 2009; Tversky & Kahneman, 1992). Table 4 provides a summary of relevant prospect theory and status quo bias literature.

Table 4

Summary of Relevant Prospect Theory and Status Quo Bias Literature

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Goel et al., 2017	Survey with experimental conditions	7,225 students at a university in Northeastern U.S.	Cybersecurity breaches via Phishing and Social engineering attacks	Susceptibility to a cyber-attack (phishing) is strongly associated with human tendencies to make hasty judgments of immediate context, people frame outcomes to affect their actions

Table 4

Summary of Relevant Prospect Theory and Status Quo Bias Literature (continued)

Study	**Methodology**	**Sample**	**Instrument or Construct**	**Main Finding or Contribution**
Kim & Kankanhalli, 2009	Field survey	375 managers in organizations around the world that were rolling out a new enterprise system	User resistance to change, rational decision making, psychological commitment	The perceived value of switching costs increased user resistance, the principle of loss aversion from status quo bias theory qualified how the perceived value of change is assessed
Lee & Joshi, 2016	Literature review and synthesis		Status quo bias perspective in IS research	Key constructs used on SQBP as insights into 'bias' in human decision-making. Identified weaknesses in the major focus on rational cost-benefit analysis
Li et al., 2016	Instrument development and survey	982 employees	Loss aversion, transaction costs. social norms, inertia, and resistance	loss aversion, transition costs and social norms had a positive effect on resistance intentions

Table 4

Summary of Relevant Prospect Theory and Status Quo Bias Literature (continued)

Study	Methodology	Sample	Instrument or Construct	Main Finding or Contribution
Liang & Xue, 2009	Theoretical development	Extant literature from psychology, health care, finance, management, marketing, risk analysis, and IS	Cognitive processes of technology threat avoidance and risk tolerance; appraisal and coping appraisal	Risk tolerance is influenced by threat perceptions; perceived threat is an evaluation mechanism used in the decision-making process that appraises the probability of losses (or failure) associated with a threat.
Polites & Karahanna, 2012	Empirical survey	603 students of a university in Southeastern U.S.	Inertia, switching costs, beliefs, social norms, and intention	Results supported the relationships between inhibiting effect of incumbent-system habit and inertia (status quo bias).
Osiyevskyy & Dewald, 2015	Empirical study via survey	288 real estate brokers (generally owner-managers of the business)	A framework of cognitive resilience, prospect theory, behavioral theory of the firm, threat-rigidity	Small business managers rely on judgment and heuristics when making critical strategic decisions, the cognitive factors drive strategic decision making and the choice is risk-averse when they perceived above a pre-set reference point

Summary of What is Known and Unknown in the Research Literature

A review of the literature was performed to provide an overview of the relevant topics of cybersecurity risk management, cybersecurity posture, and the constructs to be explored in this research study: cybersecurity preparedness and small business decision makers' perceived risk of cyber-attack. The literature provides examples of risk management frameworks; however, many publications assume organizations are sufficiently resourced to carry out the activities contained within the framework. Few researchers have examined risk management frameworks in the context of small businesses, considering their limited ability to deal with the risk of cyber-attacks (Berry & Berry, 2018). The growing adoption of the NIST Cybersecurity Framework among small businesses warrants empirical assessment of cybersecurity posture based on how 'well-prepared' the business is to prevent and protect against cyber threats, as well as their ability to maintain business continuity during and after a cyber-attack (Bodeau & Graubart, 2017; Hurley et al., 2014). Moreover, the development of an instrument is needed to measure the level of cybersecurity preparedness activities aiming to minimize cyber risk.

The common cyber-attack vectors that threaten small businesses were reviewed in the literature as well as the leading cybersecurity benchmark reports. Researchers have suggested small business decision makers have difficulty in understanding their cybersecurity needs because their concerns are more focused on the general operations that provide revenue for the business. Small businesses are often inadequate in their ability to manage cybersecurity risk because they have fewer financial resources, have limited knowledge of cybersecurity threats, and/or lack the technical expertise to deal with cyber-attacks (Hess & Cottrell, 2015; Osborn & Simpson, 2015; Paulsen, 2016). The literature provided evidence in the relationship between risk management activities and decision makers’ perceptions of threat (Rohn et al., 2016; Sumner, 2009). Adopting the theoretical lens of prospect theory may help to explain the calculus of weighting cybersecurity preparedness activities (Kahneman & Tversky, 1979, 1984; Tversky & Kahneman, 1992). Furthermore, the related perspective of status quo bias may help explain the passive resistance of indifference, risk-neutral posture, and the risk-susceptible posture of knowingly favoring business profit to cyber risk (Gordon & Loeb, 2002; Kim & Kankanhalli, 2009; Lee & Joshi, 2016; Li et al., 2016; Liang & Xue, 2009; Samuelson & Zeckhauser, 1988). Finally, the lens of prospect theory may also help explain the risk-averse posture to protect business IS assets by establishing strong cybersecurity controls, or exhibiting a high level of cybersecurity situational awareness to achieve an adequate balance between prevention and response strategies (Baskerville et al., 2014; Kim & Kankanhalli, 2009; Osiyevskyy & Dewald, 2015).

Chapter 3

Methodology

Overview of Research Design

This research study followed a multiphase developmental design utilizing both qualitative and quantitative methods (Clark & Ivankova, 2015; Creswell, Plano Clark, Gutmann, & Hanson, 2003; Ellis & Levy, 2009, 2010). The collection of both quantitative and qualitative data is appropriate in the development of a context-specific instrument that provides empirical measurement and observation (Creswell & Clark, 2017). Mixed-methods research with qualitative and quantitative data collection has emerged as a popular approach in many disciplines, including the social sciences, because it allows for a broader perspective of a problem area and addresses the weakness of monomethod modes of inquiry (Creswell, 2014; Johnson & Onwuegbuzie, 2004). According to Clark and Ivankova (2015), a researcher may advance the application of mixed methods by intentionally intersecting one or more design methods. Therefore, the approach integrated the developmental phases to construct and validate a taxonomy for empirically assessing the cybersecurity postures of small businesses with a program intended to improve risk management though the implementation of cybersecurity preparedness activities. This research study was conducted in three phases to address the main research question: what cybersecurity preparedness activities from the NIST Cybersecurity Framework can be used to assess and improve the cybersecurity posture of a small business? Figure 6 presents an overview of the methodological process this research study followed. The phases and methods were sequential (Creswell & Clark, 2017).

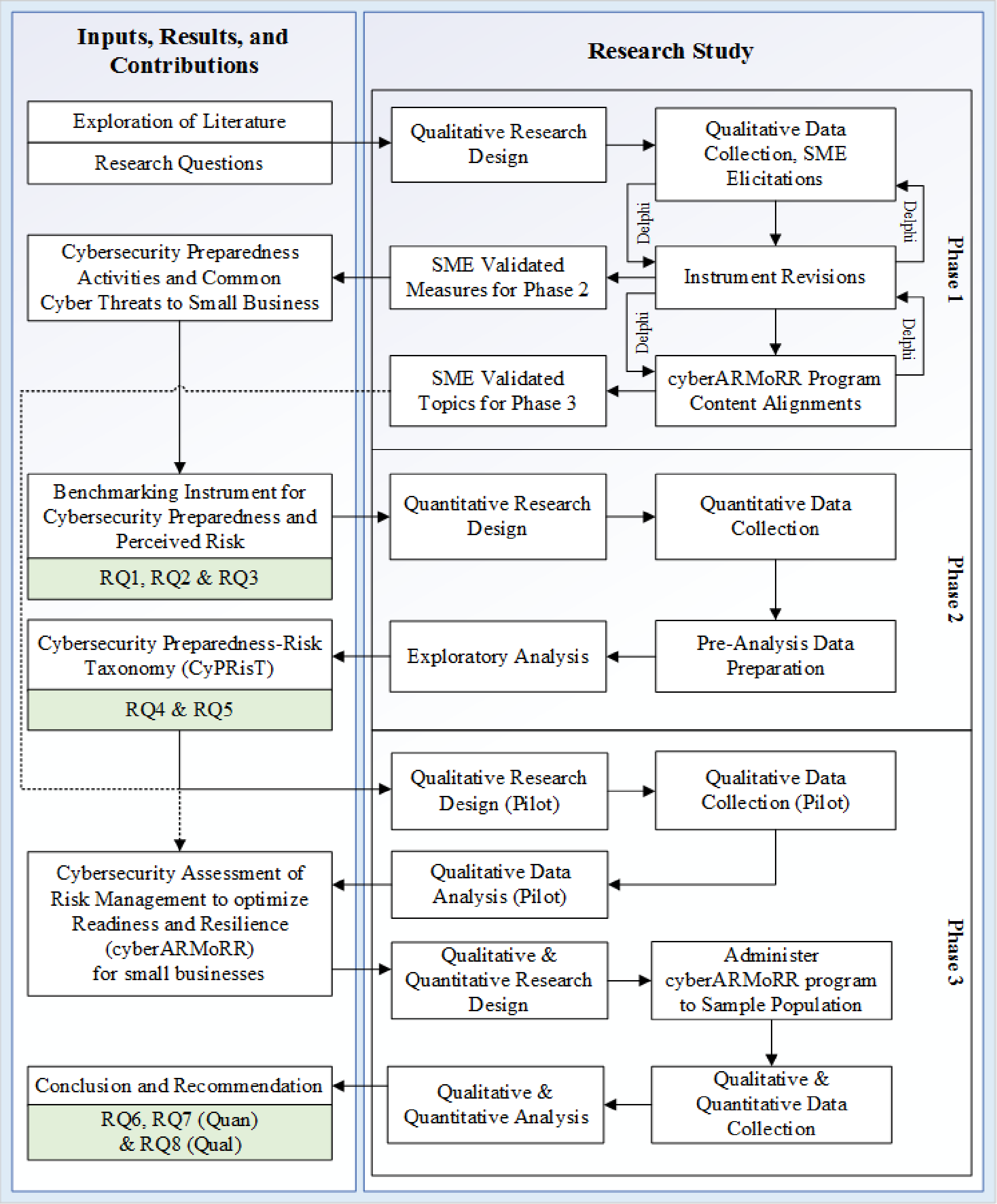

Inputs, Results, and Contributions
Research Study
Exploration of Literature
Research Questions
Qualitative Research Design
Qualitative Data Collection, SME Elicitations
Delphi
Delphi
Cybersecurity Preparedness Activities and Common Cyber Threats to Small Business
SME Validated Measures for Phase 2
Instrument Revisions
Phase 1
Delphi
Delphi
SME Validated Topics for Phase 3
cyberARMoRR Program Content Alignments
Benchmarking Instrument for Cybersecurity Preparedness and Perceived Risk
RQ1, RQ2 & RQ3
Quantitative Research Design
Quantitative Data Collection
Phase 2
Cybersecurity Preparedness-Risk Taxonomy (CyPRisT)
RQ4 & RQ5
Exploratory Analysis
Pre-Analysis Data Preparation
Qualitative Research Design (Pilot)
Qualitative Data Collection (Pilot)
Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) for small businesses
Qualitative Data Analysis (Pilot)
Phase 3
Qualitative & Quantitative Research Design
Administer cyberARMoRR program to Sample Population
Conclusion and Recommendation
RQ6, RQ7 (Quan) & RQ8 (Qual)
Qualitative & Quantitative Analysis
Qualitative & Quantitative Data Collection

Figure 6. An overview of the research design process to develop and validate the CyPRisT for empirical assessment of cybersecurity readiness and resilience, as well as the development of the cyberARMoRR strategy planning program to improve risk management for small businesses

Developmental Research

Developmental research studies are characteristically focused on problem solving with the purpose of bridging theory with practice (Ellis & Levy, 2010). In education, *design and development research* has been defined as “the systematic study of design, development, and evaluation processes with the aim of establishing an empirical basis for the creation of instructional and non-instructional products and tools and new or enhanced models that govern their development” (Richey & Klein, 2014, p. 1). In IS, scholars have used design science research to develop and improve IT artifacts (Gregor & Hevner, 2013; Hevner, 2007; Lee, Thomas, & Baskerville, 2015). Developmental research and design science research are similar in that they both involve the development of an artifact to address a research-worthy problem (Ellis & Levy, 2010).

This study was grounded in developmental research in the creation of the CyPRisT to assess cybersecurity empirically in small businesses risk management as well as the cyberARMoRR program to help small businesses improve their cybersecurity postures. Ellis and Levy (2010) described developmental research as having four distinct characteristics: (a) systematic documentation of the process; (b) use of rigorous, accepted research methods; (c) empirical testing; and (d) communication of the results (p. 110). This research methodology followed a developmental approach in the creation of a new construct and research instrument, a taxonomy for evaluating cybersecurity posture and a cybersecurity program for small businesses. The expected practical contribution of the developmental research is to generate knowledge for examining or solving a problem that is also founded in theory to help explain some of the underlying causes related to the problem (Ellis & Levy, 2010). Accordingly, the foundation of this research study is prospect theory and status quo bias in the development of the CyPRisT (Alharthi et al., 2019; Kahneman et al., 1991; Kahneman & Tversky, 1979; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992).

Lee et al. (2016) defined an *IS artifact* as being formed when the three ‘unpacked’ artifacts (technology, information, and social) are brought together and interact. This research study incorporates the perspectives of Ellis and Levy (2010) as well as Lee et al. (2016) in the development of the cyberARMoRR program for small businesses as contributions in the form of artifacts using mixed methods of data collection. Specifically, this research study addressed the research problem through the development of an IS artifact (CyPRisT) and interacting social artifact (cyberARMoRR program for small businesses) that aim to provide information to “achieve a goal for individuals, groups, organizations, societies or other social units” (Lee et al., 2016, p. 25). The next section details the research method for the development of the IS artifacts as well as empirical assessment of cybersecurity readiness and resilience in small businesses.

Specific Research Methods

The research questions were answered through the three-phased developmental study using mixed methods of data collection (Creswell, 2014). Phase 1 was a structured process using the Delphi method to answer the questions posed in RQ1, RQ2, and RQ3. Phase 2 was a quantitative study to answer the questions posed in RQ4 and RQ5. Phase 3 was a quasi-experimental study using the quantitative method to answer RQ6 and RQ7 (Levy & Ellis, 2011), followed by a qualitative method to answer RQ8 (Saldaña, 2013).

The combination of data collection drew on the strengths of each method (Creswell & Clark, 2017).

Research design – sequential exploratory (Phases 1 and 2)

The research design for Phase 1 began with a structured process using the Delphi method to develop an instrument and taxonomy (Ramim & Lichvar, 2014; Skulmoski et al., 2007). Cybersecurity SMEs were recruited from the field of IS with qualifications and bona fide knowledge of the cybersecurity domain. This phase elicited data from the SMEs using the Delphi method to develop and validate the construct of cybersecurity preparedness as well as the common cyber threats to small businesses to measure decision makers' perceived risk of cyber-attack (Ramim & Lichvar, 2014). The sequential exploratory design, as shown in Figure 7, used the structured process for the SME Delphi cycles to build the constructs of cybersecurity preparedness and decision makers' perceived risk of cyber-attack, and then quantitative methods to validate the instrument empirically. Phase 2 used the validated instrument to conduct a quantitative empirical assessment by collecting data from a sample population of small business decision makers (owners or managers) and documenting the results of the benchmark scores. The measures used in the quantitative data collection for the subgroup of participants were the pretest for Phase 3.

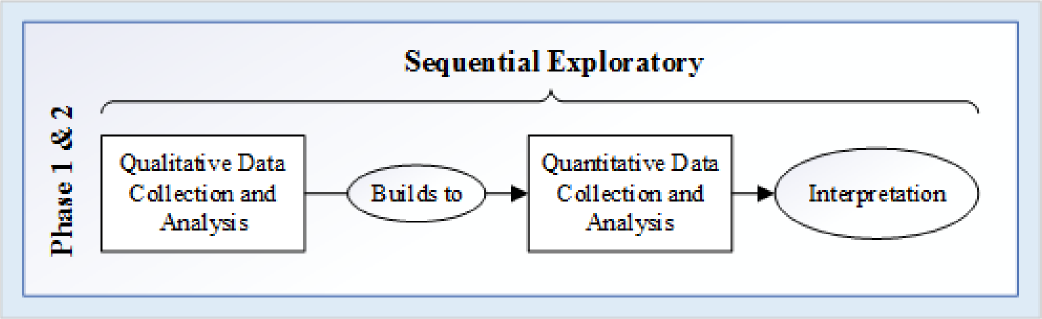

Sequential Exploratory
Phase 1 & 2
Qualitative Data Collection and Analysis
Builds to
Quantitative Data Collection and Analysis
Interpretation

Figure 7. The sequential exploratory design (Phase 1 and Phase 2) adopted from Creswell and Clark (2017).

Research design – quasi-experimental (Phase 3)

The research design of Phase 3 is a quasi-experiment that embeds a qualitative approach with the quantitative instrument to measure the cybersecurity postures of the participants (Levy & Ellis, 2011). As shown in Figure 8, the focus of Phase 3 was an intervention of the cyberARMoRR program for improving the cybersecurity postures and business continuity of the small businesses. Select volunteer participants from the previous phase were invited to participate in a pilot study. Following the pilot, additional small businesses were invited to participate in the cyberARMoRR program for small businesses. After participation in the cyberARMoRR program, the validated instrument was then used as a post measure to assess empirically the differences in small business cybersecurity preparedness and decision makers' perceived risk of cyber-attack. A qualitative inquiry using open-ended questions was used to evaluate the differences in cybersecurity postures as well as the small business owners' reasons for change (or no change). Finally, the empirical findings as well as the patterns from the comparative measures were used to interpret and summarize the results.

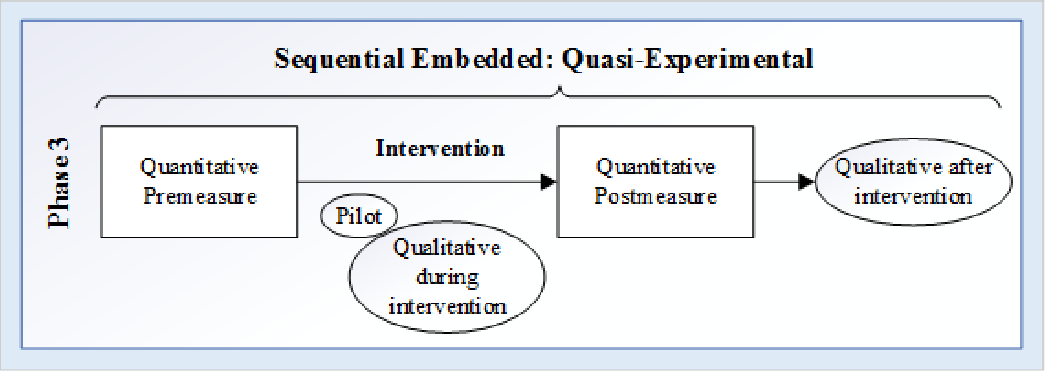

Sequential Embedded: Quasi-Experimental
Phase 3
Quantitative Premeasure
Intervention
Pilot
Qualitative during intervention
Quantitative Postmeasure
Qualitative after intervention

Figure 8. The sequential embedded: Quasi-experimental Design (Phase 3) adopted from Creswell and Clark (2017).

Figure 9 shows the overview of the developmental research design that combines the qualitative and quantitative data collection (Figures 7 and 8 combined). Represented by the dashed line, the SME validated instrument is the point of interface between the sequential exploratory design and the quasi-experimental design because it was used as a pretest and posttest measure of the small businesses' cybersecurity postures. Creswell and Clark (2017) use upper- and lower-case letters to indicate which method is prioritized in the interpretation of the results. For example, the "QUAN(qual)" will place higher priority for analyzing differences in CyPRisT positions (RQ6, RQ7) than the qualitative inquiry (RQ8). The priority relates to the emphasis placed on each method of the study (Creswell & Clark, 2017). In this model of the embedded quasi-experiment methodology using mixed methods for data collection, the qualitative method is subservient data that used in service to the guiding approach (Creswell, 2014). Accordingly, a mixed-methods research design was selected because qualitative or quantitative methods alone would not answer all research questions. The sequential exploratory design was applied in the first and second phases to integrate the sequential embedded quasi-experiment for the third phase.

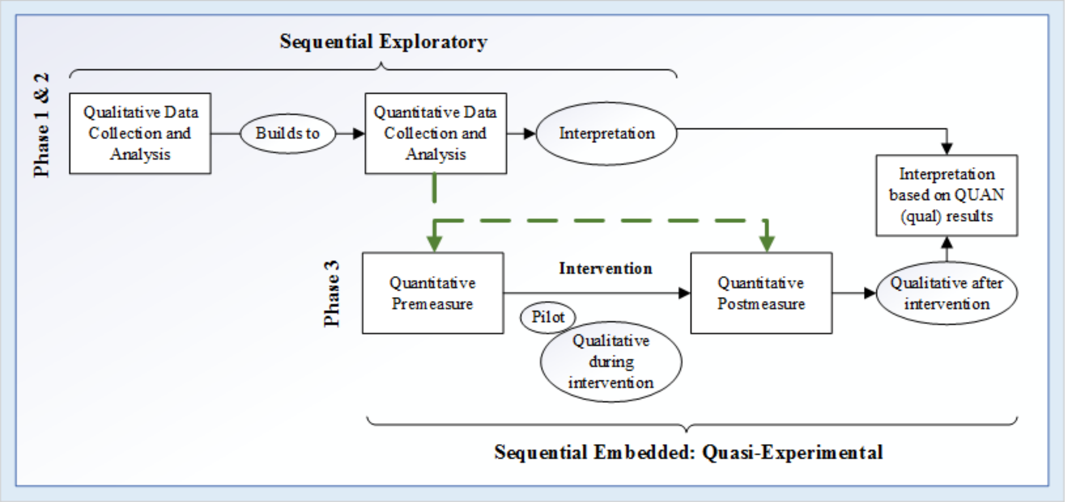

Sequential Exploratory
Phase 1 & 2
Qualitative Data Collection and Analysis
Builds to
Quantitative Data Collection and Analysis
Interpretation
Interpretation based on QUAN (qual) results
Phase 3
Quantitative Premeasure
Intervention
Pilot
Qualitative during intervention
Quantitative Postmeasure
Qualitative after intervention
Sequential Embedded: Quasi-Experimental

Figure 9. Multiphase developmental research design integrating a sequential exploratory design with a sequential embedded intervention (quasi-experimental) design adopted from Creswell and Clark (2017).

Participant Instrument Development

A survey instrument was developed during Phase 1 consisting of two constructs: cybersecurity preparedness and decision makers' perceived risk of cyber-attack. The initial list of the cybersecurity preparedness activities was derived from the actionable objectives recommended in the NIST Cybersecurity Framework v1.1 with informative references to COBIT and the ISO/IEC 27000 standards (NIST, 2018). These activities also correspond to the fundamentals of information security for small businesses and recommendations provided in extent literature (Berry & Berry, 2018; Paulsen & Toth, 2016; Rohn et al., 2016). The next two sections discuss the specific approach for developing the survey instrument and measures that were used to assess each of the constructs. The two sections are organized by quantitative and qualitative measures. The proceeding section discusses the validity and reliability of the constructs as well as the survey instrument.

Quantitative survey instrument and measure

The phases of the sequential exploratory and quasi-experiment design in this research study were predominantly quantitative (Creswell et al., 2003). The construct of cybersecurity preparedness was developed through a literature review of theoretical and empirical studies and then validated using SMEs. The construct consisted of an inventory-based measure of the prioritized cybersecurity activities, outcomes, and references for the small businesses to manage cybersecurity risk, as guided by the NIST Cybersecurity Framework (NIST, 2018; Paulsen & Toth, 2016). Data were collected from a target sample of 15 SMEs, conducting multiple Delphi rounds during Phase 1 (Okoli & Pawlowski, 2004; Skinner et al., 2015). Thus, to minimize the probability of low response rates, 35 SMEs were invited to participate in the Delphi rounds. SMEs who possess the required credentials and experience were contacted through email or social media private messaging. Using the Delphi method, the SMEs reviewed and provided feedback on the set of cybersecurity preparedness activities from the five functions of the NIST Cybersecurity Framework (NIST, 2018; Ramim & Lichvar, 2014). After consensus from the SMEs on the approved set of cybersecurity preparedness activities for small businesses, the SMEs were then asked to provide an importance weight using a 7-point Likert scale that was assessed for the hierarchal aggregation of the measure.

The construct of perceived risk was adapted from the work of Sumner (2009) and Whitman (2003) then contextually updated with the common cyber-attacks recognized in the cybersecurity benchmark reports known to present significant threats small businesses. The construct measured the small business decision makers’ perceived risk for each of the cyber-attacks using a 7-point Likert scale of perceived impact and perceived likelihood (i.e., probability of an occurrence). This research study developed the instrument using feedback from the SMEs on the construct items of cybersecurity preparedness activities and the types of cyber-attacks. The survey instrument be validated by the same SMEs using the Delphi method (Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014). An iterative process of the Delphi method through online surveys was used to validate both measures of the cybersecurity preparedness and the decision makers' perceived risk of cyber-attack (Skulmoski et al., 2007). The SME data were also used to validate the topics to align content of the cyberARMoRR program for small businesses based on the final approved measures of cybersecurity preparedness and decision makers' perceived risk of cyber-attack.

Phase 2 utilized the previously validated and weighted constructs of cybersecurity preparedness and decision makers' perceived risk of cyber-attack in a survey instrument. An anonymous survey was administered to small business decision makers across the U.S. The small business decision makers were invited through email and social media via business networking groups. A link to the recruitment letter was also shared to small business owner groups on social networking platforms such as LinkedIn and Facebook. To extend recruiting efforts, additional participants were targeted through email to increase participation rate small business contact information. The email addresses of small businesses were retrieved from public records data sources such as the Chamber of Commerce, U.S. Small Business Administration, and state business filling directories, as well as advertising publications such as Yellow Pages (online).

The data collected from this study was quantitatively analyzed and applied to the CyPRisT. The small business participants were invited through email and social media via business networking groups. The measures used in quantitative data collection during Phase 2 became the premeasure for the willing participants in Phase 3. Following the quantitative data collection, a purposeful selection of small business decision makers were invited to participate in a review of the pilot program to test the semi-structured interview protocol (Ivankova, Creswell, & Stick, 2006). This process ensured adequate preparation of the key questions and safeguards regarding the confidentiality of the small businesses when conducting interviews with the sample (Myers & Newman, 2007). Feedback from the review was used to ensure any concerns have been addressed and the program content aligns with the topics of the SME-approved measure. The Phase 3 posttest survey was made available for the participants to measure changes in security posture. A posttest survey reminder were sent to the consenting participants' email addresses 30 days after launching the CyberARMoRR program. The same SME-approved quantitative questions were used for the posttest measure. The data collected was used to analyze the differences between the pretest and posttest quantitative measures.

Qualitative Survey Instrument and Measure

The semi-structured interview "is a qualitative data collection strategy in which the researcher asks informants a series of predetermined but open-ended questions" (Given, 2008, p. 810). The following questions were used in the interviews with small business decision makers during the Phase 3 pilot of this research study. These questions are open-ended to form the basis of the interviews with voluntary participants.

1. What cybersecurity preparedness activities have helped improve the cybersecurity posture of your small business as a result of the cyberARMoRR program?
2. For each of the NIST functions, what cybersecurity preparedness activities are challenging for your small business?
3. Are any of the resources in the program difficult to follow?
4. What would you change about the cyberARMoRR program?

The posttest survey instrument also included a qualitative question after each of the five sections of the NIST Cybersecurity Framework functions: Identify, Protect, Detect, Respond, and Recover. The question for each section is: “Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. (“N/A” if none)”. The posttest, open-ended, qualitative questions in the survey instrument and voluntary semi-structured interviews with the participants were combined to address RQ8 (Creswell, 2014; Myers & Newman, 2007). The qualitative evaluation of the SME weighted activities were assessed using thematic analysis techniques for the combined responses (Saldaña, 2013).

Validity and Reliability

According to Straub (1989), literature reviews and panels of experts can provide content validity as well as construct validity for an instrument. Straub (1989) stated “instrument validation should precede other core empirical validities” (p. 150). For this research study, internal validity was established through the use of the experts.

Instrument validation and reliability may be established by sequencing a qualitative technique of exploratory research, followed by a quantitative empirical technique and then conceptual refinements (Straub, 1989). Therefore, to ensure the overall validity of the instrument, Phase 1 of this research study solicited the help of SMEs using the Delphi method (Ramim & Lichvar, 2014). A qualified expert had academic or professional experience, and at least one professional certification in the fields of information security. Example certifications include: Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM), Certified IS Security Professional (CISSP), Security+, and Global Information Assurance Certification (GIAC).

The Delphi method is a widely accepted and flexible method to advance scientific knowledge together with the IS body of knowledge (Okoli & Pawlowski, 2004; Skulmoski et al., 2007). The Delphi method "is an iterative process to collect and distill the anonymous judgments of experts using a series of data collection and analysis techniques interspersed with feedback" (Skulmoski et al., 2007, p. 1). Thus, the Delphi method contributed to construct validity (Okoli & Pawlowski, 2004; Ramim & Lichvar, 2014).

The reliability of the instrument refers to the consistency, accuracy, and stability across the unit of measure (Straub, 1989). Straub (1989) also stated "internal validity raises the question of whether the observed effects could have been caused by or correlated with a set of unhypothesized and/or unmeasured variables" (p. 151). An iterative process was used to evaluate the measurement properties of the instrumentation. This iterative process led to increased instrument reliability and validity (Onwuegbuzie, Bustamante, & Nelson, 2010).

External validity refers to the extent that a research study is generalizable across types of persons, settings, or times (Cook & Campbell, 1979). In Phase 1 of this research study, data were analyzed using Cronbach’s alpha to assess the construct reliability of the measured constructs (Cronbach, 1951). The results of the Cronbach’s analysis should indicate that all constructs provided very high reliability (greater than .70). The Phase 2 analysis verified that the data of this study had a good representation of small businesses populations. The demographic variables (industry, number of employees, years in operation, annual revenue, and IT budget) was compared with findings in the extant literature on small business cybersecurity as well as recent cybersecurity benchmark reports. Finally, both qualitative and quantitative measures were used with a pilot to ensure appropriateness of the assessment and semi-structured interviews (Onwuegbuzie et al., 2010). The questions for semi-structured interviews for RQ8 were vetted in the pilot to minimize any irregularities or problems with the collections of qualitative data. The pilot was administered to ensure the validity of the semi-structured interview questions before undertaking research on the remaining participants (Gibson & Brown, 2009).

Sample

The population and sample size for this research study varies by phase and research design method. The sequential exploratory design, Phase 1 and Phase 2, consists of the Delphi method using a panel of cybersecurity experts for validating constructs as well as instrument development, then a quantitative survey. Skulmoski et al. (2007) demonstrated that a Delphi population in research often varies greatly in both size and the number of rounds. For example, studies have ranged from 4–171 experts with 1–6 rounds of interaction (Skulmoski et al., 2007). However, Okoli and Pawlowski (2004) recommended 10–18 experts on a Delphi panel. Skinner et al. (2015) also recommended that panels range from 10–30 SMEs. Therefore, this research study targeted participation from 15 cybersecurity SMEs with at least two rounds of interaction. A qualified SME having academic or professional experience and at least one professional certification in the field of cybersecurity. The SMEs were over the age of 18 to participate in this research study.

Phase 2 of this research study approached more than 200 small businesses in the U.S. to ensure an appropriate sample size (Mertler & Reinhardt, 2017). This research study included any small business owners or managers as participants. A *small business* is a privately owned and operated entity that typically has a very small number of employees. The recruitment survey aimed to collect data from very small businesses, such as those with 10–50 employees. However, small businesses not meeting this size constraint were not excluded from voluntary participation or receiving the benefit of the cyberARMoRR program. A small business owner is the individual who owns a small business and is responsible for all the risks and rewards of his or her business venture. A small business manager is an individual who manages a small business on behalf of an owner. The participants’ age was set to 18 or older.

The participants were given the opportunity to opt-in to the next phase. If consent was provided, the email was used to invite to participate in the quasi-experiment (single group, Phase 2 survey as the pretest and Phase 3 survey as the posttest). The Phase 3 quasi-experimental pretest-posttest single group design required data collection from the same instrument (Salkind, 2010). Therefore, the comparative analysis was used in the development of the instrument for this research study during Phase 1 for the sample of small businesses participating in Phase 2 (Salkind, 2010). However, the test group was limited to the number of small business decision makers willing to continue participation in Phase 3 of this research study. Creswell and Clark (2017) stated it is acceptable for follow-up qualitative data collection to have a smaller sample than the quantitative data collection. Thus, it was anticipated that Phase 3 would include a small group size of approximately 40 small businesses.

Data Collection

Data were collected using a sequential series of three phases. In Phase 1, the SMEs were recruited via email of personal and professional contacts in cybersecurity/information security field (see Appendix B). Data collection consisted of a qualitative survey instrument to identify the cybersecurity preparedness activities, weights by functions of the NIST Cybersecurity Framework, and descriptions of the common cyber-attacks on small businesses (see Appendix C). The second Delphi round consisted of further validation of the cybersecurity preparedness activities, weighting each by importance using a 7-point Likert scale (see Appendix D). A qualitative assessment of the selected topics using highest-rated cybersecurity activities was used in the assessment of the CyPRisT as well as the development of the cyberARMoRR program.

In Phase 2, small business owners and managers were recruited through public listings of business emails, small business networking groups, and social media groups (see Appendix F). The participants were presented with the option to provide their informed consent to participate in the quasi-experiment or complete the initial survey anonymously. The online consent form (see Appendix G) provided the necessary information to participate in both Phase 2 and Phase 3 surveys without linking the participant to their responses. The SME-approved survey instrument was used to collect data from the participants in Phase 2 as a pretest measure (see Appendix H). The SME-approved survey instrument was used to collect data from the participants in Phase 3 as a posttest measure with the addition of a qualitative question on each of the functions (see Appendix K). To protect privacy, the participant survey responses were anonymous. No personal or private information was collected. The aggregated data were connected using a system generated ID that was randomly assigned to the participant upon submitting the informed consent form.

Data Analysis

Levy (2006) described pre-analysis data screening as "the process of detecting irregularities or problems with the collected data" (p. 150). This process is required before the data analysis to ensure that results and conclusions to be valid (Mertler & Reinhardt, 2017). First, to ensure construct validity, SMEs were used to conduct a prescreening of the instrument for RQ1, RQ2, and RQ3. The data collected from the SMEs were used in the development of the instrument. For RQ1, the NIST Cybersecurity Framework was used to determine which cybersecurity preparedness activities, organized by the five functions, were used to measure the level of cybersecurity preparedness for a small business. The SME-approved set of cybersecurity activities were identified through at least two Delphi rounds. The SMEs' recommended revisions in Delphi 1 were presented for approval in Delphi 2. For RQ2, in Delphi 1 the SMEs provided weights to the five functions of the NIST Cybersecurity Framework. In Delphi 2, the SMEs provided data indicating the importance of each of the cybersecurity preparedness activities. These data were analyzed and used in the development of the aggregate benchmark score for levels of preparedness. For RQ3, also using the Delphi method, a set of cyber-attack vectors were presented for the SMEs to provide feedback. These definitions were contextually updated to address the most common cyber threats to small businesses. The SME feedback from the Delphi 1 survey example (see Appendix C) was analyzed and presented in Delphi 2 (see Appendix D) to achieve consensus on the set of cybersecurity preparedness activities and common cyber-attacks that were used in the survey instrument (see Appendix E, Appendix H – pretest, and Appendix K - posttest).

In Phase 2, the survey instrument was used to collect data from 216 small business participants. For RQ4, the benchmark scores were applied to the CyPRisT to assess the cybersecurity posture level positions of the 216 small businesses. Following the process recommended by Mertler and Reinhard (2017), RQ5 and RQ6 pre-analysis data screening was performed to verify that data collected from the survey do not contain any missing or out of range values. Cronbach's alpha (Cronbach, 1951) was used to evaluate the reliability of each of the constructs. For RQ5, data were analyzed using analysis of variance (ANOVA) procedures. For RQ6, the data were analyzed using paired sample t-test procedures.

In Phase 3, semi-structured interview questions during the pilot launch of the cyberARMoRR program was assessed to minimize any irregularities or problems with the program content. The pilot was administered to ensure the validity program topics before undertaking research with the remaining participants (Gibson & Brown, 2009). For RQ7, differences between groups were quantitatively assessed using descriptive statistics while differences in the CyPRisT positions were qualitatively assessed. For RQ8, data were collected from the qualitative open-ended questions for each of the five functions on the posttest survey as well as the field notes from the semi-structured interviews. The qualitative data were analyzed following a two-cycle process of manually coding categories and emergent themes from the voluntary participant responses (Saldaña, 2013). Thus, the survey frequency counts using magnitude coding and open-ended questions as well as semi-structured response data were evaluated using a descriptive coding process (a.k.a. topic coding) (Saldaña, 2013). Pattern coding helped identify the emergent themes for the most challenging cybersecurity preparedness activities. Content analysis of thematic categories, such as patterns of participants' reported problems encountered within each of the functions, were analyzed to provide meaningful explanation (see Appendix L).

Resources

The Nova Southeastern University online library of databases were used to gather research articles for the literature review. As human subjects were involved, IRB approval was received prior to conducting the research (see Appendix A). This research study required access to the Internet, the use of email, and the use of a web browser to engage the SMEs in the field of cybersecurity for instrument development following the Delphi method. Small business owners and managers were solicited to complete an

Internet-based survey that was developed using Google Forms. A list of small business email contacts was retrieved from public records data sources such as the U.S. Small Business Administration and state business filing directories. The survey link and participation request letter were shared to small business social groups on social networking platforms such as LinkedIn and Facebook. Survey respondents voluntarily provided their contact information to receive invitation to participate in the subsequent phases of this research study. Participants were assured of their anonymity and no personal data were collected. Additionally, business owners and managers were assured that their responses related to business data were used in aggregate form only for the purposes of this research. IBM Statistical Package for the Social Sciences (SSPS) and Microsoft Excel was used to analyze the quantitative data. Various online resources were also referenced for administering the cyberARMoRR program to small business decision makers, such as public domain online videos, cybersecurity self-assessment tools, and electronic and printable materials with references to government guides.

Summary

This research followed a multiphase developmental design utilizing both qualitative and quantitative methods to construct and validate the CyPRisT for empirically assessing the cybersecurity postures of small businesses. Additionally, the cyberARMoRR program was developed with the intent to improve risk management by providing educational resources on the implementation of cybersecurity preparedness activities. The development of these artifacts was the driver for the new construct, cybersecurity preparedness, which was validated by SMEs and included in the survey instrument for empirical assessment. This chapter also discussed the methods to address the specific research goals and research questions outlined in Chapter 1. Phase 1 followed a qualitative research design and data collection by eliciting SME feedback using the Delphi method toward the development of the instrument for subsequent phases. Phase 2 followed a quantitative research design utilizing a survey instrument and exploratory analysis techniques. The survey instrument served as a pretest measure in a quasi-experiment. Phase 3 provided participants access to the cyberARMoRR consisting of the topics approved by the SMEs in the development of the instrument. Afterward, the instrument approved by the SMEs was again used as a posttest measure with the addition of a qualitative component. As a result, the multiphase approach integrated the developmental phases to construct and validate the taxonomy for empirically assessing the cybersecurity postures of small businesses with a program intended to improve risk management through the implementation of cybersecurity preparedness activities.

Chapter 4

Results

Overview

This chapter presents the results of the data collection and data analysis performed by this research study. The main goal was to develop and validate a small business Cybersecurity Preparedness-Risk Taxonomy (CyPRisT) to assess empirically the cybersecurity posture of small businesses as well as administer a program that can assist in improving small business decision maker's cyber risk management. In Phase 1, the results are presented for the two Delphi surveys using a panel of cybersecurity experts. The SMEs validated a set of cybersecurity preparedness activities based on the five functions of the NIST Cybersecurity Framework, identified weights for the cybersecurity preparedness activities, and approved a set of cyber-attacks that are common threats to small businesses. The results show how small businesses are positioned on the CyPRisT using their Cybersecurity Preparedness Scores (CPSs) and the Decision Maker's Perceived Risk of Cyber-attack (DMPRCA) as well as a statistical analysis of the data by business and participant demographics. The differences in cybersecurity posture before and after participation in the cyberARMoRR program for small businesses, changes in cybersecurity preparedness activities, and the challenges for the small businesses for improving their cybersecurity posture. This chapter concludes with a summary of the results of this study for all phases.

Phase 1 – Subject Matter Expert (SME) Panel

To answer RQ1, RQ2, and RQ3, a survey instrument was developed during Phase 1 then sent to a panel of qualified cybersecurity SMEs to validate a set of cybersecurity preparedness activities for small business. The initial set of cybersecurity preparedness activities were derived from the five functions of the NIST Cybersecurity Framework (NIST, 2018; Paulsen & Toth, 2016). Direct email invitations were sent to 35 qualified cybersecurity SMEs. A total of 22 cybersecurity SMEs agreed to participate and submitted their feedback during multiple rounds of surveys. Therefore, the response rate of the expert panel was about 62.8%. The cybersecurity SMEs assigned weights to each of the cybersecurity preparedness activities. Furthermore, the SMEs approved a set of common cyber threats to small businesses for measuring perceived risk (perceived likelihood x perceived impact).

Phase 1 – SME Panel Characteristics

The panel of cybersecurity SMEs was comprised of ranking members of cybersecurity organizations such as the NIST, InfraGard, and Information Systems Audit and Control Association (ISACA), as well as highly esteemed professors and scholars in the field of cybersecurity and information security. The panel experts were also targeted for having relevant experience advising various small businesses on cybersecurity protocols and practices. Table 5 summarizes the descriptive statistics for the SMEs.

Table 5

Descriptive Statistics of the SMEs (N=22)

Demographic Item	**N**	**%**
Gender:		
Female	4	18.18%
Male	18	81.82%
Age:		
20-29 years	2	9.09%
30-39 years	3	13.64%
40-49 years	7	31.82%
50-59 years	8	36.36%
60 or more	2	9.09%
Highest Academic degree:		
Bachelor’s degree	1	4.55%
Graduate degree	21	95.45%
Professional Role:		
Academia	7	31.82%
Industry	9	40.91%
Other (Both)	6	27.27%
Experience in Cybersecurity/Information Security:		
1-5 years	2	9.09%
6-10 years	4	18.18%
11-15 years	3	13.64%
16-20 years	6	27.27%
21 years or more	7	31.82%
Cybersecurity Certifications:		
0	2	9.09%
1	9	40.91%
2	5	22.73%
3	4	18.18%
4	1	4.55%
5 or more	1	4.55%

For gender, majority of the SMEs were male (18; 81.82%). For age, majority of the SMEs were aged 40 to 49 years old (7; 31.82%) and 50 to 59 years old (8; 36.36%).

For higher academic degree, all except one of the SMEs have a graduate degree (21; 95.45%). For professional role, 9 (40.91%) SMEs were in a senior role in the cybersecurity/information security industry, 7 (31.82%) SMEs were in academia, and 6 (27.27%) SMEs were in both academia and professional. In terms of experience in the field of cybersecurity/information security, more than half of the SMEs have 16 to 20 years (6; 27.27%) and 21 years or more (7; 31.82%) of experience. For cybersecurity certifications, the majority of SMEs one or more (20; 90.91%) cybersecurity certification. An exception was made for 2 SMEs on the cybersecurity certification qualification due to their esteemed reputation in the field of cybersecurity/information security (proven by publications and senior level experience).

Phase 1 – Data Collection (Delphi Method)

The data collection for Phase 1 utilized the Delphi Method (Ramim & Lichvar, 2014; Skinner et al., 2015). Data collection occurred between August 2019 and September 2019 using two survey instruments to receive feedback from the cybersecurity SMEs. A Google Form was used to present the survey instrument to the SMEs. The first round of Delphi method consisted of questions organized by each function of the NIST Cybersecurity Framework (see Appendix C). The SMEs were asked to Keep, Adjust, or Remove questions for each of the five functions: Identify, Protect, Detect, Respond, and Recover. Open text fields were provided for recommended adjustments and additional questions to be included in the set of cybersecurity preparedness activities for small businesses. Descriptions were also provided for 10 types of common cyber-attacks on small businesses that was used to measure the decision maker's perceived risk (Ponemon

Institute, 2018). Overall, the SMEs' feedback was positive and, based on the recommendations, revisions were made to the survey instrument to conduct the next round of survey questions.

The second round of survey questions consisted of a revised set of questions (see Appendix D). The SMEs were asked to provide a level of importance for each question using a 7-point Likert scale ranging from (1) “Not at all important” to (7) “Extremely important” to calculate weights of the cybersecurity preparedness activities. Open text fields were provided for any final recommendations to adjust the questions. The revised set of common cyber-attack definitions were provided to the cybersecurity SMEs in the same survey. Again, open text fields were offered for any final recommendations to adjust the definitions. The instrument was finalized with expert consensus of set of cybersecurity preparedness activities based on the high level of importance as well as minimal feedback to open questions (see Appendix E).

Phase 1 – Pre-Analysis Data Screening

The pre-analysis data screening did not identify any SME responses that needed to be removed. Also, there were no incomplete data sets submitted because all survey items were set to ‘required’ when developing the instrument. Instrument validation was addressed by having the SMEs screen the survey for representative questions (content validity) before other empirical validities (Straub, 1989). The expert panel using the Delphi method also assisted with the stability of the individual measures (construct validity) through their successive rounds of confirmatory judgment (Okoli & Pawlowski, 2004).

Phase 1 – Data Analysis

For RQ1, the SMEs approved a set of cybersecurity preparedness activities derived from the five functions of the NIST Cybersecurity Framework (2018) and the small business information security fundamentals (Paulsen & Toth, 2016). There were 70 cybersecurity preparedness activities that were approved and translated into question items for the participant surveys. The final approved set consisted of 20 question items for the function Identify (ID), 20 question items for the function Protect (PR), 10 question items for the function Detect (DE), 10 question items for the function Respond (RS), and 10 question items for the function Recovery (RC).

For RQ2, the SMEs identified weights for each of the cybersecurity preparedness activities to enable an aggregation score to benchmark the level of preparedness for a small business. The weights were used to generate an overall Cybersecurity Preparedness Scores (CPSs). In order to conduct an appropriate comparison, due to differences in quantity of the question items for the five functions, the weighted scores were normalized using an aggregate sum of 0 to 5, as depicted in the formula below.

$$\begin{aligned} CPSs\ (0\ to\ 5) = {} & \left(\frac{1}{140}\right) \cdot \left[\sum_{j=1}^{20} \left(W_{ID_j} \cdot ID_j\right)\right] + \left(\frac{1}{140}\right) \cdot \left[\sum_{j=1}^{20} \left(W_{PR_j} \cdot PR_j\right)\right] \\ & + \left(\frac{1}{70}\right) \cdot \left[\sum_{j=1}^{10} \left(W_{DE_j} \cdot DE_j\right)\right] + \left(\frac{1}{70}\right) \cdot \left[\sum_{j=1}^{10} \left(W_{RS_j} \cdot RS_j\right)\right] \\ & + \left(\frac{1}{70}\right) \cdot \left[\sum_{j=1}^{10} \left(W_{RC_j} \cdot RC_j\right)\right] \end{aligned}$$

Whereas, Ws are the SMEs' mean level of importance (weights). The Ws are multiplied by the participant response for each cybersecurity preparedness activity (0=No; 1=Yes) to sum each function. For example, the Identify (ID) function was calculated by using the Likert value (1-7) for each item multiplied by the corresponding participant response (0-1), the next item were calculated to sum the 20 items within the ID function (max 7x20=140). The five functions were normalized to total one (1) each maximum value (representing 100%). For example, the interval for ID is 0-140 range from the lowest possible score of 0 (no responses to all cybersecurity preparedness activities) to the highest possible score of one (100%) within the function (yes responses to all cybersecurity preparedness activities multiple by the normalization factor). Similar calculations and normalizations where done for all five functions and then added all five functions to the resulting CPSs scores from 0 to 5.

Descriptive statistics were used to address RQ2 by summarizing the scores of the assigned importance weights of each of the cybersecurity preparedness activities. Central tendency measures of mean and standard deviation were also used to summarize the data since the importance weights are continuous measured. Table 6 summarizes the descriptive statistics for the importance weights of the cybersecurity preparedness activities in each of the five functions. The results show the mean score of the assigned importance weights for the five functions of the NIST Cybersecurity Framework of identify (M= 6.25; SD = 0.26), protect (M= 6.45; SD = 0.35), detect (M= 6.16; SD = 0.31), respond (M= 6.34; SD = 0.28), and recover (M= 6.08; SD = 0.48) were between the range of the scales for (6) very important and (7) extremely important. The minimum and maximum range from high to extremely high for the importance rating of the cybersecurity preparedness activities within all five functions of the NIST Cybersecurity Framework. Accordingly, the mean values indicate that all five functions have very high importance weight.

Table 6

Descriptive Statistics of Importance Weights for the Cybersecurity Preparedness Activities in the Five Functions of NIST Cybersecurity Framework

	N of Items	**Min**	**Max**	**Mean**	**Std. Deviation**
Wid	20	5.64	6.77	6.25	0.26
Wpr	20	5.82	6.82	6.45	0.35
Wde	10	5.68	6.55	6.16	0.31
Wrs	10	5.95	6.68	6.34	0.28
Wrc	10	5.27	6.77	6.08	0.48

For RQ3, the SMEs approved a set of cyber-attack vectors which address the most common cyber threats to a small business. The Ponemen Institute (2016, 2017, 2018) has been consistently reporting 10 types of common cyber-attack on small businesses. The SMEs adopted these for the measure of perceived risk that was calculated by multiplying perceived likelihood (PL) by perceived impact (PI) using a 7-point Likert scale from extremely low to extremely high. Moreover, the SMEs provided simple definitions to each type of cyber-attack for the participants as reference within the instrument. The overall score for Decision Makers' Perceived Risk of Cyber-Attack (DMPRCA) is depicted in the formula below.

$$DMPRCA\ (in\ \%) = \left(\frac{1}{490}\right) \cdot \left[\sum_{i=1}^{10} (PL_i \cdot PI_i)\right]$$

Whereas PL and PI both range from 1 to 7 each (Likert scale), resulting in DMPRCA range of 0%-100%. The DMPRCA was calculated for each item using the Likert value (PL x PI) having a max score of 49 for the item (7x7). Thereby, 490 is the total max possible score for the 10 categories of cyber-attacks representing 100%.

Phase 2 – Sequential Exploratory

A sequential exploratory study was conducted to validate the survey from Phase 1 as well answer RQ4 and RQ5. Data were collected from a sample population of small business decision makers (owners or managers) to document the results of the benchmark scores. The CPSs and DMPRCA were used to further validate the instrument. The scores were then used to assess the position on the CyPRisT then identify differences by (a) industry, (b) number of employees, (c) years in operation, (d) annual revenue, and (e) IT budget, as well as personal demographics indicators of (f) role, (g) age, (h) gender, and (i) education. The measures of CPSs and DMPRCA used in the quantitative data collection became the pretest for participants that were willing to volunteer continuing with Phase 3 of this research study.

Phase 2 – Data Collection

Data collection occurred between September 2019 and October 2019. The participants of the survey were owners and managers from across the U.S. Google Forms was used to present the survey instrument to the participants (see Appendix H). An option was offered to participate anonymously or to complete an informed consent form (see Appendix G). Those completing the informed consent form were advised that they would receive and invitation to participate in the cyberARMoRR program for the next phase of this study approximately 1 month after submitting the initial survey. A total of 270 responses were received.

Phase 2 – Pre-Analysis Data Screening

Pre-analysis data screening is a process of detecting irregularities or problems with data collection to ensure data to be analyze is accurate and reliable (Levy, 2006). The invitations to small businesses were not limited to business size or any other demographic. This ensured that any small business owner or manager could participate in the survey and gain access to the CyberARMoRR program resources. However, because the scope of the research was delimited, the survey instrument was designed to filter those small businesses having between 10 and 49 full time employees. Accordingly, 54 cases were removed for being out of scope - having less than 10 full-time employees, 50-99 full-time employees, and 100 or more full-time employees. Prior to conducting the main analyses to address RQ4 and RQ5, the presence of multivariate outliers was first investigated using IBM's SPSS Statistics software tools. Outliers can be detected by Mahalanobis Distance procedure (Mertler & Reinhart, 2017). The data were tested for normality using the Kolmogorov-Smirnov (KS) test. The KS test showed that the empirical distribution of the Mahalanobis distance corresponds to the exact distribution since the result was insignificant (KS(216) = 0.04, p = 0.20) based on a significance of 0.05. Thus, the result indicated that no multivariate outliers were detected and the final sample size for analysis in this study was 216.

Phase 2 – Participant Demographics Characteristics

The 216 small business participants varied by business demographics and personal demographics; industry (BD1), size – number of employees (BD2), years in operation (BD3), annual revenue (BD4), IT budget (BD5), and role (PD1), age (PD2), gender (PD3), and education (PD4). The sample of small business participants were fairly distributed across the demographics. The highest for the industry demographic were other (13%), professional services (11%) and retail (10%). The lowest for the industry demographic were transportation (2%); and warehousing, logistics, and distribution (2%). The highest for the size demographic were 10 to 19 full time employees (34%) and 20 to 29 full time employees (28%). The lowest for the size demographic were 30 to 39 full time employees (17%), and 40 to 49 full time employees (20%). The highest for the years in operation demographic were 5 to 9 years (31%) and 10 to 14 years (18%). The lowest for the years in operation demographic were greater than 40 years (8%) and 15-19 years (9%). The highest for the annual revenue demographic were $1M to $4.9M (37%) and $500K to $999K (24%). The lowest for the annual revenue demographic were greater than $20M (<1%) and less than 100K (2%). The highest for the IT budget demographic were 7% to 10% (31%) and 3% to 6% (28%). The lowest for the IT budget demographic were greater than 10% (5%) and less than 1% (15%). The role demographic was nearly even. The highest for the age demographics were 30 to 39 years (45%) and 40 to 49 years (20%). The lowest for the age demographics were greater than 70 years (<1%) and less than 20 years (1%). The gender demographic was nearly even. Finally, the highest for the education demographic were bachelor’s degree (37%) and graduate level degrees (31%). The lowest for the education demographic were less than high school diploma (1%) and professional or doctoral degree (4%). Table 7 summarizes the descriptive statistics for the participant responses.

Table 7

Descriptive Statistics of the Participant Responses (N=216)

Demographic Item	N	%
Industry:		
1. Agriculture & Food Services	6	2.78%
2. Banking & Financial Services	10	4.63%
3. Communications, Entertainment, Media, & Publishing	18	8.33%
4. Construction & Real Estate	18	8.33%
5. Education & Research	13	6.02%
6. Energy & Utilities	13	6.02%
7. Healthcare Services & Pharmaceuticals	15	6.94%
8. Hospitality	11	5.09%
9. Industrial & Manufacturing Consumer Goods/Products	11	5.09%
10. Information Technology & Software	16	7.41%
11. Professional Services	23	10.65%
12. Repair & Installation Services	6	2.78%
13. Retail	21	9.72%
14. Transportation	4	1.85%
15. Warehousing, Logistics, & Distribution	4	1.85%
16. Other	27	12.50%
Size:		
2. 10-19 full-time employees	74	34.26%
3. 20-29 full-time employees	61	28.24%
4. 30-39 full-time employees	37	17.13%
5. 40-49 full-time employees	44	20.37%
Years in Operation:		
1. Less than 1 year	0	0.00%
2. 1-4 years	34	15.74%
3. 5-9 years	69	31.94%
4. 10-14 years	39	18.06%
5. 15-19 years	20	9.26%
6. 20-39 years	36	16.67%
7. 40+ years	18	8.33%
Annual Revenue:		
1. Less than $100K	4	1.85%
2. $100K to $249K	26	12.04%
3. $250K to $499K	26	12.04%
4. $500K to $999K	51	23.61%
5. $1M to $4.9M	79	36.57%
6. $5M to $20M	29	13.43%
7. More than $20M	1	0.46%

Table 7

Descriptive Statistics of the Participant Responses (N=216) (continued)

Demographic Item	**N**	**%**
IT Budget:		
1. Less than 1%	33	15.28%
2. 1% - 2%	46	21.30%
3. 3% - 6%	60	27.78%
4. 7% - 10%	67	31.02%
5. more than 10%	10	4.63%
Role:		
1. Owner	104	48.15%
2. Manager	112	51.85%
Age:		
1. Less than 20 years	2	0.93%
2. 20 to 29 years	35	16.20%
3. 30 to 39 years	97	44.91%
4. 40 to 49 years	43	19.91%
5. 50 to 59 years	26	12.04%
6. 60 to 69 years	12	5.56%
7. Over 70 years	1	0.46%
Gender:		
1. Female	87	40.28%
2. Male	129	59.72%
Education:		
1. Less than high school diploma	2	0.93%
2. High school diploma or equivalent	18	8.33%
3. Some college, no degree	26	12.04%
4. Associate degree	21	9.72%
5. Bachelor’s degree	80	37.04%
6. MBA or master’s degree	61	28.24%
7. Professional or doctoral degree	8	3.70%

Phase 2 – Additional Instrument Validation and Reliability

After pre-screening data, descriptive statistics were used to further validate the approved set of cybersecurity preparedness activities from RQ1. The results for the central tendency measures of mean and standard deviation were evaluated by obtaining the number of the cybersecurity preparedness activities in each of the five functions of the NIST Cybersecurity Framework. Table 8 summarizes the descriptive statistics for the approved set of cybersecurity preparedness activities.

For the identify function, the mean number of yes responses was 9.83 (SD = 5.59) out of the 20 question items. The mean showed that the samples of small businesses have an almost half or 49.2% approved set of cybersecurity preparedness activities in the identify function which is the function that helps increase an organization's understanding of their resources and risks. For the protect function, the mean number of yes responses was 11.66 (SD = 4.91) out of the 20 question items. The mean showed that the samples of small businesses have more than half or 58.3% approved set of cybersecurity preparedness activities in the protect function which is the function that supports the ability to limit or contain the impact of a potential information or cybersecurity event. For the detect function, the mean number of yes responses was 4.84 (SD = 2.73) out of the 10 question items. The mean showed that the samples of small businesses have an almost half or 48.43% approved set of cybersecurity preparedness activities in the detect function which is the function that enables timely discovery of information security or cybersecurity events. For the respond function, the mean number of yes responses was 4.53 (SD = 3.04) out of the 10 question items. The mean showed that the samples of small businesses have an almost half or 45.3% approved set of cybersecurity preparedness activities in the respond function which is the function that supports the ability to contain or reduce the impact of an event. For the recover function, the mean number of yes responses was 5.19 (SD = 2.64) out of the 10 question items. The mean showed that the small businesses have half or 51.9% approved set of cybersecurity preparedness activities in the recover function which is the function that helps an organization resume normal operations after an event.

Table 8

Descriptive Statistics of Cybersecurity Preparedness Activities in the Five Functions of NIST Cybersecurity Framework (N=216)

Cybersecurity Preparedness Activities	**N**	**Min**	**Max**	**Mean**	**Std. Deviation**
Identity (ID)	216	0	20	9.83	5.59
Protect (PR)	216	0	20	11.66	4.91
Detect (DE)	216	0	10	4.84	2.73
Respond (RS)	216	0	10	4.53	3.04
Recover (RC)	216	0	10	5.19	2.64

Additionally, for RQ1, the question items used to collect cybersecurity preparedness activities for the five functions of the NIST Cybersecurity Framework were evaluated using Cronbach’s alpha to test for reliability. Measures that demonstrate a reliability score over 0.70 using Cronbach’s Alpha are considered reliable (Mertler & Reinhardt, 2017). Cronbach’s alpha reliability coefficients are presented in Table 9. The results show that the individual measures of the CPSs activities in each of the five functions of the NIST Cybersecurity Framework of Identify (α = 0.89), Protect (α = 0.85), Detect (α = 0.77), Respond (α = 0.82), and Recover (α = 0.74) have Cronbach’s alpha values greater than the minimum acceptable value of 0.70 to demonstrate acceptable reliabilities. In terms of internal consistencies, the results indicate good correlations among the responses for each of the constructs.

Table 9

Cronbach's Alpha Reliability Coefficients for the Five Functions of the NIST Cybersecurity Framework (N=216)

Constructs	**Cronbach's Alpha**	**No. of Items**
Identity (ID)	0.89	20
Protect (PR)	0.85	20
Detect (DE)	0.77	10
Respond (RS)	0.82	10
Recover (RC)	0.74	10

The survey instruments used to collect data for this study variables were tested to ensure the data are reliable (Levy, 2006). The variables involved in the ANOVA included CPSs and DMPRCA. The variables were tested for internal consistency using Cronbach's alpha for reliability in terms of internal consistency. Cronbach's alpha reliability coefficients are presented in Table 10. There are a total 70 items for the CPSs, the small business decision makers' perceived risk for the 10 categories of cyber-attacks using a 7-point Likert scale (PL x PI). The results show that the survey instruments used to measure the CPS ($\alpha = 0.95$) and DMPRCA in terms of perceived likelihood ($\alpha = 0.90$) and perceived impact ($\alpha = 0.93$) have acceptable reliabilities or internal consistencies since the Cronbach's alpha values were greater than the minimum acceptable value of 0.70. In fact, these constructs have Cronbach's alpha values 0.90 and higher indicating that the measures for the dependent variables in the ANOVA to address RQ5 have excellent reliabilities or internal consistencies.

Table 10

Cronbach's Alpha Reliability Coefficients for CPSs and DMPRCA (Perceived Likelihood and Perceived Impact)

Constructs	**Cronbach's Alpha**	**No. of Items**
Cybersecurity Preparedness Scores	0.95	70
Decision Maker's Perceived Risk of Cyber-Attack (Perceived Likelihood)	0.90	10
Decision Maker's Perceived Risk of Cyber-Attack (Perceived Impact)	0.93	10

Phase 2 – Data Analysis

For RQ4, the data from the sample small businesses was evaluated and positioned on the CyPRisT using the CPS and the DMPRCA. First, these descriptive statistics were used to evaluate the data by summarizing the scores of the overall cybersecurity preparedness activities and perceived cybersecurity risk (perceived likelihood x perceived impact). Specifically, the central tendency measures of mean and standard deviation were used to summarize CPSs and DMPRCA variables. Figure 10 shows how the sample of 216 small businesses are positioned on the CyPRisT with the CPS on the vertical axis and the DMPRCA on the horizonal axis.

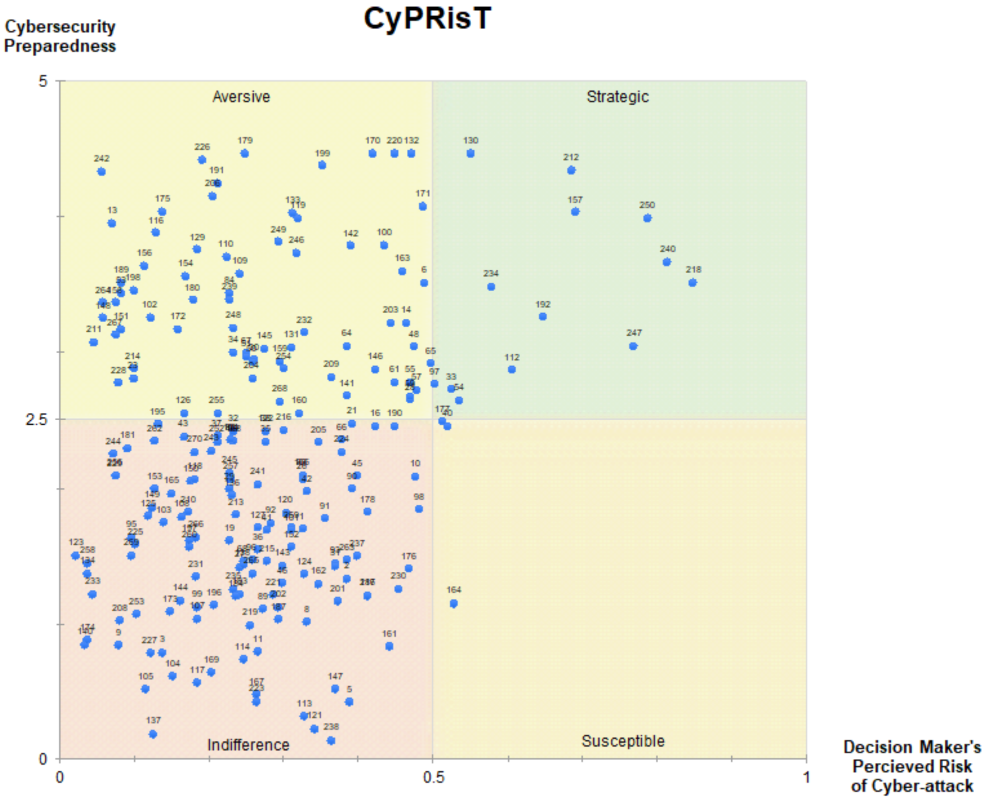


Figure 10. CyPRisT with Case Labels (N=216)

For RQ5, the data from the sample small businesses was evaluated to determine if statistically significant differences exist in the CPSs and DMPRCA based businesses demographics of (a) industry, (b) number of employees - size, (c) years in operation, (d) annual revenue, and (e) IT budget. Additionally, the data were evaluated to determine if statically significant difference also exist in the CPSs and DMPRCA based on participant demographics of (f) role – owner or manager, (g) age, (h) gender, and (i) education. One-way ANOVA was conducted to address RQ5 to determine whether there were significant differences in the scores of CPSs and DMPRCA for each of the business demographics (BD1 – BD5) and personal demographics (PD1 – PD4). A generally accepted significance level of 0.05 was used to indicate difference in the means among the demographics (Mertler & Reinhart, 2017).

Data analysis was performed on the sample of 216 small businesses. Table 11 summarizes the descriptive statistics summaries of CPSs and DMPRCA variables. For CPSs, the mean score was 2.29 (*SD* = 1.06) indicated that the samples of small businesses have low overall CPSs. For DMPRCA, the mean score was 0.28 (*SD* = 0.16) indicated that the samples of small business have low overall levels of perceived risk of cyber-attack.

Table 11

Descriptive Statistics of CPSs and DMPRCA (N=216)

Dependent Variable	**Min**	**Max**	**Mean**	**Std. Deviation**
CPSs	0.14	4.47	2.29	1.06
DMPRCA	0.02	0.85	0.28	0.16

Table 12 summarizes the descriptive statistics summaries of the responses on the DMPRCA in terms of perceived likelihood of the cyber-attack occurring at the small business. Based on the mean scores, the decision makers of small businesses perceived that they have a low likelihood (3) to moderate likelihood (4) of the cyber-attacks of general malware (*M* = 3.81; *SD* = 1.37), advanced malware/zero-day attack (*M* = 3.32; *SD* = 1.43), compromised/stolen devices (*M* = 3.32; *SD* = 1.41), cross-site scripting (*M* = 3.19; *SD* = 1.52), denial of services (*M* = 3.16; *SD* = 1.56), malicious insider (*M* = 3.24; *SD* = 1.56), phishing/social engineering (*M* = 4.00; *SD* = 1.60), SQL injection (*M* = 3.11;

SD = 1.49), web-based attack (*M* = 3.66; *SD* = 1.56), and other cyberattack (*M* = 3.59; *SD* = 1.51).

Table 12

Descriptive Statistics of DMPRCA (*Perceived Likelihood) (N=216)*

Perceived risk of cyber-attack (Perceived lowlihood)	**Min**	**Max**	**Mean**	**Std. Deviation**
PI1. General malware	1	7	3.81	1.37
PI2. Advanced malware/zero-day attack	1	7	3.32	1.43
PI3. Compromised/stolen devices	1	7	3.32	1.41
PI4. Cross-site scripting	1	7	3.19	1.52
PI5. Denial of services	1	7	3.16	1.56
PI6. Malicious insider	1	7	3.24	1.56
PI7. Phishing/social engineering	1	7	4.00	1.60
PI8. SQL injection	1	7	3.11	1.49
PI9. Web-based attack	1	7	3.66	1.56
PI10. Other cyberattack	1	7	3.59	1.51

Table 13 summarizes the descriptive statistics summaries of the responses on the DMPRCA in terms of level of impact the cyber-attack would have on the small business. Based on the mean scores, the decision makers of 216 samples of small businesses perceived that the cyber-attacks of general malware (M = 3.93; SD = 1.44), advanced malware/zero-day attack (M = 3.65; SD = 1.46), compromised/stolen devices (M = 3.76; SD = 1.45), cross-site scripting (M = 3.37; SD = 1.48), denial of services (M = 3.51; SD = 1.51), malicious insider (M = 3.74; SD = 1.61), phishing/social engineering (M = 3.75; SD = 1.50), SQL injection (M = 3.32; SD = 1.49), web-based attack (M = 3.68; SD = 1.57), and other cyberattack (*M* = 3.63; *SD* = 1.51) have a low impact (3) to moderate impact (4) on the small businesses.

Table 13

Descriptive Statistics of DMPRCA (*Perceived Impact) (N=216)*

Perceived risk of cyber-attack (Perceived impact)	**Min**	**Max**	**Mean**	**Std. Deviation**
PI1. General malware	1	7	3.93	1.44
PI2. Advanced malware/zero-day attack	1	7	3.65	1.46
PI3. Compromised/stolen devices	1	7	3.76	1.45
PI4. Cross-site scripting	1	7	3.37	1.48
PI5. Denial of services	1	7	3.51	1.51
PI6. Malicious insider	1	7	3.74	1.61
PI7. Phishing/social engineering	1	7	3.75	1.50
PI8. SQL injection	1	7	3.32	1.49
PI9. Web-based attack	1	7	3.68	1.57
PI10. Other cyberattack	1	7	3.63	1.51

A combination of descriptive statistics and one-way ANOVA were used to address RQ4 and RQ5 for the nine demographics of (a) industry, (b) number of employees, (c) years in operation, (d) annual revenue, (e) IT budget, (f) role, (g) age, (h) gender, and (i) education. First, data were examined using descriptive statistic techniques such as calculating means scores and standard deviation. The descriptive statistics and frequency distributions were also useful for detecting any irregularities and summarizing the data (Mertler & Vannatta, 2017). The aggregate CPSs and DMPCA were then positioned on the CyPRisT to understand the distribution of the data according to the position for each quadrant of the taxonomy. Additionally, the mean for each demographic were positioned on the CyPRisT for analysis. Next, a one-way ANOVA process was performed using SSPS to determine if statically significant difference exist in the CPSs and DMPRCA. The means of the CPSs and DMPRCA were plotted for analysis.

RQ4 and RQ5(a) – Industry (BD1)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the business industry focus. Based on mean comparisons shown in Table 14, the top three highest CPSs were those small businesses in the industries of communications, entertainment, media, and publishing (M = 2.98); information technology and software (M = 2.89); and construction and real estate (M = 2.76). On the other hand, the bottom three least CPSs were those small businesses in the industries of transportation (M = 1.24); agriculture and food services (M = 1.70); and retail (M = 1.85). Based on mean comparisons shown in Table 15, the top three highest DMPRCA were in small businesses in the industries of banking and financial services (M = 0.43); information technology and software (M = 0.38); and education and research (M = 0.37). On the other hand, the three lowest DMPRCA were those small businesses in the industries of transportation (M = 0.16); warehousing, logistics, and distribution (M = 0.17); and agriculture and food services (M = 0.22). Figure 11 shows the CyPRisT by industry category and Figure 12 shows the CyPRisT by mean for each industry category.

Table 14

Descriptive Statistics of CPSs by Industry (N=216)

Industry focus of business	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
					Lower Bound	**Upper Bound**
1. Agriculture & Food Services	6	1.70	1.41	0.58	0.22	3.18
2. Banking & Financial Services	10	2.71	0.91	0.29	2.06	3.36
3. Communications, Entertainment, Media, & Publishing	18	2.98	0.90	0.21	2.54	3.43
4. Construction & Real Estate	18	2.76	1.43	0.34	2.05	3.47
5. Education & Research	13	2.16	0.86	0.24	1.64	2.68
6. Energy (Oil, Gas, & Electricity)	13	2.17	1.01	0.28	1.56	2.78
7. Healthcare Services & Pharmaceuticals	15	2.14	0.89	0.23	1.64	2.63
8. Hospitality	11	2.03	0.89	0.27	1.44	2.63
9. Industrial & Manufacturing Consumer Goods/Products	11	2.52	1.09	0.33	1.79	3.25
10. Information Technology & Software	16	2.89	1.04	0.26	2.33	3.44
11. Professional Services (Accounting, Legal, Consulting, Veterinary, etc.)	23	2.09	1.06	0.22	1.63	2.54
12. Repair & Installation Services	6	2.58	1.09	0.45	1.43	3.72
13. Retail	21	1.85	1.03	0.23	1.38	2.32
14. Transportation	4	1.24	0.63	0.31	0.24	2.24
15. Warehousing, Logistics, & Distribution	4	1.96	1.11	0.55	0.20	3.72
16. Other	27	1.98	0.75	0.14	1.68	2.27
Total	216	2.29	1.06	0.07	2.14	2.43

Table 15

Descriptive Statistics of DMPRCA by Industry (N=216)

Industry focus of business	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
					Lower Bound	**Upper Bound**
1. Agriculture & Food Services	6	0.22	0.15	0.06	0.06	0.38
2. Banking & Financial Services	10	0.43	0.21	0.07	0.29	0.58
3. Communications, Entertainment, Media, & Publishing	18	0.27	0.13	0.03	0.21	0.33
4. Construction & Real Estate	18	0.29	0.22	0.05	0.18	0.40
5. Education & Research	13	0.37	0.12	0.03	0.29	0.44
6. Energy (Oil, Gas, & Electricity)	13	0.29	0.17	0.05	0.19	0.40
7. Healthcare Services & Pharmaceuticals	15	0.30	0.12	0.03	0.24	0.37
8. Hospitality	11	0.23	0.08	0.02	0.18	0.28
9. Industrial & Manufacturing Consumer Goods/Products	11	0.24	0.17	0.05	0.12	0.35
10. Information Technology & Software	16	0.38	0.18	0.05	0.28	0.48
11. Professional Services (Accounting, Legal, Consulting, Veterinary, etc.)	23	0.29	0.11	0.02	0.24	0.34
12. Repair & Installation Services	6	0.26	0.09	0.04	0.16	0.36
13. Retail	21	0.23	0.18	0.04	0.15	0.31
14. Transportation	4	0.16	0.07	0.04	0.04	0.27
15. Warehousing, Logistics, & Distribution	4	0.17	0.10	0.05	0.01	0.33
16. Other	27	0.23	0.11	0.02	0.19	0.28
Total	216	0.28	0.16	0.01	0.26	0.30

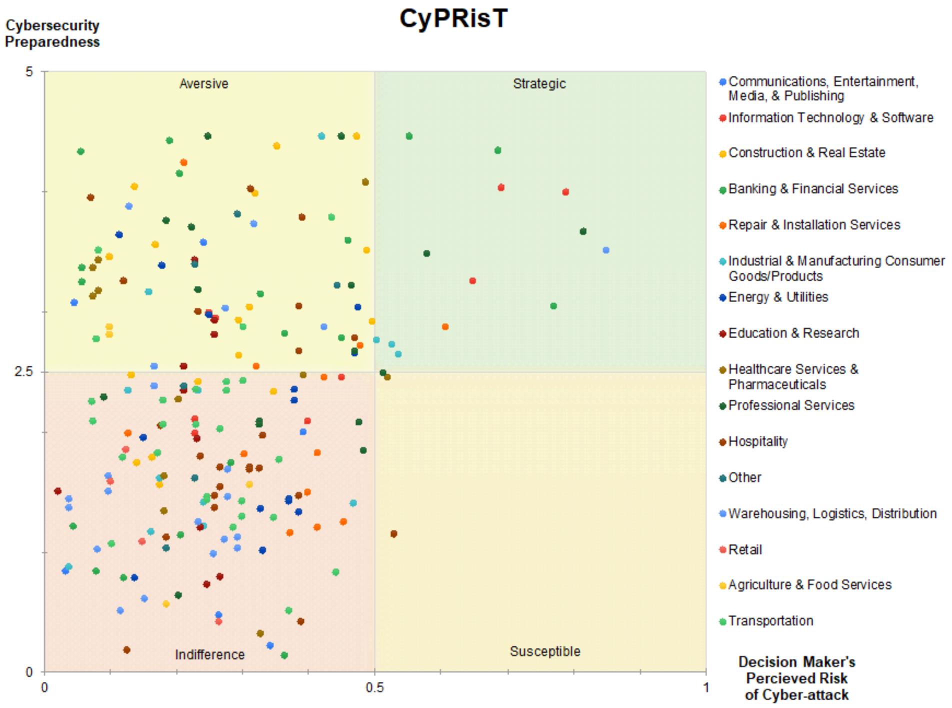


Figure 11. CyPRisT by Industry (N=216)

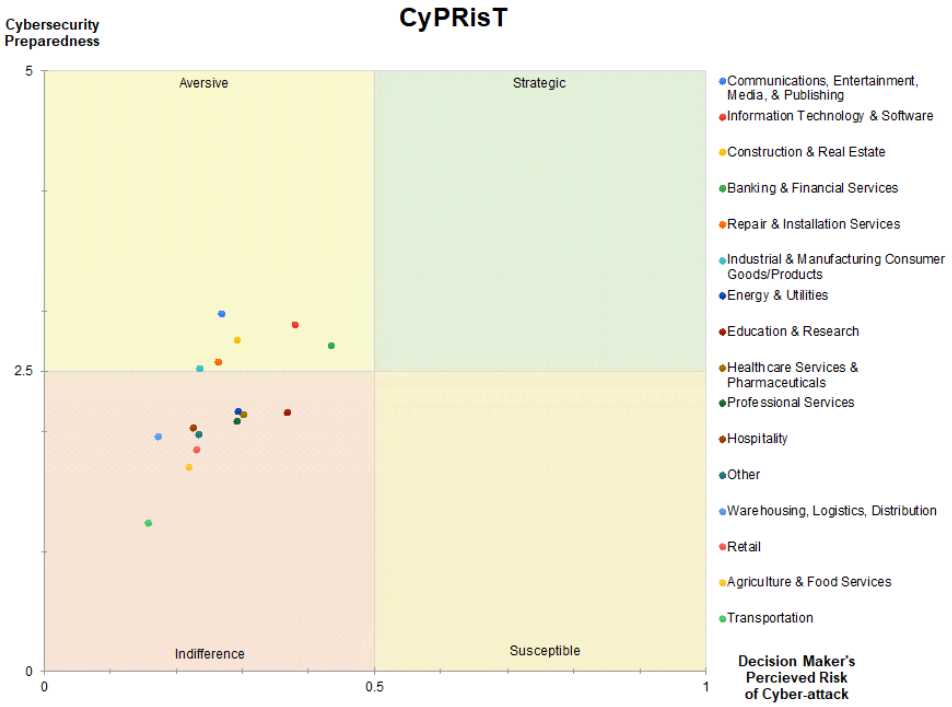


Figure 12. CyPRisT by Mean of Industry (N=216)

Table 16 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on their industry focus. The results of the one-way ANOVA showed that there were significant differences in both the CPSs (*F*(15, 200) = 2.42, *p* < 0.01) and DMPRCA (*F*(15, 200) = 2.39, *p* < 0.01) for small businesses based on industry focus of business. There were significant differences in the one-way ANOVA results since the *p*-values of the *F*-test were less than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 13) and DMPRCA (Figure 14) significantly vary by industry categories of the small businesses.

Table 16

ANOVA Results of Difference in CPSs and DMPRCA by Industry (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	37.26	15	2.48	2.42	0.003**
	Within Groups	205.41	200	1.03		
	Total	242.67	215			
DMPRCA	Between Groups	0.81	15	0.05	2.39	0.003**
	Within Groups	4.50	200	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

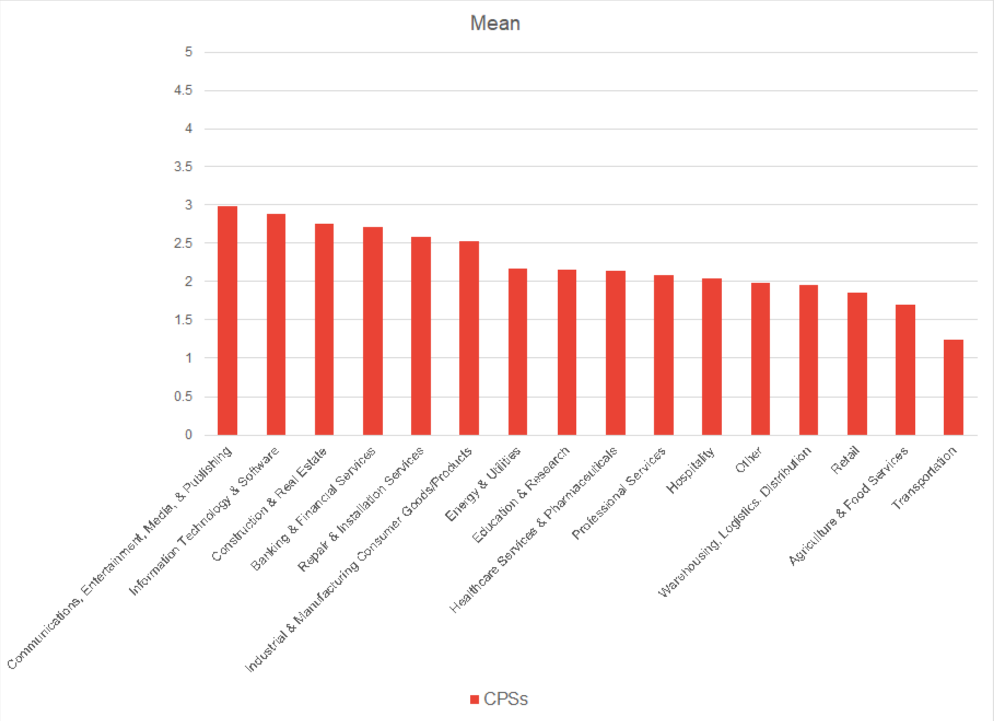


Figure 13. CPSs by Mean of Industry (N=216)

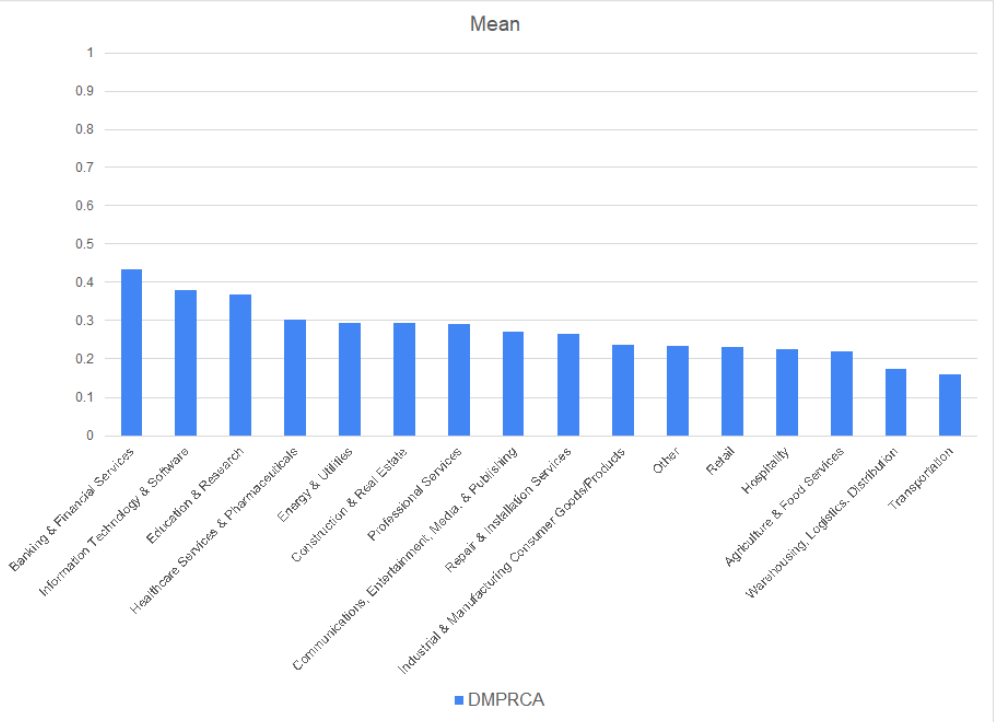


Figure 14. DMPRCA by Mean of Industry (N=216)

RQ4 and RQ5(b) – Number of Employees [size] (BD2)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the number employees (business size). Based on mean comparisons shown in Table 17 and graphical representation in Figure 15, those small businesses with higher number of employees in business (e.g., 20 to 29 full time employees; 30 to 39 full time employees) have greater CPSs and higher DMPRCA. Small businesses with lesser number of employees in business (e.g., 10 to 19 full time employees; 20 to 29 full time employees) have lower CPSs and lower DMPRCA. Figure 16 shows the CyPRisT by mean number of employees.

Table 17

Descriptive Statistics of CPSs and DMPRCA by Number of Employees (N=216)

DV	**Number of employees**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. 10-19 full-time employees	74	1.89	1.09	0.13	1.64	2.14
	2. 20-29 full-time employees	61	2.59	1.10	0.14	2.31	2.87
	3. 30-39 full-time employees	37	2.43	0.89	0.15	2.13	2.73
	4. 40-49 full-time employees	44	2.40	0.93	0.14	2.12	2.68
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. 10-19 full-time employees	74	0.23	0.15	0.02	0.20	0.27
	2. 20-29 full-time employees	61	0.29	0.15	0.02	0.25	0.33
	3. 30-39 full-time employees	37	0.31	0.18	0.03	0.25	0.37
	4. 40-49 full-time employees	44	0.33	0.13	0.02	0.29	0.37
	Total	216	0.28	0.16	0.01	0.26	0.30

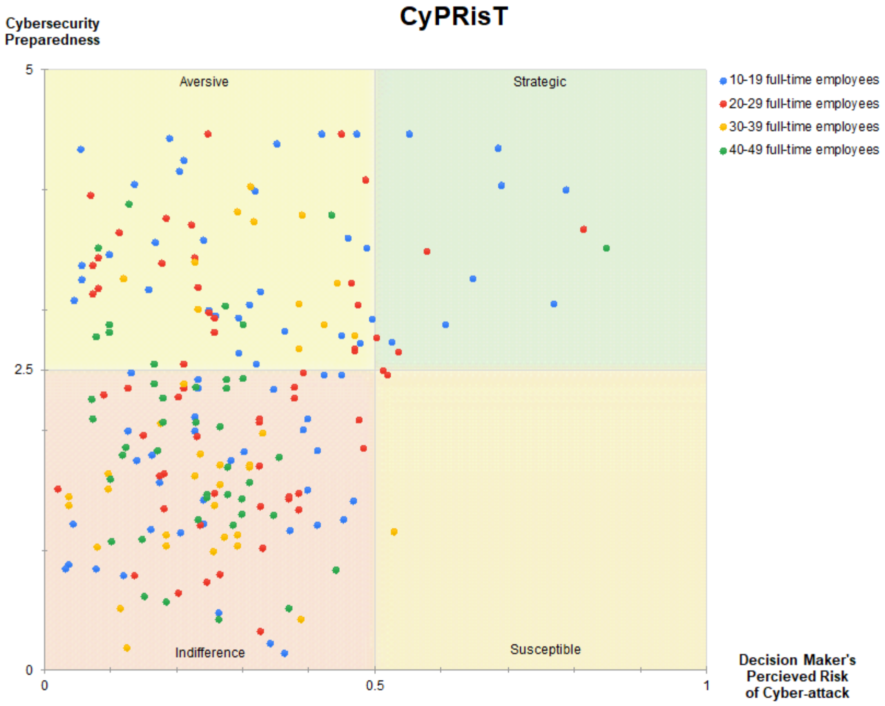


Figure 15. CyPRisT by Number of Employees (N=216)

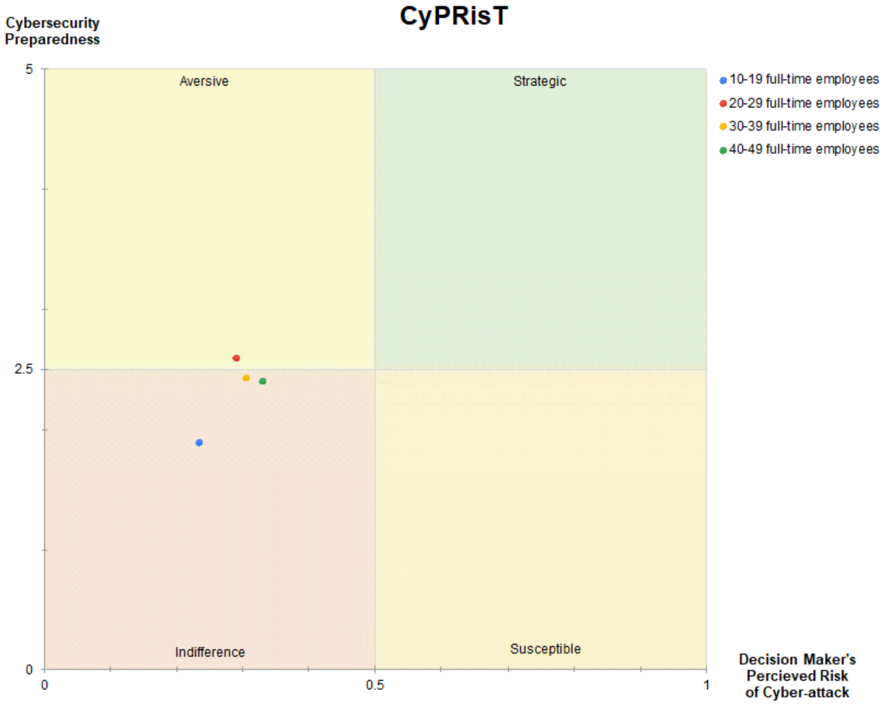


Figure 16. CyPRisT by Mean of Number of Employees (N=216)

Table 18 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on their size. The results of the one-way ANOVA showed that there were significant differences in both the CPSs (*F*(3, 212) = 5.89, *p* < 0.001) and DMPRCA (*F*(3, 212) = 4.24, *p* < 0.01) for small businesses based on number of employees in the business. There were significant differences in the one-way ANOVA results since the *p*-values of the *F*-test were less than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 17) and DMPRCA (Figure 18) significantly vary by size of the small businesses.

Table 18

ANOVA Results of Difference in CPSs and DMPRCA by Number of Employees (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	18.66	3	6.22	5.89	0.001***
	Within Groups	224.00	212	1.06		
	Total	242.67	215			
DMPRCA	Between Groups	0.30	3	0.10	4.24	0.006**
	Within Groups	5.01	212	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

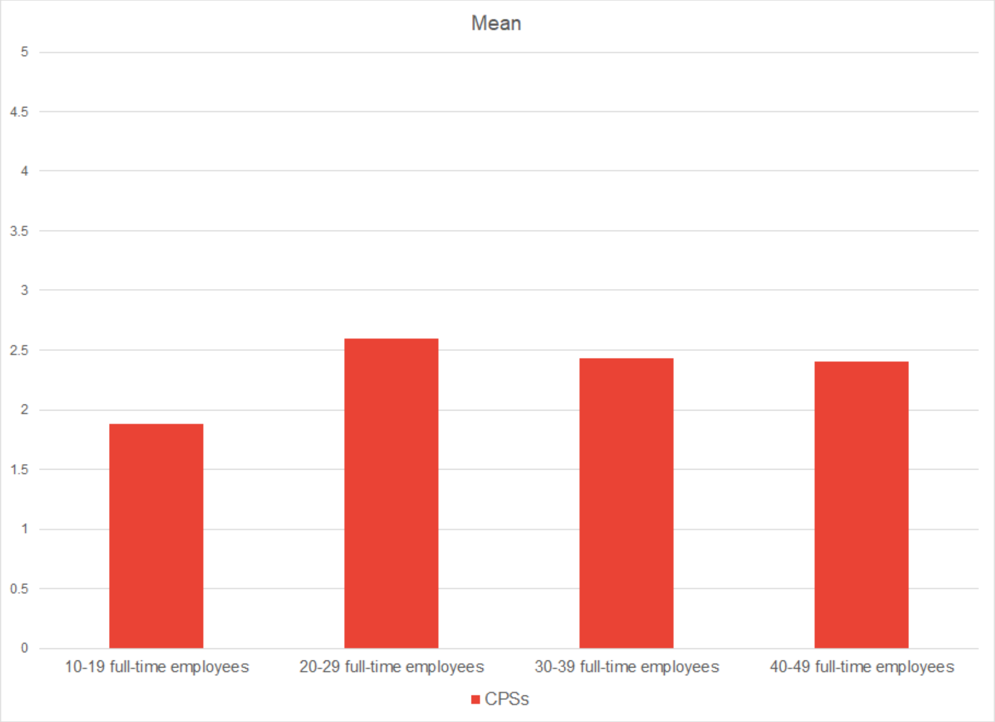


Figure 17. CPSs by Mean of Number of Employees (N=216)

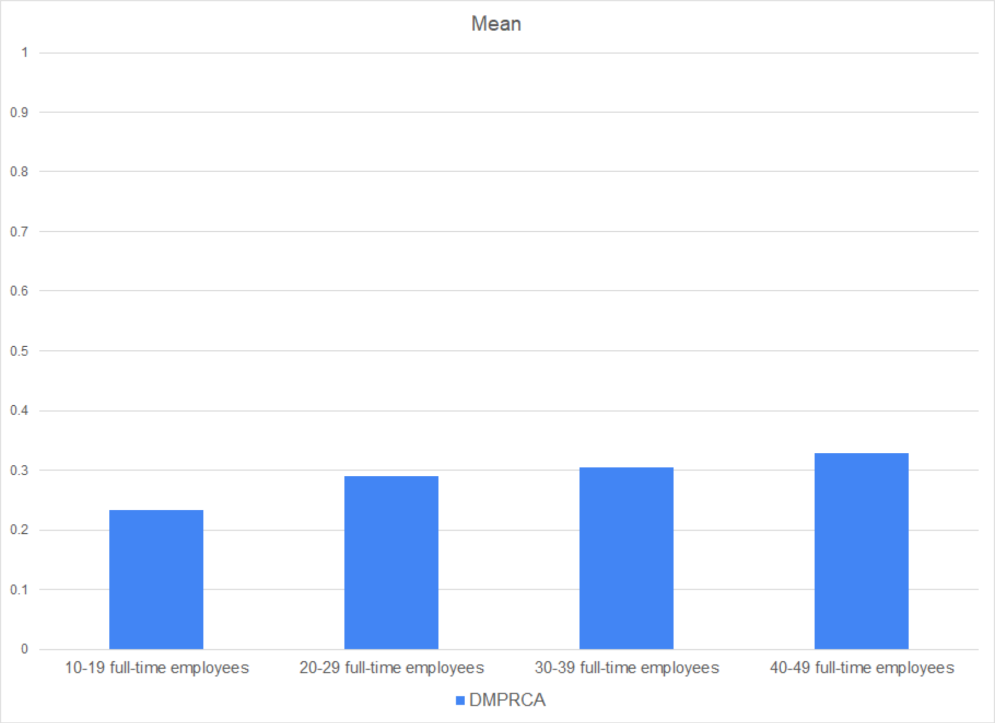


Figure 18. DMPRCA by Mean of Number of Employees (N=216)

RQ4 and RQ5(c) – Years in Operation (BD3)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by years in operation. Based on mean comparisons shown in Table 19 and graphical representation in Figure 19, those small businesses with 10 to 14 years in operation and 1 to 4 have the greatest CPSs while those small businesses with the highest years in operation (e.g., 40+ years, M = 1.65) have the lowest CPSs. The DMPRCA were near equal in their mean DMPRCA. Figure 20 shows the CyPRisT by mean for years in operation.

Table 19

Descriptive Statistics of CPSs and DMPRCA by Years in Operation (N=216)

DV	**Years in operation**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	2. 1-4 years	34	2.60	0.92	0.16	2.27	2.92
	3. 5-9 years	69	2.05	1.06	0.13	1.80	2.31
	4. 10-14 years	39	2.74	0.98	0.16	2.42	3.06
	5. 15-19 years	20	2.25	1.09	0.24	1.74	2.76
	6. 20-39 years	36	2.28	1.11	0.19	1.90	2.65
	7. 40+ years	18	1.65	0.90	0.21	1.20	2.10
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	2. 1-4 years	34	0.29	0.13	0.02	0.24	0.33
	3. 5-9 years	69	0.29	0.17	0.02	0.25	0.33
	4. 10-14 years	39	0.30	0.18	0.03	0.24	0.36
	5. 15-19 years	20	0.27	0.21	0.05	0.17	0.37
	6. 20-39 years	36	0.25	0.12	0.02	0.21	0.29
	7. 40+ years	18	0.27	0.13	0.03	0.21	0.34
	Total	216	0.28	0.16	0.01	0.26	0.30

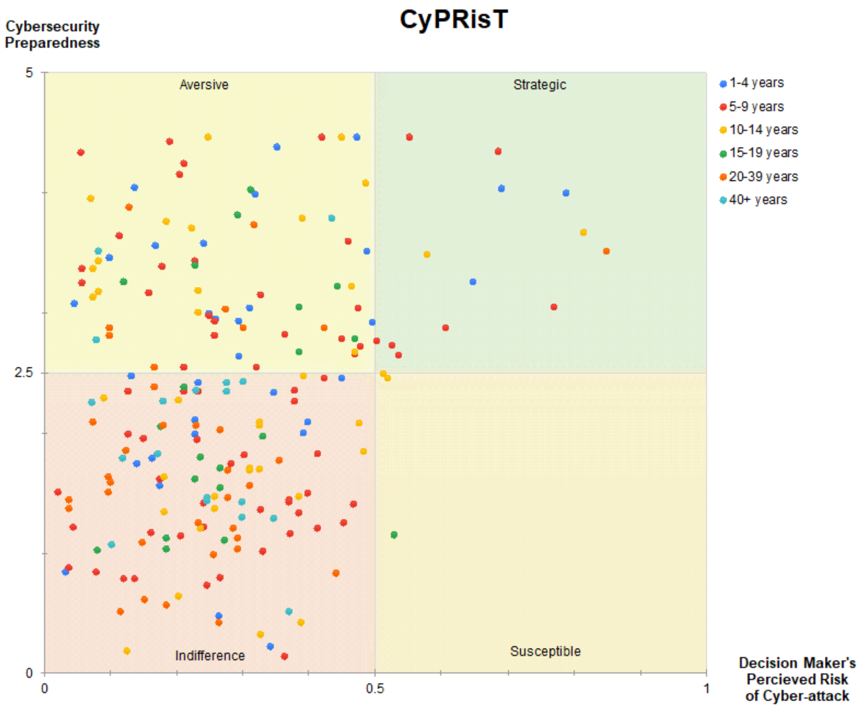


Figure 19. CyPRisT by Years in Operation (N=216)

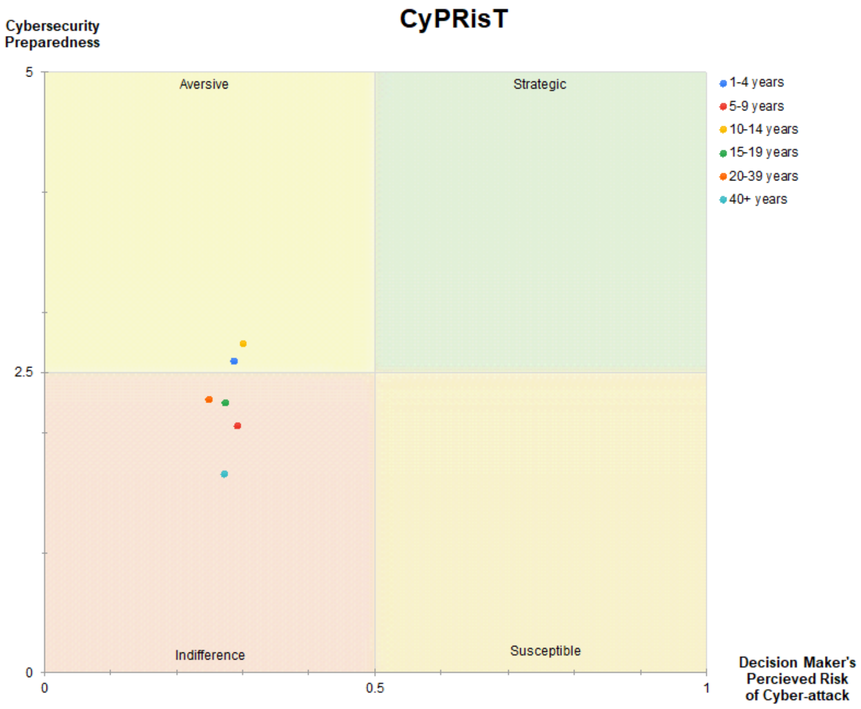


Figure 20. CyPRisT by Mean of Years in Operation (N=216)

Table 20 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on years in operation. The results of the one-way ANOVA showed that there was significant difference only in the CPSs (*F*(5, 210) = 4.25, *p* < 0.01) for small businesses based on years in operation. The mean plots graphically showed that the CPSs (Figure 21) for small businesses significantly vary for small businesses with different years in operation. However, the results of the one-way ANOVA and mean plots (Figure 22) showed that there were no significant difference in the DMPRCA (*F*(5, 210) = 0.50, *p* = 0.78) for small businesses based on years in operation.

Table 20

ANOVA Results of Difference in CPSs and DMPRCA by Years in Operation (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	22.29	5	4.46	4.25	0.001**
	Within Groups	220.38	210	1.05		
	Total	242.67	215			
DMPRCA	Between Groups	0.06	5	0.01	0.50	0.777
	Within Groups	5.25	210	0.03		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

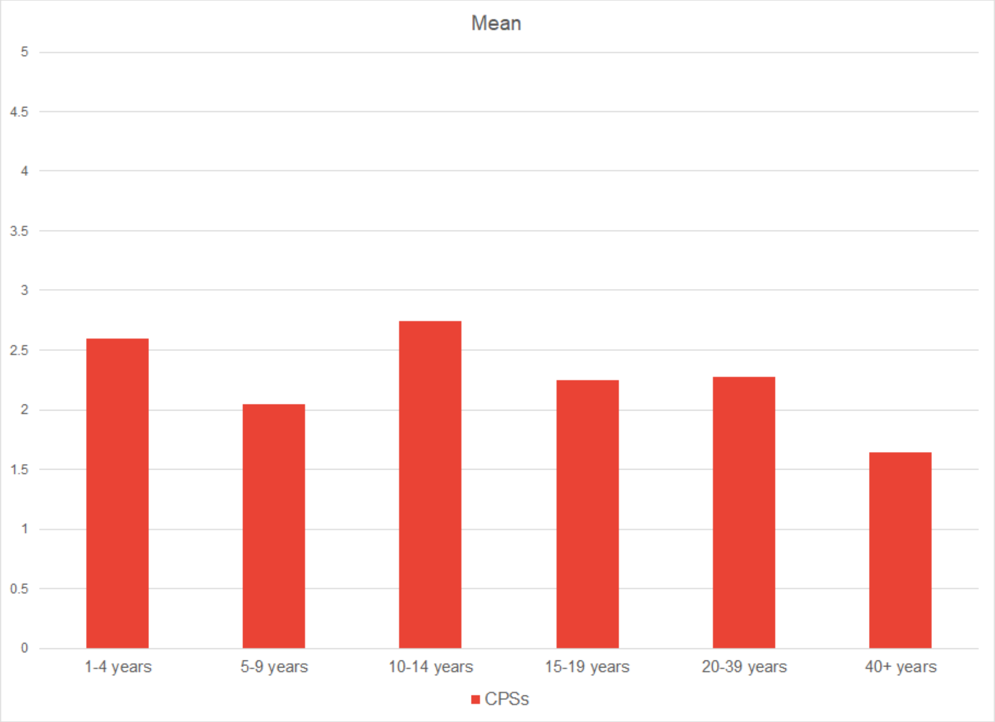


Figure 21. CPSs by Mean of Years in Operation (N=216)

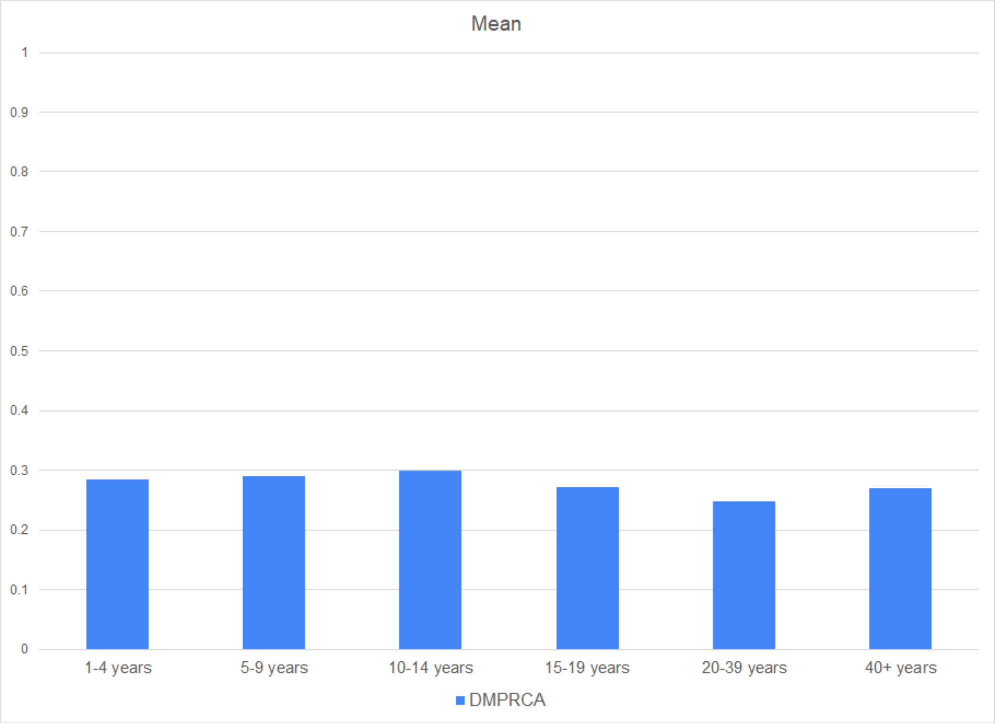


Figure 22. DMPRCA by Mean of Years in Operation (N=216)

RQ4 and RQ5(d) – Annual Revenue (BD4)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by annual revenue. Based on mean comparisons shown in Table 21 and graphical representation in Figure 23, those small businesses with average annual revenues (e.g., $500K to $999K; $1M to $4.9M) have greater CPSs. Small businesses with lesser annual revenue (e.g., Less than $100K) appear from the data in this study to be higher DMPRCA. Figure 24 shows the CyPRisT by annual revenue.

Table 21

Descriptive Statistics of CPSs and DMPRCA by Annual Revenue (N=216)

DV	**Annual Revenue**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. Less than $100K	4	2.18	1.61	0.80	-0.38	4.73
	2. $100K to $249K	26	2.12	1.15	0.22	1.66	2.58
	3. $250K to $499K	26	1.98	0.94	0.18	1.60	2.36
	4. $500K to $999K	51	2.56	0.96	0.14	2.29	2.84
	5. $1M to $4.9M	79	2.38	1.07	0.12	2.14	2.62
	6. $5M to $20M	29	2.01	1.10	0.20	1.60	2.43
	7. More than $20M	1	1.29	.	.	.	.
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. Less than $100K	4	0.36	0.08	0.04	0.23	0.49
	2. $100K to $249K	26	0.34	0.20	0.04	0.26	0.42
	3. $250K to $499K	26	0.21	0.11	0.02	0.17	0.25
	4. $500K to $999K	51	0.28	0.17	0.02	0.23	0.32
	5. $1M to $4.9M	79	0.29	0.15	0.02	0.26	0.33
	6. $5M to $20M	29	0.26	0.14	0.03	0.21	0.31
	7. More than $20M	1	0.35	.	.	.	.
	Total	216	0.28	0.16	0.01	0.26	0.30

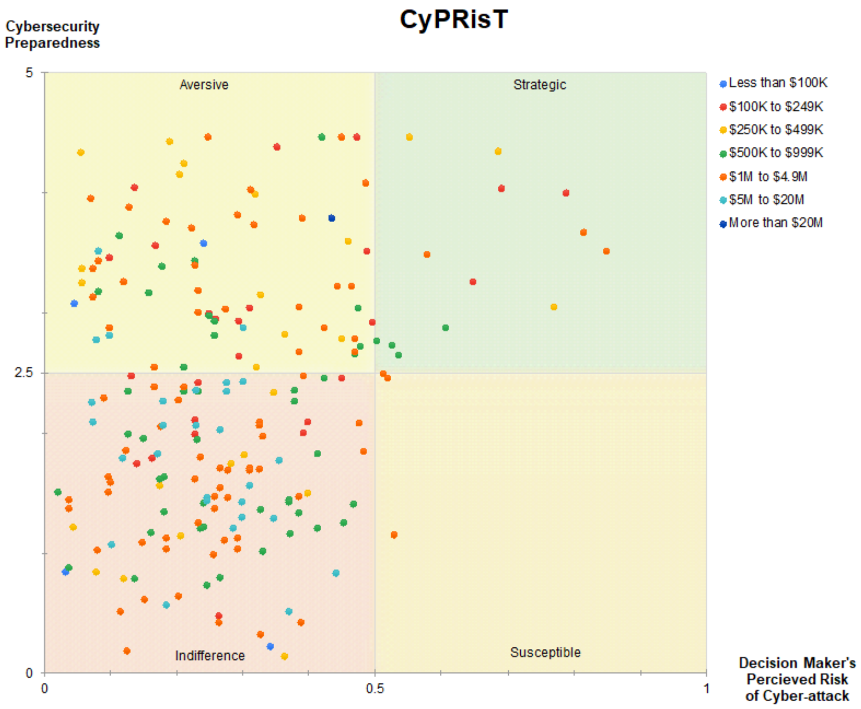


Figure 23. CyPRisT by Annual Revenue (N=216)

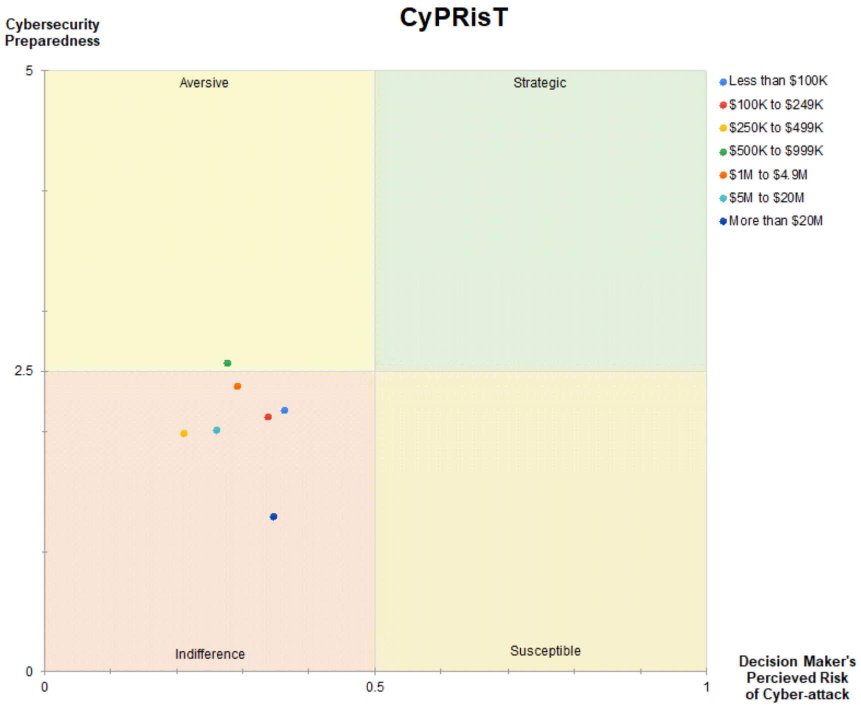


Figure 24. CyPRisT by Mean of Annual Revenue (N=216)

Table 22 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on annual revenue. The results of the one-way ANOVA showed that there were no significant differences in both the CPSs (*F*(6, 209) = 1.65, *p* = 0.14) and DMPRCA (*F*(6, 209) = 1.84, *p* = 0.09) for small businesses based on annual revenue. There were no significant differences in the one-way ANOVA results since the *p*-values of the *F*-test were greater than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 25) and DMPRCA (Figure 26) were not significantly different by annual revenue categories of the small businesses.

Table 22

ANOVA Results of Difference in CPSs and DMPRCA by Annual Revenue (N=216)

		Sum of Squares	df	Mean Square	F	Sig.
CPSs	Between Groups	10.95	6	1.82	1.65	0.136
	Within Groups	231.72	209	1.11		
	Total	242.67	215			
DMPRCA	Between Groups	0.27	6	0.04	1.84	0.092
	Within Groups	5.04	209	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

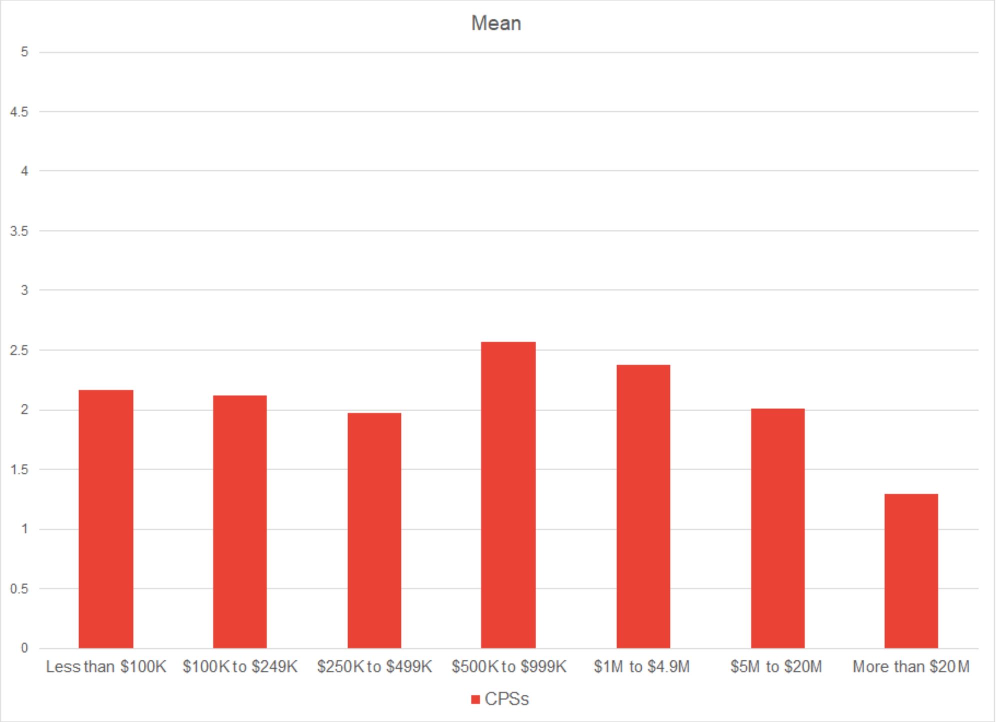


Figure 25. CPSs by Mean of Annual Revenue (N=216)

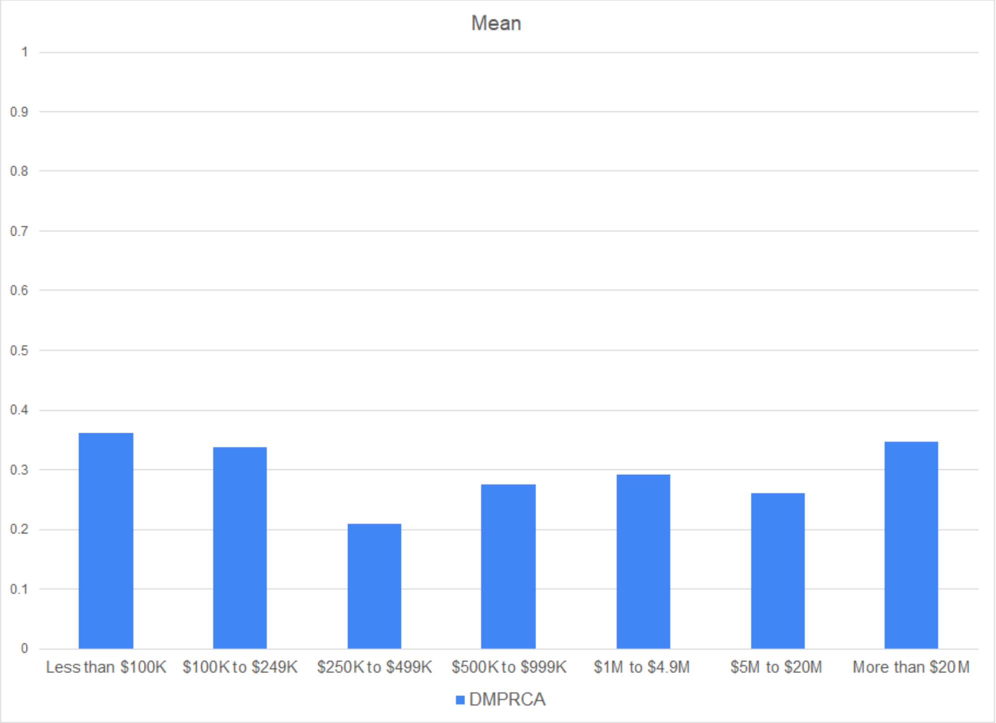


Figure 26. DMPRCA by Mean of Annual Revenue (N=216)

RQ4 and RQ5(e) – IT Budget (BD5)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by IT budget. Based on mean comparisons shown in Table 23 and graphical representation in Figure 27, those small businesses with higher IT budget (e.g., More than 10%; 7% - 10%, and 3%-6%) have greater CPSs and higher DMPRCA. Small businesses with lesser IT budget (e.g., Less than 1%; 1% - 2%) have lower CPSs and lower DMPRCA. Figure 28 shows the CyPRisT by annual revenue.

Table 23

Descriptive Statistics of CPSs and DMPRCA by IT Budget (N=216)

DV	**IT budget**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. Less than 1%	33	1.35	0.67	0.12	1.11	1.59
	2. 1% - 2%	46	1.85	0.79	0.12	1.62	2.08
	3. 3% - 6%	60	2.53	0.96	0.12	2.28	2.78
	4. 7% - 10%	67	2.77	1.07	0.13	2.51	3.03
	5. More than 10%	10	2.66	1.13	0.36	1.85	3.47
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. Less than 1%	33	0.23	0.11	0.02	0.19	0.26
	2. 1% - 2%	46	0.24	0.13	0.02	0.20	0.28
	3. 3% - 6%	60	0.29	0.15	0.02	0.25	0.33
	4. 7% - 10%	67	0.33	0.18	0.02	0.29	0.38
	5. More than 10%	10	0.29	0.16	0.05	0.17	0.40
	Total	216	0.28	0.16	0.01	0.26	0.30

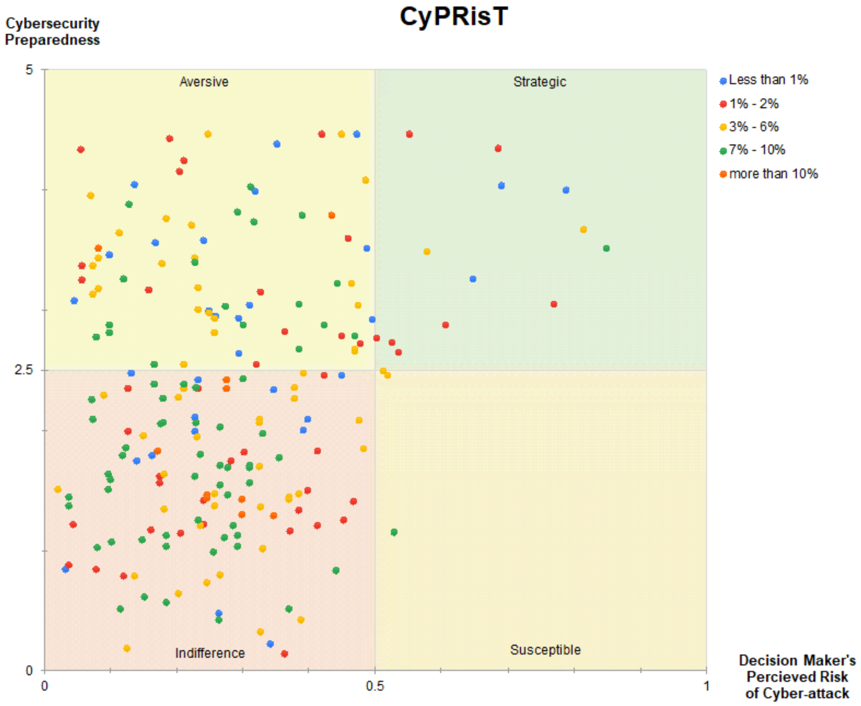


Figure 27. CyPRisT by IT Budget (N=216)

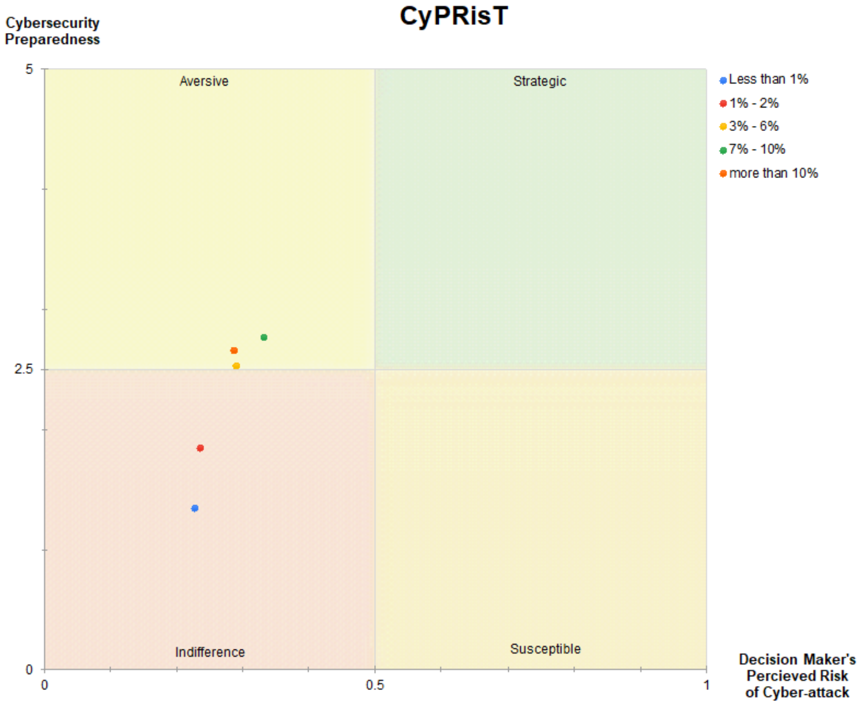


Figure 28. CyPRisT by Mean of IT Budget (N=216)

Table 24 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on categories of IT budget. The results of the one-way ANOVA showed that there were significant differences in both the CPSs (*F*(4, 211) = 16.79, *p* < 0.001) and DMPRCA (*F*(4, 211) = 3.93, *p* < 0.01) for small businesses based on IT budget. There were significant differences in the one-way ANOVA results since the *p*-values of the *F*-test were less than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 29) and DMPRCA (Figure 30) significantly vary by IT Budget of the small businesses.

Table 24

ANOVA Results of Difference in CPSs and DMPRCA by IT Budget (N=216)

		Sum of Squares	df	Mean Square	F	Sig.
CPSs	Between Groups	58.60	4	14.65	16.79	0.000***
	Within Groups	184.07	211	0.87		
	Total	242.67	215			
DMPRCA	Between Groups	0.37	4	0.09	3.93	0.004**
	Within Groups	4.94	211	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

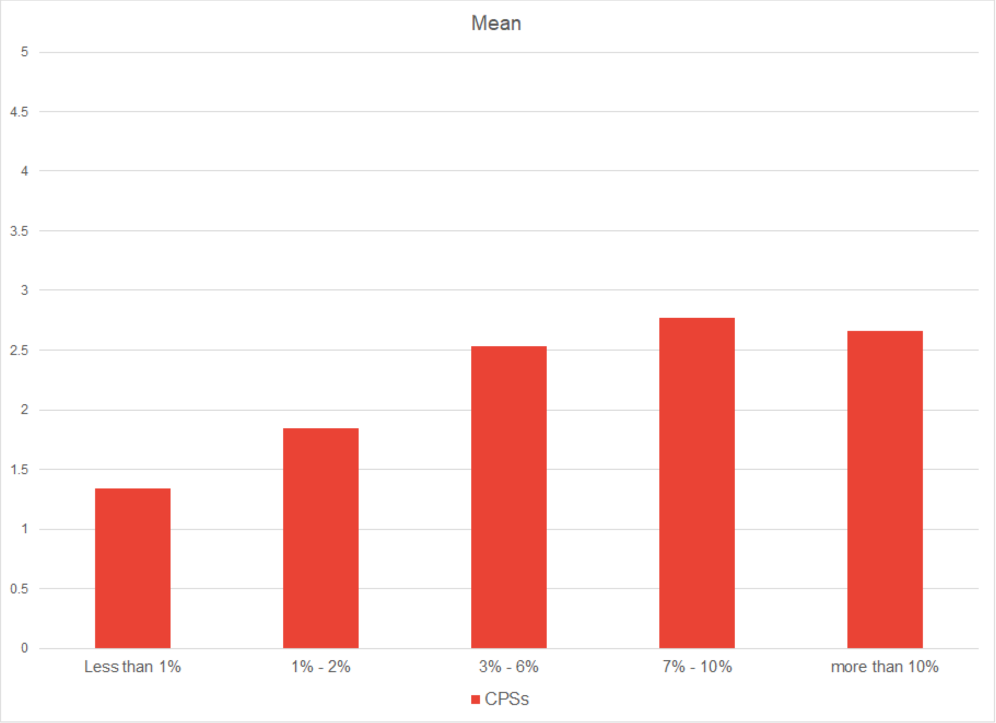


Figure 29. CPSs by Mean of IT Budget (N=216)

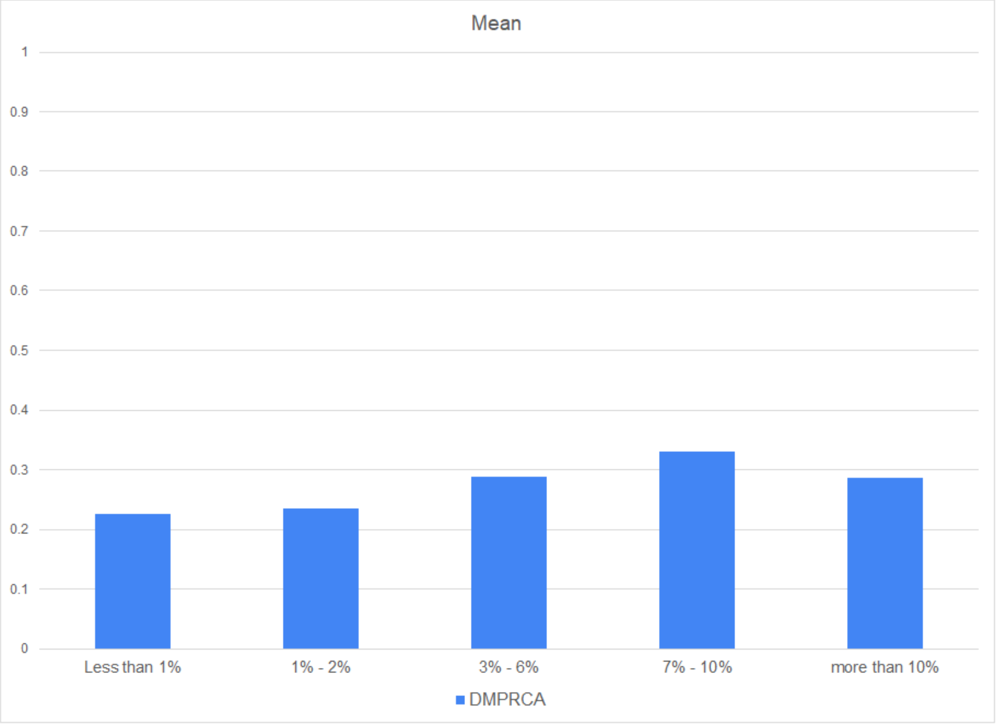


Figure 30. DMPRCA by Mean of IT Budget (N=216)

RQ4 and RQ5(f) – Role (PD1)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the participant's role (owner or manager). Based on mean comparisons shown in Table 25 and graphical representation in Figure 31, the participants were near equal in their mean of CPSs and DMPRCA. Figure 32 shows the CyPRisT by mean of the participant's role.

Table 25

Descriptive Statistics of CPSs and DMPRCA by Role (N=216)

DV	**Participant's Role**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. Owner	104	2.28	1.06	0.10	2.07	2.48
	2. Manger	112	2.29	1.07	0.10	2.09	2.49
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. Owner	104	0.27	0.15	0.01	0.24	0.30
	2. Manager	112	0.29	0.16	0.02	0.26	0.32
	Total	216	0.28	0.16	0.01	0.26	0.30

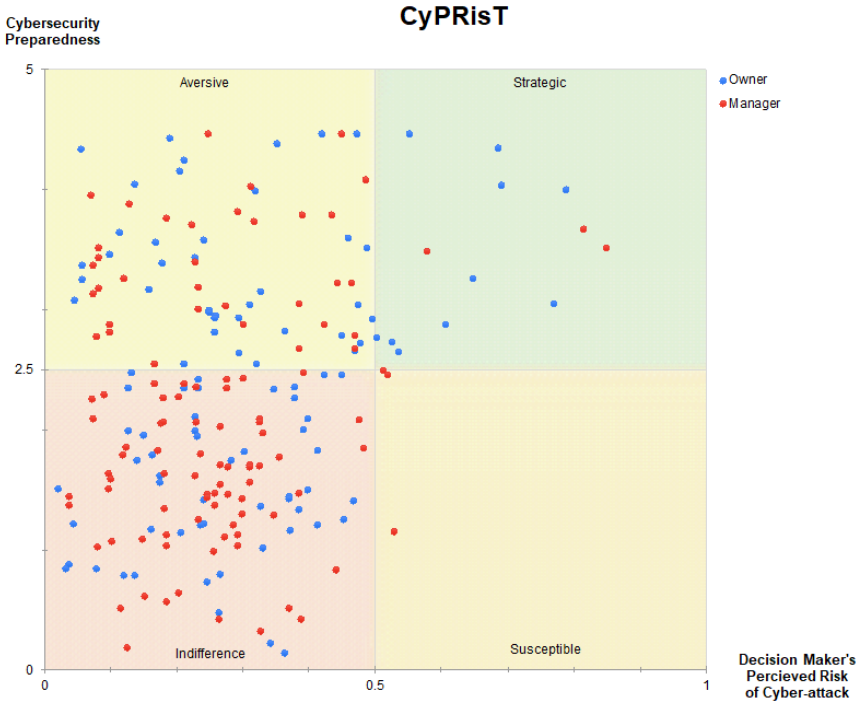


Figure 31. CyPRisT by Role (N=216)

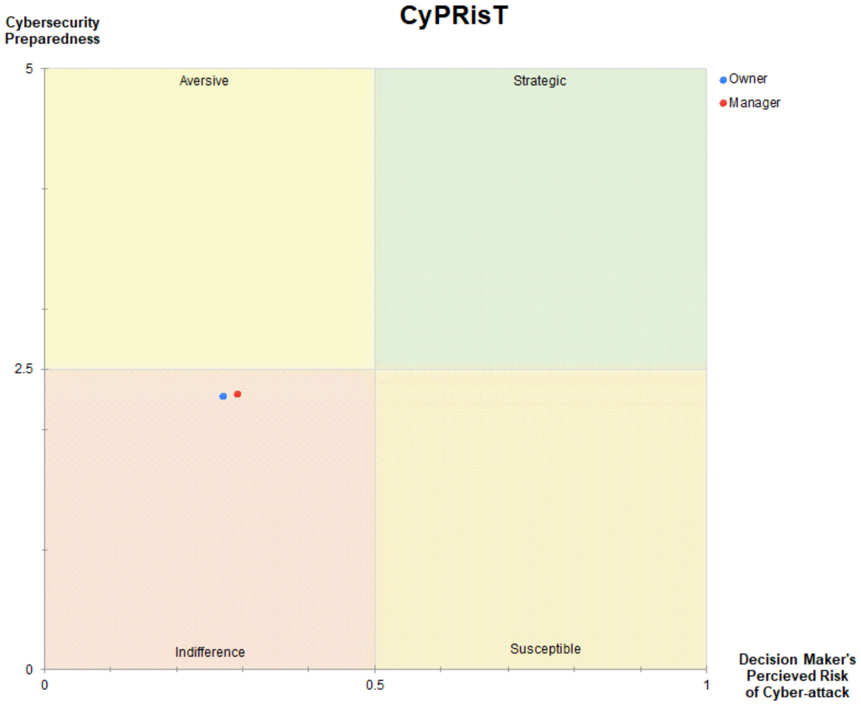


Figure 32. CyPRisT by Mean of Role (N=216)

Table 26 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on the participant's role. The results of the one-way ANOVA showed that there were no significant differences in both the CPSs (*F*(1, 214) = 0.01, *p* = 0.91) and DMPRCA (*F*(1, 214) = 0.96, *p* = 0.33) for small businesses based on role since the *p*-values of the *F*-test were greater than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 33) and DMPRCA (Figure 34) were not significantly different by the participant's role.

Table 26

ANOVA Results of Difference in CPSs and DMPRCA by Role (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	0.02	1	0.02	0.01	0.905
	Within Groups	242.65	214	1.13		
	Total	242.67	215			
DMPRCA	Between Groups	0.02	1	0.02	0.96	0.328
	Within Groups	5.29	214	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

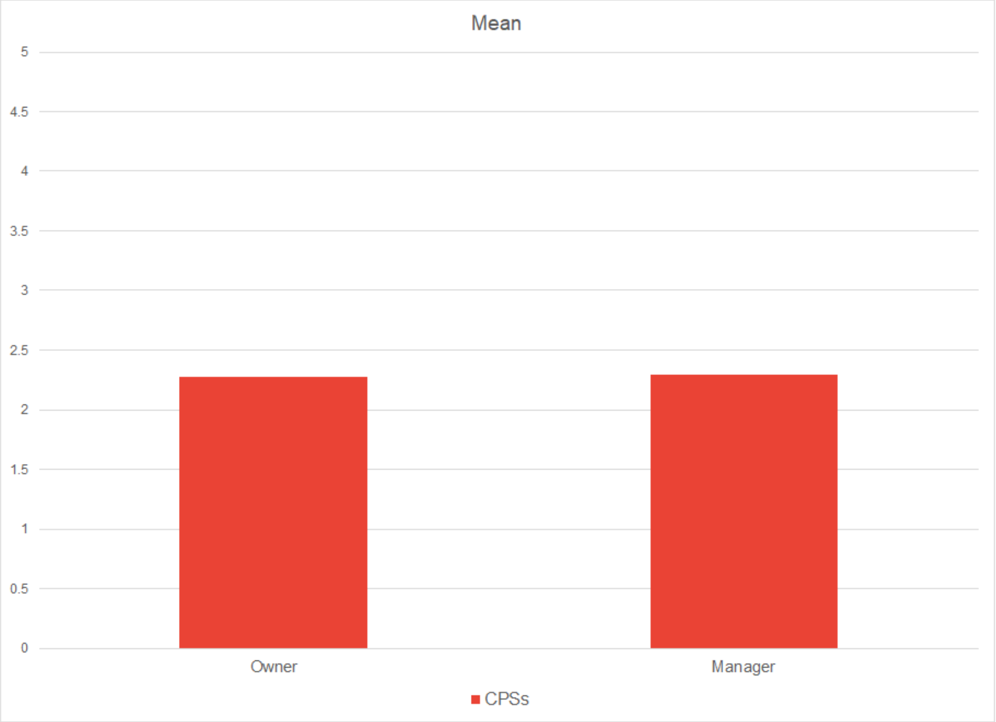


Figure 33. CPSs by Mean of Role (N=216)

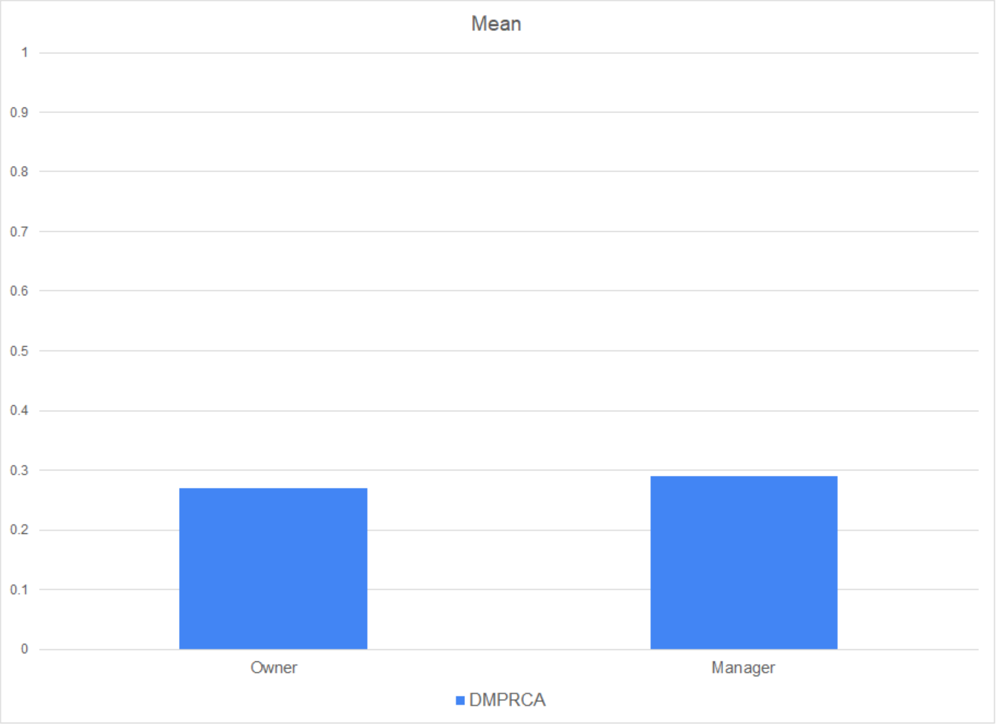


Figure 34. DMPRCA by Mean of Role (N=216)

RQ4 and RQ5(g) – Age (PD2)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the participant's age. Based on mean comparisons shown in Table 27 and graphical representation in Figure 35, the participants in age group 20 to 29 years have highest CPSs. Participant in the oldest age group, over 70 years, appear from the data in this study to have the lowest CPSs and highest DMPRCA. Figure 36 shows the CyPRisT by mean of the participant's age.

Table 27

Descriptive Statistics of CPSs and DMPRCA by Age (N=216)

DV	**Participant's Age**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. < 20 years	2	2.09	0.03	0.02	1.81	2.37
	2. 20 to 29 years	35	2.70	0.87	0.15	2.40	3.00
	3. 30 to 39 years	97	2.13	1.02	0.10	1.93	2.34
	4. 40 to 49 years	43	2.41	1.15	0.17	2.06	2.76
	5. 50 to 59 years	26	2.24	1.35	0.26	1.69	2.78
	6. 60 to 69 years	12	2.03	0.73	0.21	1.57	2.50
	7. Over 70 years	1	2.00				
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. < 20 years	2	0.23	0.00	0.00	.21	0.24
	2. 20 to 29 years	35	0.27	0.19	0.03	.20	0.33
	3. 30 to 39 years	97	0.29	0.13	0.01	.26	0.31
	4. 40 to 49 years	43	0.32	0.20	0.03	.26	0.38
	5. 50 to 59 years	26	0.22	0.11	0.02	.17	0.26
	6. 60 to 69 years	12	0.28	0.09	0.03	.22	0.34
	7. Over 70 years	1	0.39				
	Total	216	0.28	0.16	0.01	0.26	0.30

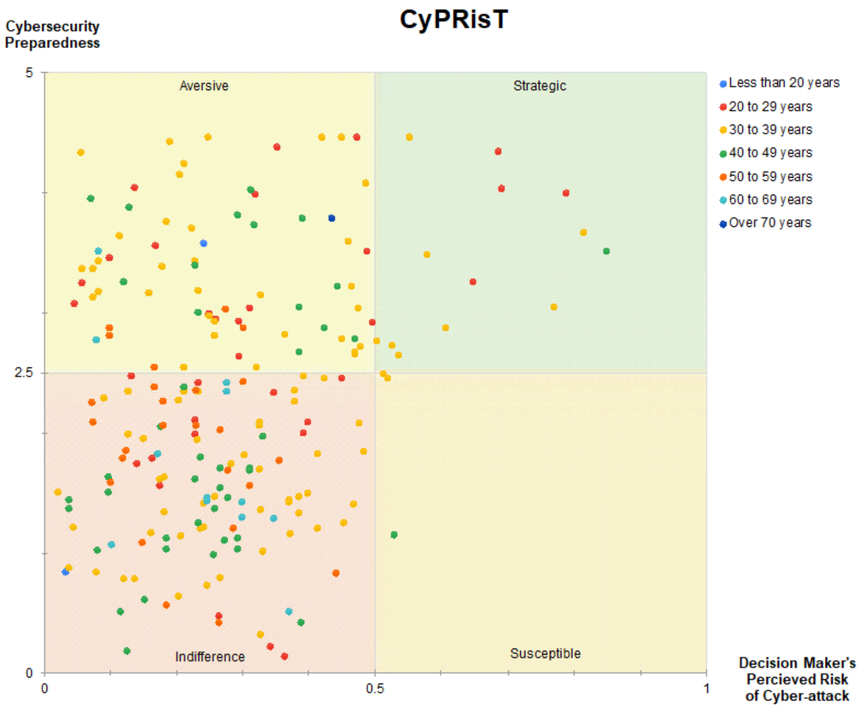


Figure 35. CyPRisT by Age (N=216)

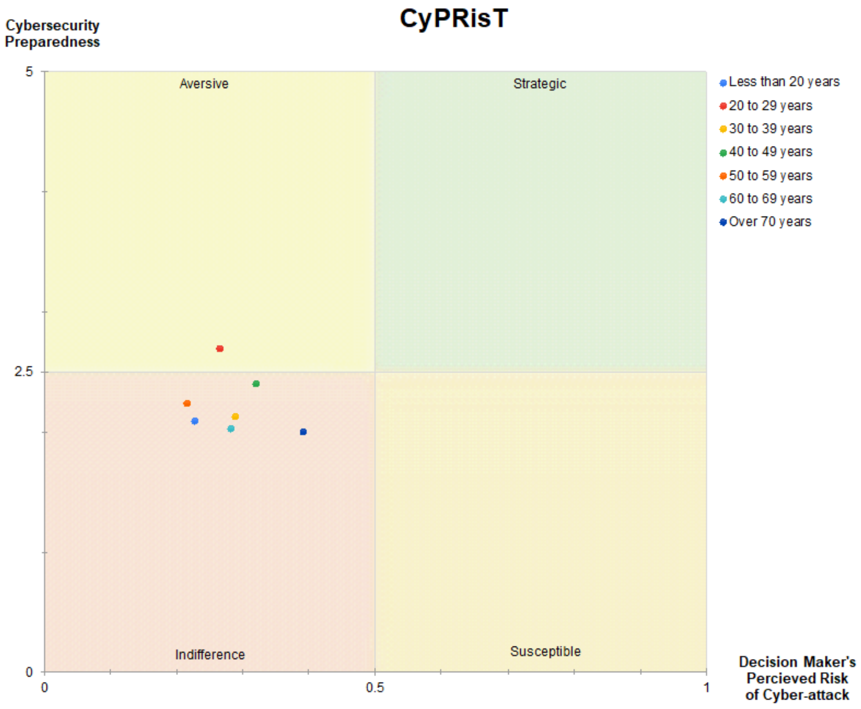


Figure 36. CyPRisT by Mean of Age (N=216)

Table 28 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on the participant's age. The results of the one-way ANOVA showed that there were no significant differences in both the CPSs (*F*(6, 209) = 1.47, *p* = 0.19) and DMPRCA (*F*(6, 209) = 1.40, *p* = 0.22) for small businesses based on age since the *p*-values of the *F*-test were greater than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 37) and DMPRCA (Figure 38) were not significantly different by the participant's age.

Table 28

ANOVA Results of Difference in CPSs and DMPRCA by Age (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	9.81	6	1.63	1.47	0.191
	Within Groups	232.86	209	1.11		
	Total	242.67	215			
DMPRCA	Between Groups	0.20	6	0.03	1.40	0.218
	Within Groups	5.11	209	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

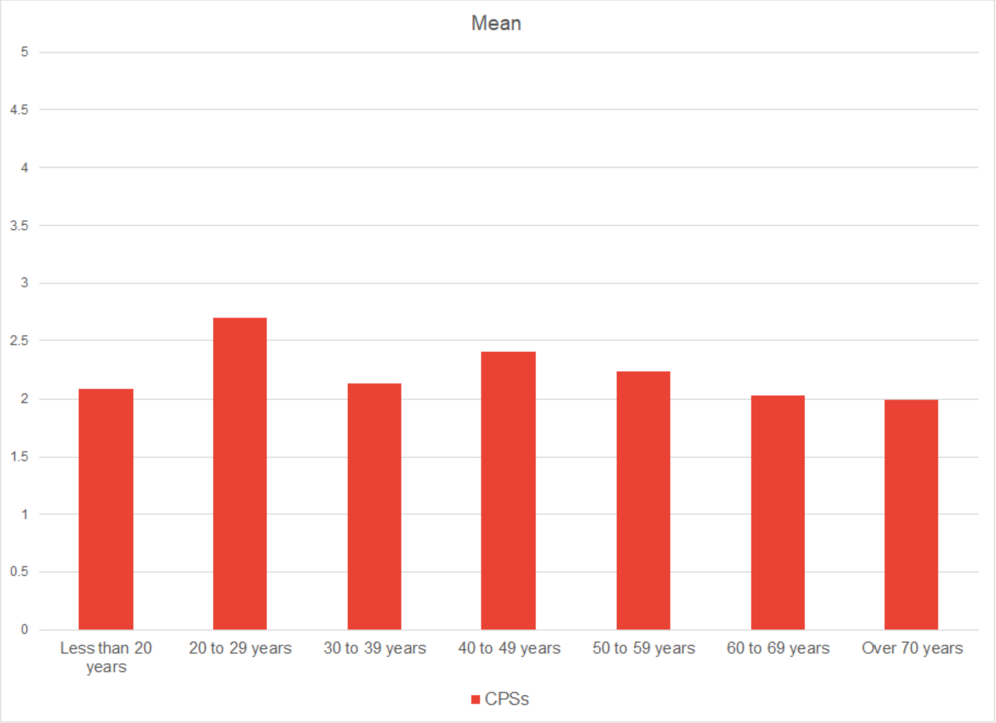


Figure 37. CPSs by Mean of Age (N=216)

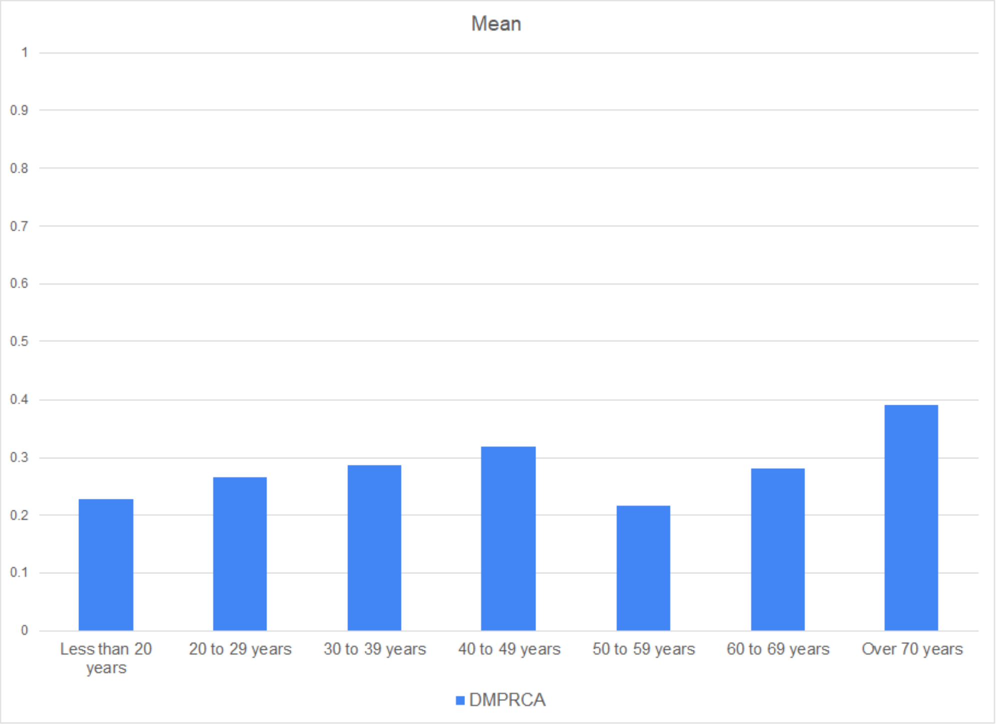


Figure 38. DMPRCA by Mean of Age (N=216)

RQ4 and RQ5(h) – Gender (PD3)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the participant's gender. Based on mean comparisons shown in Table 29 and graphical representation in Figure 39, the female participants were slightly higher in the mean of CPSs and equal in the mean of DMPRCA. Figure 40 shows the CyPRisT by mean of the participant's gender.

Table 29

Descriptive Statistics of CPSs and DMPRCA by Gender (N=216)

DV	**Participant's Gender**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. Female	87	2.40	1.09	0.12	2.16	2.63
	2. Male	129	2.21	1.04	0.09	2.03	2.39
	Total	216	2.29	1.06	0.07	2.14	2.43
DMPRCA	1. Female	87	0.28	0.17	0.02	0.24	0.32
	2. Male	129	0.28	0.15	0.01	0.26	0.31
	Total	216	0.28	0.16	0.01	0.26	0.30

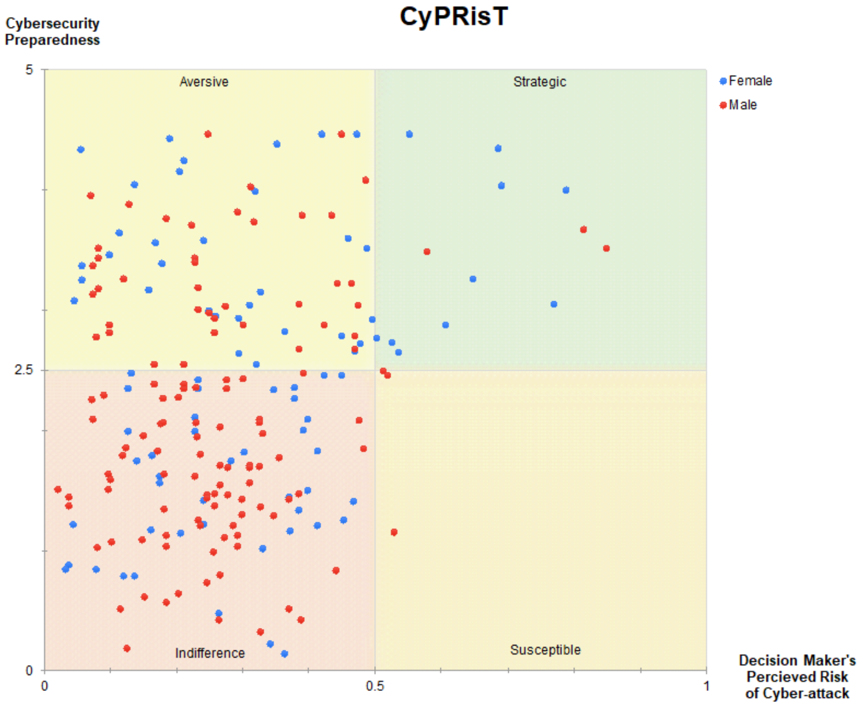


Figure 39. CyPRisT by Gender (N=216)

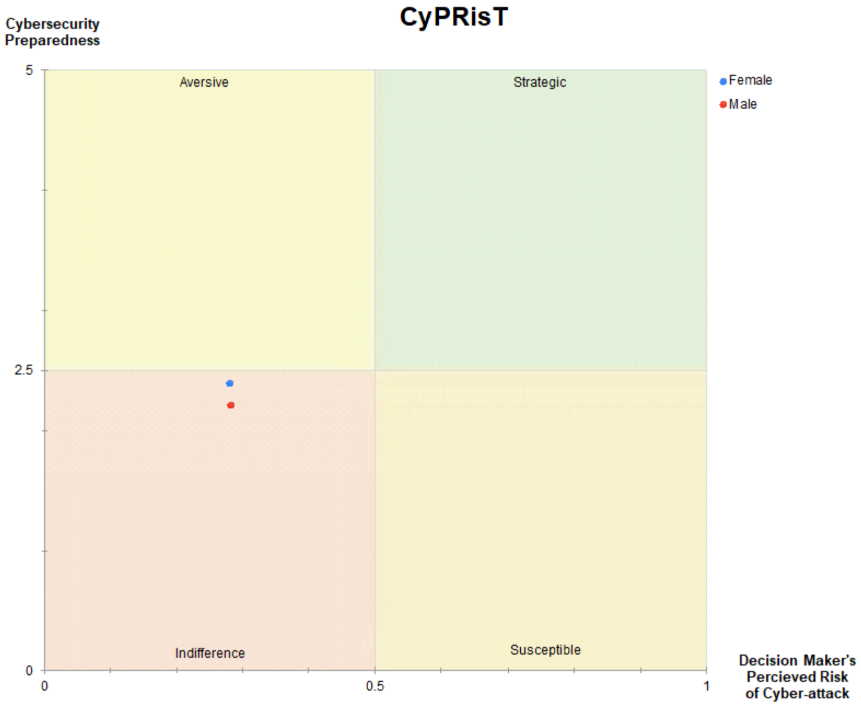


Figure 40. CyPRisT by Mean of Gender (N=216)

Table 30 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on the participant's gender. The results of the one-way ANOVA showed that there were no significant differences in both the CPSs (*F*(1, 214) = 1.58, *p* = 0.21) and DMPRCA (*F*(1, 214) = 0.01, *p* = 0.92) for small businesses based on gender since the *p*-values of the *F*-test were greater than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 41) and DMPRCA (Figure 42) were not significantly different by the participant's gender.

Table 30

ANOVA Results of Difference in CPSs and DMPRCA by Gender (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	1.78	1	1.78	1.58	0.210
	Within Groups	240.88	214	1.13		
	Total	242.67	215			
DMPRCA	Between Groups	0.00	1	0.00	0.01	0.923
	Within Groups	5.31	214	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

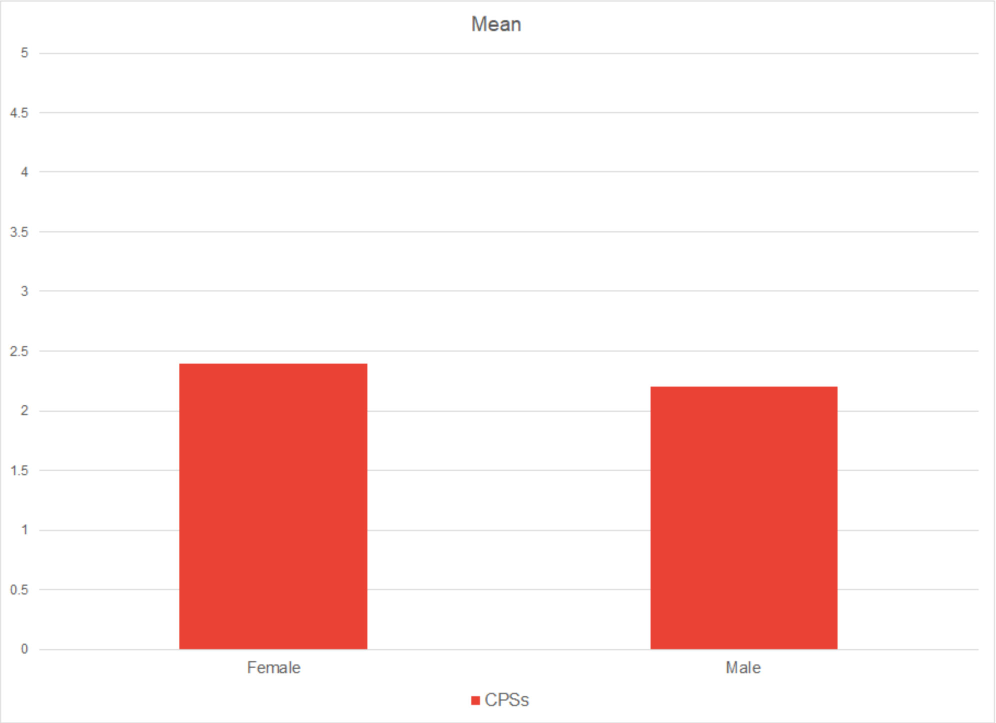


Figure 41. CPSs by Mean of Gender (N=216)

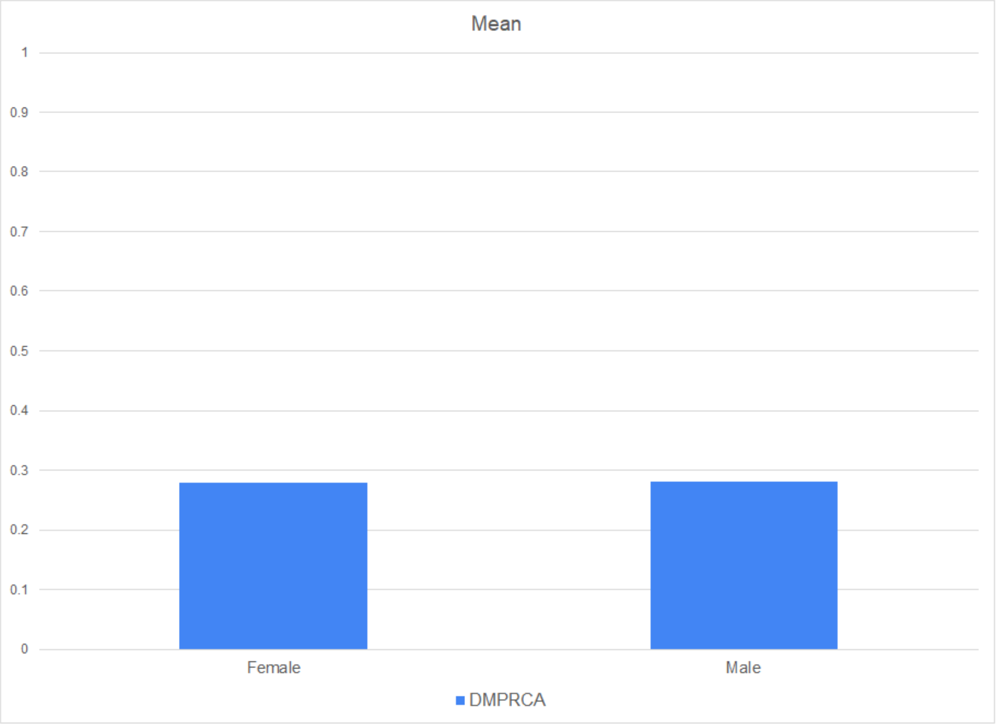


Figure 42. DMPRCA by Mean of Gender (N=216)

RQ4 and RQ5(i) – Education (PD4)

This section presents the results of the descriptive statistics, CyPRisT positions, differences between groups, mean plots of CPSs and DMPRCA, as well as the CyPRisT mean for the sample of small businesses categorized by the participant's education level. Based on mean comparisons shown in Table 31 and Table 32 as well as the graphical representation in Figure 43, the participants with high school diploma and college degrees have greater CPSs and lower DMPRCA. Figure 44 shows the CyPRisT by mean of the participant's education level.

Table 31

Descriptive Statistics of CPSs by Education (N=216)

DV	**Participant's Education**	**N**	**Mean**	**SD**	**S.E.**	**95% Confidence Interval for Mean**	
						Lower Bound	**Upper Bound**
CPSs	1. Less than high school diploma	2	1.43	0.00	0.00	1.43	1.43
	2. High school diploma or equivalent	18	2.22	1.23	0.29	1.61	2.83
	3. Some college, no degree	26	2.07	1.29	0.25	1.55	2.59
	4. Associate degree	21	2.37	1.10	0.24	1.87	2.87
	5. Bachelor's degree	80	2.31	1.06	0.12	2.07	2.55
	6. MBA or master's degree	61	2.38	0.88	0.11	2.16	2.61
	7. Professional or doctoral degree	8	2.12	1.31	0.46	1.02	3.21
	Total	216	2.29	1.06	0.07	2.14	2.43

Table 32

Descriptive Statistics of DMPRCA by Education (N=216)

DV	Participant's Education	N	Mean	SD	S.E.	95% Confidence Interval for Mean	
						Lower Bound	Upper Bound
DMPRCA	1. Less than high school diploma	2	0.33	0.05	0.04	-0.12	0.79
	2. High school diploma or equivalent	18	0.29	0.19	0.04	0.20	0.39
	3. Some college, no degree	26	0.22	0.17	0.03	0.15	0.28
	4. Associate degree	21	0.28	0.14	0.03	0.21	0.34
	5. Bachelor's degree	80	0.27	0.15	0.02	0.24	0.31
	6. MBA or master's degree	61	0.32	0.15	0.02	0.28	0.36
	7. Professional or doctoral degree	8	0.25	0.14	0.05	0.13	0.37
	Total	216	0.28	0.16	0.01	0.26	0.30

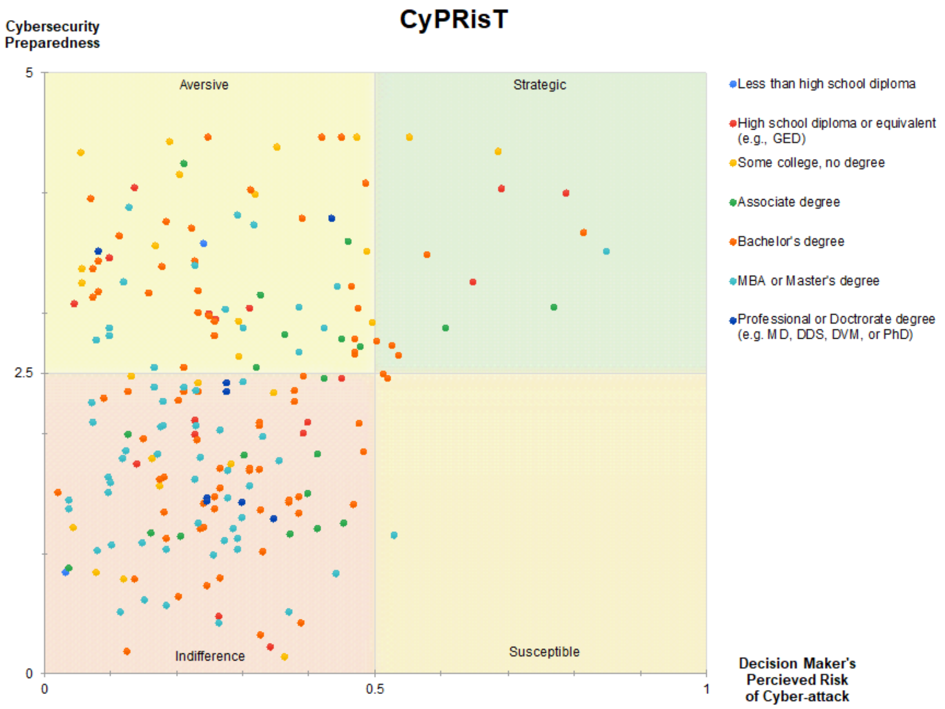


Figure 43. CyPRisT by Education (N=216)

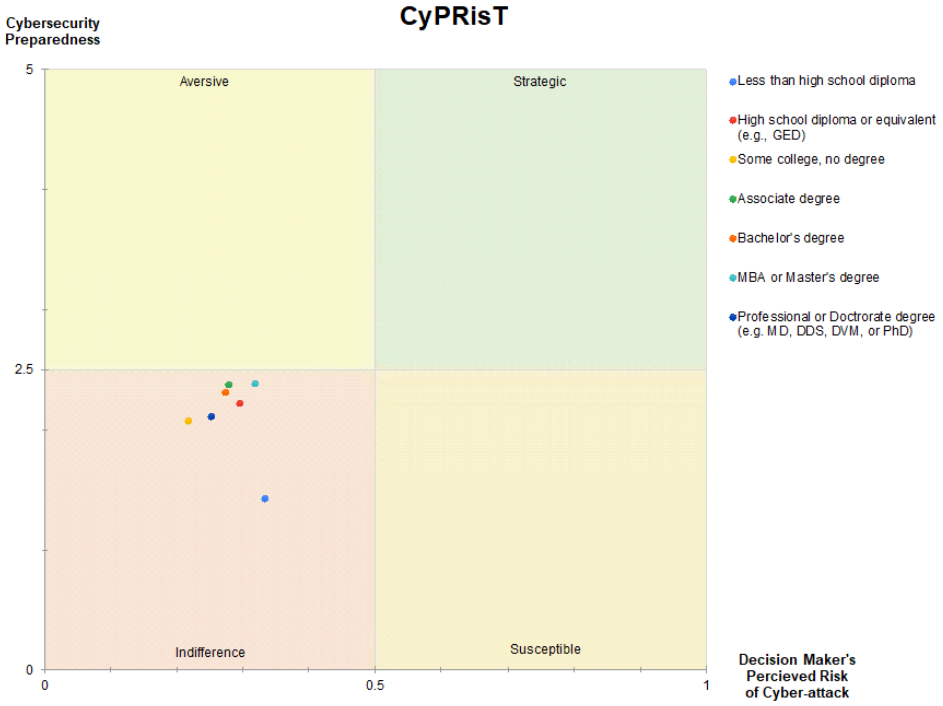


Figure 44. CyPRisT by Mean of Education (N=216)

Table 33 summarizes the results of the one-way ANOVA to determine whether there were significant differences between the CPSs and DMPRCA of the small businesses based on the participant's education level. The results of the one-way ANOVA showed that there were no significant differences in both the CPSs (*F*(6, 209) = 0.54, *p* = 0.77) and DMPRCA (*F*(6, 209) = 1.42, *p* = 0.21) for participant's education level since the *p*-values of the *F*-test were greater than the level of significance of 0.05. The mean plots graphically showed that the CPSs (Figure 45) and DMPRCA (Figure 46) were not significantly different by the participant's education level.

Table 33

ANOVA Results of Difference in CPSs and DMPRCA by Education (N=216)

		Sum of Squares	**df**	**Mean Square**	**F**	**Sig.**
CPSs	Between Groups	3.73	6	0.62	0.54	0.774
	Within Groups	238.93	209	1.14		
	Total	242.67	215			
DMPRCA	Between Groups	0.21	6	0.03	1.42	0.209
	Within Groups	5.10	209	0.02		
	Total	5.31	215			

* p <.05, ** p <.01, *** p <.001

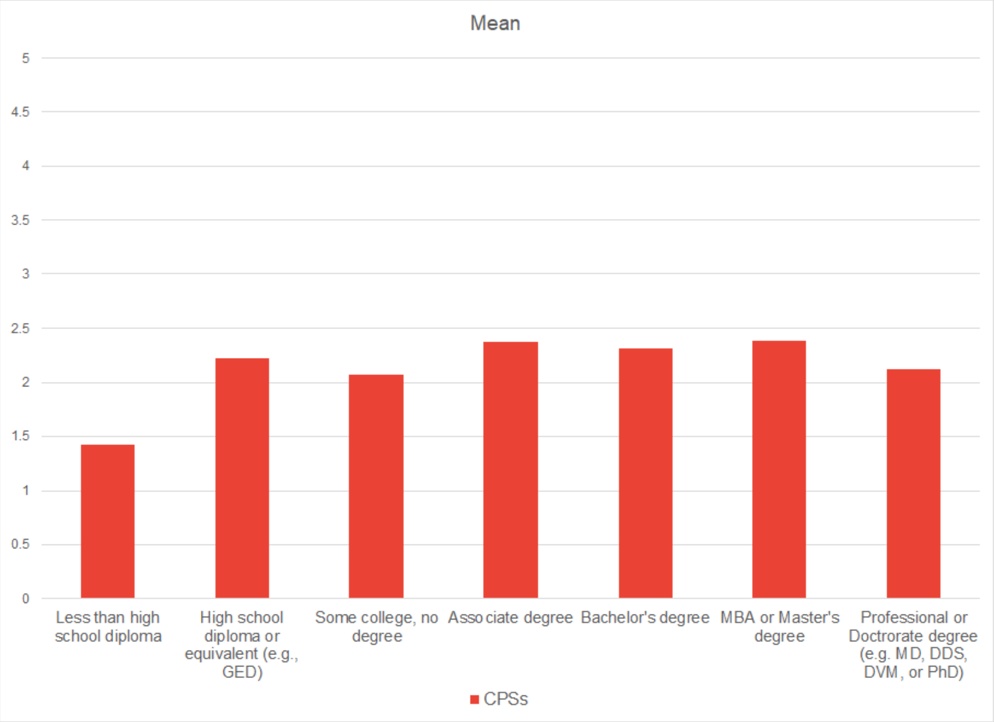


Figure 45. CPSs by Mean of Education (N=216)

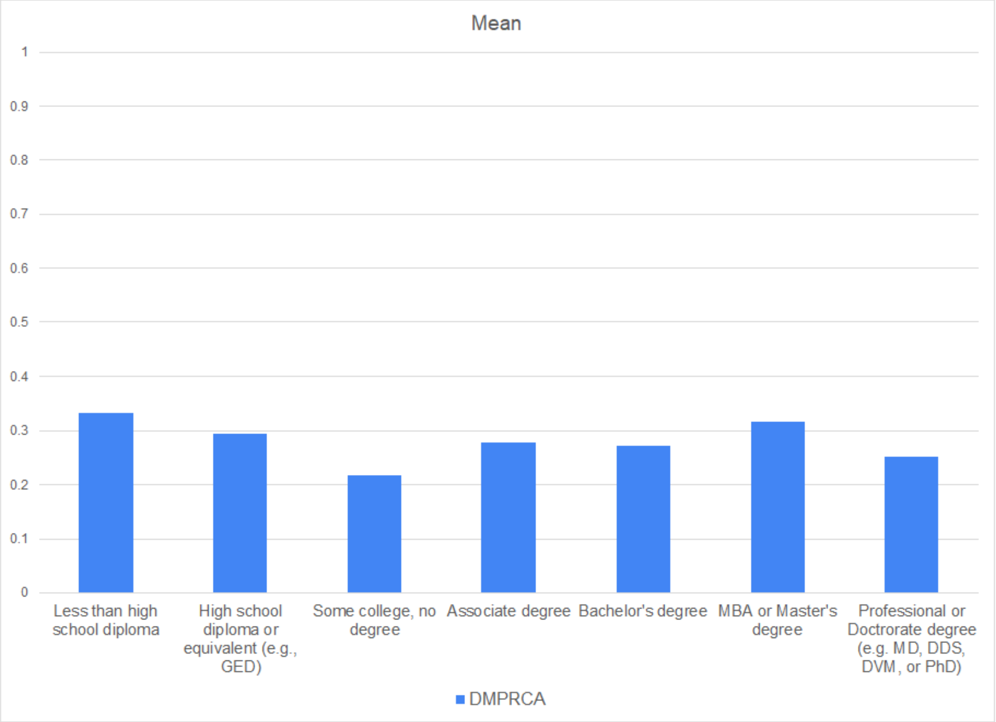


Figure 46. DMPRCA by Mean of Education (N=216)

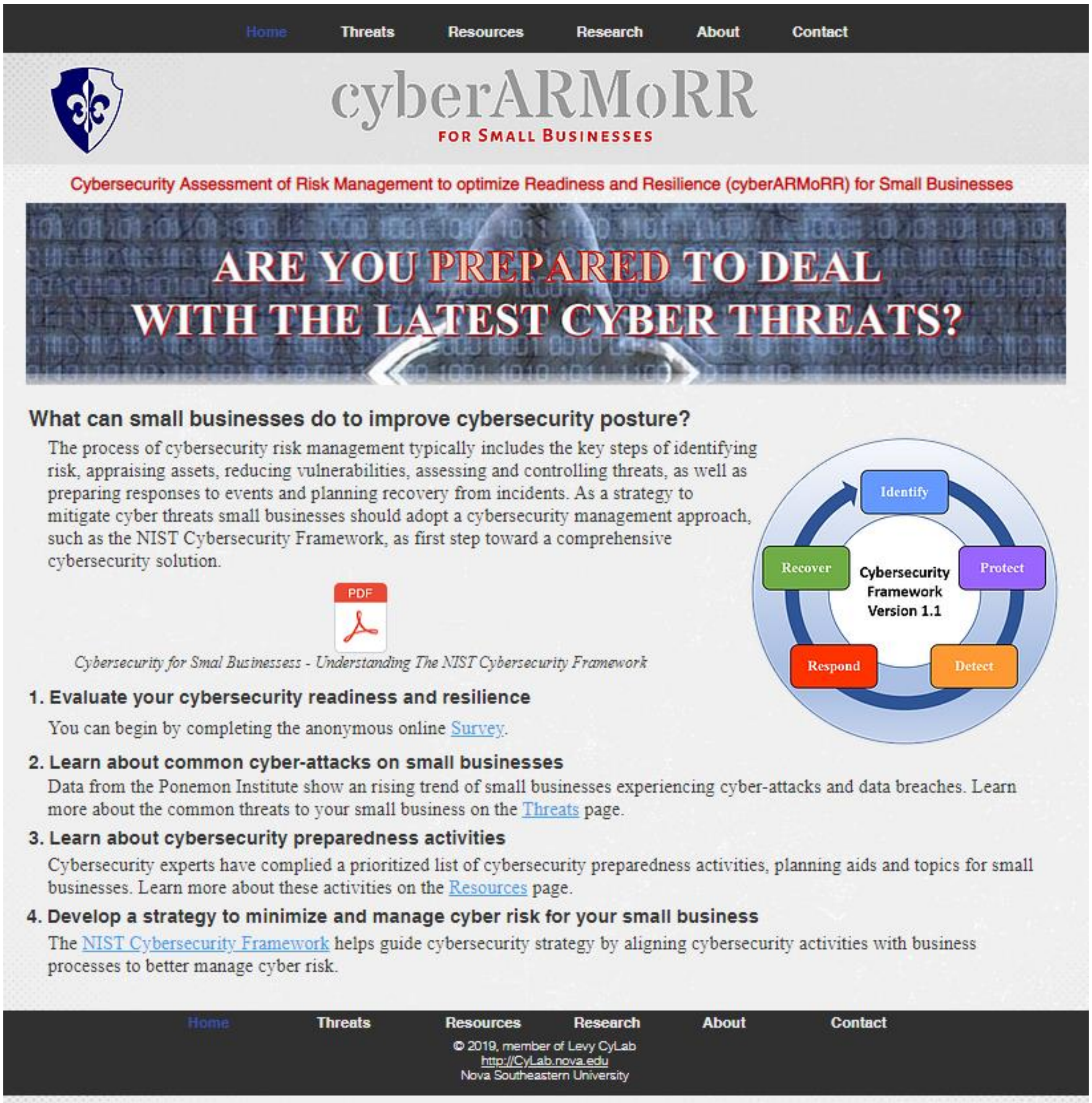
Phase 3 – Quasi-Experiment

A quasi-experimental study was conducted to evaluate pretest-posttest results after their participation in the cyberARMoRR program for small businesses. To answer RQ6, RQ7, and RQ8, data were collected from a subgroup of the sample population of small business decision makers. First, a quantitative analysis of the pretest and posttest measures were used to identify difference's in the CPSs and DMPRCA. A qualitative analysis was then completed for the cybersecurity preparedness activities that were implemented after participation in the cyberARMoRR program for small businesses. To conclude Phase 3 of this study, is a qualitative analysis of the participant's decision to implement cybersecurity preparedness activities.

The cyberARMoRR Program and Pilot

The cyberARMoRR program was developed using the topics that were approved by the cybersecurity SMEs during Phase 1 of this research study. Figure 47 presents the website home page that were provided to the participants. An overview of the program consisted of a high-level explanation of the NIST Cybersecurity Framework (NIST, 2018), general guidance on how to incorporate the framework as a security program for small businesses, resources and guides, as well as select case samples for adoption. Participants were introduced to the 10 common threats to small businesses (Ponemon Institute, 2018) and the SME descriptions. Additionally, the cybersecurity preparedness activities were explained as part of the fundamentals for adopting the NIST Cybersecurity Framework (Paulsen & Toth, 2016). Resources were provided for the common cyber threats (see Appendix I) as well as the five functions of the NIST cybersecurity framework (see Appendix J). The resources were mapped by cybersecurity preparedness activity and aligned to the appropriate framework function according to the primary content of subject matter.

A pilot of the cyberARMoRR program for small businesses and website was provided to three small business owner participants. The initial feedback received from the owners were used to modify the design layout, organization and delivery of the program. Semi-structured interviews were completed after the program was finalized for this study. The participant interview questions to address RQ7 and RQ8 as well as solicitation of further enhancements that could be made to the cyberARMoRR program.



Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) for Small Businesses

What can small businesses do to improve cybersecurity posture?

The process of cybersecurity risk management typically includes the key steps of identifying risk, appraising assets, reducing vulnerabilities, assessing and controlling threats, as well as preparing responses to events and planning recovery from incidents. As a strategy to mitigate cyber threats small businesses should adopt a cybersecurity management approach, such as the NIST Cybersecurity Framework, as first step toward a comprehensive cybersecurity solution.

Cybersecurity for Smal Businessess - Understanding The NIST Cybersecurity Framework

1. Evaluate your cybersecurity readiness and resilience

You can begin by completing the anonymous online Survey.

2. Learn about common cyber-attacks on small businesses

Data from the Ponemon Institute show an rising trend of small businesses experiencing cyber-attacks and data breaches. Learn more about the common threats to your small business on the Threats page.

3. Learn about cybersecurity preparedness activities

Cybersecurity experts have complied a prioritized list of cybersecurity preparedness activities, planning aids and topics for small businesses. Learn more about these activities on the Resources page.

4. Develop a strategy to minimize and manage cyber risk for your small business

The NIST Cybersecurity Framework helps guide cybersecurity strategy by aligning cybersecurity activities with business processes to better manage cyber risk.

© 2019, member of Levy CyLab
http://CyLab.nova.edu
Nova Southeastern University

Figure 47. *The Cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) for Small Businesses Program, website www.cyberarmorr.org*

Phase 3 – Data Collection

Data collection occurred between October 2019 and November 2019. A Google Form was used to present the survey instrument as a posttest measure (see Appendix K). A total of 50 survey responses were received and 15 semi-structured interviews were conducted with participants during the time period. The data collection and analysis for Phase 3 included the same Phase 1 measures for the CPSs and DMPRCA, in addition to open-ended questions about the challenges of the cybersecurity preparedness activities for each function of the NIST Cybersecurity Framework.

Phase 3 – Data Analysis (Quantitative)

For RQ6, the CaseIDs from the posttest sample were used to filter pretest responses to ensure that results of the quasi-experiment were compared to the corresponding pretest sample data. The results for the pretest and posttest were analyzed using a paired sample t-test to compare the calculated means and determine if statistically significant differences exist in the dependent variables (Mertler & Reinhart, 2017). Thus, the results for the pretest and posttest were grouped representing the before and after participation in the cyberARMoRR program for small businesses, respectively. The result of the paired sample t-test indicated that there were no significant differences between the groups. Although, there was an observed increase in both the CPSs and DMPRCA that moved the position toward the ‘aversive’ quadrant of the CyPRisT. Table 34 shows the means, standard deviation of the CPSs and DMPRCA as well as the paired sample means of the pretest and posttest. Figure 48 presents the CyPRisT by mean for pretest (blue) and posttest (red). The result of the paired means t-test are presented in Figure 49 for the CPSs, and Figure 50 for the DMPRCA.

Table 34

Pretest-Posttest Group Statistics of CPSs and DMPRCA (n=50)

	CPSs		**DMPRCA**		**Paired Means**	
	Mean	**SD**	**Mean**	**SD**	**t**	**Sig.**
Pretest	2.26	1.13	0.28	0.13	-0.835	.406
Posttest	2.45	1.09	0.33	0.12	-1.783	.078

* p <.05, ** p <.01, *** p <.001

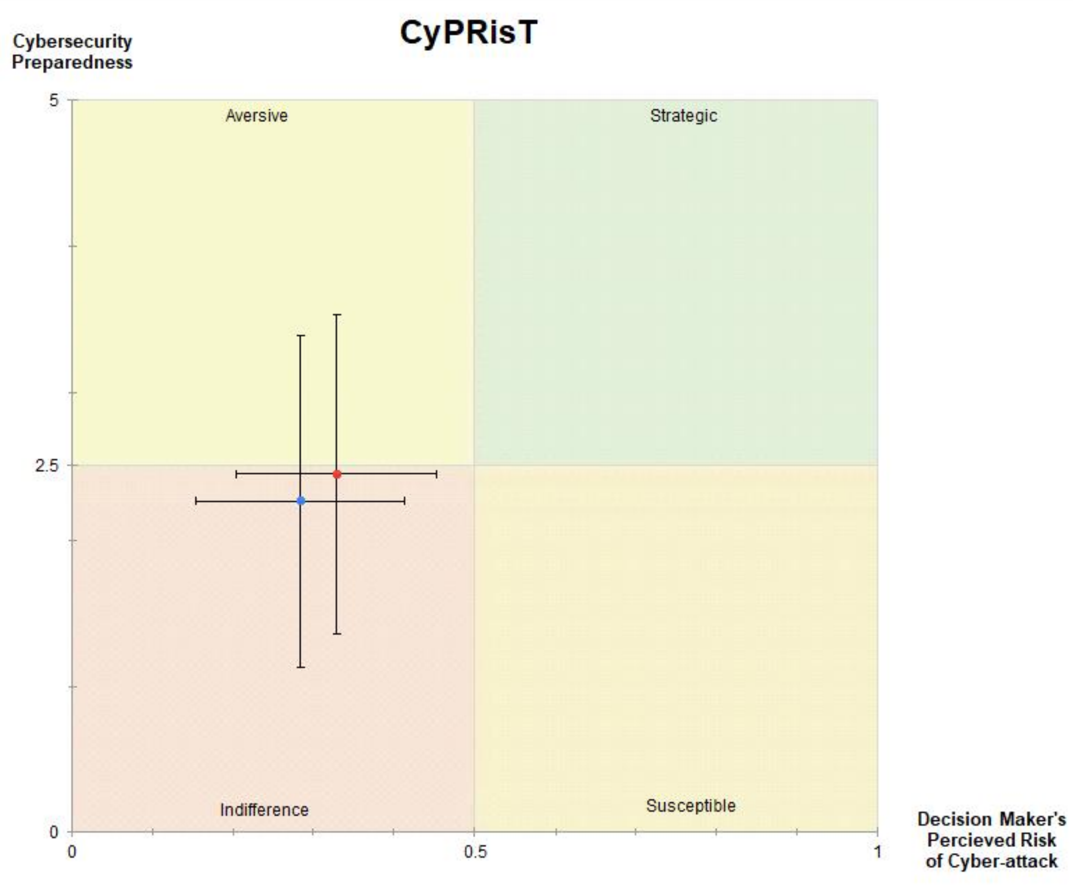


Figure 48. CyPRisT Pretest and Posttest Mean Score and Std.Dev. Intervals (n=50)

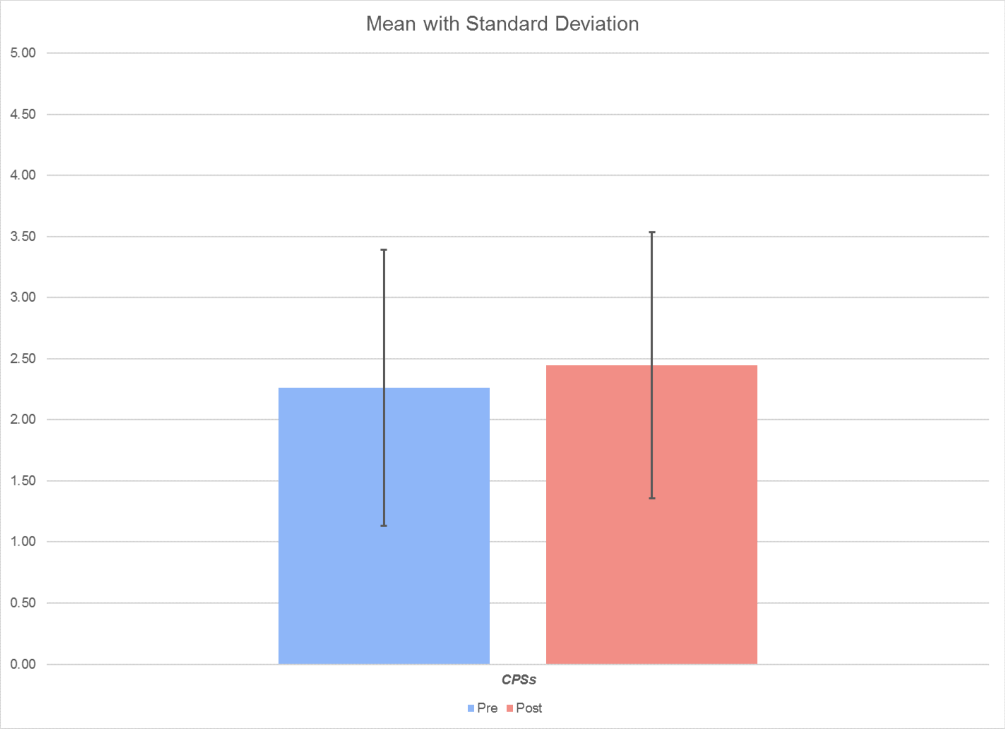


Figure 49. Pretest and Posttest Mean Score of CPS (n=50)

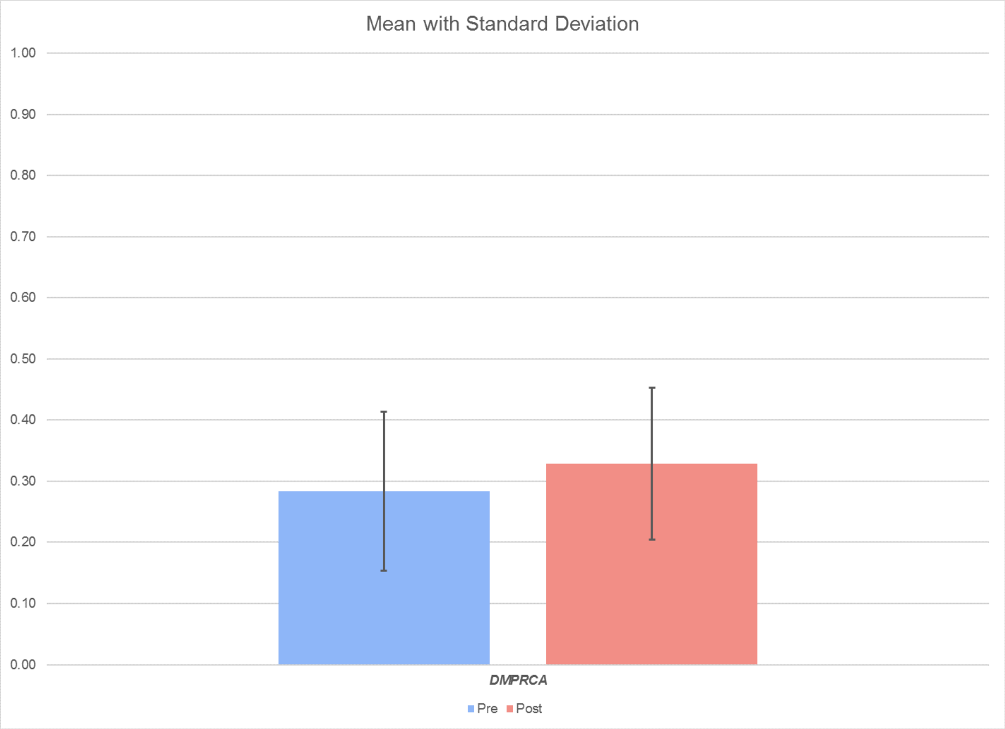


Figure 50. Pretest and Posttest Mean Score of DMPRCA (n=50)

For RQ7, the pretest and posttest data were compared to identify the cybersecurity preparedness activities that small business decision makers responded they have implemented after participation in cyberARMoRR program for small businesses. The changes in participant increased the CPSs and DMPRCA. Table 35 shows the most changed cybersecurity preparedness activities by function of the NIST Cybersecurity Framework, ranked in order of high to low. Conversely, Table 36 shows the least changed responses of cybersecurity preparedness activities by function of the NIST Cybersecurity Framework, ranked in order low to high.

Table 35

Most Changed Cybersecurity Preparedness Activities by Functions of the NIST Cybersecurity Framework (n=50)

Function	**Cybersecurity Preparedness Activities**
Identity	1. [ID9] Maintain an inventory of technology assets
	2. [ID12] Assign risk values to information resources
	3. [ID11] Develop a cybersecurity risk management strategy
	4. [ID3] Allocate a budget specifically for cybersecurity
Protect	1. [PR1] Regularly patch operating systems and applications, at least monthly
	2. [PR10] Protect information assets from physical intrusion
	3. [PR20] Safely dispose of old computers and media by scrubbing information from drives
	4. [PR11] Enforce password management
Detect	1. [DE2] Update anti-virus software, at least daily
	2. [DE6] Perform vulnerability assessments, at least quarterly
	3. [DE9] Maintain and analyze cybersecurity event logs
Respond	1. [RS9] Have the ability to quickly stop or contain a cyber-attack
	2. [RS4] Have an incident response plan with established roles and responsibilities
	3. [RS1] Require training for employees to recognize cybersecurity events
Recover	1. [RC2] Routinely backup essential computers and servers, at least monthly
	2. [RC8] Make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly
	3. [RC7] Review backup processes / procedures / technologies, at least twice a year

Table 36

Least Changed Cybersecurity Preparedness Activities by Function of the NIST Cybersecurity Framework (n=50)

Function	Cybersecurity Preparedness Activities
Identity	1. [ID19] Identify cyber supply chain risks associated with the products and services that it provides and uses 2. [ID20] Require service level agreements (SLAs) with technology service providers 3. [ID17] Conduct cybersecurity gap analysis to determine what controls need to be implemented
Protect	1. [PR4] Have an insider threat management program 2. [PR12] Use multi-factor authentication 3. [PR5] Use encryption for sensitive information
Detect	1. [DE5] Baseline network utilization and detect anomalies in traffic patterns 2. [DE4] Use an intrusion detection and prevention system 3. [DE7] Perform test procedures at discrete intervals to identify cybersecurity events
Respond	1. [RS10] Have the ability to collect digital forensic data about a cyber-attack or data breach 2. [RS6] Coordinate cyber incident response activities with internal stakeholders or external organizations 3. [RS8] Test disaster recovery / business continuity plan, at least annually.
Recover	1. [RC6] Conduct mock exercises to test for failure of technology resources 2. [RC5] Coordinate restoration activities with internal stakeholders or external stakeholders 3. [RC9] Train employees on data breach reporting requirements for compliance with federal/state and industry regulations.

DMPRCA were evaluated to determine what changes by perceived likelihood and perceived impact responses. Table 37 shows the most changed perceived risk after participation in the cyberARMoRR program for small businesses, ranked in order of high to low. Conversely, Table 38 shows the least changed perceived risk after participation in the cyberARMoRR program for small businesses, ranked in order of low to high.

Table 37

Most Changed Perceived Risk of Cyber-attack (n=50)

Construct	**Cyber-attack category**
Perceived Likelihood	1. [PL7] Phishing / social engineering
	2. [PL6] Malicious insider
	3. [PL1] General malware
	4. [PL3] Compromised / stolen devices
	5. [PL2] Advanced malware / zero-day attack
Perceived Impact	1. [PI7] Phishing / social engineering
	2. [PI3] Compromised / stolen devices
	3. [PI6] Malicious insider
	4. [PI2] Advanced malware / zero-day attack
	5. [PI1] General malware

Table 38

Least Changed Perceived Risk of Cyber-attack (n=50)

Construct	**Cyber-attack category**
Perceived Likelihood	1. [PL8] SQL injection
	2. [PL5] Denial of services
	3. [PL9] Web-based attack
	4. [PL4] Cross-site scripting
	5. [PL10] Other cyber-attack
Perceived Impact	1. [PI5] Denial of services
	2. [PI9] Web-based attack
	3. [PI8] SQL injection
	4. [PI10] Other cyber-attack
	5. [PI4] Cross-site scripting

Phase 3 – Data Analysis (Qualitative)

For RQ8, five sources of data were used to analyze what cybersecurity preparedness activities were most challenging for small businesses to implement and why. The first data source was the frequency of 'No' responses to the cybersecurity preparedness activities for the sample population of small business collected during Phase 2 (N=216). The second data source was the frequency of 'No' responses to the cybersecurity preparedness activities for the subgroup population collected (n=50). The third data source was the amount of change between the pretest and posttest measures. The fourth was the open-ended question on the posttest for each of the functions. The fifth data source were notes taken from the semi-structured interviews (n=15).

The goal of data analysis in qualitative research is to generate interpretative explanations from the data collected based on categories and themes that are developed into patterns (Creswell, 2014). Guided by Saldaña's (2013) coding manual, a two-cycle coding process was used for the data analysis. For the first cycle, a magnitude coding process was used to differentiate the cybersecurity preparedness activities with frequent 'No' responses, then a descriptive coding process was used for the open-ended survey responses as well as the notes recorded during the semi-structured interviews. For the second cycle, a pattern coding process was used to identify the emergent themes and explanations. The following tables are ordered low (least) to mid. Table 39 shows the least implemented cybersecurity preparedness activities from the Phase 2 sample of small businesses. Table 40 shows the least implemented cybersecurity preparedness activities from the pretest subset sample of small businesses. Table 41 shows the least implemented cybersecurity preparedness activities from the posttest subset sample of small businesses.

Table 39

Least Implemented Cybersecurity Preparedness Activities by Function of the NIST Cybersecurity Framework – Phase 2 (N=216)

Function	**Cybersecurity Preparedness Activities**
Identity	1. [ID3] Allocate a budget specifically for cybersecurity
	2. [ID19] Identify cyber supply chain risks associated with the products and services that it provides and uses
	3. [ID12] Assign risk values to information resources
	4. [ID16] Prioritize actions based on potential impacts of a cybersecurity incident
	5. [ID18] Have a plan for implementing new cybersecurity controls over time
Protect	1. [PR4] Have an insider threat management program
	2. [PR19] Have a data disposal policy
	3. [PR12] Use multi-factor authentication
	4. [PR15] Use web filters
	5. [PR5] Use encryption for sensitive information
Detect	1. [DE4] Use an intrusion detection and prevention system
	2. [DE5] Baseline network utilization and detect anomalies in traffic patterns
	3. [DE6] Maintain and analyze cybersecurity event logs
	4. [DE10] Perform penetration testing, at least annually
	5. [DE7] Perform test procedures at discrete intervals to identify cybersecurity events
Respond	1. [RS6] Coordinate cyber incident response activities with internal stakeholders or external organizations
	2. [RS8] Test disaster recovery / business continuity plan, at least annually
	3. [RS10] Have the ability to collect digital forensic data about a cyber-attack or data breach
	4. [RS4] Have an incident response plan with established roles and responsibilities
	5. [RS5] Review incident response procedures, at least annually
Recover	1. [RC6] Conduct mock exercises to test for failure of technology resources
	2. [RC10] Have cyber insurance
	3. [RC8] Make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly
	4. [RC5] Coordinate restoration activities with internal stakeholders or external stakeholders
	5. [RC9] Train employees on data breach reporting requirements for compliance with federal/state and industry regulations

Table 40

Least Implemented Cybersecurity Preparedness Activities by Function of the NIST Cybersecurity Framework – Pretest Subgroup (n=50)

Function	**Cybersecurity Preparedness Activities**
Identity	1. [ID3] Allocate a budget specifically for cybersecurity
	2. [ID19] Identify cyber supply chain risks associated with the products and services
	3. [ID16] Prioritize actions based on potential impacts of a cybersecurity incident
	4. [ID18] Have a plan for implementing new cybersecurity controls over time
	5. [ID1] Use a framework to manage cybersecurity
Protect	1. [PR4] Have an insider threat management program
	2. [PR19] Have a data disposal policy
	3. [PR12] Use multi-factor authentication
	4. [PR5] Use encryption for sensitive information
	5. [PR14] Educate employees about social engineering and phishing scams
Detect	1. [DE5] Baseline network utilization and detect anomalies in traffic patterns
	2. [DE4] Use an intrusion detection and prevention system
	3. [DE9] Perform vulnerability assessments, at least quarterly
	4. [DE7] Perform test procedures at discrete intervals to identify cybersecurity events
	10. [DE10] Perform penetration testing, at least annually
Respond	1. [RS10] Have the ability to collect digital forensic data about a cyber-attack or data breach
	2. [RS6] Coordinate cyber incident response activities with internal stakeholders or external organizations
	3. [RS8] Test disaster recovery / business continuity plan, at least annually
	4. [RS4] Have an incident response plan with established roles and responsibilities
	5. [RS7] Have a disaster recovery / business continuity plan
Recover	1. [RC8] Make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly
	2. [RC6] Conduct mock exercises to test for failure of technology resources
	3. [RC5] Coordinate restoration activities with internal stakeholders or external stakeholders
	4. [RC10] Have cyber insurance
	5. [RC9] Train employees on data breach reporting requirements for compliance with federal/state and industry regulations

Table 41

Least Implemented Cybersecurity Preparedness Activities by Function of NIST Cybersecurity Framework – Posttest Subgroup (n=50)

Function	Cybersecurity Preparedness Activities
Identity	1. [ID19] Identify cyber supply chain risks associated with the products and services
	2. [ID3] Allocate a budget specifically for cybersecurity
	3. [ID16] Prioritize actions based on potential impacts of a cybersecurity incident
	4. [ID18] Have a plan for implementing new cybersecurity controls over time
	5. [ID20] Require service level agreements with technology service providers
Protect	1. [PR4] Have an insider threat management program
	2. [PR19] Have a data disposal policy
	3. [PR12] Use multi-factor authentication
	4. [PR5] Use encryption for sensitive information
	5. [PR15] Educate employees about social engineering and phishing scams
Detect	1. [DE5] Baseline network utilization and detect anomalies in traffic patterns
	2. [DE4] Use an intrusion detection and prevention system
	3. [DE7] Perform test procedures at discrete intervals to identify cybersecurity events
	4. [DE9] Perform vulnerability assessments, at least quarterly
	5. [DE10] Perform penetration testing, at least annually
Respond	1. [RS10] Have the ability to collect digital forensic data about a cyber-attack or data breach
	2. [RS6] Coordinate cyber incident response activities with internal stakeholders or external organizations
	3. [RS8] Test disaster recovery / business continuity plan, at least annually
	4. [RS4] Have an incident response plan with established roles and responsibilities
	5. [RS7] Have a disaster recovery / business continuity plan
Recover	1. [RC6] Conduct mock exercises to test for failure of technology resources
	2. [RC8] Make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly
	3. [RC5] Coordinate restoration activities with internal stakeholders or external stakeholders
	4. [RC10] Have cyber insurance
	5. [RC9] Train employees on data breach reporting requirements for compliance with federal/state and industry regulations

The cyber preparedness activities were coded by magnitude of improved (+) or challenging (-) according the frequency of 'Yes' or 'No' responses, respectively. Descriptive reason codes, such as resources, time, and education, were assigned to the most challenging cyber preparedness activities as well as the participant's explanation of the challenge (BBB, 2017). The codes were assigned using the "text clouds" technique in Microsoft Word following the suggested manual coding process of Chenail (2012) (see Appendix L). The first cycle involved coding the values of the cyber preparedness activities into categories for the open-ended survey questions and semi-structure interview responses. The categories of the combined responses were evaluated using thematic analysis in the second cycle to confirm the patterns (Creswell, 2014; Saldaña, 2013). Cybersecurity benchmark reports, as well as cybersecurity researchers, have found the primary reasons limiting the ability of small businesses to improve their cybersecurity posture were lack of time, cyber-education, and resources (BBB, 2017; Hess & Cottrell, 2015; Osborn & Simpson, 2015; Paulsen, 2016). Therefore, the a priori themes of Time, Education, and Resources were adopted for the analysis.

Figure 51 presents the themes and categories of the qualitative analysis that led to changes in the CPSs of the small business or challenges expressed why changes were not made. The theme of education includes categories of knowledge, applicability, and experience that contributed to the participants perceived risk of cyber-attacks. The theme of resources includes a category for materials for training and guidance, technology, costs, expertise. The resource theme of time is distinct because of the general time-demand to focus on the cybersecurity preparedness activities. Hence, the themes signify a function of the overall cybersecurity posture and ability of the small business decision maker to strategically balance cybersecurity readiness and resilience (Baskerville et al., 2014; Hiscox, 2017). Furthermore, the analysis helps explain what cybersecurity preparedness activities were most challenging for small businesses and why. The participants commonly indicated that the cybersecurity preparedness activities were most challenging when the training/guidance was unclear which made it difficult to comprehend (gain knowledge), the technologies did not apply to their small business or was too advanced/expensive, that they possess the technical/experience, or they needed to focus on the business operations over cybersecurity. In most cases there were several reasons given – not just a single reason. Also, many decision makers indicated that they delegated the responsibility of cybersecurity to their IT specialist or an external service provider when the resource was available.

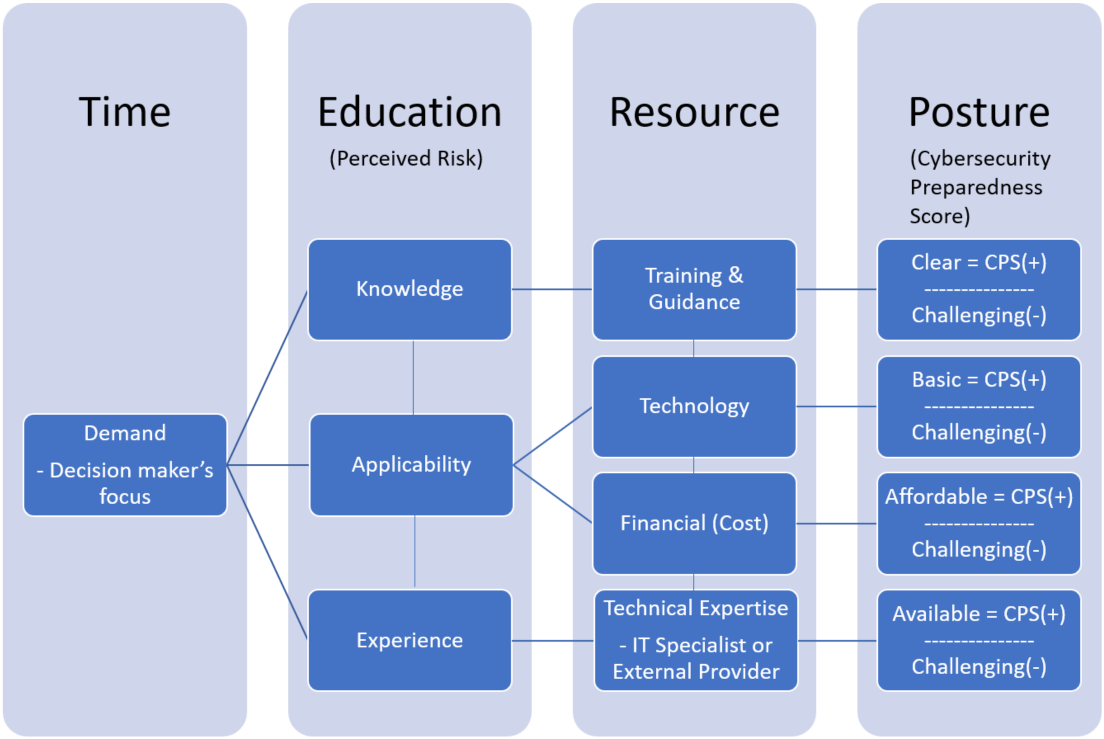


Figure 51. Qualitative Analysis – Themes and Categories of Cybersecurity Preparedness Activities

Summary

The results of the data collection and data analysis were presented by phase. In Phase 1, a panel of SMEs were used to address RQ1, RQ2, and RQ3. In Phase 2 a sequential exploratory study was conducted to address RQ4 and RQ5. In Phase 3, a quasi-experimental study was conducted to address RQ6, RQ7, and RQ8.

The results of Phase 1 were presented for the Delphi surveys. The SMEs had validated a set of cybersecurity preparedness activities that were based on the five functions of the NIST Cybersecurity Framework. The SMEs also provided weights for the cybersecurity preparedness activities and approved a set of cyber-attacks that are common threats to small businesses. The set of cybersecurity preparedness activities, and their weighted values, were used for a benchmark CPSs. The set of common threats, and their descriptions, were used for the measure of DMPRCA.

The results of Phase 2 were presented to show how small businesses are positioned on the CyPRisT using the CPSs and the DMPRCA. Further statistical analysis was conducted on the business demographic data of industry, number of employees, years in operation, annual revenue, IT budget as well as the participants demographic data of role, age, gender, and education. The results showed that there was a significant difference in both CPSs and DMPRCA when compared by industry, number of employees, and IT budget. There was a significant difference in the CPSs but not DMPRCA when compared by years in operation. There were no significant differences found in CPSs and DMPRCA when compared by annual revenue, role, age, gender, and education. The results also show how each demographic category were position on the CyPRisT.

The results of Phase 3 were presented to show differences in cybersecurity posture before and after participation in the cyberARMoRR program for small businesses. A sample of 50 small business participants were used in the analysis. Although the mean score was not statistically different, there was an observable uptick in both the CPSs and DMPRCA. The thematic analysis of the participant responses describing the challenges of cybersecurity preparedness activities suggest that decision makers are more likely to improve their ability to mitigate cyber threats when resources are easy to comprehend, applicable technologies are uncomplicated and reasonably priced, technical expertise is obtainable, and does not demand a substantial amount of time.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Overview

This chapter presents conclusions drawn from the data analysis and results. The findings and contribution to the body of knowledge within the IS field of study are discussed per the dissertation goals. The implications to practice and research are provided as well as recommendations for future research. Finally, the chapter summary section concludes this dissertation report with a synopsis of the research problem, the main goal of this study, a review of the research questions, the research methodology, and a summation of the findings and contribution.

Conclusions

Small business decision makers should strive to achieve a strategically balanced cybersecurity posture that considers both cyber readiness and resilience. This posture includes being prepared to minimize and manage risk as well as having the ability to maintain business operations during and after a cyber-attack (Bodeau & Graubart, 2017; Hurley, et al., 2014). If a small business is not prepared to deal with cyber threats it can be costly when a cyber-attack or data breach occurs (Ponemon, 2018). Considering the rising trend of cyber-attacks and the impacts on small businesses, it is imperative that small businesses overcome their limited ability to mitigate cyber threats. The decision to improve the cybersecurity posture of a small business can significantly reduce the risk of disruption and loss.

Among the top challenges that small businesses decision makers must overcome in order to improve their cybersecurity posture are knowing what to protect and the common cyber threats (Berry & Berry, 2018; Osborn & Simpson, 2018; Paulsen, 2016). The cybersecurity preparedness activities, as guided by the NIST Cybersecurity Framework (NIST, 2018), are fundamentally useful resources for small business owners and managers to consider adopting into their routine business processes (Paulsen & Toth, 2016). The information can help develop or enhance resources to assist small businesses achieve a balance of cyber threat prevention and cyber-attack response strategies (Baskerville et al., 2014; Berry & Berry, 2018).

The U.S. government and non-profit organizations are taking the initial steps to address limited availability of cybersecurity product materials as well as risk management programs that are tailored to meet the needs of the small businesses (Berry & Berry, 2018). While conducting this research study, in fall 2019, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) released their *Cyber Essentials* guide for leaders of small businesses that provided recommendations for how to build a culture of cyber readiness (CISA, n.d.). The recommended actions appeared to be consistent with the cyber preparedness activities. Specific examples include developing a strategy for cyber activities to preparing for cyber-attacks, backing up data, patch and application update management, as well as responding and recovering from compromise (data-breach). The NIST *Small Business Cybersecurity Corner* (NIST, n.d.-b) and the NCSA's *StaySafeOnline* and *Stop.Think.Connect* resource libraries (NCSA, n.d.) are reliable sources of online free resources directed toward small business leaders. The NIST and NCSA publish articles and videos specifically aimed at helping small business. The NCSA also conducts training seminars, called *Cybersecure MyBusiness,* across the country for small business leaders. The workshops, monthly webinars, and expert discussion panels help educate the small business community on the NIST Cybersecurity Framework (NCSA, n.d.).

Discussion

This research study explored the relationship between two constructs associated with cybersecurity readiness and resilience of small businesses. Paulsen (2016) as well as Osborn and Simpson (2018) argued that small businesses were high risk for systems compromise because owners did not know what to protect. To address this issue, cybersecurity resources, educational materials and tools, for minimizing the vulnerabilities of small businesses are being developed. Cybersecurity guidance, such as the NIST Cybersecurity Framework (NIST, 2018), can help small businesses improve cybersecurity posture by informing what cybersecurity preparedness activities to perform. Furthermore, a well-balanced cybersecurity program can help small businesses develop a strategy for improving their cybersecurity risk management. Complimentary cybersecurity educational materials and guidance should help increase knowledge and awareness for interested small business decision makers. Uncomplicated, or easy to follow, guidance as well as simple cybersecurity tools should help those small businesses with limited technical experience to overcome the time demands. Part of the effort, and one of the goals of this research study was to identify the essential cybersecurity preparedness activities within the NIST Cybersecurity Framework guidance to assess the level of cybersecurity preparedness for a small business.

The SMEs approved a set of cybersecurity preparedness activities that represent the recommended fundamental procedures, practices, and policies for small businesses (Paulsen & Toth, 2016). Rohn et al. (2016) suggested that small business owners lacked commensurate action in cybersecurity because the decision makers were underestimating risk of cyber-attack and limited in their ability probabilities and impact. Thus, the SMEs also approved a set of common cyber threats with descriptions that provided the businesses decision makers a point of reference to the top cyber-attacks on small businesses from actual reported data and trends (Ponemon Institute, 2016, 1017, 2018).

Berry and Berry (2018) suggested that differences in the perception of common cyber threats to small businesses were likely related to their lack of mitigating cyber risk. Accordingly, a research instrument was developed, and validated by SMEs, consisting of cybersecurity preparedness activities within the five functions of the NIST Cybersecurity Framework as well as 10 categories of common cyber-attack vectors that threaten small businesses. The SMEs assigned weights to the cybersecurity preparedness activities that enabled an aggregated benchmark score for the small businesses. The Ponemon Institute (2016, 2017, 2018) cyber-attack categories were used to provide familiarity to the small business decision maker as a frame of reference to the cyber threats. The SMEs also approved basic descriptions for the 10 common threat vectors to measure the small business decision makers’ perceived likelihood and perceived impact following the process of Sumner (2009) to calculate the perceived risk of cyber-attack.

The set of 70 SMEs approved cybersecurity preparedness activities within the five functions of the NIST Cybersecurity Framework were then used to empirically assess the level of cybersecurity preparedness of small businesses according to their risk perception. A CyPRisT taxonomy was proposed to assess the benchmark scores cybersecurity posture level positions of the small businesses. The CPSs, and DMPRCA were positioned on the CyPRisT for a sample of 216 small businesses having 10-49 full-time employees. Statistical differences were found in CPSs and DMPRCA for the demographic categories of industry, number of employees, and IT budget. Yet, only the CPSs were statistically different among the categories of years in operation. This finding suggests that cybersecurity guidance may be enhanced further by developing resources that target specific industry focus or taking into consideration the smaller sizes as well as limited budgets for smaller size businesses. The statistical difference in CPSs suggest that small businesses may focus on cybersecurity processes in early years, then move toward status quo biases as the focus shifts from startup infrastructure investment to routine business operations. It is suspected that the trend follows major technology innovations and business markets. Therefore, additional research is recommended on the cybersecurity cycles of small businesses over an extended period.

The statistical differences in industry is likely due to the nature of business and information exchange that are associated with each industry focus. For example, the highest CPSs were small businesses in communications, entertainment, media, and publishing; information technology and software; and construction and real estate. These small businesses industries generally involve the protection of intellectual property as well as protection of sensitive information that may be governed by regulations and law.

The highest DMPRCA were those in banking & financial services; information technology & software, education and research. The small businesses in those industries are often targeted by cybercriminals, and among the more sophisticated attacks, because of their information assets (Ponemon Institute, 2018). An example is financial institution data such as bank account numbers and login information (Hayes et al., 2012). A reasonable assumption is that IT and software small businesses have high CPSs as well as DMPRCA because the technical nature of their business and knowledge of cyber threats.

The lowest CPSs were small businesses in transportation; agriculture and food services; and retail. While the lowest DMPRCA were small business in transportation; warehousing, logistics, and distribution; and agriculture and food services. This suggests that these small businesses may be less technology dependent or may have stronger focus on their products and services. However, there were limited responses for these industries per the sample size. This appears to be a challenge with many small business studies and cybersecurity reports. For example, the Verizon DBIR (Verizon Enterprise, 2018), there were 0 results from small businesses in agriculture, and single digit results from real estate, transportation, energy and utilities. Another example can be drawn from the Ponemon Institute (2018) report where a sample of 383 had 2% or less in five of the industry categories. The limitation for business demographics, particularly in the industry focus, was expected because of the smaller percentage of registered small businesses within these categories (U.S. Census Bureau, 2015). Thus, future research is recommended to investigate the cybersecurity preparedness activities and perceived risk of cyber-attack for these underrepresented industries.

In IS research, social theories have been used to explain the lack of security controls among small businesses and their limited ability to improve their cybersecurity posture (Rohn et al., 2016). Applying the theoretical lens of prospect theory and status quo bias (Kahneman & Tversky, 1979; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992), provides insight into the relation between perceived risk and actual cybersecurity preparedness activities of the sample small businesses. The CyPRisT was developed for the assessment of cybersecurity postures of small businesses. The quadrants are based on the heuristics for risk perception and using decision weights inspired by cumulative prospect theory as well as status quo bias.

The bottom left quadrant of the CyPRisT represented small businesses that are *Indifferent*, low DMPRCA and low CPSs. Indifference can be used to explain the decision maker's unwillingness to abandon the status quo (Polites & Karahanna, 2012). The results of this research study showed that more than half of small businesses were potentially indifferent toward cybersecurity. This finding is consistent with the cybersecurity benchmark reports demonstrating nearly half of small businesses are vulnerable to cyber-attacks (BBB, 2017; Ponemon Institute, 2018; Symantec Corporation, 2018; Verizon Enterprise, 2018). This finding may help explain why approximately half of small businesses remain at risk of loss due to a cyber-attack.

The bottom right quadrant of the CyPRisT represented small businesses that were *Susceptible* to losses, high DMPRCA and low CPSs. Susceptibility, also referred to as risk-seeking behaviors (Liang & Xue, 2009), can help explain the relation between high levels of perceived risk and a low level of cyber preparedness. The results of this study showed that few small businesses exhibited risk-seeking cybersecurity postures. This finding suggests that small business decision maker's awareness of cyber threats and potential loss may motivate action toward mitigating cyber threats through the essential cybersecurity preparedness activities.

The top left quadrant of the CyPRisT represented a risk *Aversive* posture, low DMPRCA and high CPSs. Loss aversion can help explain the effect in relation between rational decision making when the choice to become risk-averse is based on the perceived point of reference for cyber risk and potential loss (Li et al., 2016). The results showed that slightly less than half the small businesses were risk averse. Many of these small businesses implemented the fundamental cybersecurity controls through their IT department, were regulated by their industry (e.g., Banking & Financial Services, Healthcare), and were committed to protecting their customer information (e.g., Hospitality, Construction & Real Estate). This finding suggests that small business decision makers with low perceived risk of cyber-attack were less focused on managing cyber risk.

The top right quadrant of the CyPRisT represented a *Strategic* balance between understanding cyber risk and the security controls necessary for being prepared to deal with cyber-attacks, high DMPRCA and high CPSs. The strategic actions for mitigating threats were based on the biases, judgment and heuristics, found in small business decision maker's need to maintain business continuity when faced with adversity (Osiyevskyy & Dewald, 2015). This finding suggests that a small percentage of small business are taking appropriate action to establish strong cybersecurity posture or exhibiting a high level of cybersecurity situational awareness to achieve an adequate balance between cybersecurity readiness and resilience.

The SME-approved cybersecurity preparedness activities were evaluated along with the perception of cyber risk to assess the decision maker's ability to improve cybersecurity posture of small businesses. For this research study, the cyberARMoRR for small business program was developed into a resource consisting of references to the publicly available resources for small business decision makers (e.g., NIST and NCSA publications). The survey instrument, consisting of cybersecurity preparedness activities and decision maker's perceived risk of cyber-attack, was used for a quasi-experiment (pretest and posttest) measure of small businesses. The quasi-experimental results revealed there were no statistically significant differences in the CPSs as well as the DMPRCA before and after participation in the cyberARMoRR program. The differences did have a variation in responses demonstrated by the standard deviation for the dependent variables. However, there was an observable improvement in the cybersecurity posture for the participants of the cyberARMoRR program. Both CPSs and DMPRA moved toward achieving a strategically balanced approach for managing cyber risk.

The small business owners and managers responded on the specific cybersecurity preparedness activities that were implemented after participation in the cyberARMoRR program. The participants of the 15 semi-structured interviews also described what cybersecurity preparedness activities were most challenging for their small businesses to implement and why. In cases where the perceived risk of cyber-attack was increased in the posttest, the decision makers had taken multiple actions to mitigate cyber risk. The results showed that easy to implement cyber preparedness activities (e.g., allocating a budget for cybersecurity, regularly operating systems and applications, updating-virus software, reviewing backups) slightly helped to improve their cybersecurity posture.

The more challenging cybersecurity preparedness activities were often delegated to IT specialists, or external providers, with advanced technical expertise. The small business decision makers explained that there was not enough time to focus on cybersecurity, they did not possess the knowledge, or they did not consider the technology / cyber risk applicable to their small business. These findings help to explain why many small businesses are underprepared to deal with the cyber risk (Hiscox, 2017; Rohn et al., 2016). The participants that showed improvements to their cybersecurity posture incorporated the cybersecurity preparedness activities into their routine businesses processes as a function of managing their overall business risk.

Paulsen (2016) previously suggested that cybersecurity practices may be tailored by industry because their training and requirements vary on the nature of their business. Additionally, the impact of a cybersecurity event could depend on the industry specific cyber threats (Paulsen & Toth, 2016). The size of the business demographic finding was consistent with extant research (Rohn et al., 2016). The Ponemon Institute (2018) suggested that small businesses not having an adequate budget and expertise were less likely to achieve a strong cybersecurity posture. The results of this study confirmed empirically that the cybersecurity posture, as positioned on the CyPRisT, was not as strong for small businesses with lower budget allocations.

Implications

There are several implications for practice and research. From a practical perspective, the implications of this research study can be used to further develop programs that help small businesses overcome their lack of cybersecurity preparedness and the limited ability deal with cyber-attacks. From a theoretical perspective, the implications are within IS studies relative to social theories in organizational and business management as well as human decision-making processes in areas of phycology and economics. The implications for practice and research are discussed in the next sections followed by recommendations for future research.

Implications for Practice

Cybersecurity educational providers should offer materials that focus on increasing awareness of cyber threats that are targeting the vulnerabilities of small businesses. A contribution to practice was the development of the cyberARMoRR program for small businesses that serves as a useful resource to assist small business decision makers in their continuous efforts to mitigate cyber threats through a prioritized set of cybersecurity preparedness activities. The survey instrument can be used as a basic risk assessment benchmarking tool to identify areas for improving cybersecurity postures. The cyberARMoRR program for small businesses also provides an introduction to the NIST Cybersecurity Framework and outlines specific recommendations for small businesses to adopt into their business routines. The resources associated with common cyber threats and the cybersecurity preparedness activities can help simplify efforts for small business owners and managers that are seeking information on related topics. In particular, the information can help small businesses understand better what fundamental security controls are needed and how to react to a cybersecurity incident (Osborn & Simpson, 2018).

Implications for Research

The theoretical implications, using the lens of prospect theory and status quo bias, add to the understanding of decision-making under conditions of uncertainty. A contribution to research was the instrument and CyPRisT Taxonomy that can be used to compare the distribution of small businesses in quadrants, thereby providing insight into small businesses cybersecurity posture relative to their perception of cyber risk. For example, limited technical knowledge and experience may contribute to a status quo bias that inhibits the decision maker's ability to assess cybersecurity risk and management (Berry & Berry, 2018). A rise in the business decision maker's cybersecurity awareness and basic understanding of identifying cyber-attack methods can inspire small businesses to become more risk adverse (Bhattacharya, 2015). The decision makers' perceptions of likelihood and impact can be used to influence decisions away from indifference toward a strategically balanced approach for managing risk. This research study provides empirically validated set of cybersecurity preparedness activities and taxonomy, as well as cybersecurity resources, to use for measuring and improving the cybersecurity posture of small businesses.

Recommendations and Future Research

As with any research study, there are strengths, weaknesses, and limitations inherent to the problem and questions, as well as the methodology. A strength of this research study was the relevance and significance of the problem to address a gap in IS literature that focused on the small business community for cybersecurity IS research (Gafni & Pavel, 2019). The theoretical foundations of status quo bias and advances in prospect theory have been distinguished by the work of senior scholars and published in top ranking journals (Kim & Kankanhalli, 2009; Lee & Joshi, 2016; Li et al., 2016; Liang & Xue, 2009; Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992). Another strength was the mixed-methods approach of data collection to draw on the strengths of each method (Creswell & Clark, 2017). Learning from the weaknesses and limitations of this study provides opportunity for recommendations. The results, conclusions, and implications can also expose several opportunities for future research.

The first recommendation is further development to the proposed construct of cybersecurity preparedness. Future research projects may consider a condensed list of the most crucial cybersecurity preparedness activities (e.g., 5 or 10 in each function). The survey instruments did not include an ‘I do not know option’ for the participants. This information may be useful in identifying the activities that the participant did not have direct knowledge, such as those delegated to IT resources. Similarly, the measure of the decision makers’ perceived risk did not include an option for assessing their understanding of the threat definitions. The scope of this research study was delimited to a sample of small businesses in the U.S. with 10-49 employees because they were considered among the most vulnerable (BBB, 2017; Hiscox, 2017; Rohn et al., 2016; Sumner, 2009). Future studies are recommended to contrast findings of small-medium or medium size businesses, or those of small size with greater populations in specific industries. For the quasi-experiment, a longer period may be taken between the pretest and posttest to observe and better understand the cybersecurity preparedness activities that are more challenging for small businesses. It is recommended that future research broaden the sample population of small businesses by conducting comparative studies of small businesses in other countries as part of a larger on-going research effort to help improve the cybersecurity postures. Future studies may explore the possibility of developing additional education material for small business decision makers to mitigate the common threats. Using a similar quasi experimental method of pretest and posttest, formal training on select cybersecurity preparedness activities may provide insight on some of the advanced concepts of cybersecurity risk management.

The CyPRisT can be applied to more robust data analysis to determine the effects of multivariate factors. As Lee and Joshi (2016) point out, there are several key constructs used in prospect theory and status quo bias that have been oversimplified in research. For example, this research study intentionally did not evaluate the cost factors as it relates to status quo and loss aversion. Kim and Kankanhalli (2009) applied status quo bias to address the problem of how users evaluate IS technologies and subsequently their decision to resist change (i.e., remain status quo). Their study identified gaps in understanding cognitive misperception underlying resistance, such as psychological (sunk costs, social norms, and control) and rational decision-making mechanisms (net benefits, transition costs, and uncertainty costs). Kim and Kankanhalli (2009) also observed that an explanation of user resistance due to status quo bias, or the preference to stay with the current situation was particularly absent from literature. The results of their testing justified a new construct of switching costs which mediates the relationship between user resistance and other antecedents. This likely applies to small businesses in the context of cybersecurity preparedness activities based on their perception of risk. In Kim and Kankanhalli (2009), the costs compared for perceived value are referred to as switching benefits and switching costs, respectively, because they apply to the switch (change) from the status quo. This phenomenon can be evaluated in the context of small businesses decision makers' resistance to change their cybersecurity posture.

An interesting finding of this study was the disparity in the low DMPRCA when the CPS was high. One possible explanation is that the DMPRCA was low because the decision makers were confident in their cybersecurity readiness and resilience. For example, if the company is making routine backups of critical data and testing those backups frequently then they may not be as vulnerable to a ransomware cyber-attack. However, in most cases where perceived risk of cyber-attack was elevated, the decision makers indicated action toward mitigating cyber risk through the implementation of the cybersecurity preparedness activities. Future research can further investigate a causal relationship of implemented cybersecurity preparedness to cyber risk perceptions.

Among the weaknesses of this research study was participant fatigue. As indicated in the responses small business decision makers were limited by their time and availability. Although the design of the survey instrument included short and clearly written questions, the amount of questions may have been a deterrent to some participants. Nearly all participants expressed a genuine desire to improve their cybersecurity posture. However, the participation involvement averaged 30-45 minutes for pretest survey, several hours of instruction and resource reviews for the cyberARMoRR program, an un-determined amount of time implementing the cybersecurity preparedness activities, and another 30-45 minutes for the posttest survey. For the remaining participants, the final leg of this study, a 15-30 minutes semi-structured interview, peaked their participation threshold. The complexity of this research study demanded a considerable amount of the participants time during a short period.

Recommendation for future research would be to conduct a longitudinal study that focuses on small businesses overcoming the challenges of limited resources to improve their cybersecurity posture.

Finally, there are areas of research in the which the ‘calculus’ of cybersecurity decision-making process may be studied. Prospect theory and status quo bias are rooted on concepts of the framing effect, heuristics as well as biases, and decision weights for gains or losses (Samuelson & Zeckhauser, 1988; Tversky & Kahneman, 1992). These concepts are used for establishing reference points for judgments and choices based on risk preferences (Tversky & Kahneman, 1992). However, in cybersecurity, loss aversion appears to be the principle driver for decision biases. Risk factors can be evaluated through further experimentation of potential outcomes of cyber-attacks based on the resource investment costs of time and effort. Accordingly, future work is recommended in the ‘Psychonomics of cybersecurity’, which considers both phycological and economic weights in decision-making for cybersecurity counter measures and controls.

Summary

This research addressed the problem of small businesses having limited ability to mitigate cyber threats, which leads to significant losses from cyber-attacks or data breaches (Berry & Berry, 2018; Paulsen, 2016; Rohn et al., 2016). The research focused on small businesses in the U.S. with 10-49 employees because they are among the most vulnerable to cyber-attack (BBB, 2017; Hiscox, 2017; Rohn et al., 2016). The main goal of this research study was to develop and validate a small business CyPRisT to empirically assess small businesses’ cybersecurity postures, then to develop a strategy program for small businesses to improve their cybersecurity risk management. The empirical assessment of cybersecurity readiness and resilience in small businesses provided insight into the decision-making process toward improving cybersecurity strategic posture. It also provided information into an area with a limited number of research studies that assesses the cybersecurity activities in small businesses for dealing with cyber threats (Gafni & Pavel, 2019).

This research study followed a three-phase approach to address the research goal. Phase 1 utilized the Delphi method having 2 rounds of interaction with participation from 22 cybersecurity SMEs. The Delphi method was used for instrument development. The SMEs validated the proposed construct of *cybersecurity preparedness* and updated the construct of *decision maker's perceived risk of cyber-attack*. The SMEs feedback also helped identify topics for the cyberARMoRR program for small businesses. Phase 2 was a sequential exploratory to evaluate 216 small businesses in the U.S. Phase 3 was a sequential embedded quasi-experiment of 50 small business using the same instrument to measure before (pretest) and after (posttest) participation in the cyberARMoRR program.

During Phase 1 data were collected from the SMEs for development of the instrument to addresses RQ1, RQ2, and RQ3. For RQ1, the NIST Cybersecurity Framework was used as the basis for determining which cybersecurity preparedness activities, organized by the five functions, could be used to measure the level of cybersecurity preparedness for a small business. For RQ2, SMEs provided weights to the cybersecurity preparedness activities that were used in the development of the aggregate benchmark score for levels of preparedness. For RQ3, cyber-attacks were defined for the most common cyber threats to small business. The approved survey instrument was used as pretest and posttest measures of participants in the Phase 2 & Phase 3 quasi-experiment.

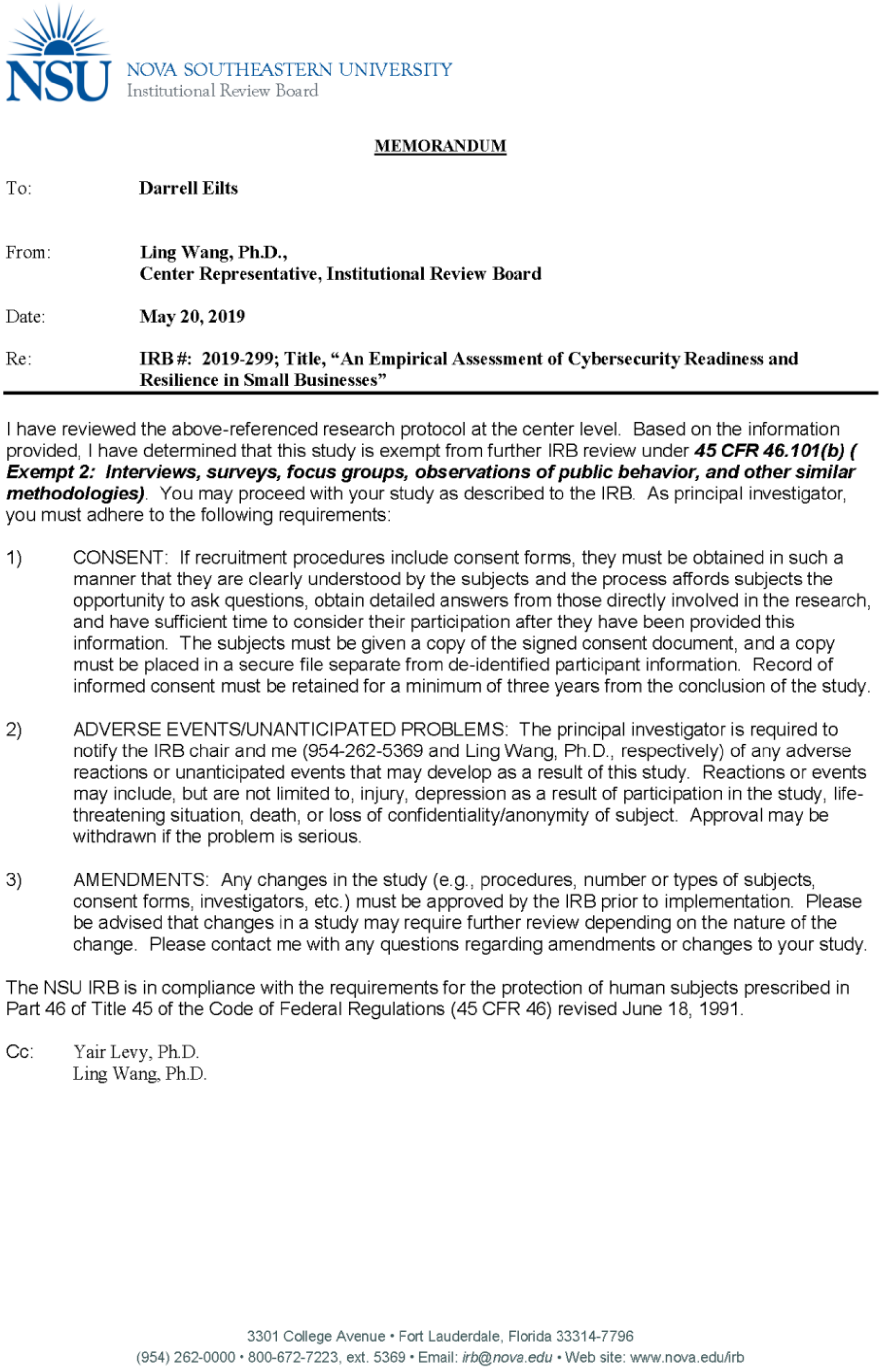
During Phase 2, data were collected from 216 small business owners and managers using the SME validated instrument to conduct a quantitative empirical assessment documenting the results of the benchmark scores, thereby addressing RQ4 and RQ5. For RQ4, the CPS and DMPRCA were applied to the CyPRisT to assess the cybersecurity posture level positions of the 216 small businesses. For RQ5, the data were analyzed using analysis of variance procedures (Mertler & Reinhard, 2017). This study found that there were significant differences between the CPSs and DMPRCA for the industry focus of small businesses, as well as significant differences when categorized by size (number of employees) and IT budget (%). The CPSs and DMPRCA were positioned on the CyPRisT for a sample of 216 small businesses. Through the theoretical lens of prospect theory and status quo bias, the results showed that approximately half of the small business were indifferent – unwilling to abandon their status quo – in order to achieve a strategically balanced approach for managing cyber risk. The results also revealed that small businesses did not typically demonstrate risk-seeking postures. Slightly less than half of the small businesses demonstrated that they were either risk adverse or strategically balanced.

During Phase 3, the cyberARMoRR for small business program was developed and administered to a sub-sample of 50 research participants to address RQ6, RQ7, and RQ8. For RQ6, pretest and posttest data were analyzed using a paired sample t-test to compare the calculated means and determine if statistically significant differences exist in the dependent variables (Mertler & Reinhart, 2017). For RQ7, the differences between groups were quantitatively assessed using descriptive statistics of the change in cybersecurity preparedness and qualitatively by differences in the CyPRisT positions. For RQ8, data were analyzed from the open-ended questions of the survey instrument. There were 15 semi-structured interviews conducted with the voluntary participants. The open questions in the survey instrument were combined with the interview notes then coded for qualitative analysis (Creswell, 2014; Myers & Newman, 2007). A two-cycle process of manually coding categories and emergent themes was used to analyze the data (Saldaña, 2013).

The quasi-experimental results did not show statistically significant differences in the CPSs as well as the DMPRCA before and after participation in the cyberARMoRR program. However, the data collected from the participants on cybersecurity preparedness activities that were implemented after participation in the cyberARMoRR program for small business provided insight into the bias for, or against, the decision maker's choices to improve their small businesses' cybersecurity posture. The small business owners and managers described what cybersecurity preparedness activities were most challenging for small businesses to implement and why. The thematic analysis suggest that decision makers are more likely to improve their ability to mitigate cyber threats when resources are easy to comprehend, applicable technologies are uncomplicated and reasonably priced, technical expertise is obtainable, and implementing the activities into practice does not demand a substantial amount of time. Most importantly, small business decision makers should continue to strive toward a strategy for improving their cybersecurity posture; a balanced of being prepared to manage cyber risk and the ability to minimize loss by becoming resilient against cyber-attacks.

Appendix A

Institutional Review Board Approval Letter



NSU NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Darrell Eilts**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **May 20, 2019**

Re: **IRB #: 2019-299; Title, "An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under ***45 CFR 46.101(b) (Exempt 2: Interviews, surveys, focus groups, observations of public behavior, and other similar methodologies)***. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

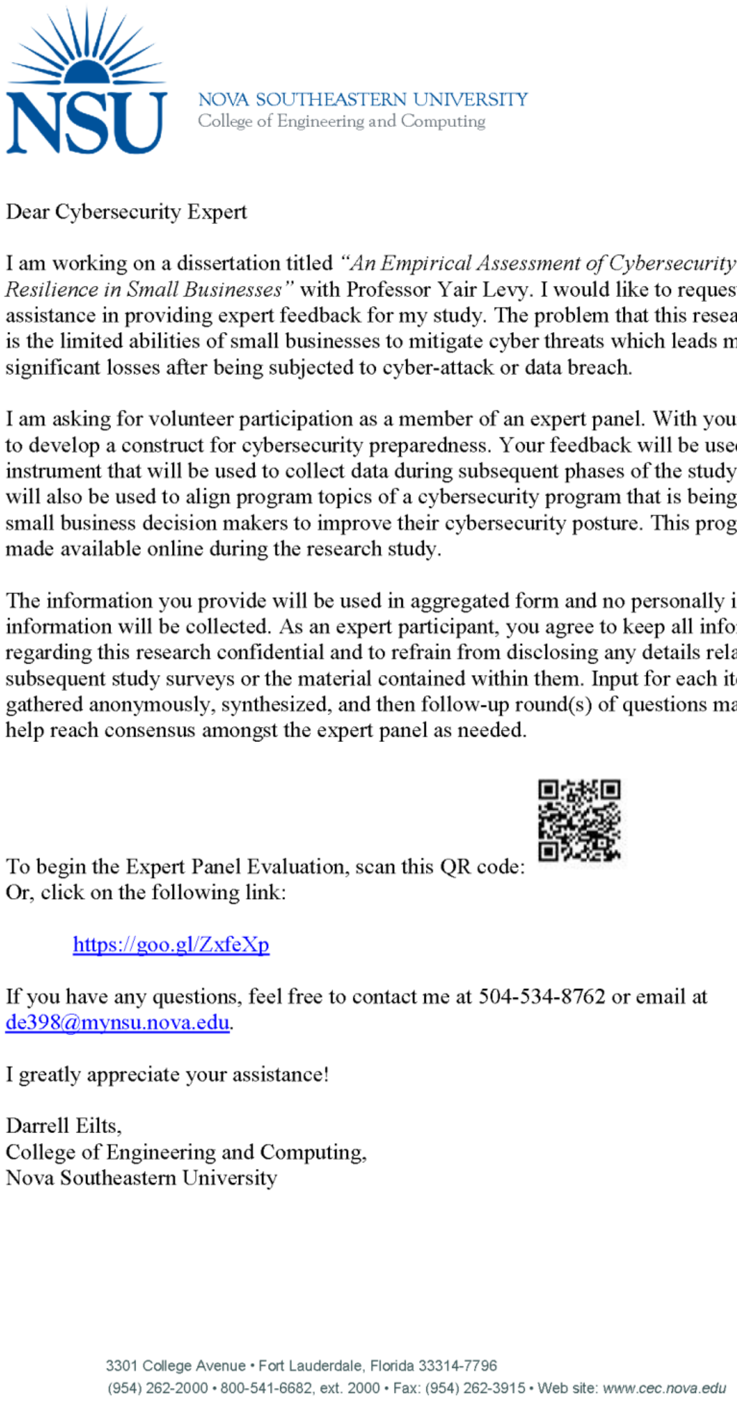
The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Yair Levy, Ph.D.
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

Appendix B

Phase 1 Expert Recruitment Email



NSU

NOVA SOUTHEASTERN UNIVERSITY
College of Engineering and Computing

Dear Cybersecurity Expert

I am working on a dissertation titled *"An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses"* with Professor Yair Levy. I would like to request your assistance in providing expert feedback for my study. The problem that this research will address is the limited abilities of small businesses to mitigate cyber threats which leads many to significant losses after being subjected to cyber-attack or data breach.

I am asking for volunteer participation as a member of an expert panel. With your support, I seek to develop a construct for cybersecurity preparedness. Your feedback will be used to validate the instrument that will be used to collect data during subsequent phases of the study. The measure will also be used to align program topics of a cybersecurity program that is being developed for small business decision makers to improve their cybersecurity posture. This program will be made available online during the research study.

The information you provide will be used in aggregated form and no personally identifiable information will be collected. As an expert participant, you agree to keep all information regarding this research confidential and to refrain from disclosing any details related to subsequent study surveys or the material contained within them. Input for each item will be gathered anonymously, synthesized, and then follow-up round(s) of questions may be sent to help reach consensus amongst the expert panel as needed.

To begin the Expert Panel Evaluation, scan this QR code:
Or, click on the following link:

https://goo.gl/ZxfeXp

If you have any questions, feel free to contact me at 504-534-8762 or email at de398@mynsu.nova.edu.

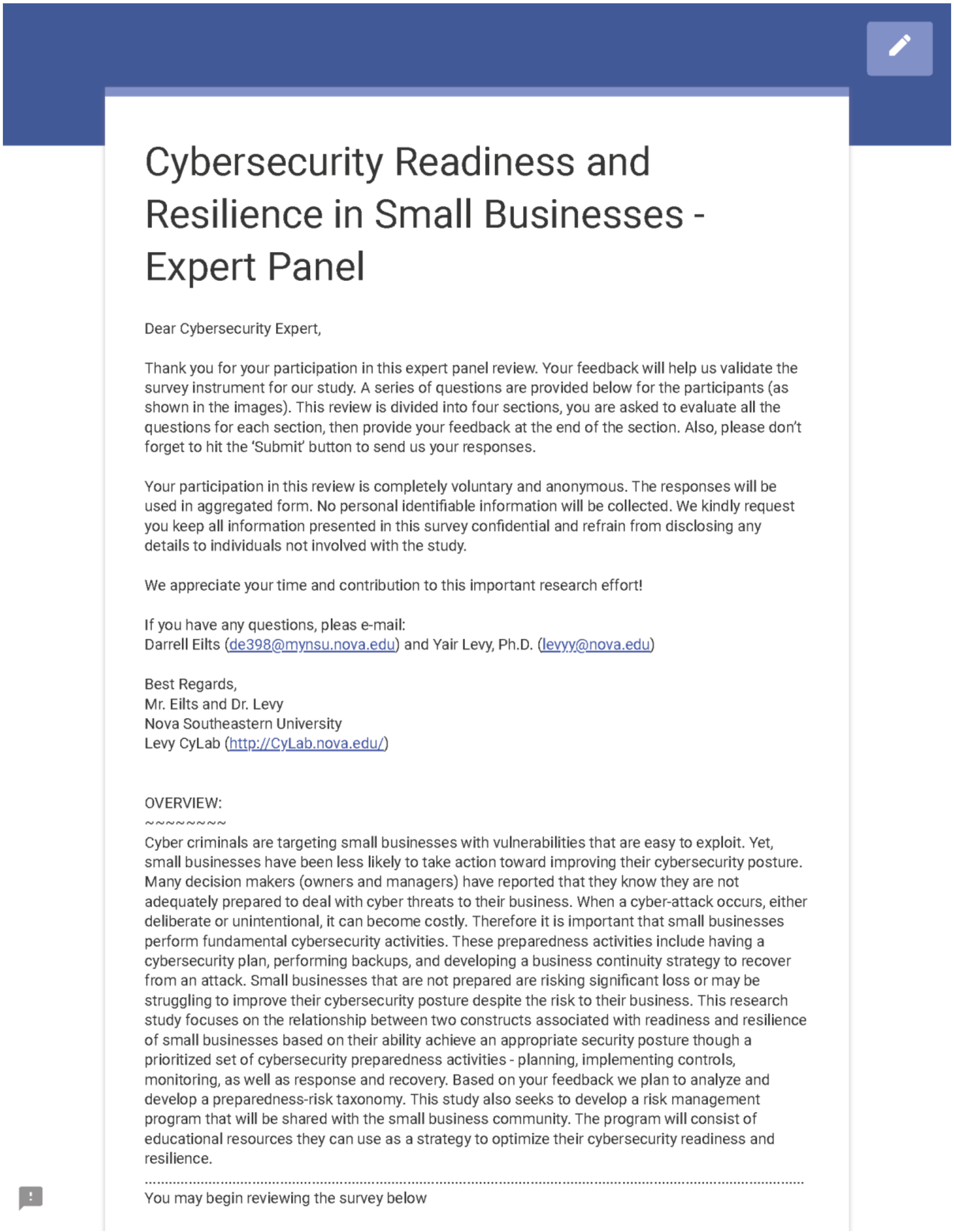
I greatly appreciate your assistance!

Darrell Eilts,
College of Engineering and Computing,
Nova Southeastern University

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-2000 • 800-541-6682, ext. 2000 • Fax: (954) 262-3915 • Web site: *www.cec.nova.edu*

Appendix C

Phase 1 Expert Panel Survey Instrument (Delphi 1)



Cybersecurity Readiness and Resilience in Small Businesses - Expert Panel

Dear Cybersecurity Expert,

Thank you for your participation in this expert panel review. Your feedback will help us validate the survey instrument for our study. A series of questions are provided below for the participants (as shown in the images). This review is divided into four sections, you are asked to evaluate all the questions for each section, then provide your feedback at the end of the section. Also, please don't forget to hit the 'Submit' button to send us your responses.

Your participation in this review is completely voluntary and anonymous. The responses will be used in aggregated form. No personal identifiable information will be collected. We kindly request you keep all information presented in this survey confidential and refrain from disclosing any details to individuals not involved with the study.

We appreciate your time and contribution to this important research effort!

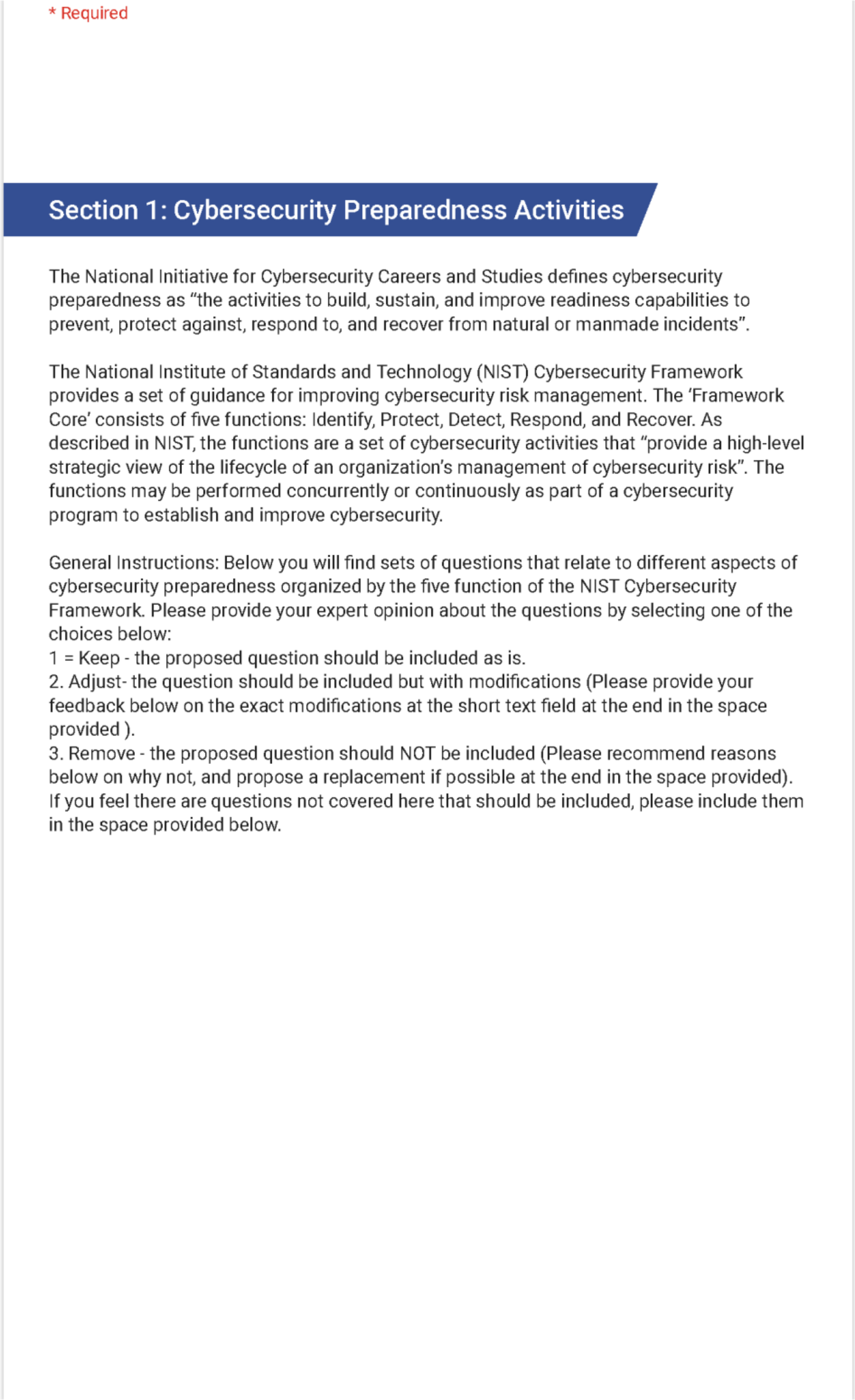
If you have any questions, pleas e-mail:
Darrell Eilts (de398@mynsu.nova.edu) and Yair Levy, Ph.D. (levyy@nova.edu)

Best Regards,
Mr. Eilts and Dr. Levy
Nova Southeastern University
Levy CyLab (http://CyLab.nova.edu/)

OVERVIEW:
~~~~~~~~~
Cyber criminals are targeting small businesses with vulnerabilities that are easy to exploit. Yet, small businesses have been less likely to take action toward improving their cybersecurity posture. Many decision makers (owners and managers) have reported that they know they are not adequately prepared to deal with cyber threats to their business. When a cyber-attack occurs, either deliberate or unintentional, it can become costly. Therefore it is important that small businesses perform fundamental cybersecurity activities. These preparedness activities include having a cybersecurity plan, performing backups, and developing a business continuity strategy to recover from an attack. Small businesses that are not prepared are risking significant loss or may be struggling to improve their cybersecurity posture despite the risk to their business. This research study focuses on the relationship between two constructs associated with readiness and resilience of small businesses based on their ability achieve an appropriate security posture though a prioritized set of cybersecurity preparedness activities - planning, implementing controls, monitoring, as well as response and recovery. Based on your feedback we plan to analyze and develop a preparedness-risk taxonomy. This study also seeks to develop a risk management program that will be shared with the small business community. The program will consist of educational resources they can use as a strategy to optimize their cybersecurity readiness and resilience.

....

You may begin reviewing the survey below
~~~~~~~~~



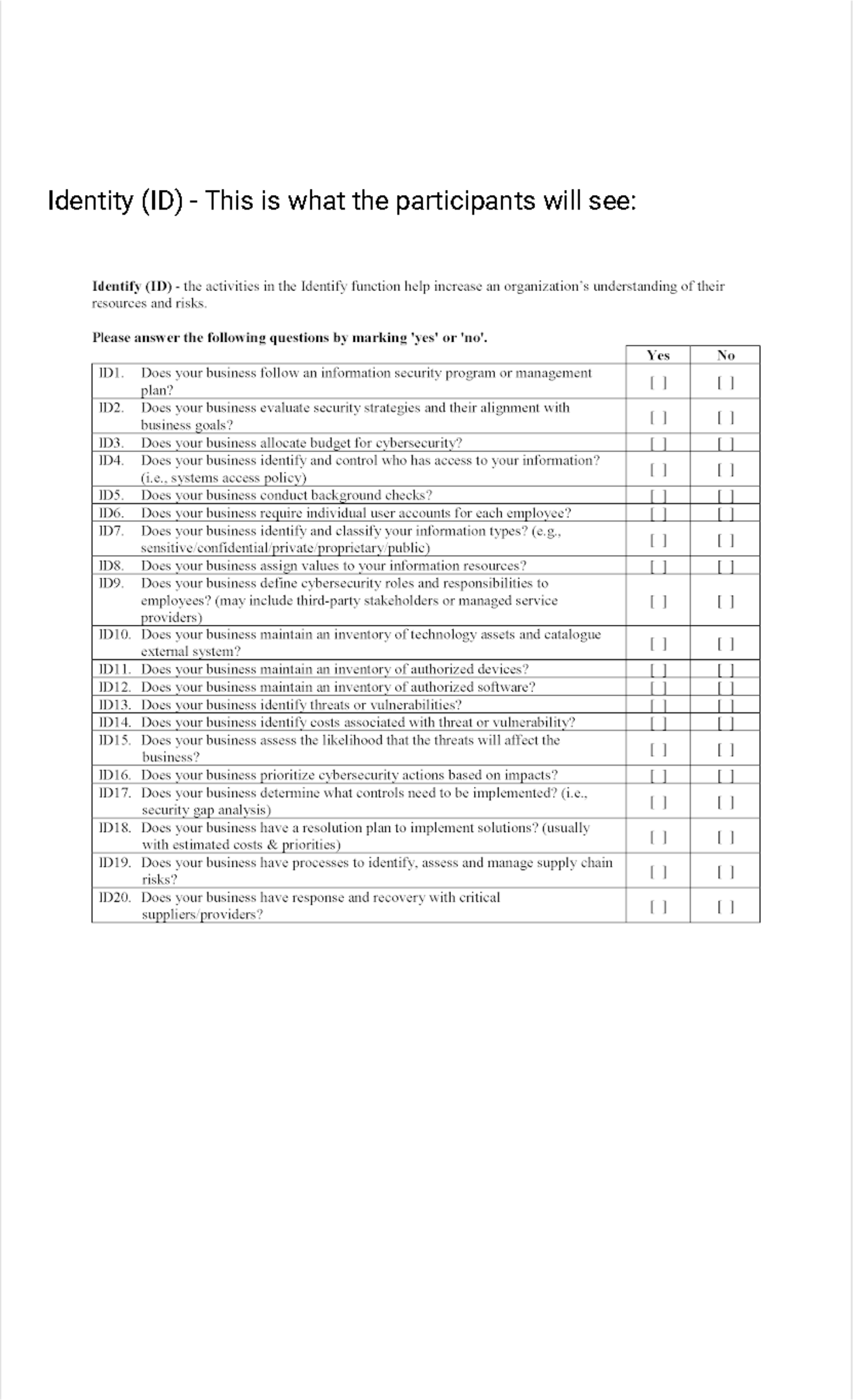
* Required

Section 1: Cybersecurity Preparedness Activities

The National Initiative for Cybersecurity Careers and Studies defines cybersecurity preparedness as “the activities to build, sustain, and improve readiness capabilities to prevent, protect against, respond to, and recover from natural or manmade incidents”.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of guidance for improving cybersecurity risk management. The ‘Framework Core’ consists of five functions: Identify, Protect, Detect, Respond, and Recover. As described in NIST, the functions are a set of cybersecurity activities that “provide a high-level strategic view of the lifecycle of an organization’s management of cybersecurity risk”. The functions may be performed concurrently or continuously as part of a cybersecurity program to establish and improve cybersecurity.

General Instructions: Below you will find sets of questions that relate to different aspects of cybersecurity preparedness organized by the five function of the NIST Cybersecurity Framework. Please provide your expert opinion about the questions by selecting one of the choices below:
1 = Keep - the proposed question should be included as is.
2. Adjust- the question should be included but with modifications (Please provide your feedback below on the exact modifications at the short text field at the end in the space provided).
3. Remove - the proposed question should NOT be included (Please recommend reasons below on why not, and propose a replacement if possible at the end in the space provided).
If you feel there are questions not covered here that should be included, please include them in the space provided below.

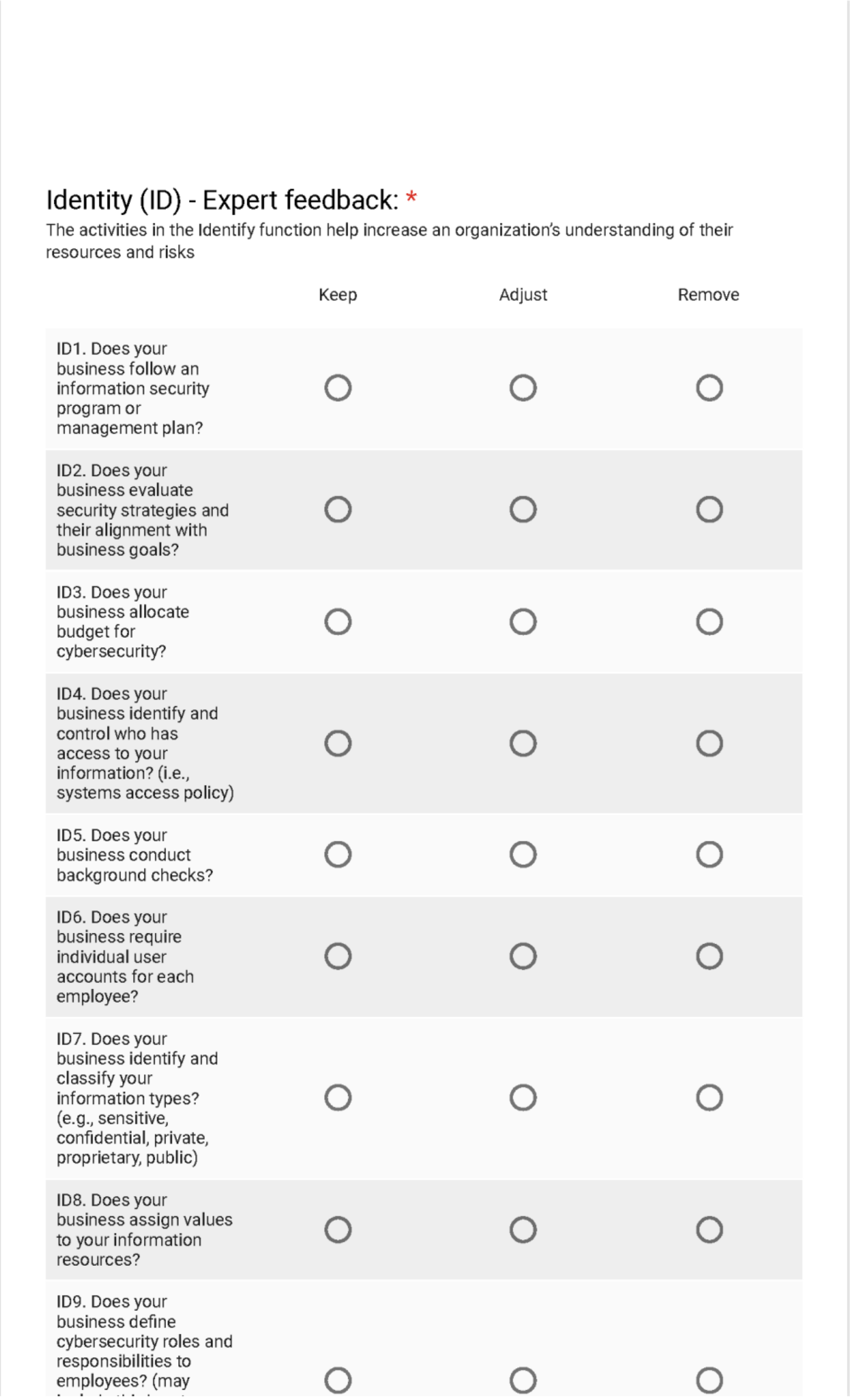


Identity (ID) - This is what the participants will see:

Identify (ID) - the activities in the Identify function help increase an organization's understanding of their resources and risks.

Please answer the following questions by marking 'yes' or 'no'.

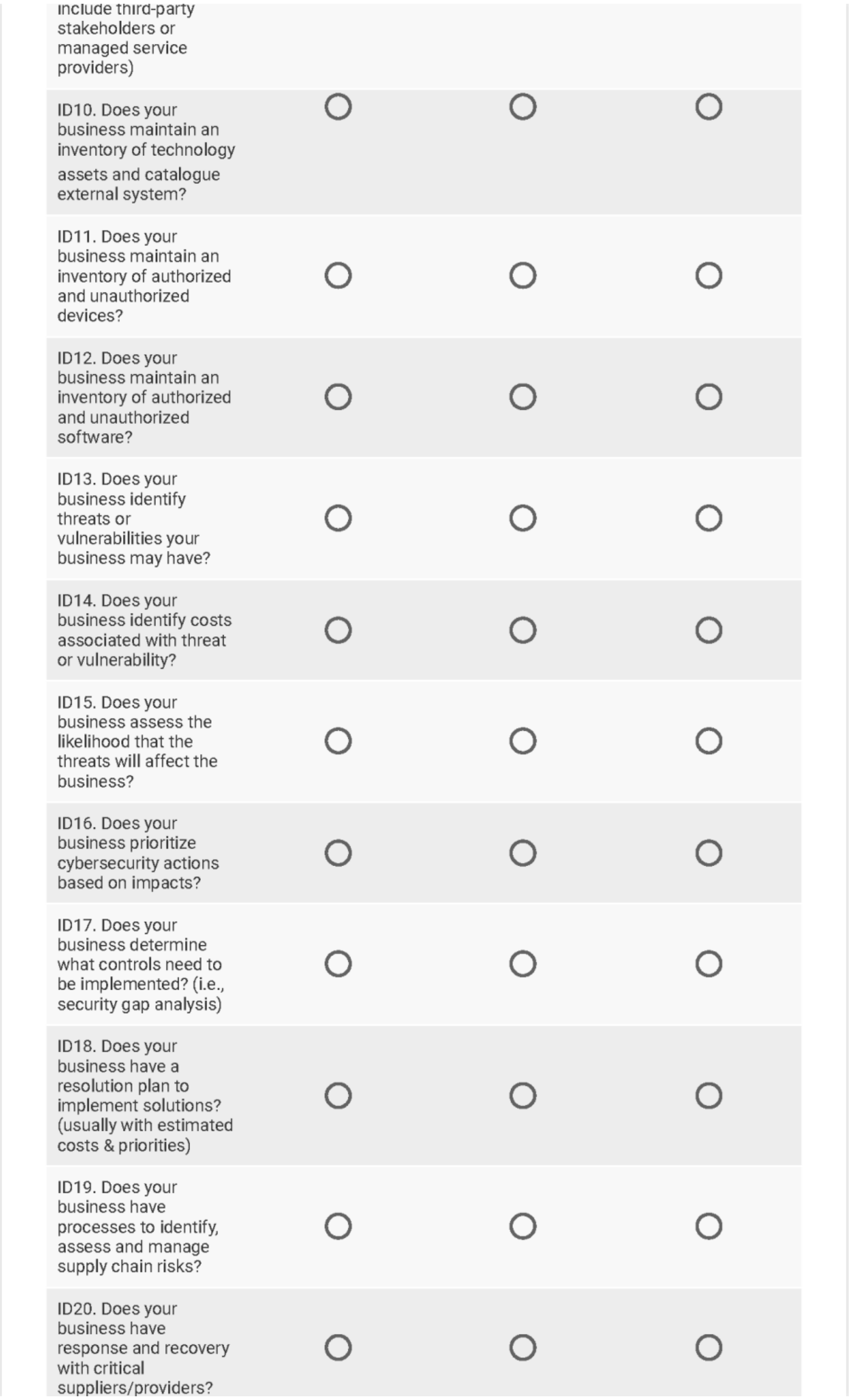
		Yes	No
ID1.	Does your business follow an information security program or management plan?	[ ]	[ ]
ID2.	Does your business evaluate security strategies and their alignment with business goals?	[ ]	[ ]
ID3.	Does your business allocate budget for cybersecurity?	[ ]	[ ]
ID4.	Does your business identify and control who has access to your information? (i.e., systems access policy)	[ ]	[ ]
ID5.	Does your business conduct background checks?	[ ]	[ ]
ID6.	Does your business require individual user accounts for each employee?	[ ]	[ ]
ID7.	Does your business identify and classify your information types? (e.g., sensitive/confidential/private/proprietary/public)	[ ]	[ ]
ID8.	Does your business assign values to your information resources?	[ ]	[ ]
ID9.	Does your business define cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	[ ]	[ ]
ID10.	Does your business maintain an inventory of technology assets and catalogue external system?	[ ]	[ ]
ID11.	Does your business maintain an inventory of authorized devices?	[ ]	[ ]
ID12.	Does your business maintain an inventory of authorized software?	[ ]	[ ]
ID13.	Does your business identify threats or vulnerabilities?	[ ]	[ ]
ID14.	Does your business identify costs associated with threat or vulnerability?	[ ]	[ ]
ID15.	Does your business assess the likelihood that the threats will affect the business?	[ ]	[ ]
ID16.	Does your business prioritize cybersecurity actions based on impacts?	[ ]	[ ]
ID17.	Does your business determine what controls need to be implemented? (i.e., security gap analysis)	[ ]	[ ]
ID18.	Does your business have a resolution plan to implement solutions? (usually with estimated costs & priorities)	[ ]	[ ]
ID19.	Does your business have processes to identify, assess and manage supply chain risks?	[ ]	[ ]
ID20.	Does your business have response and recovery with critical suppliers/providers?	[ ]	[ ]



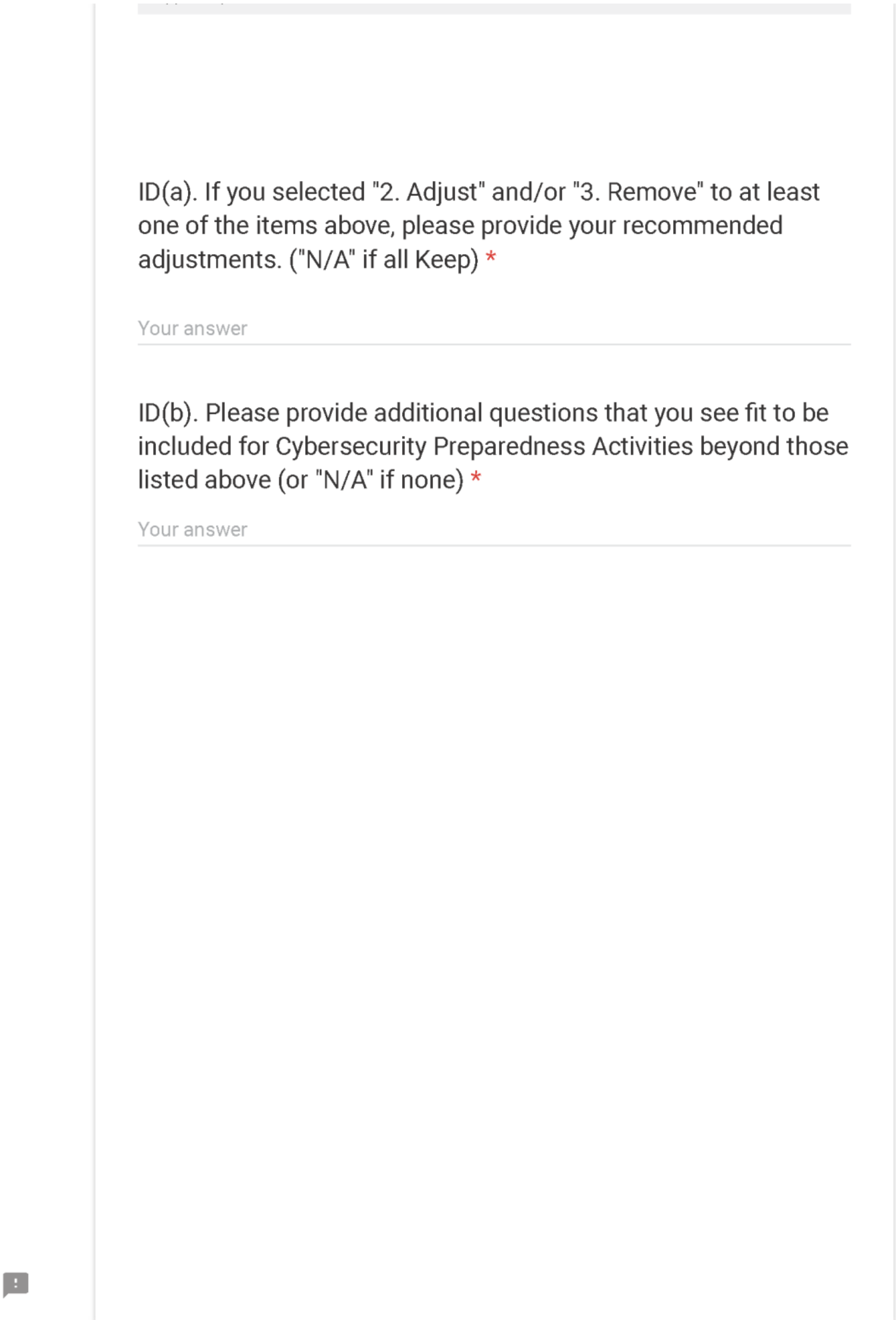
Identity (ID) - Expert feedback: *

The activities in the Identify function help increase an organization’s understanding of their resources and risks

	Keep	Adjust	Remove
ID1. Does your business follow an information security program or management plan?	○	○	○
ID2. Does your business evaluate security strategies and their alignment with business goals?	○	○	○
ID3. Does your business allocate budget for cybersecurity?	○	○	○
ID4. Does your business identify and control who has access to your information? (i.e., systems access policy)	○	○	○
ID5. Does your business conduct background checks?	○	○	○
ID6. Does your business require individual user accounts for each employee?	○	○	○
ID7. Does your business identify and classify your information types? (e.g., sensitive, confidential, private, proprietary, public)	○	○	○
ID8. Does your business assign values to your information resources?	○	○	○
ID9. Does your business define cybersecurity roles and responsibilities to employees? (may	○	○	○



include third-party stakeholders or managed service providers)			
ID10. Does your business maintain an inventory of technology assets and catalogue external system?	○	○	○
ID11. Does your business maintain an inventory of authorized and unauthorized devices?	○	○	○
ID12. Does your business maintain an inventory of authorized and unauthorized software?	○	○	○
ID13. Does your business identify threats or vulnerabilities your business may have?	○	○	○
ID14. Does your business identify costs associated with threat or vulnerability?	○	○	○
ID15. Does your business assess the likelihood that the threats will affect the business?	○	○	○
ID16. Does your business prioritize cybersecurity actions based on impacts?	○	○	○
ID17. Does your business determine what controls need to be implemented? (i.e., security gap analysis)	○	○	○
ID18. Does your business have a resolution plan to implement solutions? (usually with estimated costs & priorities)	○	○	○
ID19. Does your business have processes to identify, assess and manage supply chain risks?	○	○	○
ID20. Does your business have response and recovery with critical suppliers/providers?	○	○	○

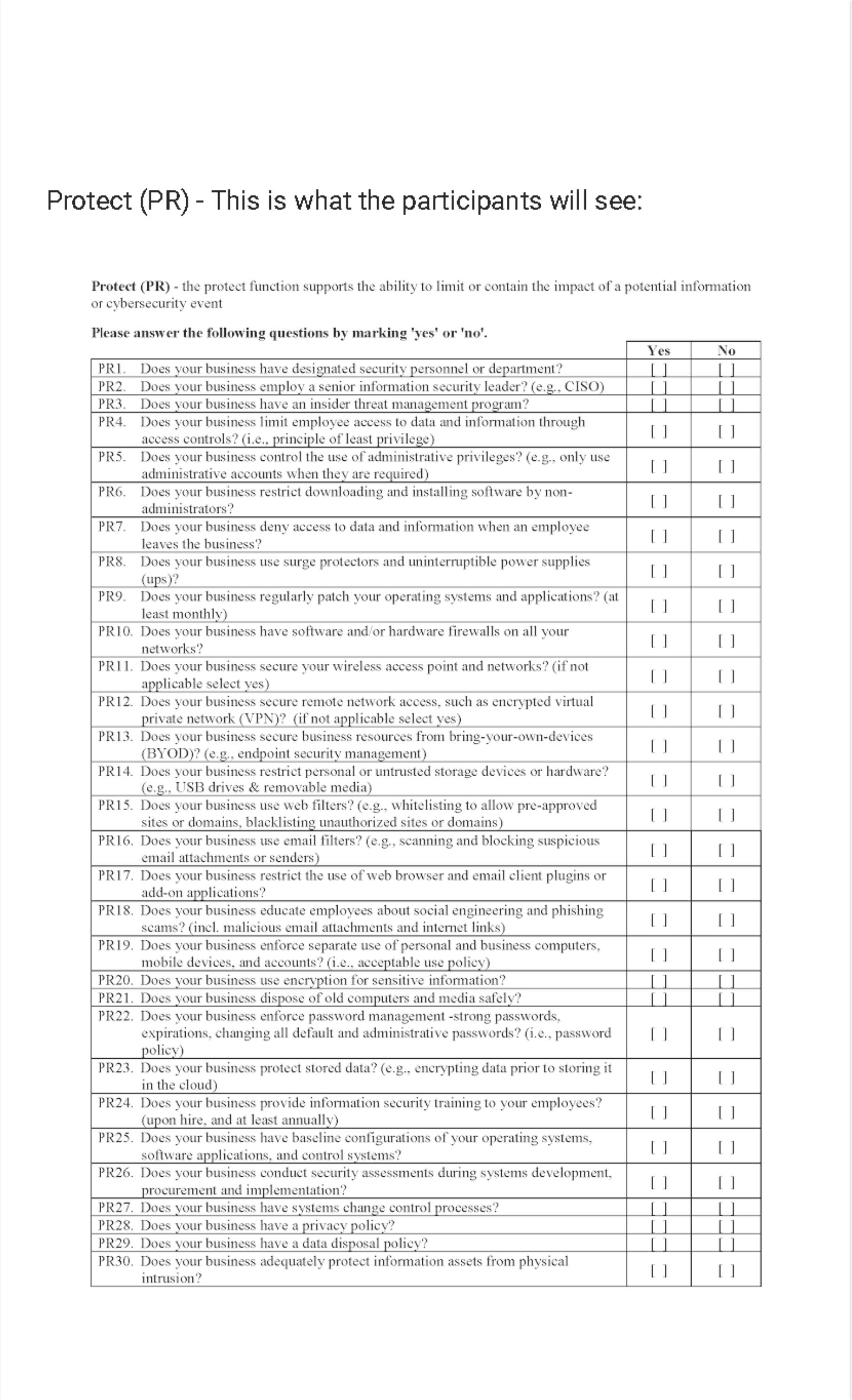


ID(a). If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments. ("N/A" if all Keep) *

Your answer

ID(b). Please provide additional questions that you see fit to be included for Cybersecurity Preparedness Activities beyond those listed above (or "N/A" if none) *

Your answer

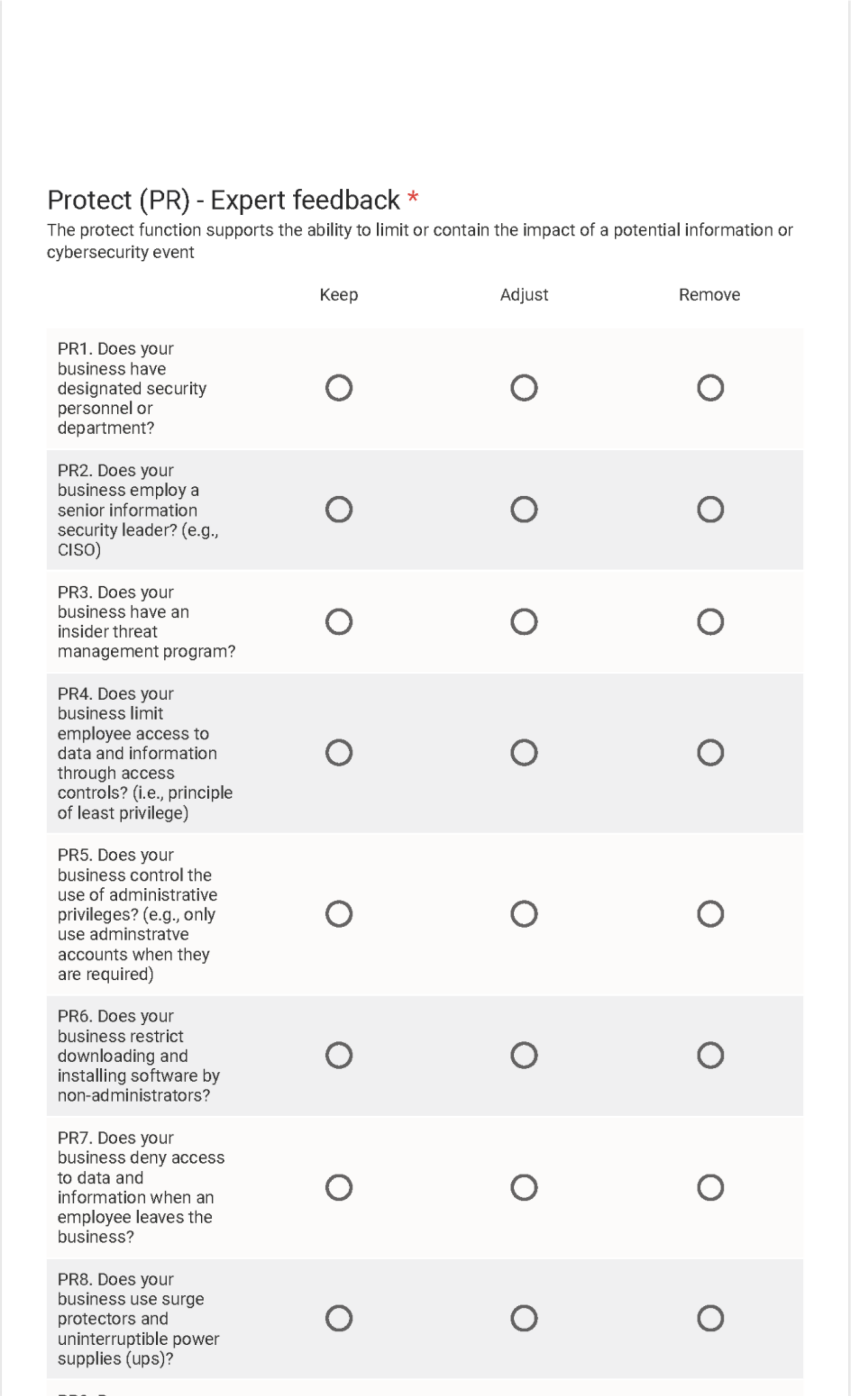


Protect (PR) - This is what the participants will see:

Protect (PR) - the protect function supports the ability to limit or contain the impact of a potential information or cybersecurity event

Please answer the following questions by marking 'yes' or 'no'.

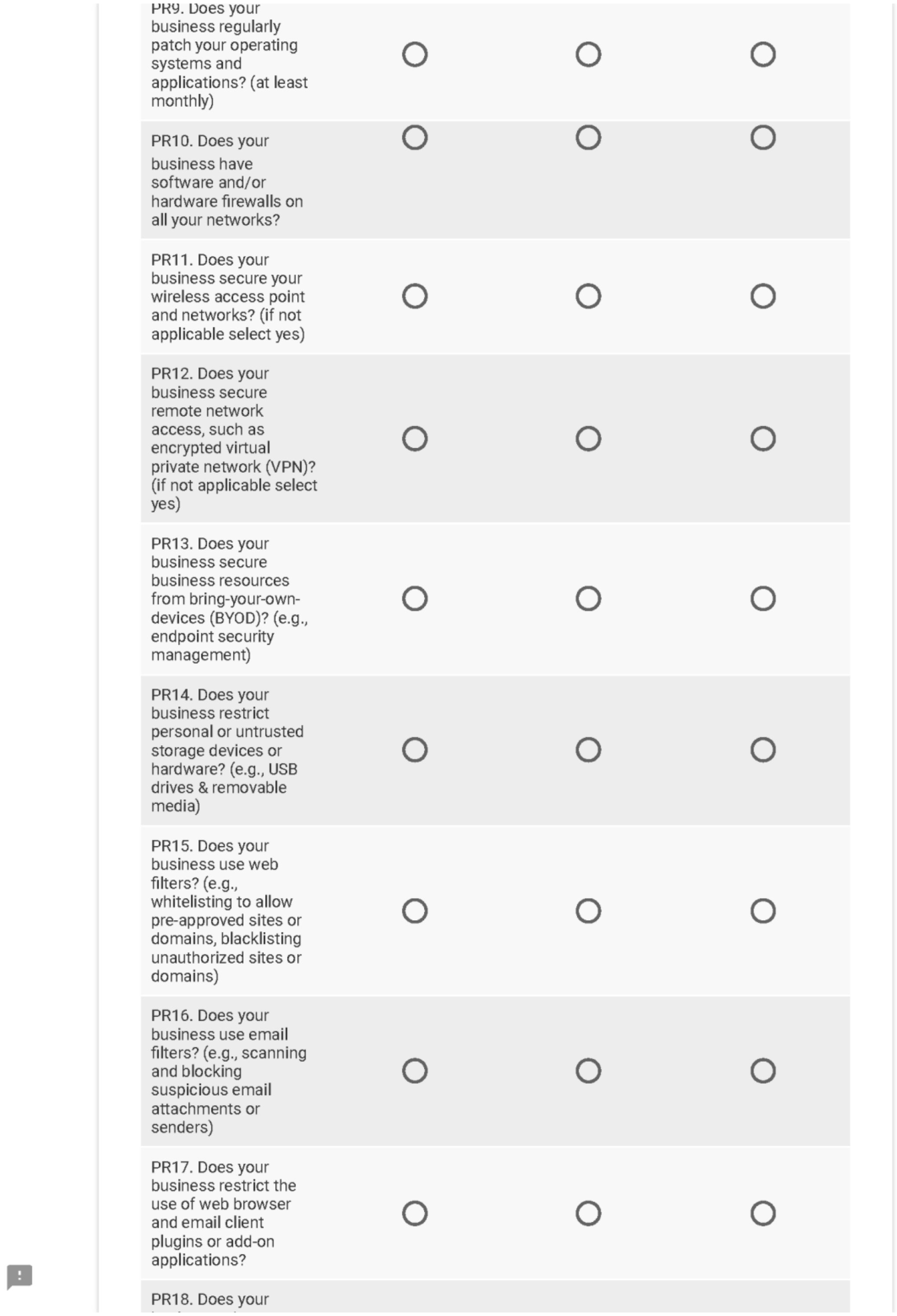
	Yes	No
PR1. Does your business have designated security personnel or department?	[ ]	[ ]
PR2. Does your business employ a senior information security leader? (e.g., CISO)	[ ]	[ ]
PR3. Does your business have an insider threat management program?	[ ]	[ ]
PR4. Does your business limit employee access to data and information through access controls? (i.e., principle of least privilege)	[ ]	[ ]
PR5. Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	[ ]	[ ]
PR6. Does your business restrict downloading and installing software by non-administrators?	[ ]	[ ]
PR7. Does your business deny access to data and information when an employee leaves the business?	[ ]	[ ]
PR8. Does your business use surge protectors and uninterruptible power supplies (ups)?	[ ]	[ ]
PR9. Does your business regularly patch your operating systems and applications? (at least monthly)	[ ]	[ ]
PR10. Does your business have software and/or hardware firewalls on all your networks?	[ ]	[ ]
PR11. Does your business secure your wireless access point and networks? (if not applicable select yes)	[ ]	[ ]
PR12. Does your business secure remote network access, such as encrypted virtual private network (VPN)? (if not applicable select yes)	[ ]	[ ]
PR13. Does your business secure business resources from bring-your-own-devices (BYOD)? (e.g., endpoint security management)	[ ]	[ ]
PR14. Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	[ ]	[ ]
PR15. Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	[ ]	[ ]
PR16. Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	[ ]	[ ]
PR17. Does your business restrict the use of web browser and email client plugins or add-on applications?	[ ]	[ ]
PR18. Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	[ ]	[ ]
PR19. Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (i.e., acceptable use policy)	[ ]	[ ]
PR20. Does your business use encryption for sensitive information?	[ ]	[ ]
PR21. Does your business dispose of old computers and media safely?	[ ]	[ ]
PR22. Does your business enforce password management -strong passwords, expirations, changing all default and administrative passwords? (i.e., password policy)	[ ]	[ ]
PR23. Does your business protect stored data? (e.g., encrypting data prior to storing it in the cloud)	[ ]	[ ]
PR24. Does your business provide information security training to your employees? (upon hire, and at least annually)	[ ]	[ ]
PR25. Does your business have baseline configurations of your operating systems, software applications, and control systems?	[ ]	[ ]
PR26. Does your business conduct security assessments during systems development, procurement and implementation?	[ ]	[ ]
PR27. Does your business have systems change control processes?	[ ]	[ ]
PR28. Does your business have a privacy policy?	[ ]	[ ]
PR29. Does your business have a data disposal policy?	[ ]	[ ]
PR30. Does your business adequately protect information assets from physical intrusion?	[ ]	[ ]



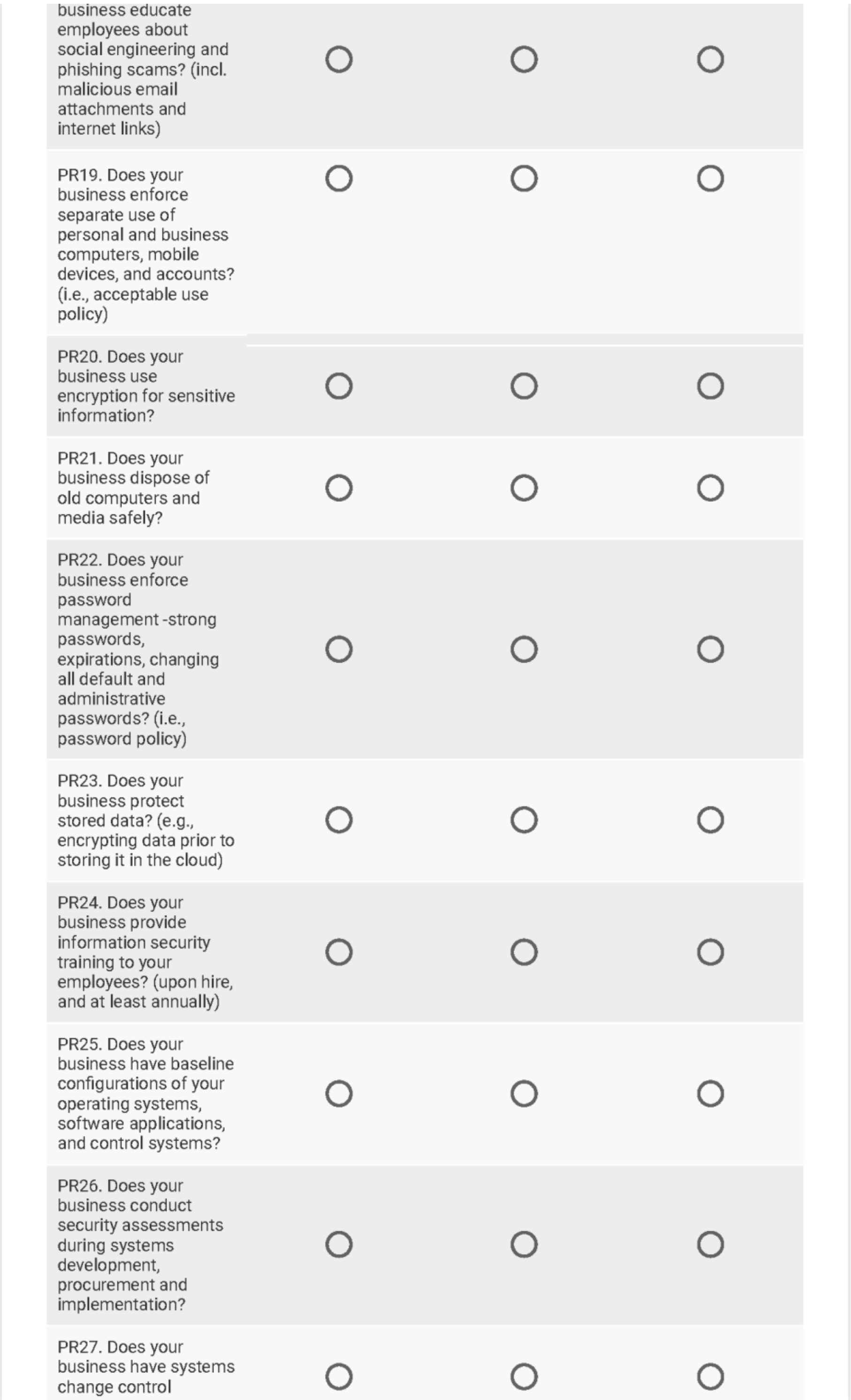
Protect (PR) - Expert feedback *

The protect function supports the ability to limit or contain the impact of a potential information or cybersecurity event

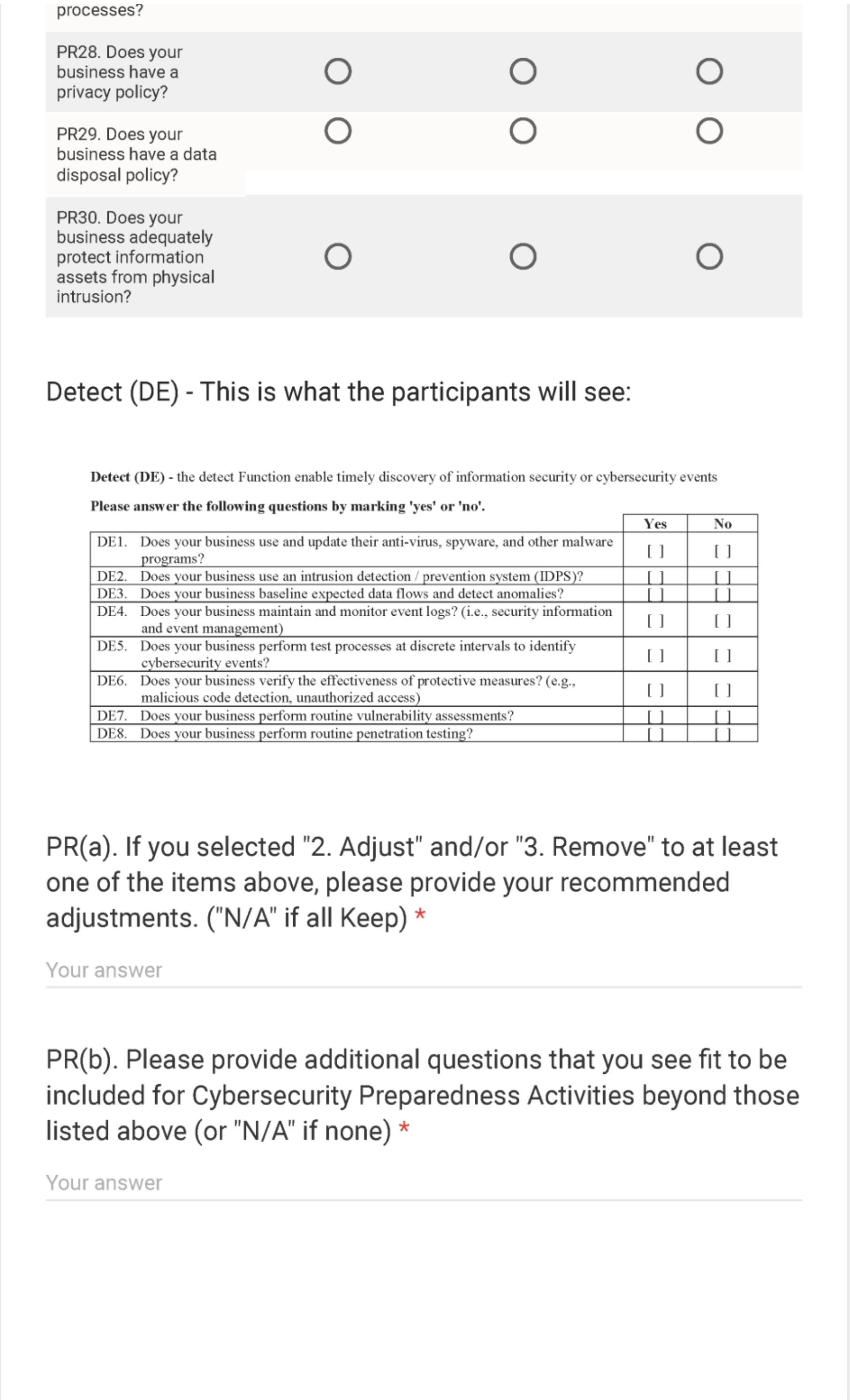
	Keep	Adjust	Remove
PR1. Does your business have designated security personnel or department?	○	○	○
PR2. Does your business employ a senior information security leader? (e.g., CISO)	○	○	○
PR3. Does your business have an insider threat management program?	○	○	○
PR4. Does your business limit employee access to data and information through access controls? (i.e., principle of least privilege)	○	○	○
PR5. Does your business control the use of administrative privileges? (e.g., only use adminstratve accounts when they are required)	○	○	○
PR6. Does your business restrict downloading and installing software by non-administrators?	○	○	○
PR7. Does your business deny access to data and information when an employee leaves the business?	○	○	○
PR8. Does your business use surge protectors and uninterruptible power supplies (ups)?	○	○	○



PR9. Does your business regularly patch your operating systems and applications? (at least monthly)	○	○	○
PR10. Does your business have software and/or hardware firewalls on all your networks?	○	○	○
PR11. Does your business secure your wireless access point and networks? (if not applicable select yes)	○	○	○
PR12. Does your business secure remote network access, such as encrypted virtual private network (VPN)? (if not applicable select yes)	○	○	○
PR13. Does your business secure business resources from bring-your-own-devices (BYOD)? (e.g., endpoint security management)	○	○	○
PR14. Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	○	○	○
PR15. Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	○	○	○
PR16. Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	○	○	○
PR17. Does your business restrict the use of web browser and email client plugins or add-on applications?	○	○	○
PR18. Does your			



business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	○	○	○
PR19. Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (i.e., acceptable use policy)	○	○	○
PR20. Does your business use encryption for sensitive information?	○	○	○
PR21. Does your business dispose of old computers and media safely?	○	○	○
PR22. Does your business enforce password management -strong passwords, expirations, changing all default and administrative passwords? (i.e., password policy)	○	○	○
PR23. Does your business protect stored data? (e.g., encrypting data prior to storing it in the cloud)	○	○	○
PR24. Does your business provide information security training to your employees? (upon hire, and at least annually)	○	○	○
PR25. Does your business have baseline configurations of your operating systems, software applications, and control systems?	○	○	○
PR26. Does your business conduct security assessments during systems development, procurement and implementation?	○	○	○
PR27. Does your business have systems change control	○	○	○



processes?			
PR28. Does your business have a privacy policy?	○	○	○
PR29. Does your business have a data disposal policy?	○	○	○
PR30. Does your business adequately protect information assets from physical intrusion?	○	○	○

Detect (DE) - This is what the participants will see:

Detect (DE) - the detect Function enable timely discovery of information security or cybersecurity events

Please answer the following questions by marking 'yes' or 'no'.

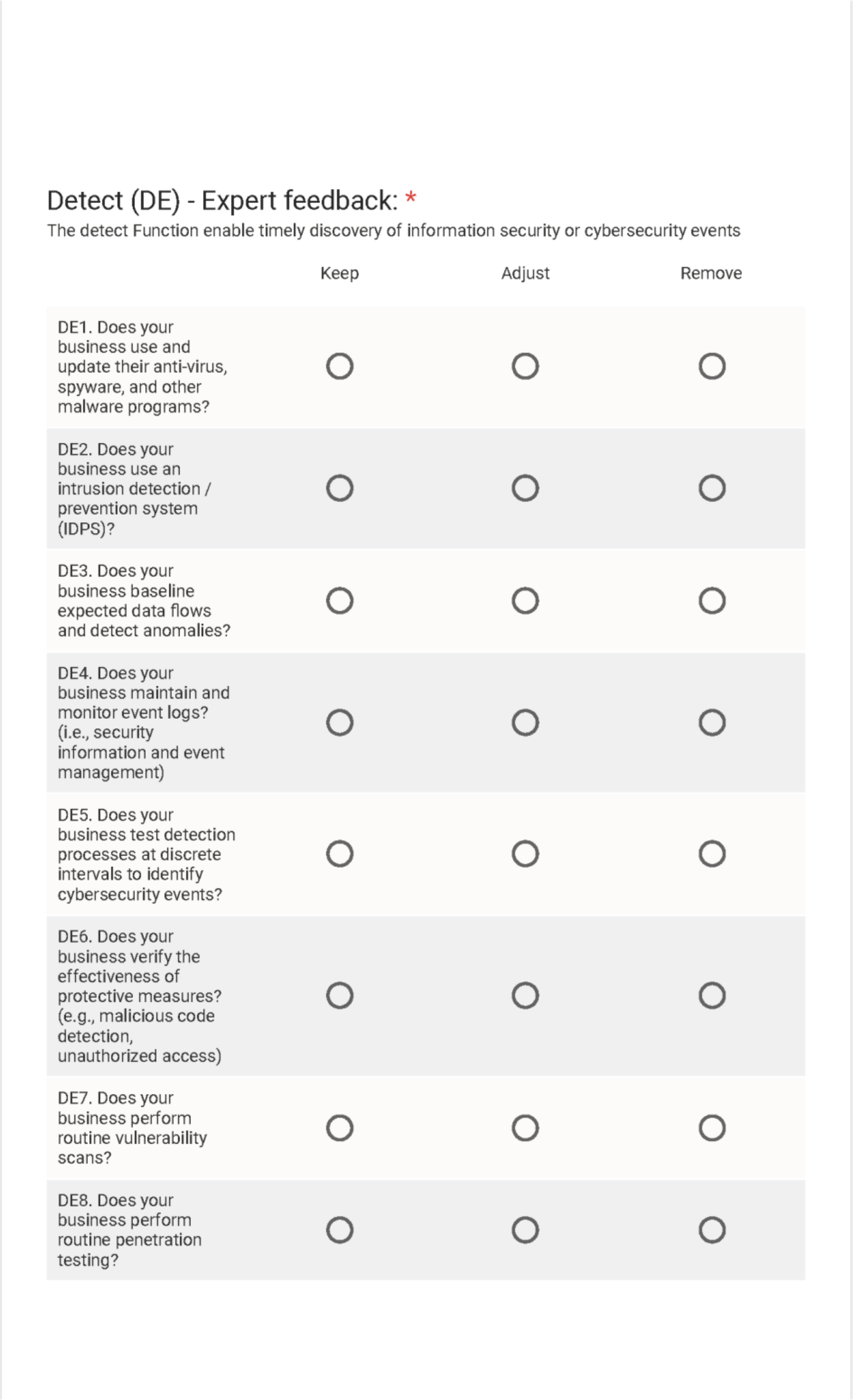
		Yes	No
DE1.	Does your business use and update their anti-virus, spyware, and other malware programs?	[ ]	[ ]
DE2.	Does your business use an intrusion detection / prevention system (IDPS)?	[ ]	[ ]
DE3.	Does your business baseline expected data flows and detect anomalies?	[ ]	[ ]
DE4.	Does your business maintain and monitor event logs? (i.e., security information and event management)	[ ]	[ ]
DE5.	Does your business perform test processes at discrete intervals to identify cybersecurity events?	[ ]	[ ]
DE6.	Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	[ ]	[ ]
DE7.	Does your business perform routine vulnerability assessments?	[ ]	[ ]
DE8.	Does your business perform routine penetration testing?	[ ]	[ ]

PR(a). If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments. ("N/A" if all Keep) *

Your answer

PR(b). Please provide additional questions that you see fit to be included for Cybersecurity Preparedness Activities beyond those listed above (or "N/A" if none) *

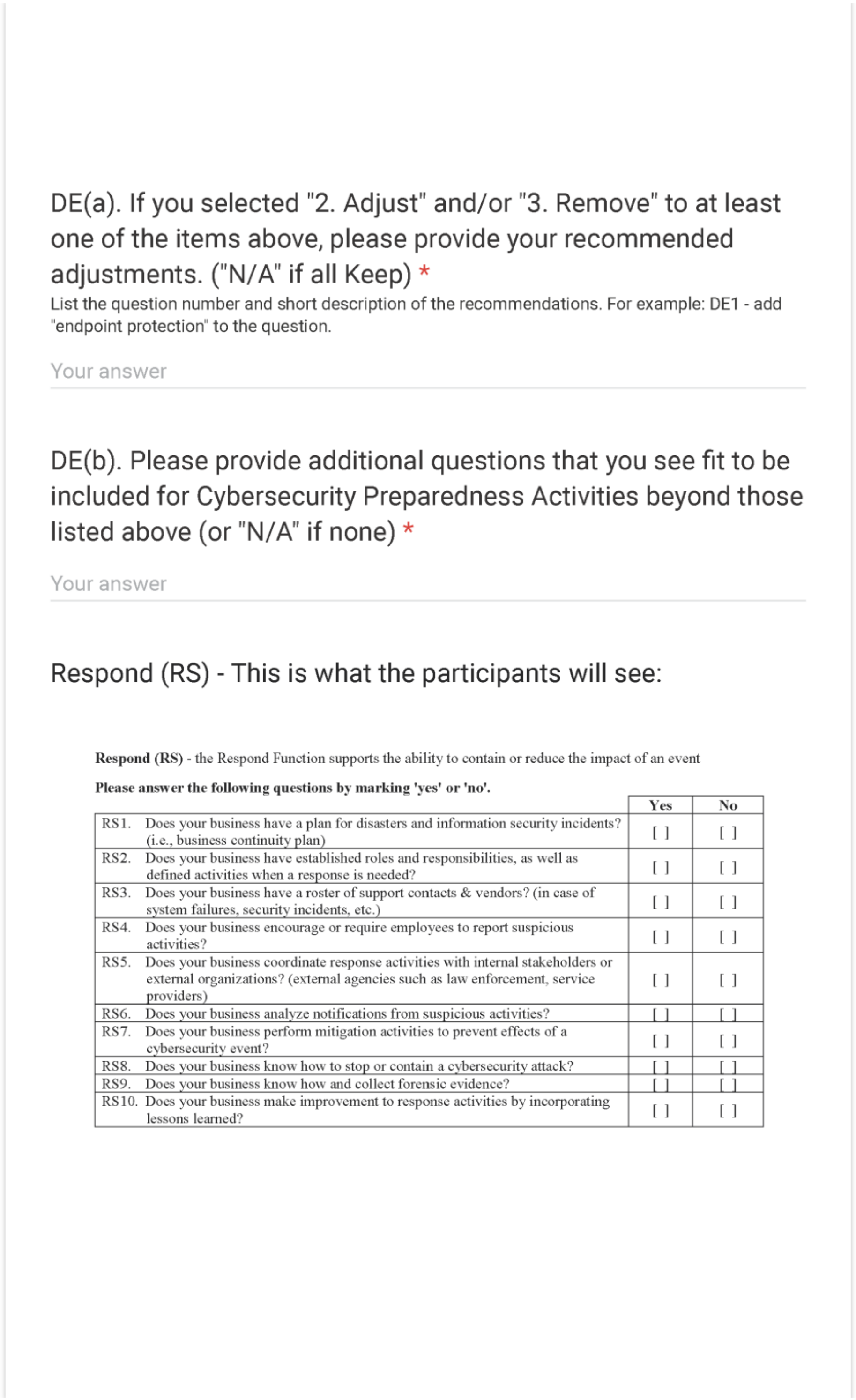
Your answer



Detect (DE) - Expert feedback: *

The detect Function enable timely discovery of information security or cybersecurity events

	Keep	Adjust	Remove
DE1. Does your business use and update their anti-virus, spyware, and other malware programs?	○	○	○
DE2. Does your business use an intrusion detection / prevention system (IDPS)?	○	○	○
DE3. Does your business baseline expected data flows and detect anomalies?	○	○	○
DE4. Does your business maintain and monitor event logs? (i.e., security information and event management)	○	○	○
DE5. Does your business test detection processes at discrete intervals to identify cybersecurity events?	○	○	○
DE6. Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	○	○	○
DE7. Does your business perform routine vulnerability scans?	○	○	○
DE8. Does your business perform routine penetration testing?	○	○	○



DE(a). If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments. ("N/A" if all Keep) *

List the question number and short description of the recommendations. For example: DE1 - add "endpoint protection" to the question.

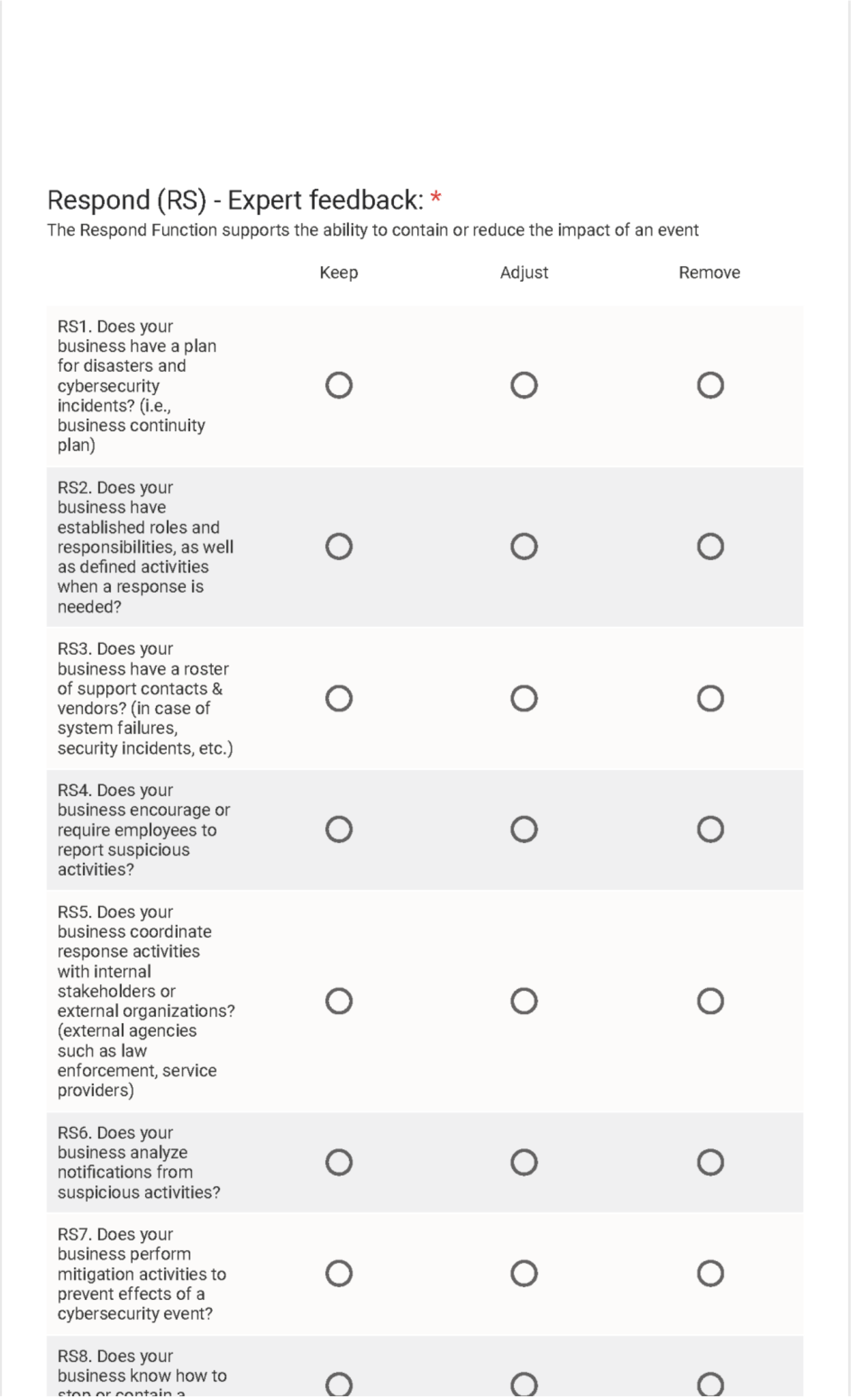
DE(b). Please provide additional questions that you see fit to be included for Cybersecurity Preparedness Activities beyond those listed above (or "N/A" if none) *

Respond (RS) - This is what the participants will see:

Respond (RS) - the Respond Function supports the ability to contain or reduce the impact of an event

Please answer the following questions by marking 'yes' or 'no'.

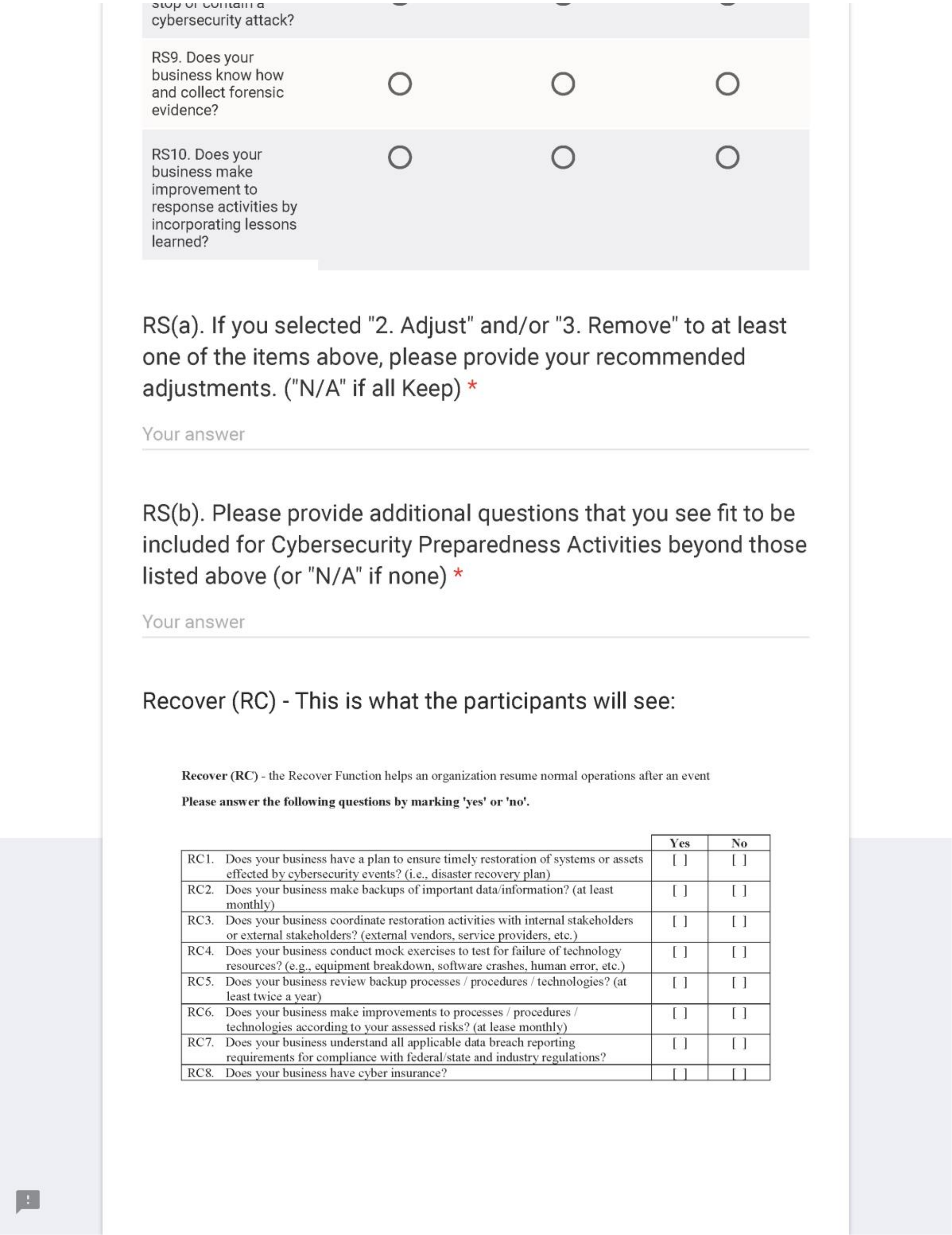
	Yes	**No**
RS1. Does your business have a plan for disasters and information security incidents? (i.e., business continuity plan)	[ ]	[ ]
RS2. Does your business have established roles and responsibilities, as well as defined activities when a response is needed?	[ ]	[ ]
RS3. Does your business have a roster of support contacts & vendors? (in case of system failures, security incidents, etc.)	[ ]	[ ]
RS4. Does your business encourage or require employees to report suspicious activities?	[ ]	[ ]
RS5. Does your business coordinate response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	[ ]	[ ]
RS6. Does your business analyze notifications from suspicious activities?	[ ]	[ ]
RS7. Does your business perform mitigation activities to prevent effects of a cybersecurity event?	[ ]	[ ]
RS8. Does your business know how to stop or contain a cybersecurity attack?	[ ]	[ ]
RS9. Does your business know how and collect forensic evidence?	[ ]	[ ]
RS10. Does your business make improvement to response activities by incorporating lessons learned?	[ ]	[ ]



Respond (RS) - Expert feedback: *

The Respond Function supports the ability to contain or reduce the impact of an event

	Keep	Adjust	Remove
RS1. Does your business have a plan for disasters and cybersecurity incidents? (i.e., business continuity plan)	○	○	○
RS2. Does your business have established roles and responsibilities, as well as defined activities when a response is needed?	○	○	○
RS3. Does your business have a roster of support contacts & vendors? (in case of system failures, security incidents, etc.)	○	○	○
RS4. Does your business encourage or require employees to report suspicious activities?	○	○	○
RS5. Does your business coordinate response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	○	○	○
RS6. Does your business analyze notifications from suspicious activities?	○	○	○
RS7. Does your business perform mitigation activities to prevent effects of a cybersecurity event?	○	○	○
RS8. Does your business know how to stop or contain a	○	○	○



stop or contain a cybersecurity attack?	○	○	○
RS9. Does your business know how and collect forensic evidence?	○	○	○
RS10. Does your business make improvement to response activities by incorporating lessons learned?	○	○	○

RS(a). If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments. ("N/A" if all Keep) *

Your answer

RS(b). Please provide additional questions that you see fit to be included for Cybersecurity Preparedness Activities beyond those listed above (or "N/A" if none) *

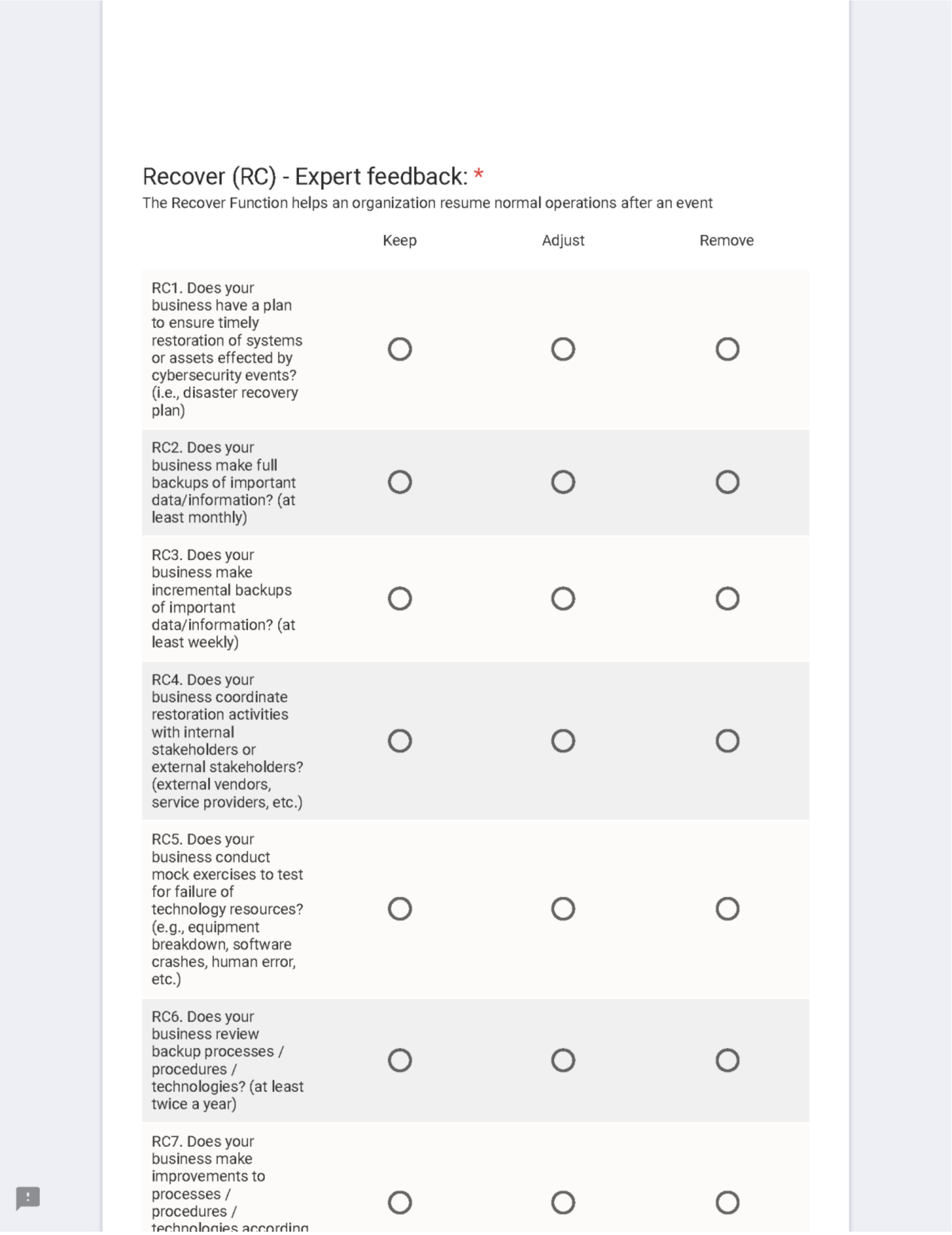
Your answer

Recover (RC) - This is what the participants will see:

Recover (RC) - the Recover Function helps an organization resume normal operations after an event

Please answer the following questions by marking 'yes' or 'no'.

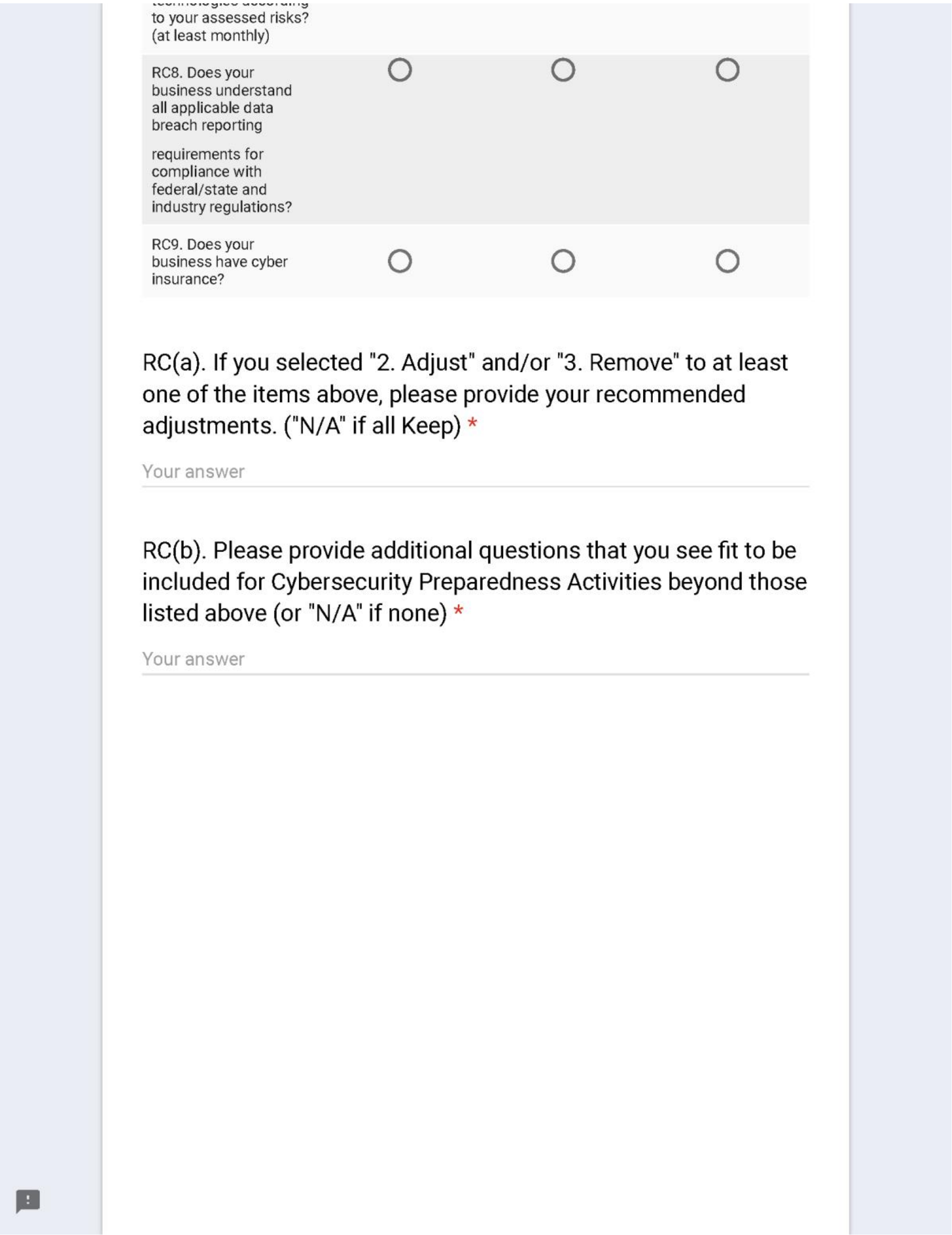
	Yes	No
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	[ ]	[ ]
RC2. Does your business make backups of important data/information? (at least monthly)	[ ]	[ ]
RC3. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	[ ]	[ ]
RC4. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	[ ]	[ ]
RC5. Does your business review backup processes / procedures / technologies? (at least twice a year)	[ ]	[ ]
RC6. Does your business make improvements to processes / procedures / technologies according to your assessed risks? (at lease monthly)	[ ]	[ ]
RC7. Does your business understand all applicable data breach reporting requirements for compliance with federal/state and industry regulations?	[ ]	[ ]
RC8. Does your business have cyber insurance?	[ ]	[ ]



Recover (RC) - Expert feedback: *

The Recover Function helps an organization resume normal operations after an event

	Keep	Adjust	Remove
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	○	○	○
RC2. Does your business make full backups of important data/information? (at least monthly)	○	○	○
RC3. Does your business make incremental backups of important data/information? (at least weekly)	○	○	○
RC4. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	○	○	○
RC5. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	○	○	○
RC6. Does your business review backup processes / procedures / technologies? (at least twice a year)	○	○	○
RC7. Does your business make improvements to processes / procedures / technologies according	○	○	○



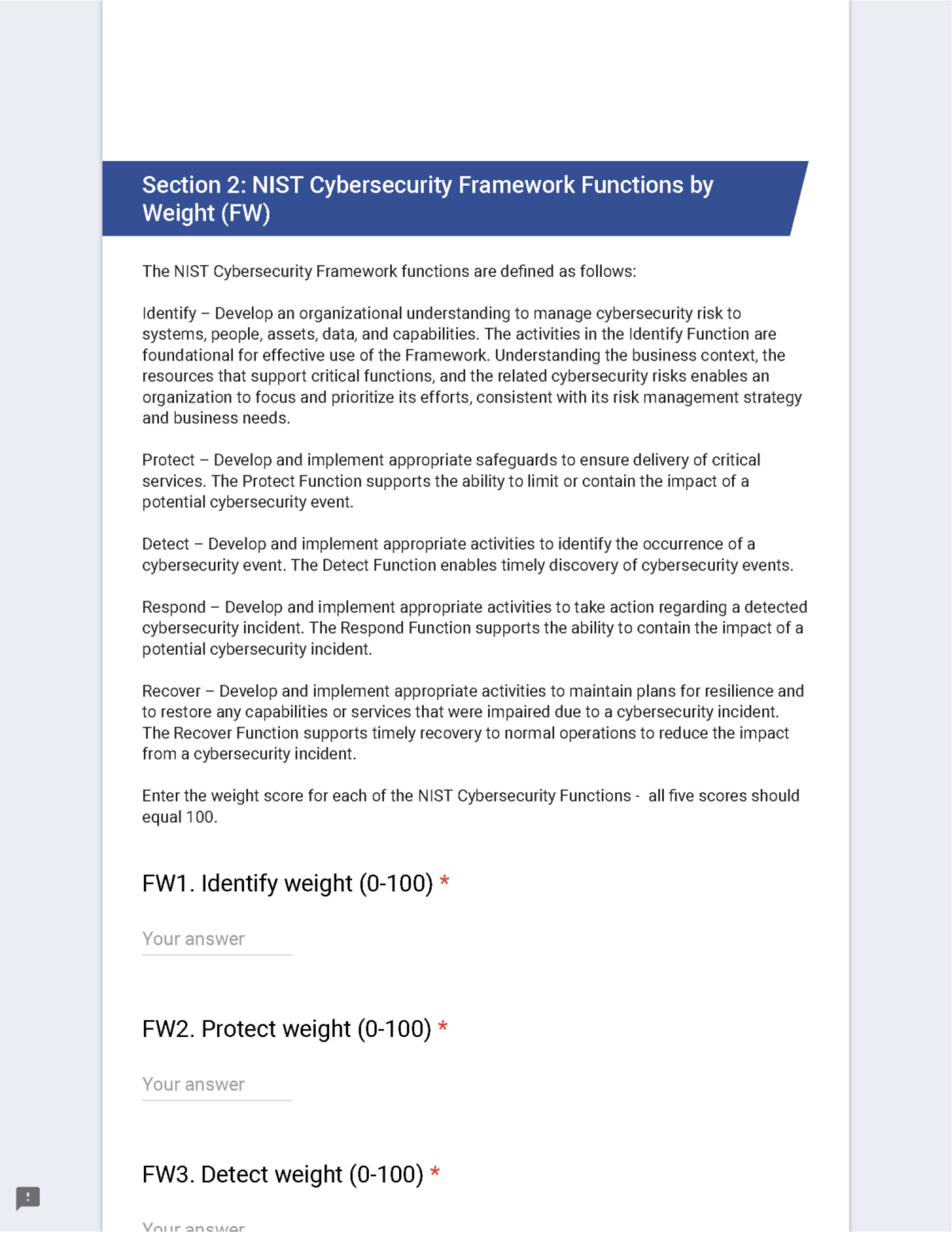
technologies according to your assessed risks? (at least monthly)			
RC8. Does your business understand all applicable data breach reporting requirements for compliance with federal/state and industry regulations?	○	○	○
RC9. Does your business have cyber insurance?	○	○	○

RC(a). If you selected "2. Adjust" and/or "3. Remove" to at least one of the items above, please provide your recommended adjustments. ("N/A" if all Keep) *

Your answer

RC(b). Please provide additional questions that you see fit to be included for Cybersecurity Preparedness Activities beyond those listed above (or "N/A" if none) *

Your answer



Section 2: NIST Cybersecurity Framework Functions by Weight (FW)

The NIST Cybersecurity Framework functions are defined as follows:

Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events.

Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

Enter the weight score for each of the NIST Cybersecurity Functions - all five scores should equal 100.

FW1. Identify weight (0-100) *

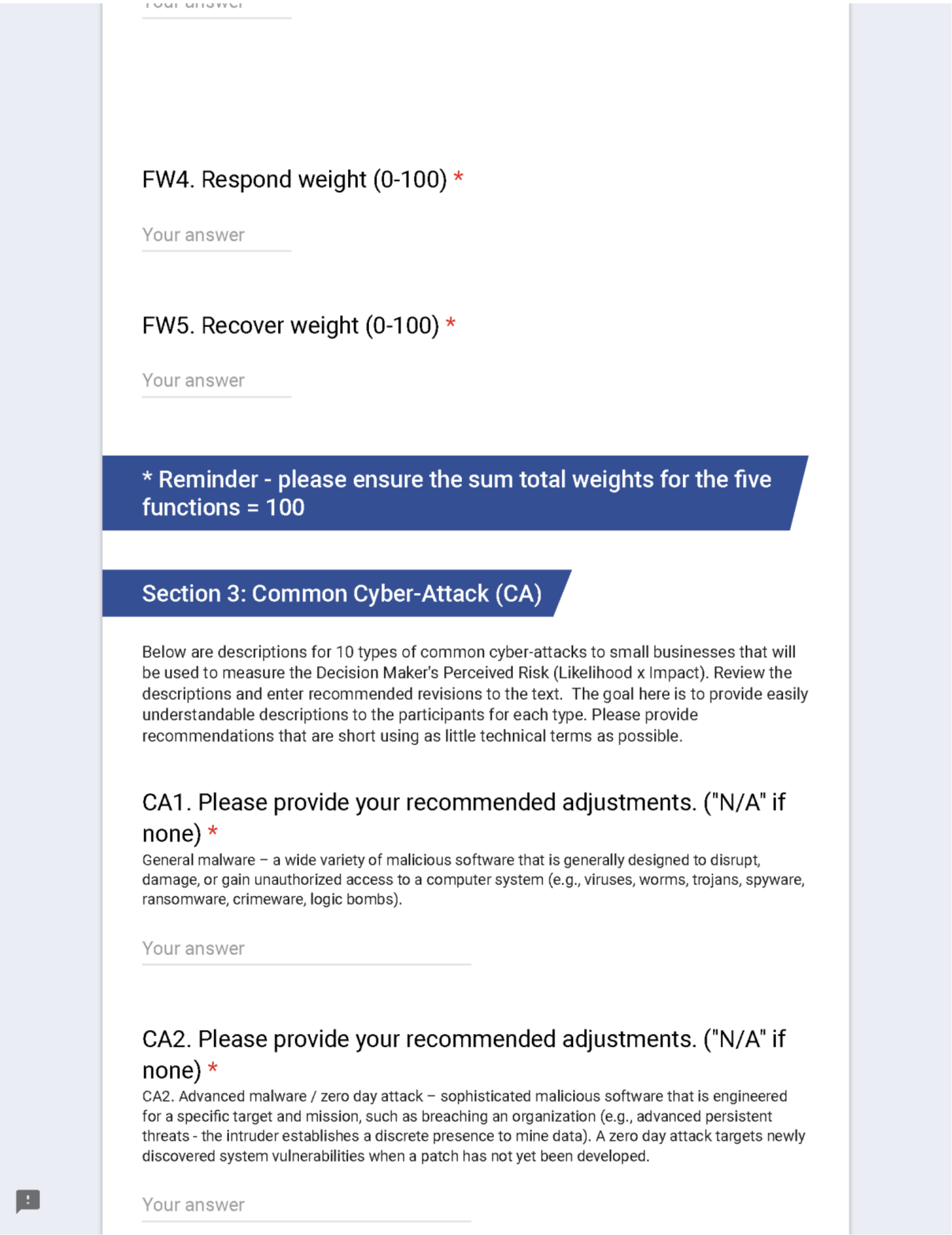
Your answer

FW2. Protect weight (0-100) *

Your answer

FW3. Detect weight (0-100) *

Your answer



Your answer

FW4. Respond weight (0-100) *

Your answer

FW5. Recover weight (0-100) *

Your answer

*** Reminder - please ensure the sum total weights for the five functions = 100**

Section 3: Common Cyber-Attack (CA)

Below are descriptions for 10 types of common cyber-attacks to small businesses that will be used to measure the Decision Maker's Perceived Risk (Likelihood x Impact). Review the descriptions and enter recommended revisions to the text. The goal here is to provide easily understandable descriptions to the participants for each type. Please provide recommendations that are short using as little technical terms as possible.

CA1. Please provide your recommended adjustments. ("N/A" if none) *

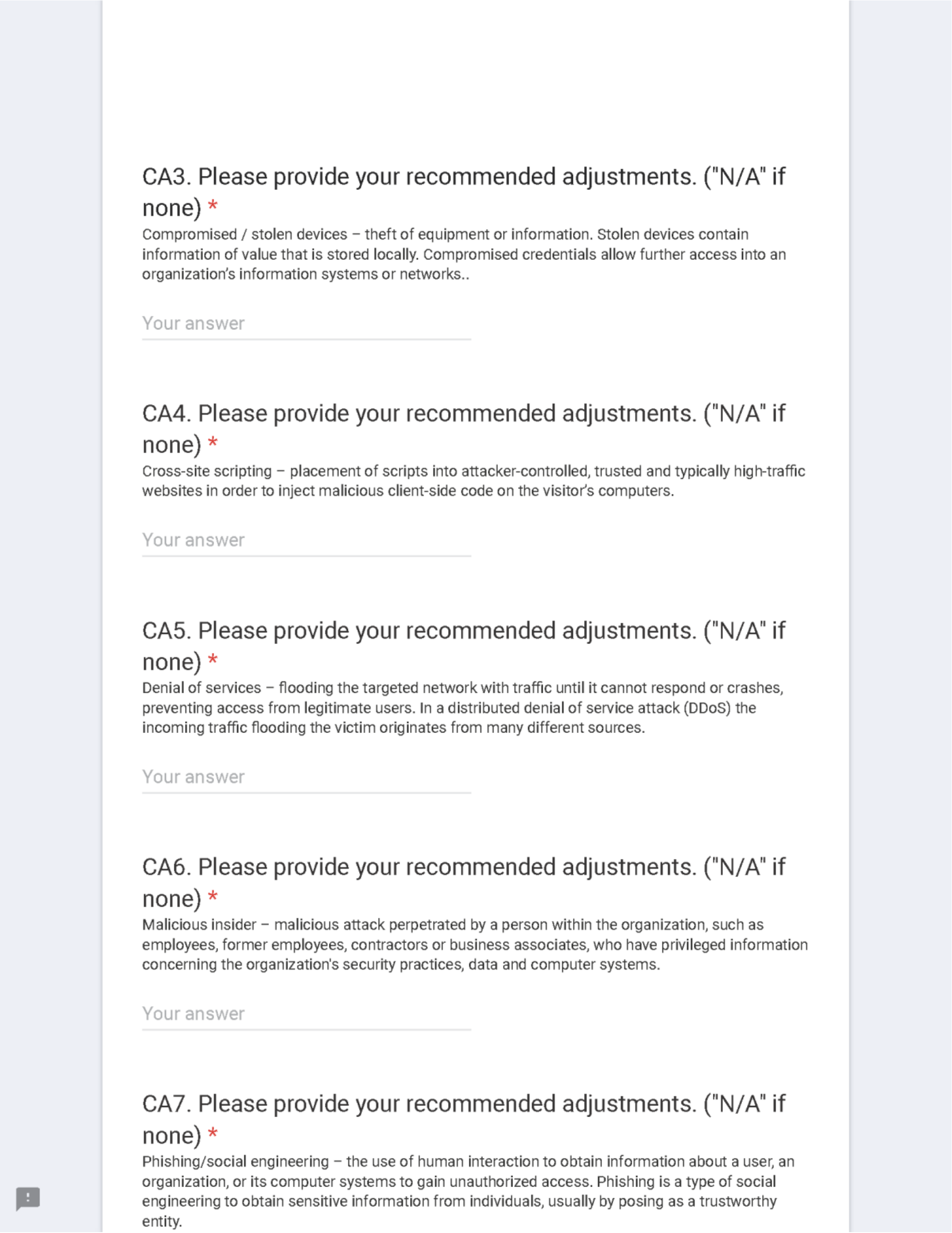
General malware – a wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs).

Your answer

CA2. Please provide your recommended adjustments. ("N/A" if none) *

CA2. Advanced malware / zero day attack – sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats - the intruder establishes a discrete presence to mine data). A zero day attack targets newly discovered system vulnerabilities when a patch has not yet been developed.

Your answer



CA3. Please provide your recommended adjustments. ("N/A" if none) *

Compromised / stolen devices – theft of equipment or information. Stolen devices contain information of value that is stored locally. Compromised credentials allow further access into an organization's information systems or networks..

Your answer

CA4. Please provide your recommended adjustments. ("N/A" if none) *

Cross-site scripting – placement of scripts into attacker-controlled, trusted and typically high-traffic websites in order to inject malicious client-side code on the visitor's computers.

Your answer

CA5. Please provide your recommended adjustments. ("N/A" if none) *

Denial of services – flooding the targeted network with traffic until it cannot respond or crashes, preventing access from legitimate users. In a distributed denial of service attack (DDoS) the incoming traffic flooding the victim originates from many different sources.

Your answer

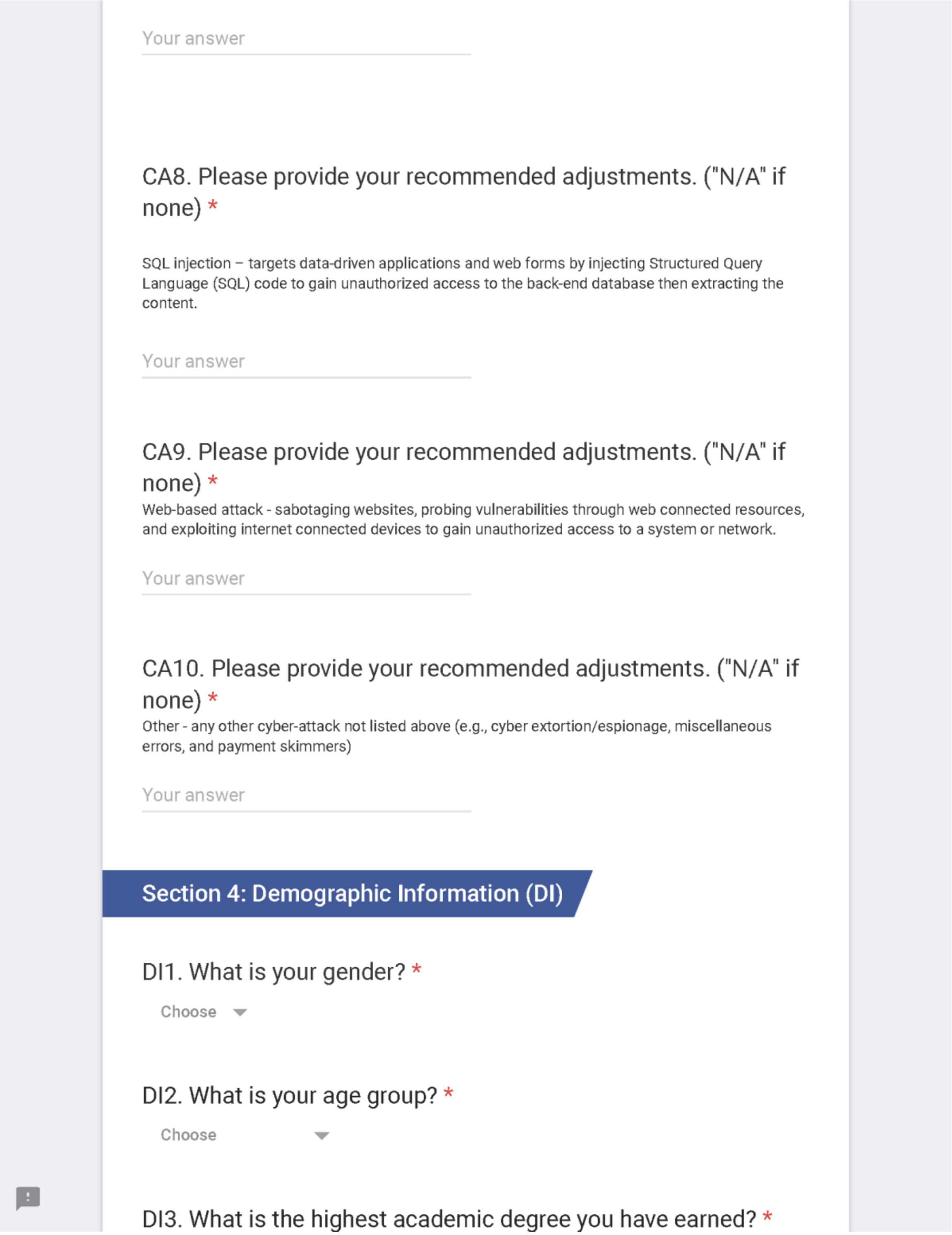
CA6. Please provide your recommended adjustments. ("N/A" if none) *

Malicious insider – malicious attack perpetrated by a person within the organization, such as employees, former employees, contractors or business associates, who have privileged information concerning the organization's security practices, data and computer systems.

Your answer

CA7. Please provide your recommended adjustments. ("N/A" if none) *

Phishing/social engineering – the use of human interaction to obtain information about a user, an organization, or its computer systems to gain unauthorized access. Phishing is a type of social engineering to obtain sensitive information from individuals, usually by posing as a trustworthy entity.



Your answer

CA8. Please provide your recommended adjustments. ("N/A" if none) *

SQL injection – targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database then extracting the content.

Your answer

CA9. Please provide your recommended adjustments. ("N/A" if none) *

Web-based attack - sabotaging websites, probing vulnerabilities through web connected resources, and exploiting internet connected devices to gain unauthorized access to a system or network.

Your answer

CA10. Please provide your recommended adjustments. ("N/A" if none) *

Other - any other cyber-attack not listed above (e.g., cyber extortion/espionage, miscellaneous errors, and payment skimmers)

Your answer

Section 4: Demographic Information (DI)

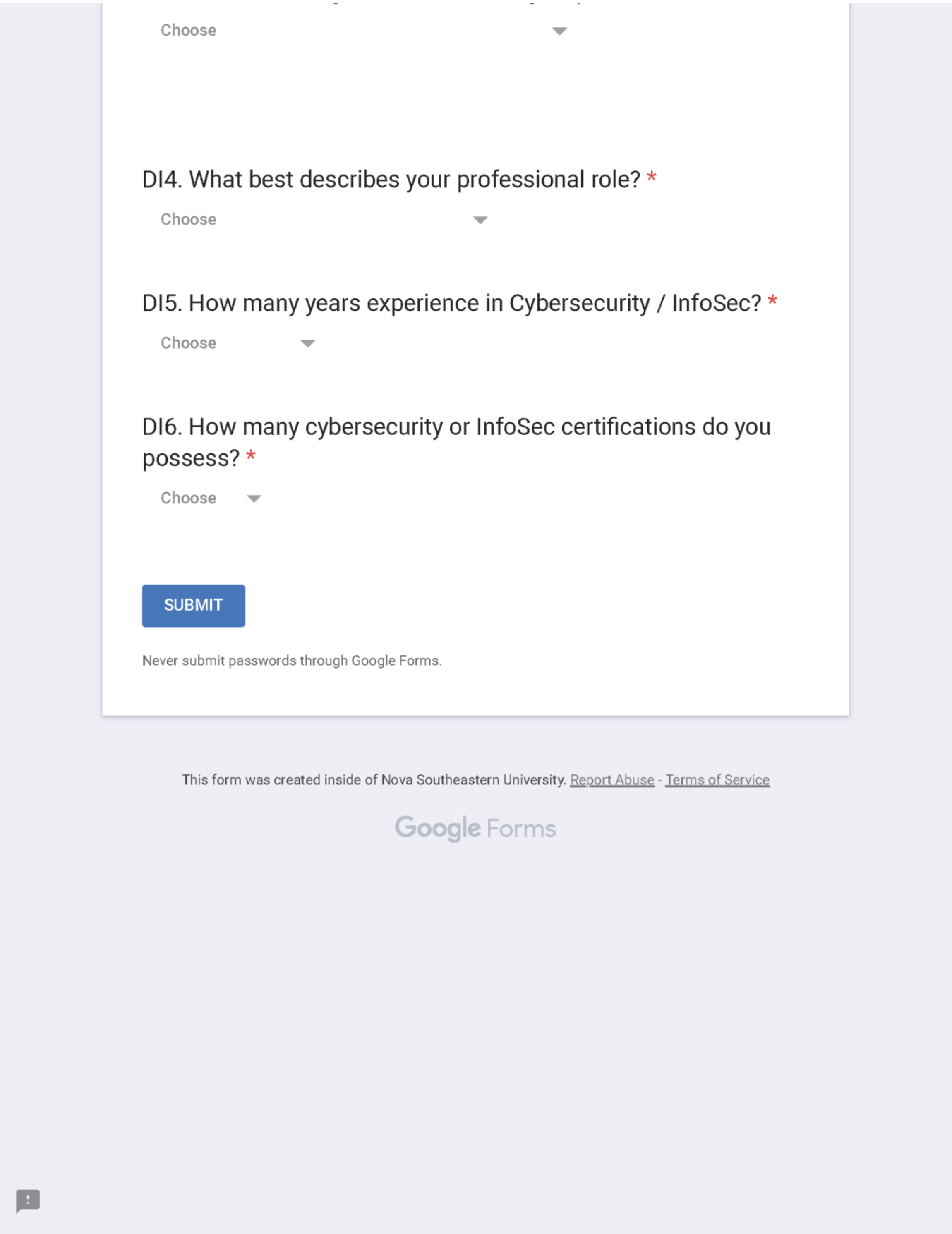
DI1. What is your gender? *

Choose ▾

DI2. What is your age group? *

Choose ▾

DI3. What is the highest academic degree you have earned? *



Choose ▾

DI4. What best describes your professional role? *

Choose ▾

DI5. How many years experience in Cybersecurity / InfoSec? *

Choose ▾

DI6. How many cybersecurity or InfoSec certifications do you possess? *

Choose ▾

SUBMIT

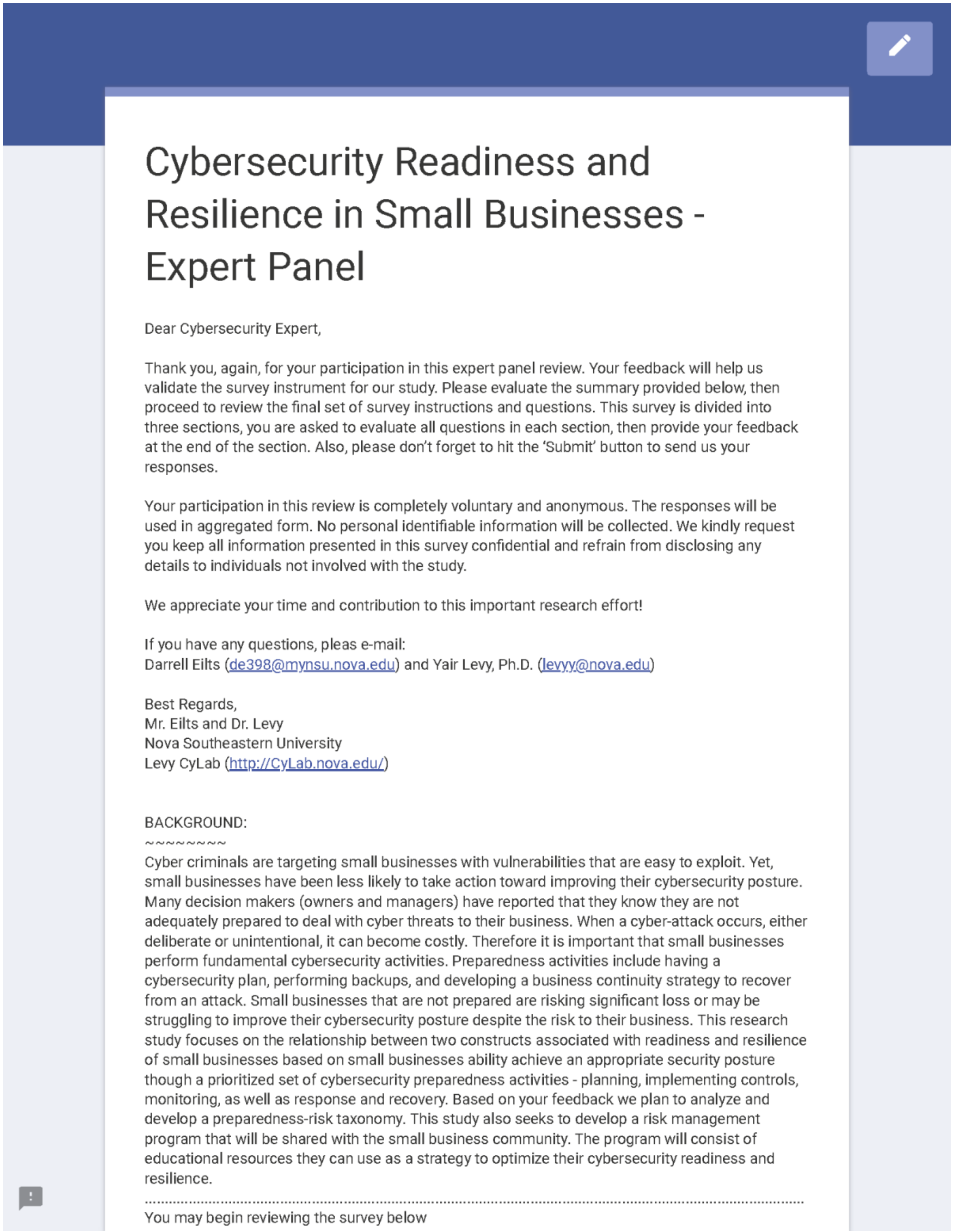
Never submit passwords through Google Forms.

This form was created inside of Nova Southeastern University. Report Abuse - Terms of Service

Google Forms

Appendix D

Phase 1 Expert Panel Survey Instrument (Delphi 2)



Cybersecurity Readiness and Resilience in Small Businesses - Expert Panel

Dear Cybersecurity Expert,

Thank you, again, for your participation in this expert panel review. Your feedback will help us validate the survey instrument for our study. Please evaluate the summary provided below, then proceed to review the final set of survey instructions and questions. This survey is divided into three sections, you are asked to evaluate all questions in each section, then provide your feedback at the end of the section. Also, please don't forget to hit the 'Submit' button to send us your responses.

Your participation in this review is completely voluntary and anonymous. The responses will be used in aggregated form. No personal identifiable information will be collected. We kindly request you keep all information presented in this survey confidential and refrain from disclosing any details to individuals not involved with the study.

We appreciate your time and contribution to this important research effort!

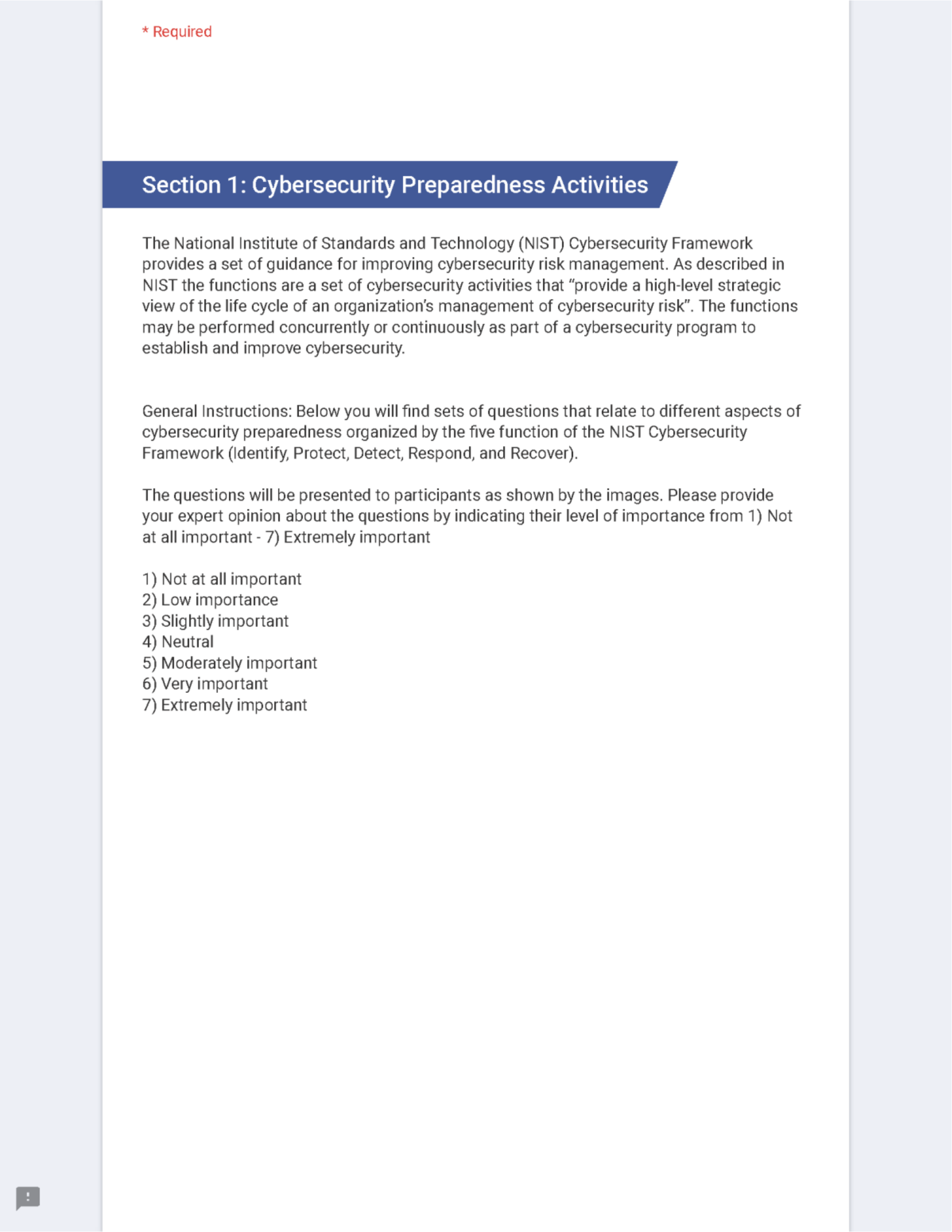
If you have any questions, pleas e-mail:
Darrell Eilts (de398@mynsu.nova.edu) and Yair Levy, Ph.D. (levyy@nova.edu)

Best Regards,
Mr. Eilts and Dr. Levy
Nova Southeastern University
Levy CyLab (http://CyLab.nova.edu/)

BACKGROUND:
~~~~~~~~~
Cyber criminals are targeting small businesses with vulnerabilities that are easy to exploit. Yet, small businesses have been less likely to take action toward improving their cybersecurity posture. Many decision makers (owners and managers) have reported that they know they are not adequately prepared to deal with cyber threats to their business. When a cyber-attack occurs, either deliberate or unintentional, it can become costly. Therefore it is important that small businesses perform fundamental cybersecurity activities. Preparedness activities include having a cybersecurity plan, performing backups, and developing a business continuity strategy to recover from an attack. Small businesses that are not prepared are risking significant loss or may be struggling to improve their cybersecurity posture despite the risk to their business. This research study focuses on the relationship between two constructs associated with readiness and resilience of small businesses based on small businesses ability achieve an appropriate security posture though a prioritized set of cybersecurity preparedness activities - planning, implementing controls, monitoring, as well as response and recovery. Based on your feedback we plan to analyze and develop a preparedness-risk taxonomy. This study also seeks to develop a risk management program that will be shared with the small business community. The program will consist of educational resources they can use as a strategy to optimize their cybersecurity readiness and resilience.

....

You may begin reviewing the survey below
~~~~~~~~~



* Required

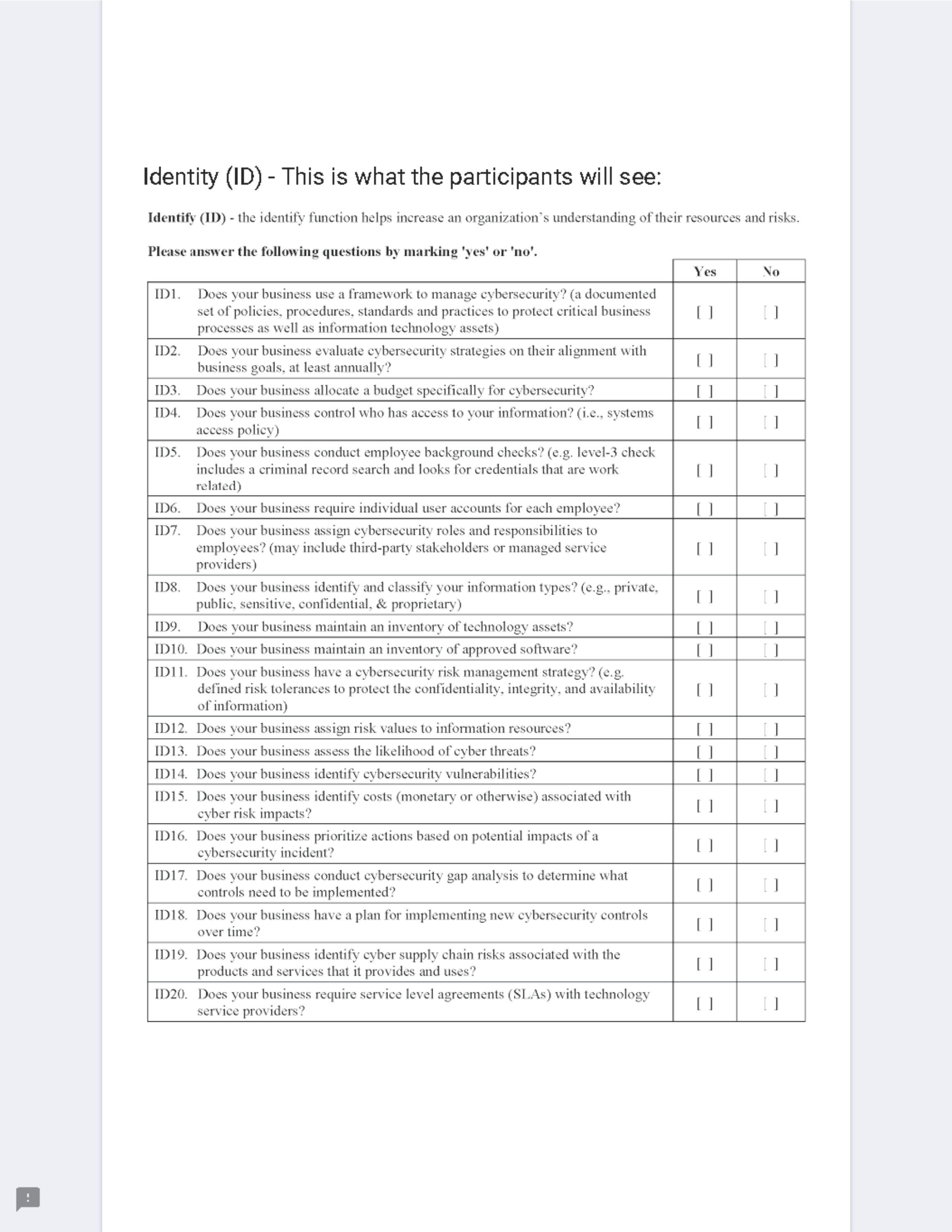
Section 1: Cybersecurity Preparedness Activities

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of guidance for improving cybersecurity risk management. As described in NIST the functions are a set of cybersecurity activities that “provide a high-level strategic view of the life cycle of an organization’s management of cybersecurity risk”. The functions may be performed concurrently or continuously as part of a cybersecurity program to establish and improve cybersecurity.

General Instructions: Below you will find sets of questions that relate to different aspects of cybersecurity preparedness organized by the five function of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

The questions will be presented to participants as shown by the images. Please provide your expert opinion about the questions by indicating their level of importance from 1) Not at all important - 7) Extremely important

1) Not at all important
2) Low importance
3) Slightly important
4) Neutral
5) Moderately important
6) Very important
7) Extremely important

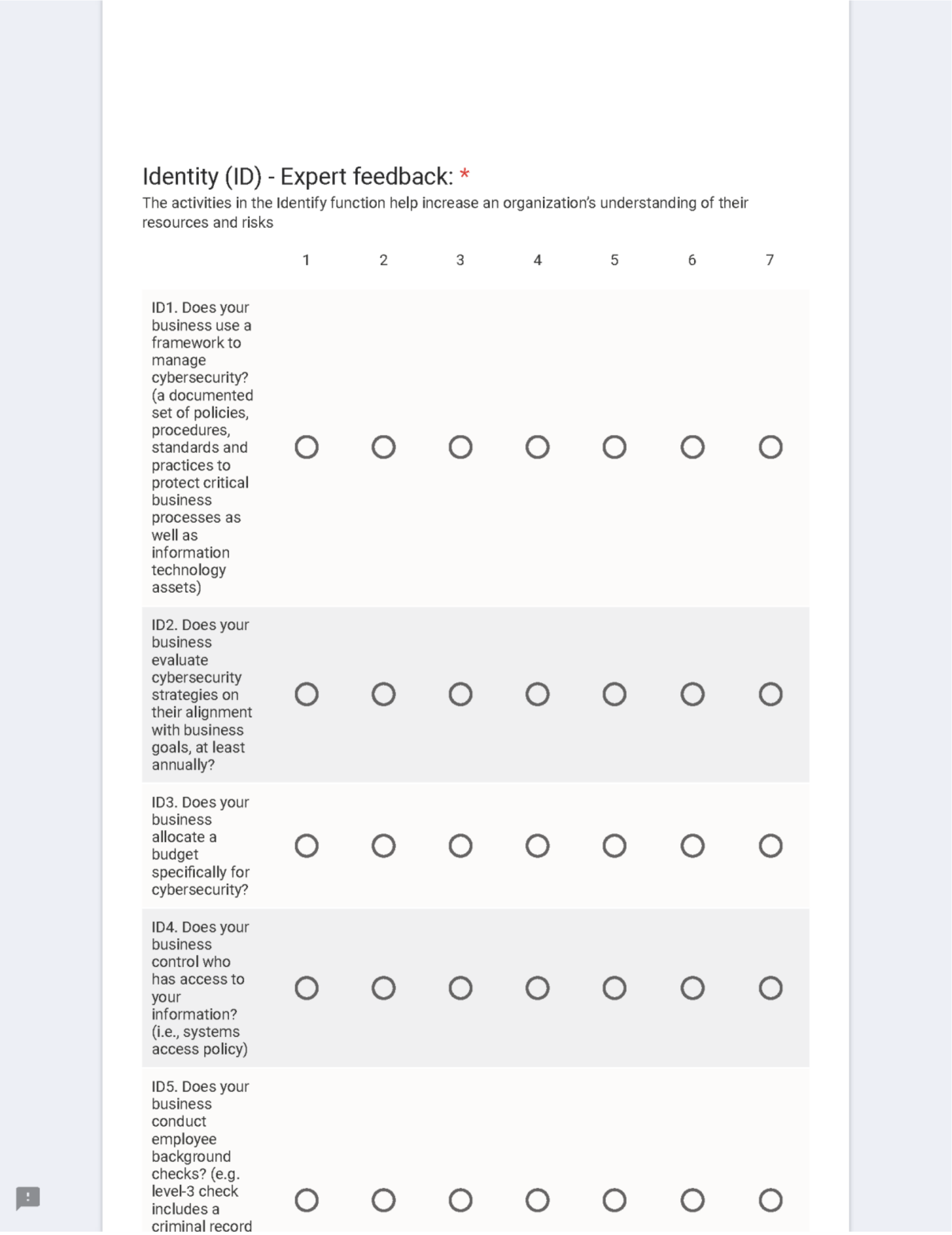


Identity (ID) - This is what the participants will see:

Identify (ID) - the identify function helps increase an organization's understanding of their resources and risks.

Please answer the following questions by marking 'yes' or 'no'.

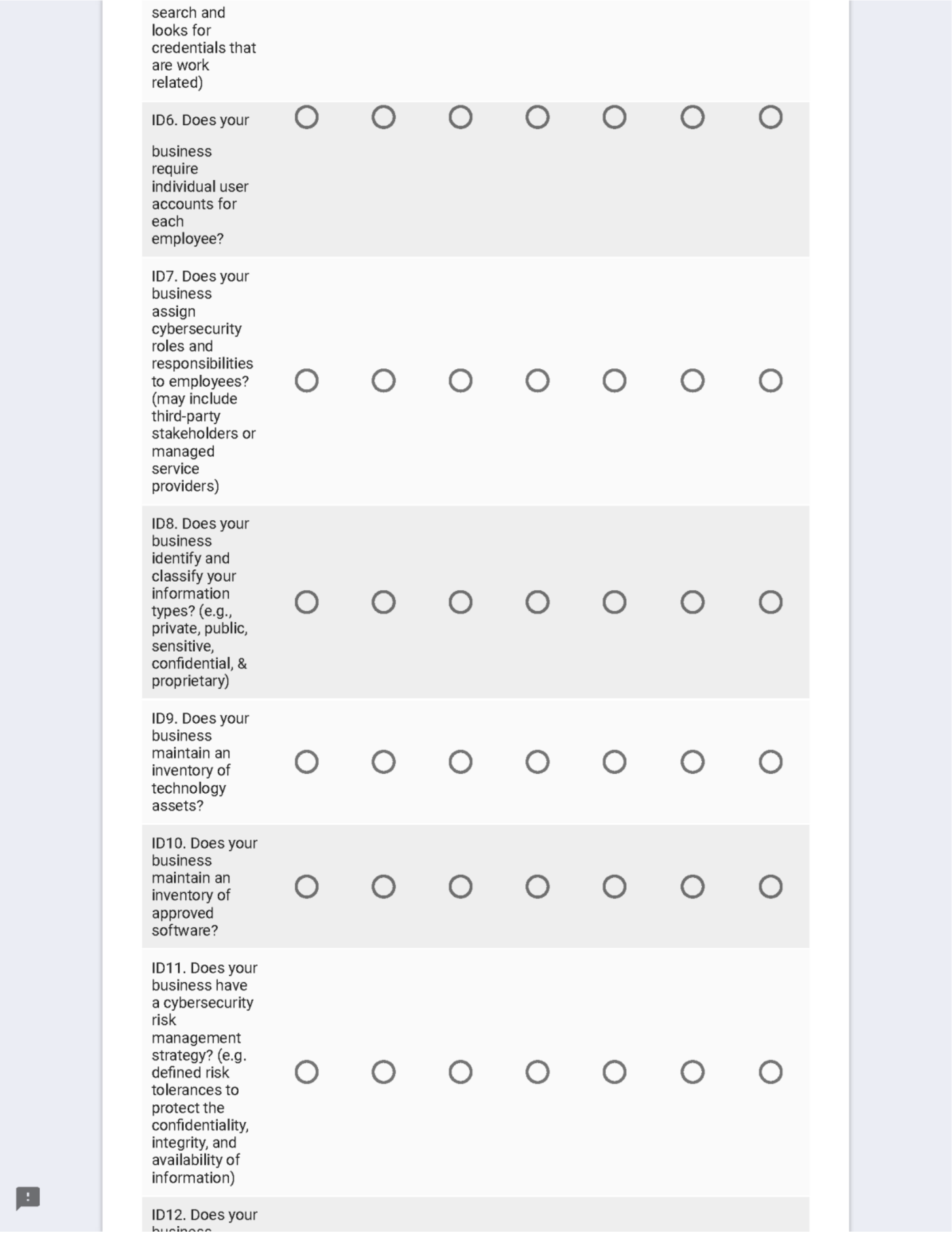
	Yes	**No**
ID1. Does your business use a framework to manage cybersecurity? (a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets)	[ ]	[ ]
ID2. Does your business evaluate cybersecurity strategies on their alignment with business goals, at least annually?	[ ]	[ ]
ID3. Does your business allocate a budget specifically for cybersecurity?	[ ]	[ ]
ID4. Does your business control who has access to your information? (i.e., systems access policy)	[ ]	[ ]
ID5. Does your business conduct employee background checks? (e.g. level-3 check includes a criminal record search and looks for credentials that are work related)	[ ]	[ ]
ID6. Does your business require individual user accounts for each employee?	[ ]	[ ]
ID7. Does your business assign cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	[ ]	[ ]
ID8. Does your business identify and classify your information types? (e.g., private, public, sensitive, confidential, & proprietary)	[ ]	[ ]
ID9. Does your business maintain an inventory of technology assets?	[ ]	[ ]
ID10. Does your business maintain an inventory of approved software?	[ ]	[ ]
ID11. Does your business have a cybersecurity risk management strategy? (e.g. defined risk tolerances to protect the confidentiality, integrity, and availability of information)	[ ]	[ ]
ID12. Does your business assign risk values to information resources?	[ ]	[ ]
ID13. Does your business assess the likelihood of cyber threats?	[ ]	[ ]
ID14. Does your business identify cybersecurity vulnerabilities?	[ ]	[ ]
ID15. Does your business identify costs (monetary or otherwise) associated with cyber risk impacts?	[ ]	[ ]
ID16. Does your business prioritize actions based on potential impacts of a cybersecurity incident?	[ ]	[ ]
ID17. Does your business conduct cybersecurity gap analysis to determine what controls need to be implemented?	[ ]	[ ]
ID18. Does your business have a plan for implementing new cybersecurity controls over time?	[ ]	[ ]
ID19. Does your business identify cyber supply chain risks associated with the products and services that it provides and uses?	[ ]	[ ]
ID20. Does your business require service level agreements (SLAs) with technology service providers?	[ ]	[ ]



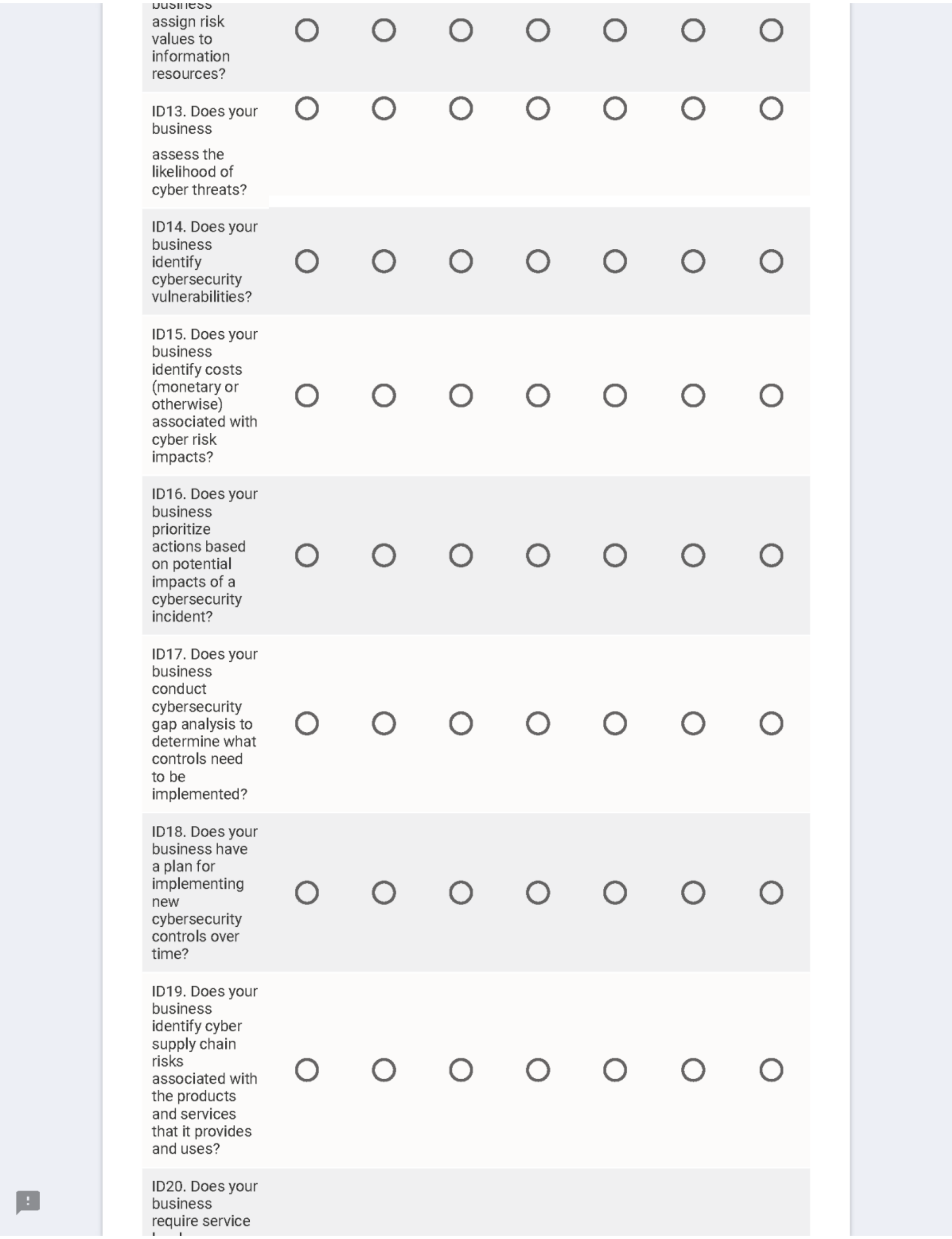
Identity (ID) - Expert feedback: *

The activities in the Identify function help increase an organization's understanding of their resources and risks

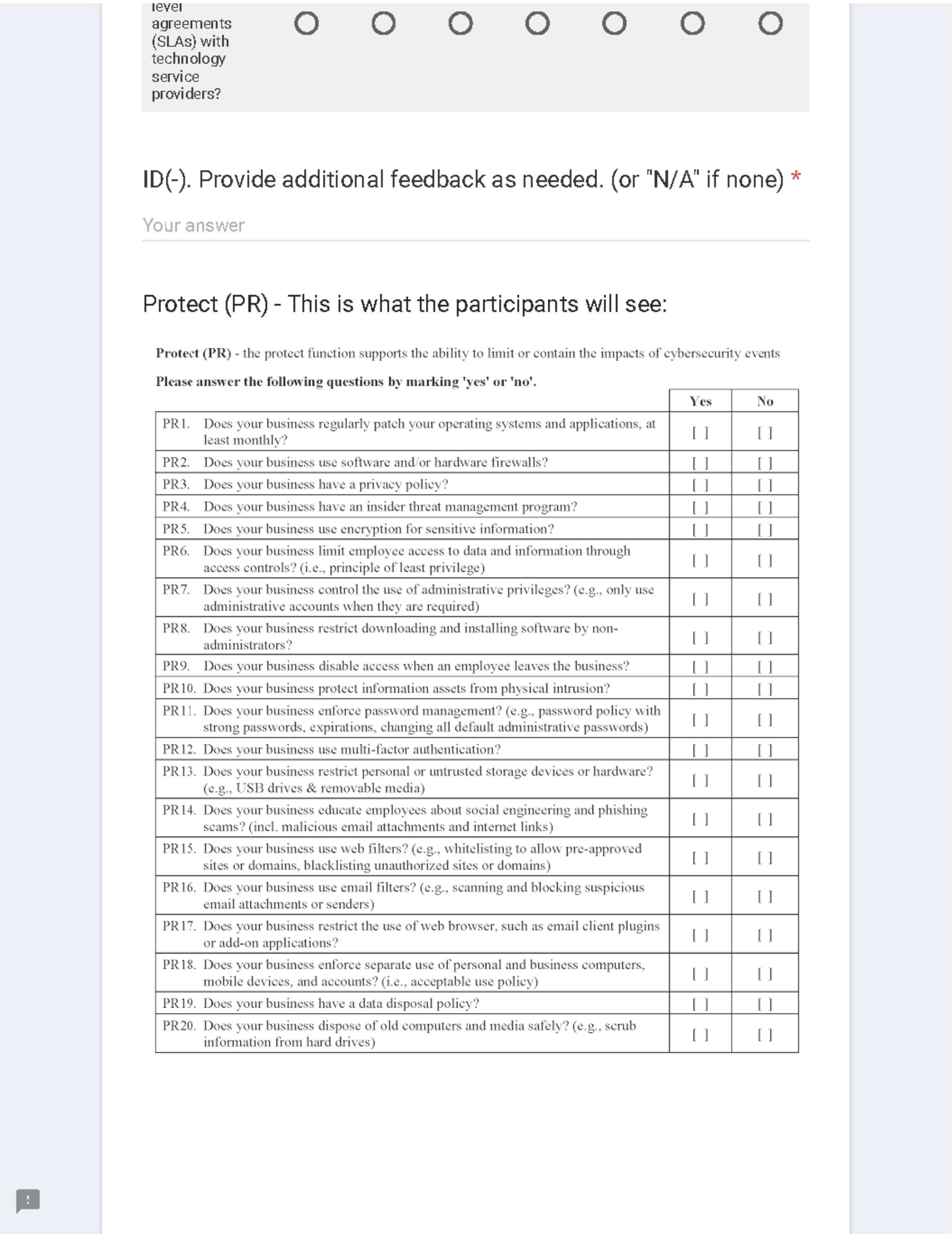
	1	2	3	4	5	6	7
ID1. Does your business use a framework to manage cybersecurity? (a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets)	○	○	○	○	○	○	○
ID2. Does your business evaluate cybersecurity strategies on their alignment with business goals, at least annually?	○	○	○	○	○	○	○
ID3. Does your business allocate a budget specifically for cybersecurity?	○	○	○	○	○	○	○
ID4. Does your business control who has access to your information? (i.e., systems access policy)	○	○	○	○	○	○	○
ID5. Does your business conduct employee background checks? (e.g. level-3 check includes a criminal record	○	○	○	○	○	○	○



search and looks for credentials that are work related)							
ID6. Does your business require individual user accounts for each employee?	○	○	○	○	○	○	○
ID7. Does your business assign cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	○	○	○	○	○	○	○
ID8. Does your business identify and classify your information types? (e.g., private, public, sensitive, confidential, & proprietary)	○	○	○	○	○	○	○
ID9. Does your business maintain an inventory of technology assets?	○	○	○	○	○	○	○
ID10. Does your business maintain an inventory of approved software?	○	○	○	○	○	○	○
ID11. Does your business have a cybersecurity risk management strategy? (e.g. defined risk tolerances to protect the confidentiality, integrity, and availability of information)	○	○	○	○	○	○	○
ID12. Does your							



business assign risk values to information resources?	○	○	○	○	○	○	○
ID13. Does your business assess the likelihood of cyber threats?	○	○	○	○	○	○	○
ID14. Does your business identify cybersecurity vulnerabilities?	○	○	○	○	○	○	○
ID15. Does your business identify costs (monetary or otherwise) associated with cyber risk impacts?	○	○	○	○	○	○	○
ID16. Does your business prioritize actions based on potential impacts of a cybersecurity incident?	○	○	○	○	○	○	○
ID17. Does your business conduct cybersecurity gap analysis to determine what controls need to be implemented?	○	○	○	○	○	○	○
ID18. Does your business have a plan for implementing new cybersecurity controls over time?	○	○	○	○	○	○	○
ID19. Does your business identify cyber supply chain risks associated with the products and services that it provides and uses?	○	○	○	○	○	○	○
ID20. Does your business require service							



level agreements (SLAs) with technology service providers?	○	○	○	○	○	○	○

ID(-). Provide additional feedback as needed. (or "N/A" if none) *

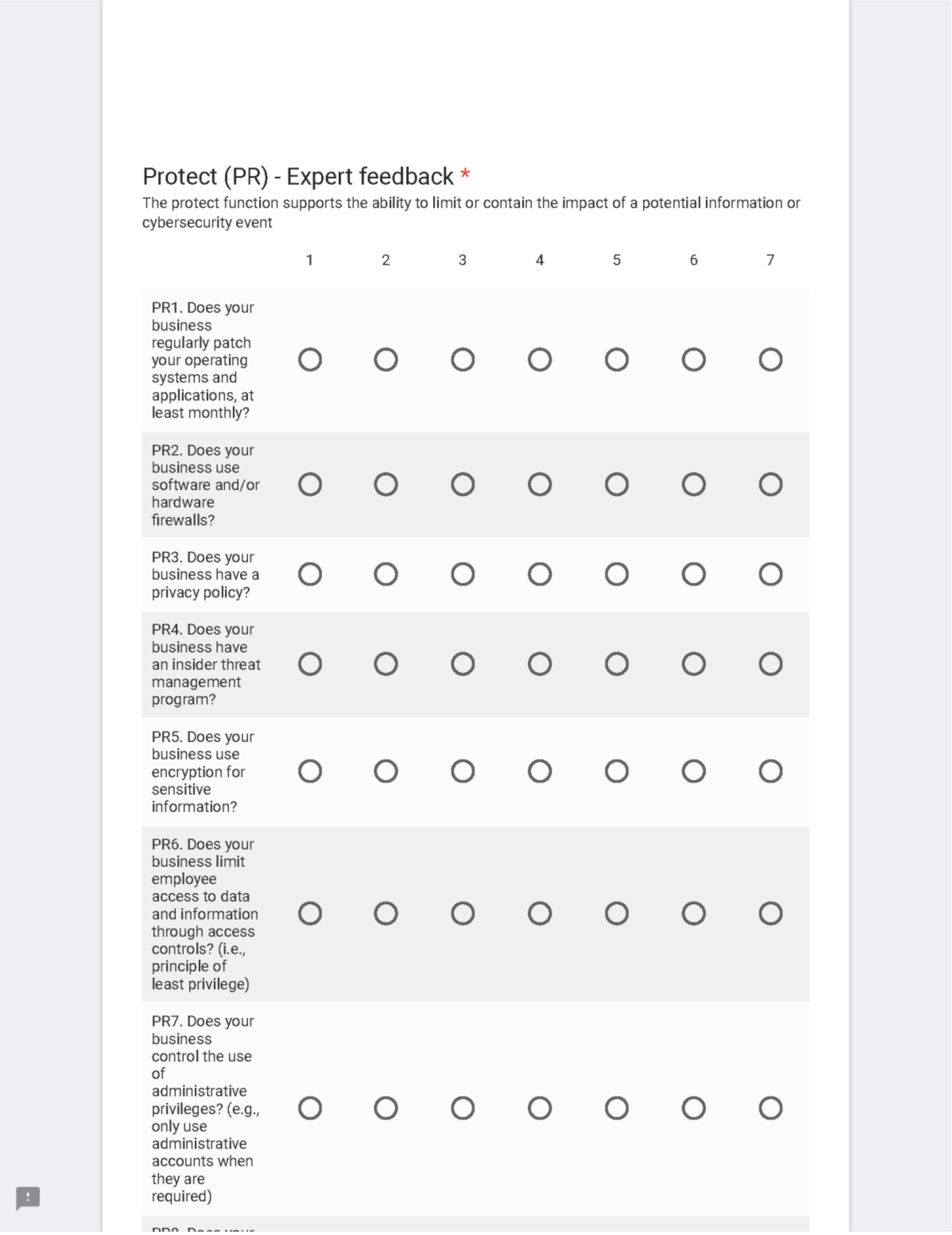
Your answer

Protect (PR) - This is what the participants will see:

Protect (PR) - the protect function supports the ability to limit or contain the impacts of cybersecurity events

Please answer the following questions by marking 'yes' or 'no'.

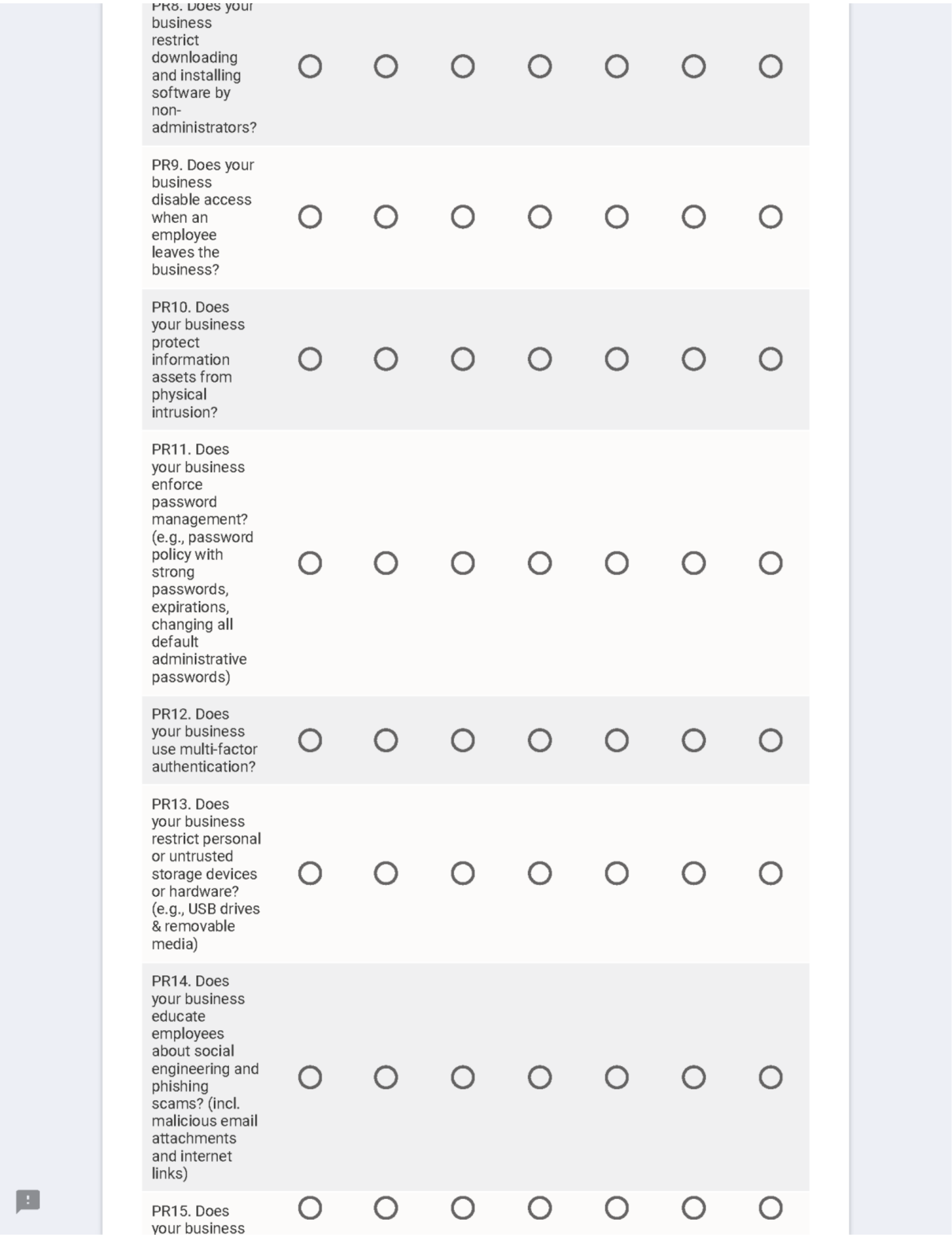
		Yes	No
PR1.	Does your business regularly patch your operating systems and applications, at least monthly?	[ ]	[ ]
PR2.	Does your business use software and/or hardware firewalls?	[ ]	[ ]
PR3.	Does your business have a privacy policy?	[ ]	[ ]
PR4.	Does your business have an insider threat management program?	[ ]	[ ]
PR5.	Does your business use encryption for sensitive information?	[ ]	[ ]
PR6.	Does your business limit employee access to data and information through access controls? (i.e., principle of least privilege)	[ ]	[ ]
PR7.	Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	[ ]	[ ]
PR8.	Does your business restrict downloading and installing software by non-administrators?	[ ]	[ ]
PR9.	Does your business disable access when an employee leaves the business?	[ ]	[ ]
PR10.	Does your business protect information assets from physical intrusion?	[ ]	[ ]
PR11.	Does your business enforce password management? (e.g., password policy with strong passwords, expirations, changing all default administrative passwords)	[ ]	[ ]
PR12.	Does your business use multi-factor authentication?	[ ]	[ ]
PR13.	Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	[ ]	[ ]
PR14.	Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	[ ]	[ ]
PR15.	Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	[ ]	[ ]
PR16.	Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	[ ]	[ ]
PR17.	Does your business restrict the use of web browser, such as email client plugins or add-on applications?	[ ]	[ ]
PR18.	Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (i.e., acceptable use policy)	[ ]	[ ]
PR19.	Does your business have a data disposal policy?	[ ]	[ ]
PR20.	Does your business dispose of old computers and media safely? (e.g., scrub information from hard drives)	[ ]	[ ]



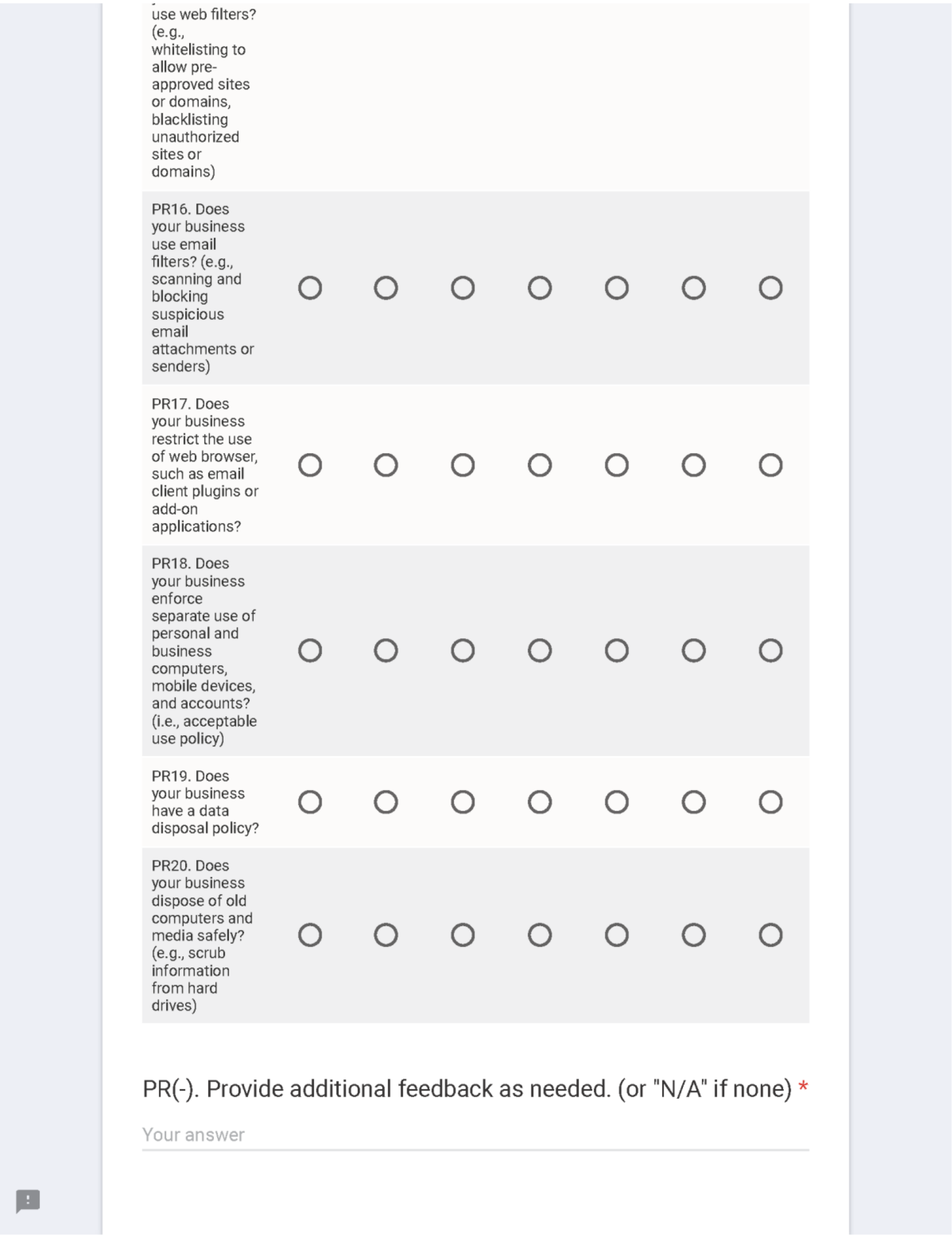
Protect (PR) - Expert feedback *

The protect function supports the ability to limit or contain the impact of a potential information or cybersecurity event

	1	2	3	4	5	6	7
PR1. Does your business regularly patch your operating systems and applications, at least monthly?	○	○	○	○	○	○	○
PR2. Does your business use software and/or hardware firewalls?	○	○	○	○	○	○	○
PR3. Does your business have a privacy policy?	○	○	○	○	○	○	○
PR4. Does your business have an insider threat management program?	○	○	○	○	○	○	○
PR5. Does your business use encryption for sensitive information?	○	○	○	○	○	○	○
PR6. Does your business limit employee access to data and information through access controls? (i.e., principle of least privilege)	○	○	○	○	○	○	○
PR7. Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	○	○	○	○	○	○	○
PR8. Does your							



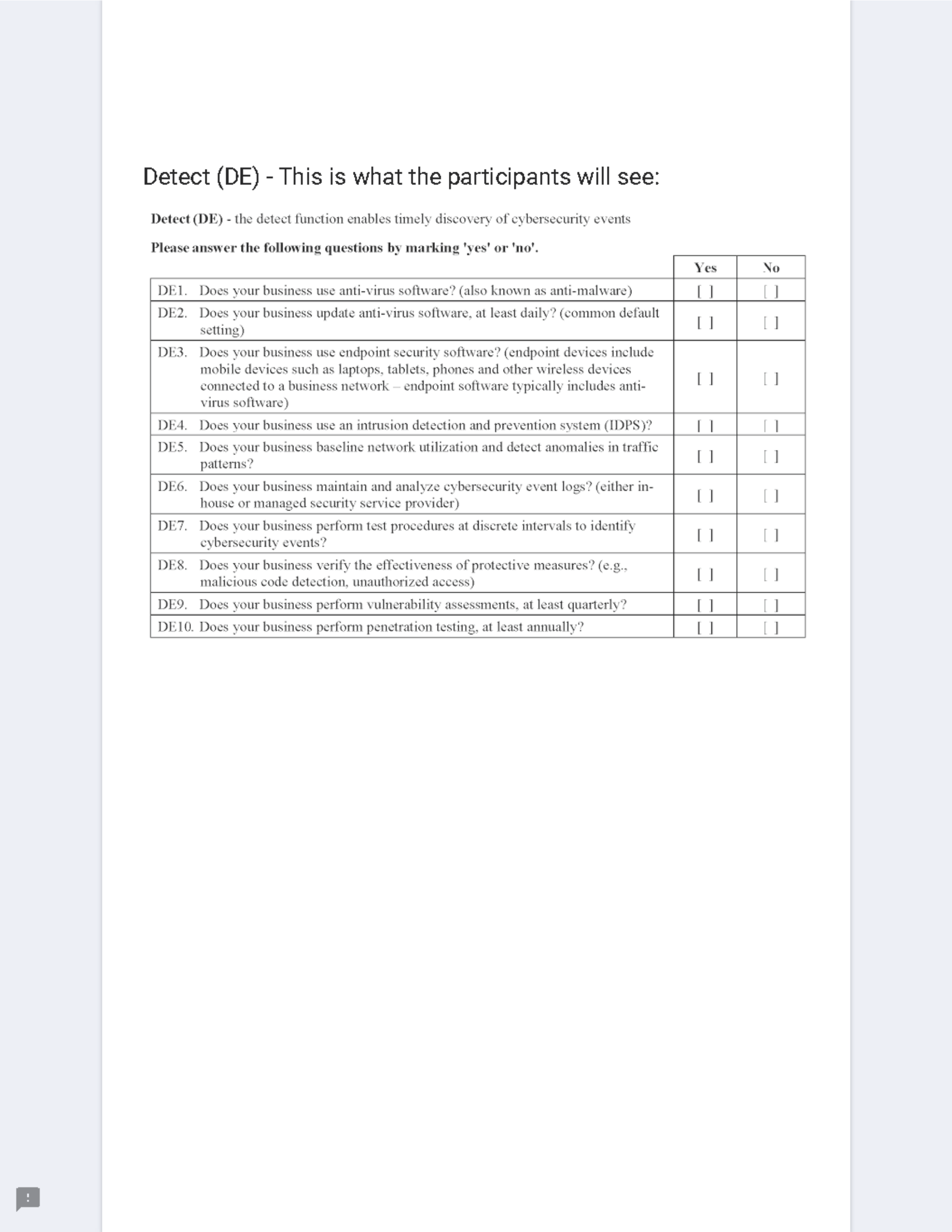
PR8. Does your business restrict downloading and installing software by non-administrators?	○	○	○	○	○	○	○
PR9. Does your business disable access when an employee leaves the business?	○	○	○	○	○	○	○
PR10. Does your business protect information assets from physical intrusion?	○	○	○	○	○	○	○
PR11. Does your business enforce password management? (e.g., password policy with strong passwords, expirations, changing all default administrative passwords)	○	○	○	○	○	○	○
PR12. Does your business use multi-factor authentication?	○	○	○	○	○	○	○
PR13. Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	○	○	○	○	○	○	○
PR14. Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	○	○	○	○	○	○	○
PR15. Does your business	○	○	○	○	○	○	○



use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)							
PR16. Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	○	○	○	○	○	○	○
PR17. Does your business restrict the use of web browser, such as email client plugins or add-on applications?	○	○	○	○	○	○	○
PR18. Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (i.e., acceptable use policy)	○	○	○	○	○	○	○
PR19. Does your business have a data disposal policy?	○	○	○	○	○	○	○
PR20. Does your business dispose of old computers and media safely? (e.g., scrub information from hard drives)	○	○	○	○	○	○	○

PR(-). Provide additional feedback as needed. (or "N/A" if none) *

Your answer

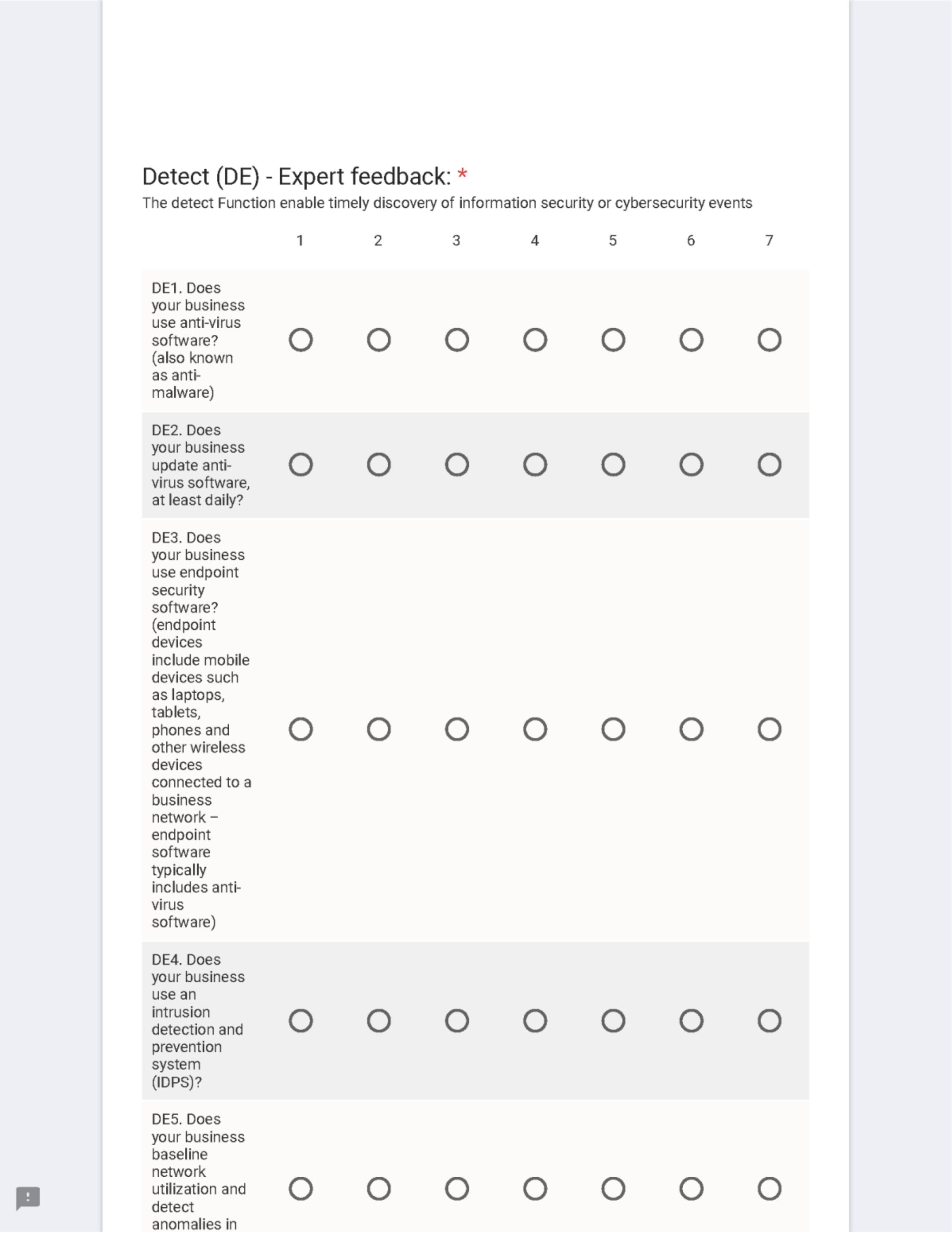


Detect (DE) - This is what the participants will see:

Detect (DE) - the detect function enables timely discovery of cybersecurity events

Please answer the following questions by marking 'yes' or 'no'.

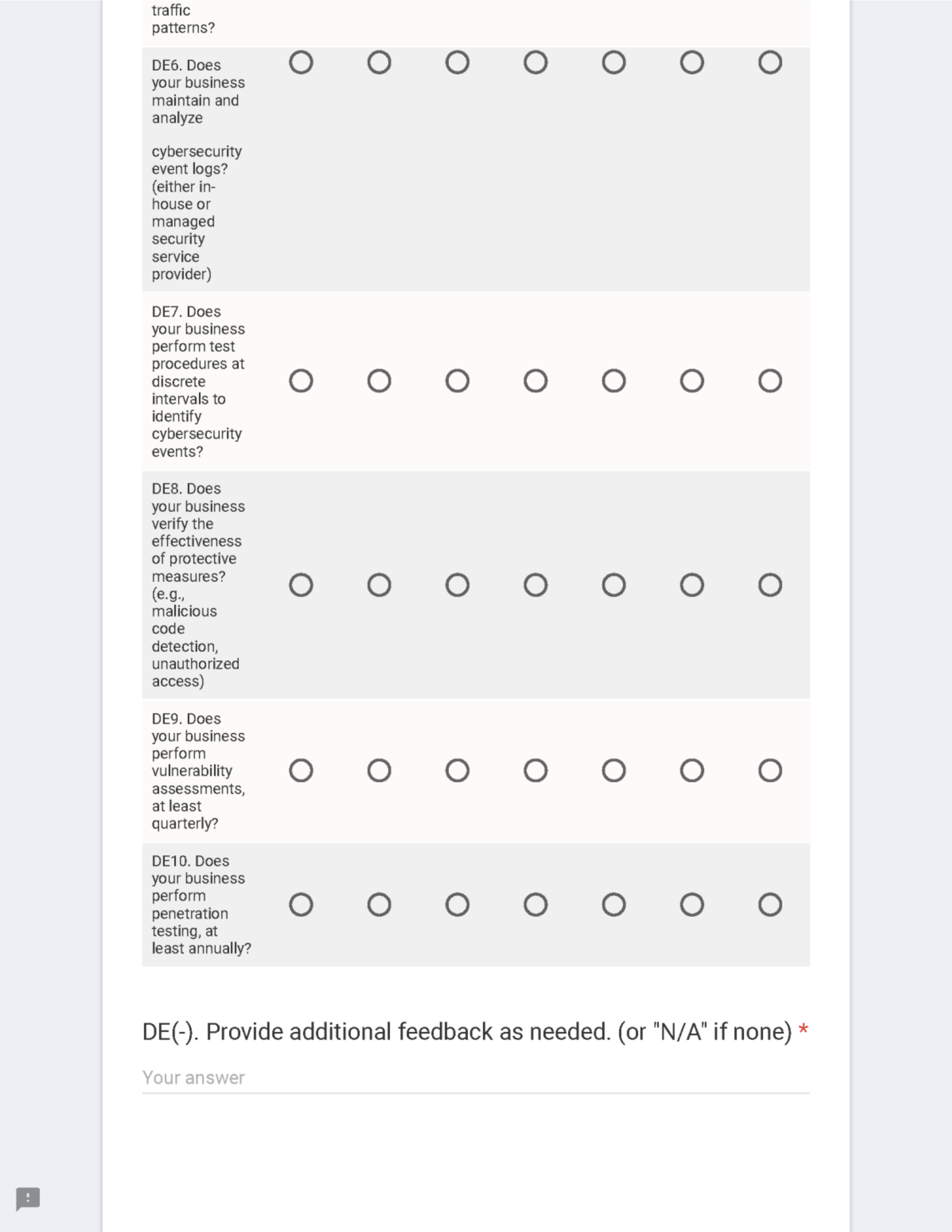
	Yes	No
DE1. Does your business use anti-virus software? (also known as anti-malware)	[ ]	[ ]
DE2. Does your business update anti-virus software, at least daily? (common default setting)	[ ]	[ ]
DE3. Does your business use endpoint security software? (endpoint devices include mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network – endpoint software typically includes anti-virus software)	[ ]	[ ]
DE4. Does your business use an intrusion detection and prevention system (IDPS)?	[ ]	[ ]
DE5. Does your business baseline network utilization and detect anomalies in traffic patterns?	[ ]	[ ]
DE6. Does your business maintain and analyze cybersecurity event logs? (either in-house or managed security service provider)	[ ]	[ ]
DE7. Does your business perform test procedures at discrete intervals to identify cybersecurity events?	[ ]	[ ]
DE8. Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	[ ]	[ ]
DE9. Does your business perform vulnerability assessments, at least quarterly?	[ ]	[ ]
DE10. Does your business perform penetration testing, at least annually?	[ ]	[ ]



Detect (DE) - Expert feedback: *

The detect Function enable timely discovery of information security or cybersecurity events

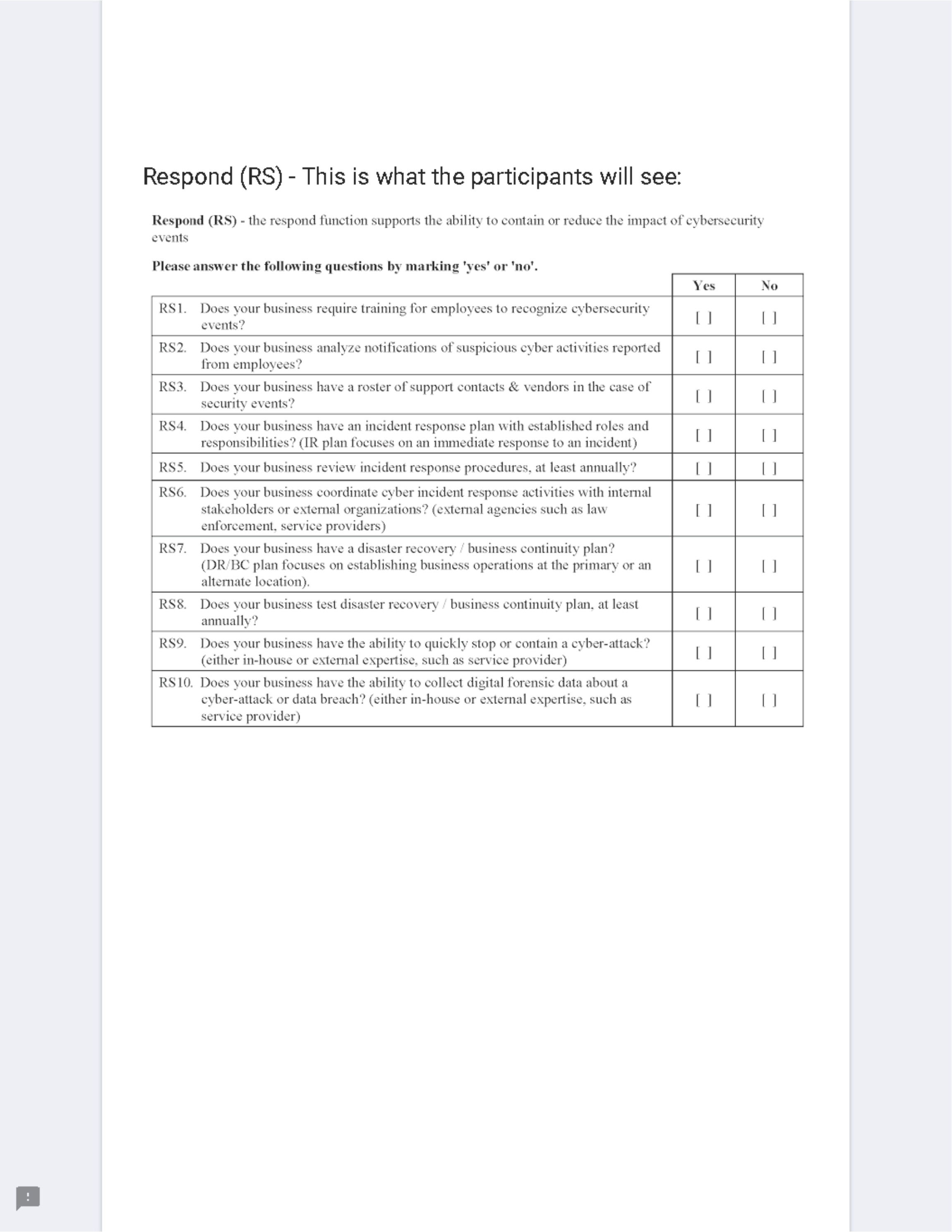
	1	2	3	4	5	6	7
DE1. Does your business use anti-virus software? (also known as anti-malware)	○	○	○	○	○	○	○
DE2. Does your business update anti-virus software, at least daily?	○	○	○	○	○	○	○
DE3. Does your business use endpoint security software? (endpoint devices include mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network – endpoint software typically includes anti-virus software)	○	○	○	○	○	○	○
DE4. Does your business use an intrusion detection and prevention system (IDPS)?	○	○	○	○	○	○	○
DE5. Does your business baseline network utilization and detect anomalies in	○	○	○	○	○	○	○



traffic patterns?							
DE6. Does your business maintain and analyze cybersecurity event logs? (either in-house or managed security service provider)	○	○	○	○	○	○	○
DE7. Does your business perform test procedures at discrete intervals to identify cybersecurity events?	○	○	○	○	○	○	○
DE8. Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	○	○	○	○	○	○	○
DE9. Does your business perform vulnerability assessments, at least quarterly?	○	○	○	○	○	○	○
DE10. Does your business perform penetration testing, at least annually?	○	○	○	○	○	○	○

DE(-). Provide additional feedback as needed. (or "N/A" if none) *

Your answer

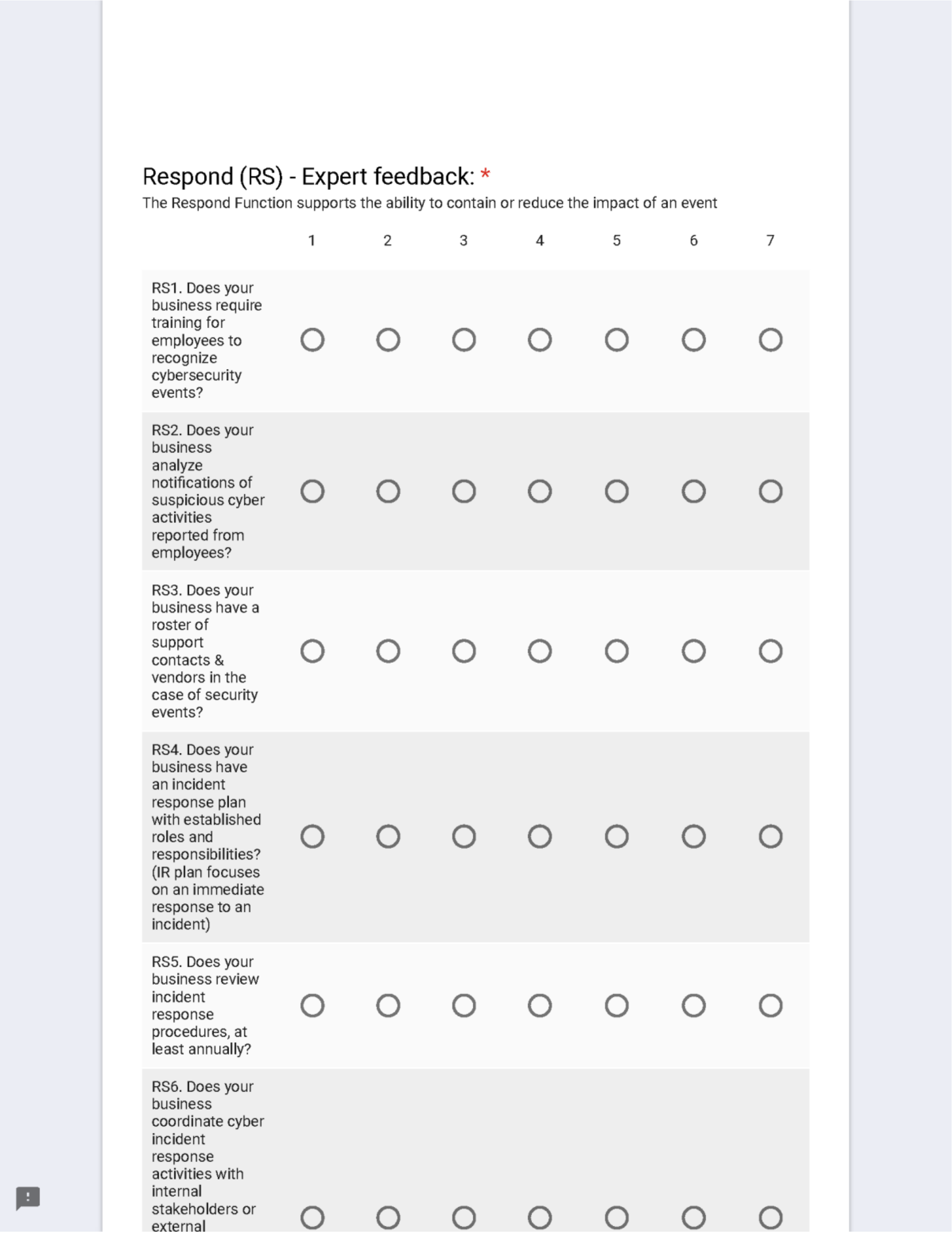


Respond (RS) - This is what the participants will see:

Respond (RS) - the respond function supports the ability to contain or reduce the impact of cybersecurity events

Please answer the following questions by marking 'yes' or 'no'.

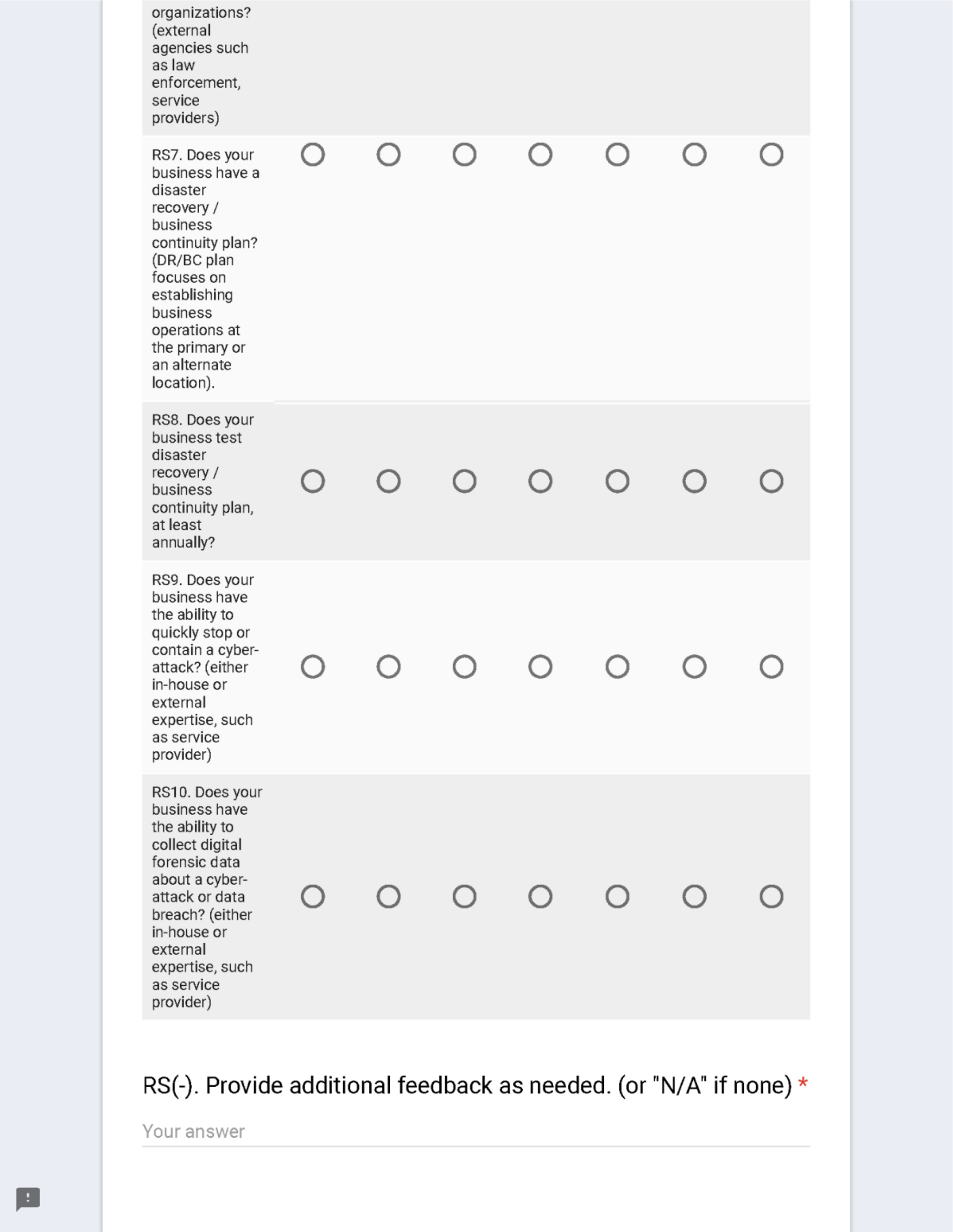
	Yes	**No**
RS1. Does your business require training for employees to recognize cybersecurity events?	[ ]	[ ]
RS2. Does your business analyze notifications of suspicious cyber activities reported from employees?	[ ]	[ ]
RS3. Does your business have a roster of support contacts & vendors in the case of security events?	[ ]	[ ]
RS4. Does your business have an incident response plan with established roles and responsibilities? (IR plan focuses on an immediate response to an incident)	[ ]	[ ]
RS5. Does your business review incident response procedures, at least annually?	[ ]	[ ]
RS6. Does your business coordinate cyber incident response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	[ ]	[ ]
RS7. Does your business have a disaster recovery / business continuity plan? (DR/BC plan focuses on establishing business operations at the primary or an alternate location).	[ ]	[ ]
RS8. Does your business test disaster recovery / business continuity plan, at least annually?	[ ]	[ ]
RS9. Does your business have the ability to quickly stop or contain a cyber-attack? (either in-house or external expertise, such as service provider)	[ ]	[ ]
RS10. Does your business have the ability to collect digital forensic data about a cyber-attack or data breach? (either in-house or external expertise, such as service provider)	[ ]	[ ]



Respond (RS) - Expert feedback: *

The Respond Function supports the ability to contain or reduce the impact of an event

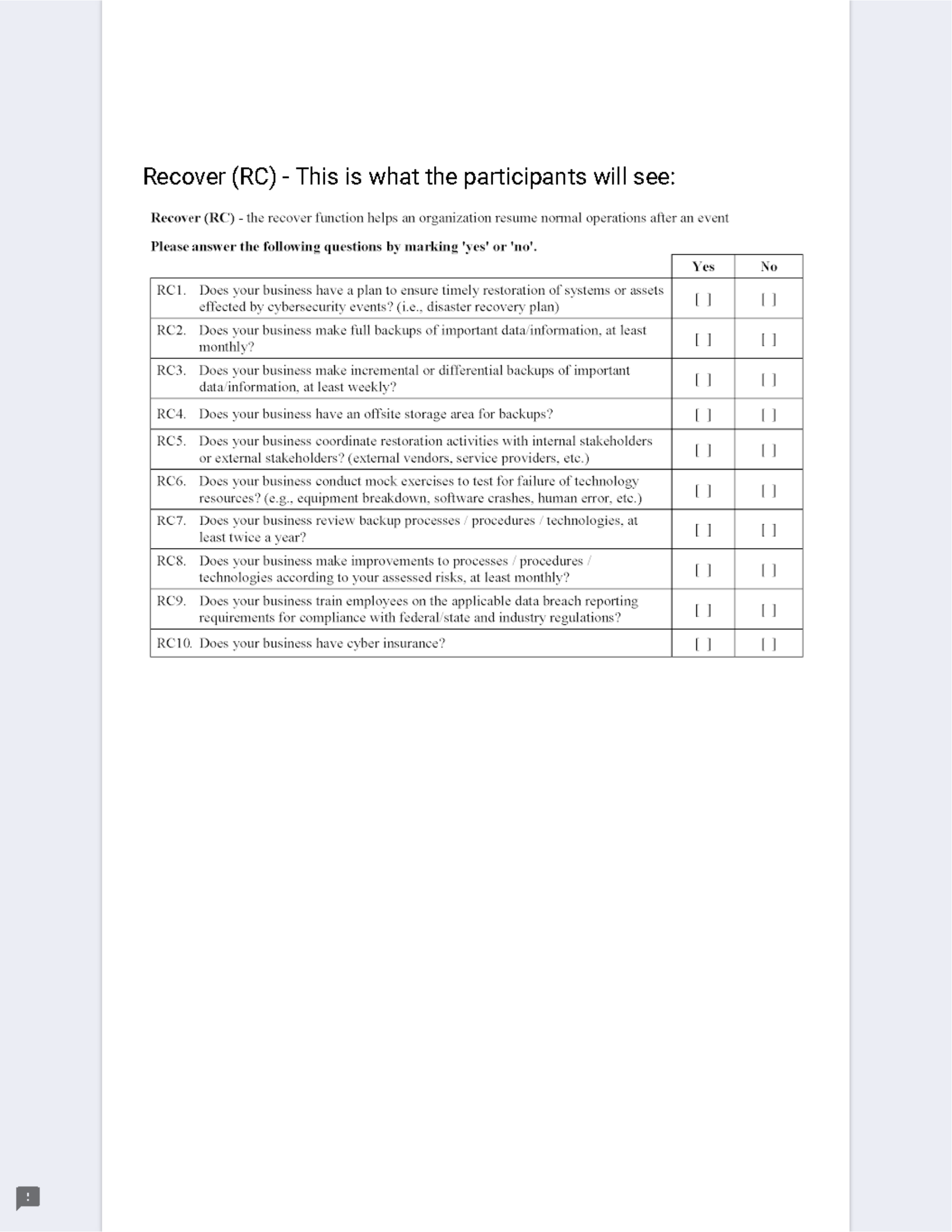
	1	2	3	4	5	6	7
RS1. Does your business require training for employees to recognize cybersecurity events?	○	○	○	○	○	○	○
RS2. Does your business analyze notifications of suspicious cyber activities reported from employees?	○	○	○	○	○	○	○
RS3. Does your business have a roster of support contacts & vendors in the case of security events?	○	○	○	○	○	○	○
RS4. Does your business have an incident response plan with established roles and responsibilities? (IR plan focuses on an immediate response to an incident)	○	○	○	○	○	○	○
RS5. Does your business review incident response procedures, at least annually?	○	○	○	○	○	○	○
RS6. Does your business coordinate cyber incident response activities with internal stakeholders or external	○	○	○	○	○	○	○



organizations? (external agencies such as law enforcement, service providers)							
RS7. Does your business have a disaster recovery / business continuity plan? (DR/BC plan focuses on establishing business operations at the primary or an alternate location).	○	○	○	○	○	○	○
RS8. Does your business test disaster recovery / business continuity plan, at least annually?	○	○	○	○	○	○	○
RS9. Does your business have the ability to quickly stop or contain a cyber-attack? (either in-house or external expertise, such as service provider)	○	○	○	○	○	○	○
RS10. Does your business have the ability to collect digital forensic data about a cyber-attack or data breach? (either in-house or external expertise, such as service provider)	○	○	○	○	○	○	○

RS(-). Provide additional feedback as needed. (or "N/A" if none) *

Your answer

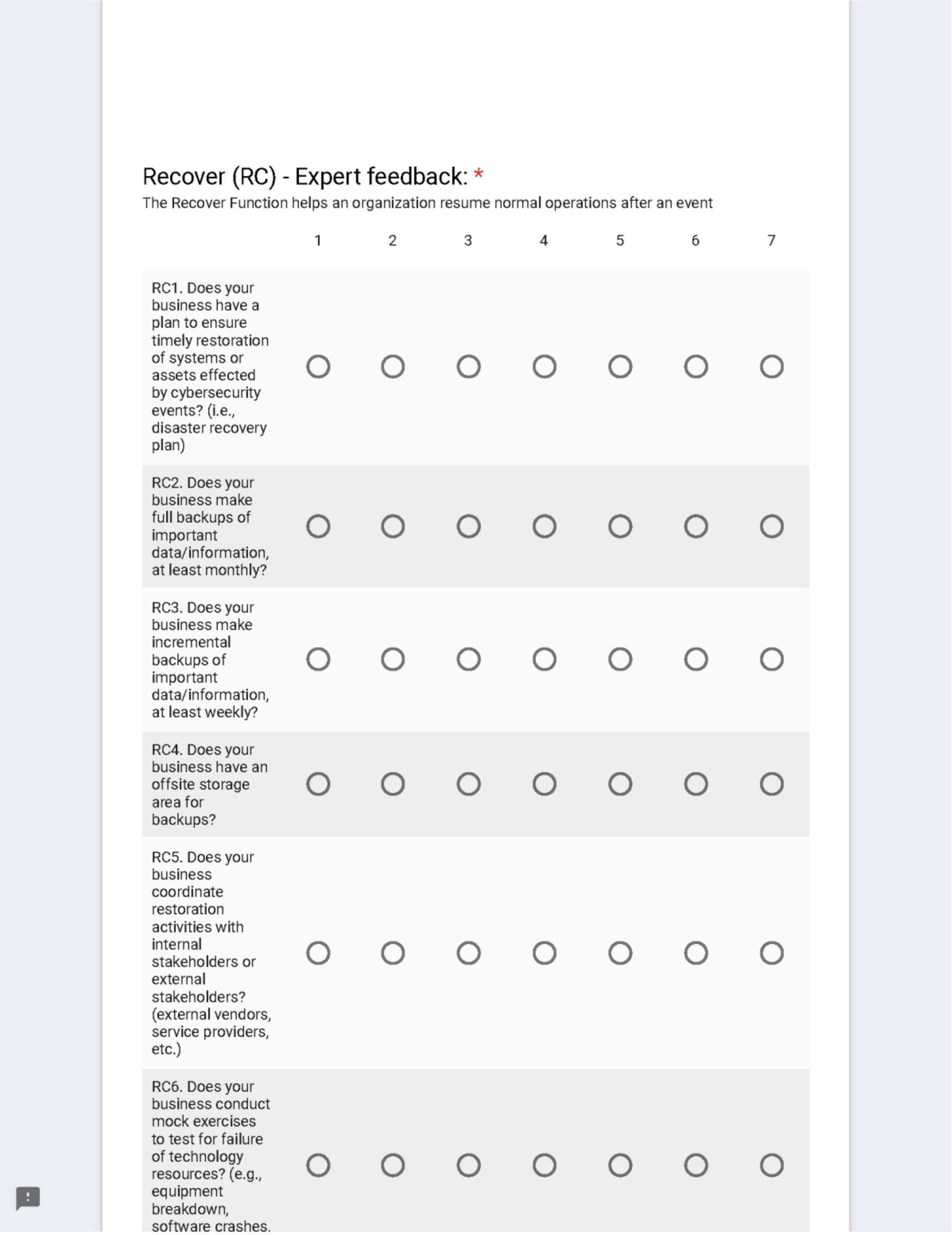


Recover (RC) - This is what the participants will see:

Recover (RC) - the recover function helps an organization resume normal operations after an event

Please answer the following questions by marking 'yes' or 'no'.

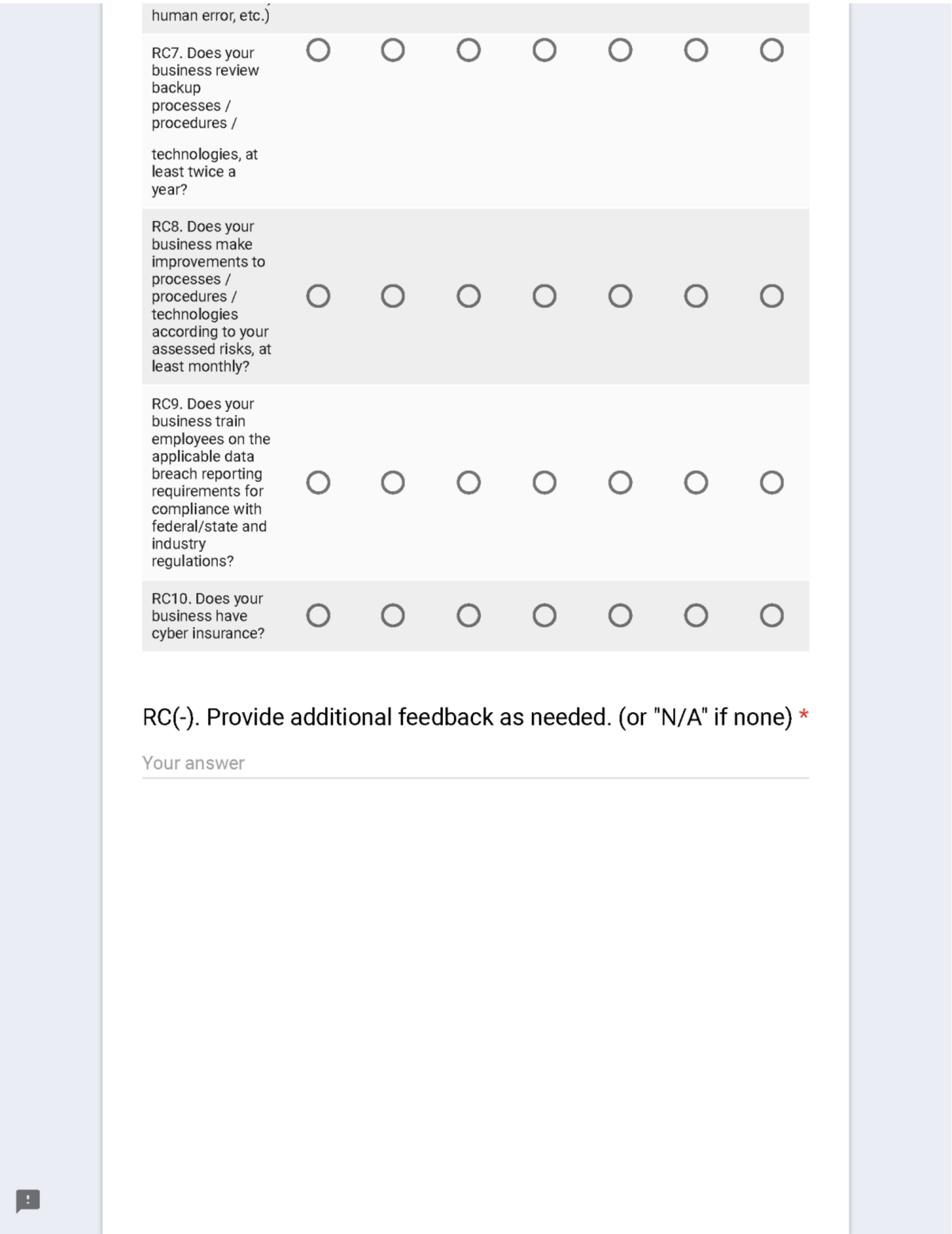
	Yes	No
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	[ ]	[ ]
RC2. Does your business make full backups of important data/information, at least monthly?	[ ]	[ ]
RC3. Does your business make incremental or differential backups of important data/information, at least weekly?	[ ]	[ ]
RC4. Does your business have an offsite storage area for backups?	[ ]	[ ]
RC5. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	[ ]	[ ]
RC6. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	[ ]	[ ]
RC7. Does your business review backup processes / procedures / technologies, at least twice a year?	[ ]	[ ]
RC8. Does your business make improvements to processes / procedures / technologies according to your assessed risks, at least monthly?	[ ]	[ ]
RC9. Does your business train employees on the applicable data breach reporting requirements for compliance with federal/state and industry regulations?	[ ]	[ ]
RC10. Does your business have cyber insurance?	[ ]	[ ]



Recover (RC) - Expert feedback: *

The Recover Function helps an organization resume normal operations after an event

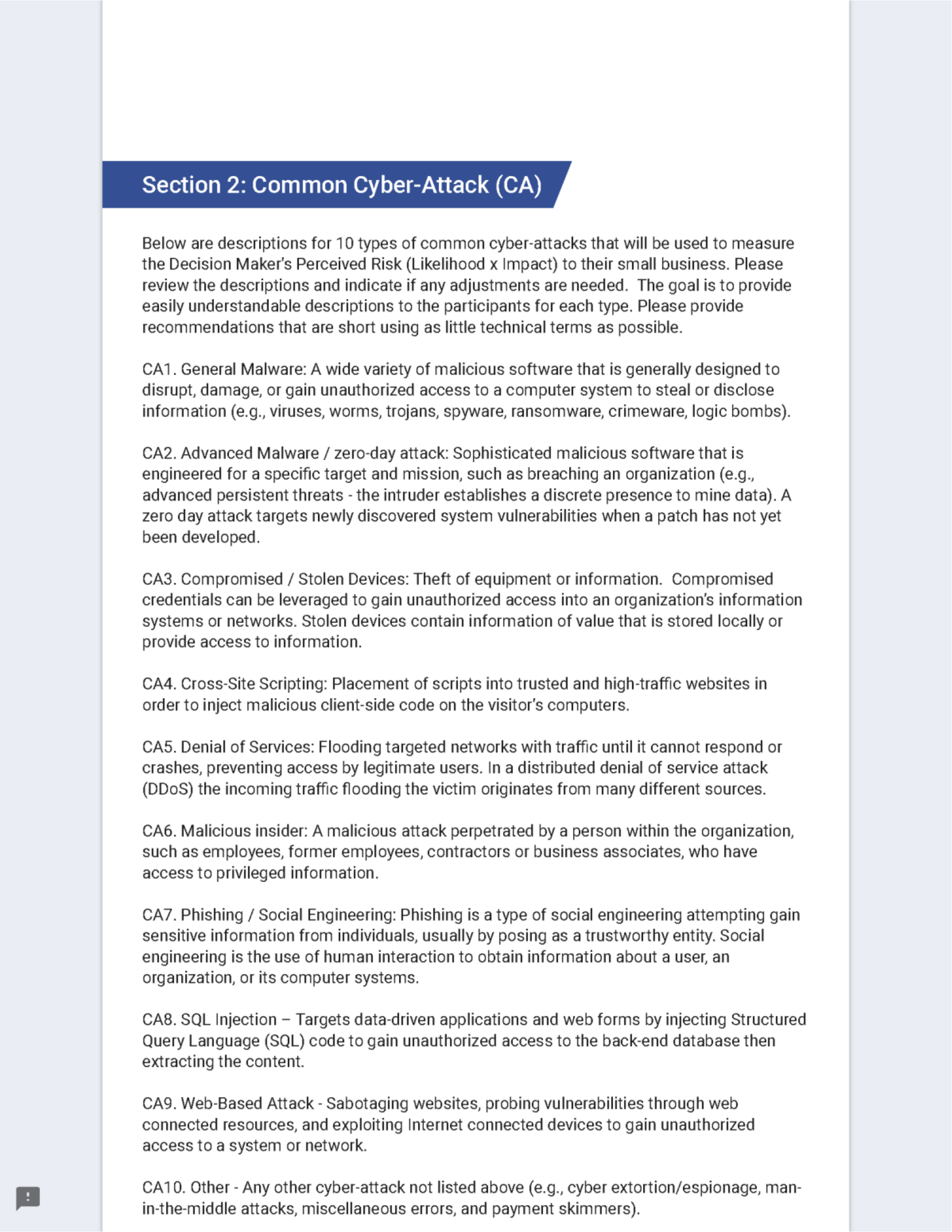
	1	2	3	4	5	6	7
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	○	○	○	○	○	○	○
RC2. Does your business make full backups of important data/information, at least monthly?	○	○	○	○	○	○	○
RC3. Does your business make incremental backups of important data/information, at least weekly?	○	○	○	○	○	○	○
RC4. Does your business have an offsite storage area for backups?	○	○	○	○	○	○	○
RC5. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	○	○	○	○	○	○	○
RC6. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes,	○	○	○	○	○	○	○



human error, etc.)							
RC7. Does your business review backup processes / procedures / technologies, at least twice a year?	○	○	○	○	○	○	○
RC8. Does your business make improvements to processes / procedures / technologies according to your assessed risks, at least monthly?	○	○	○	○	○	○	○
RC9. Does your business train employees on the applicable data breach reporting requirements for compliance with federal/state and industry regulations?	○	○	○	○	○	○	○
RC10. Does your business have cyber insurance?	○	○	○	○	○	○	○

RC(-). Provide additional feedback as needed. (or "N/A" if none) *

Your answer



Section 2: Common Cyber-Attack (CA)

Below are descriptions for 10 types of common cyber-attacks that will be used to measure the Decision Maker's Perceived Risk (Likelihood x Impact) to their small business. Please review the descriptions and indicate if any adjustments are needed. The goal is to provide easily understandable descriptions to the participants for each type. Please provide recommendations that are short using as little technical terms as possible.

CA1. General Malware: A wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system to steal or disclose information (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs).

CA2. Advanced Malware / zero-day attack: Sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats - the intruder establishes a discrete presence to mine data). A zero day attack targets newly discovered system vulnerabilities when a patch has not yet been developed.

CA3. Compromised / Stolen Devices: Theft of equipment or information. Compromised credentials can be leveraged to gain unauthorized access into an organization's information systems or networks. Stolen devices contain information of value that is stored locally or provide access to information.

CA4. Cross-Site Scripting: Placement of scripts into trusted and high-traffic websites in order to inject malicious client-side code on the visitor's computers.

CA5. Denial of Services: Flooding targeted networks with traffic until it cannot respond or crashes, preventing access by legitimate users. In a distributed denial of service attack (DDoS) the incoming traffic flooding the victim originates from many different sources.

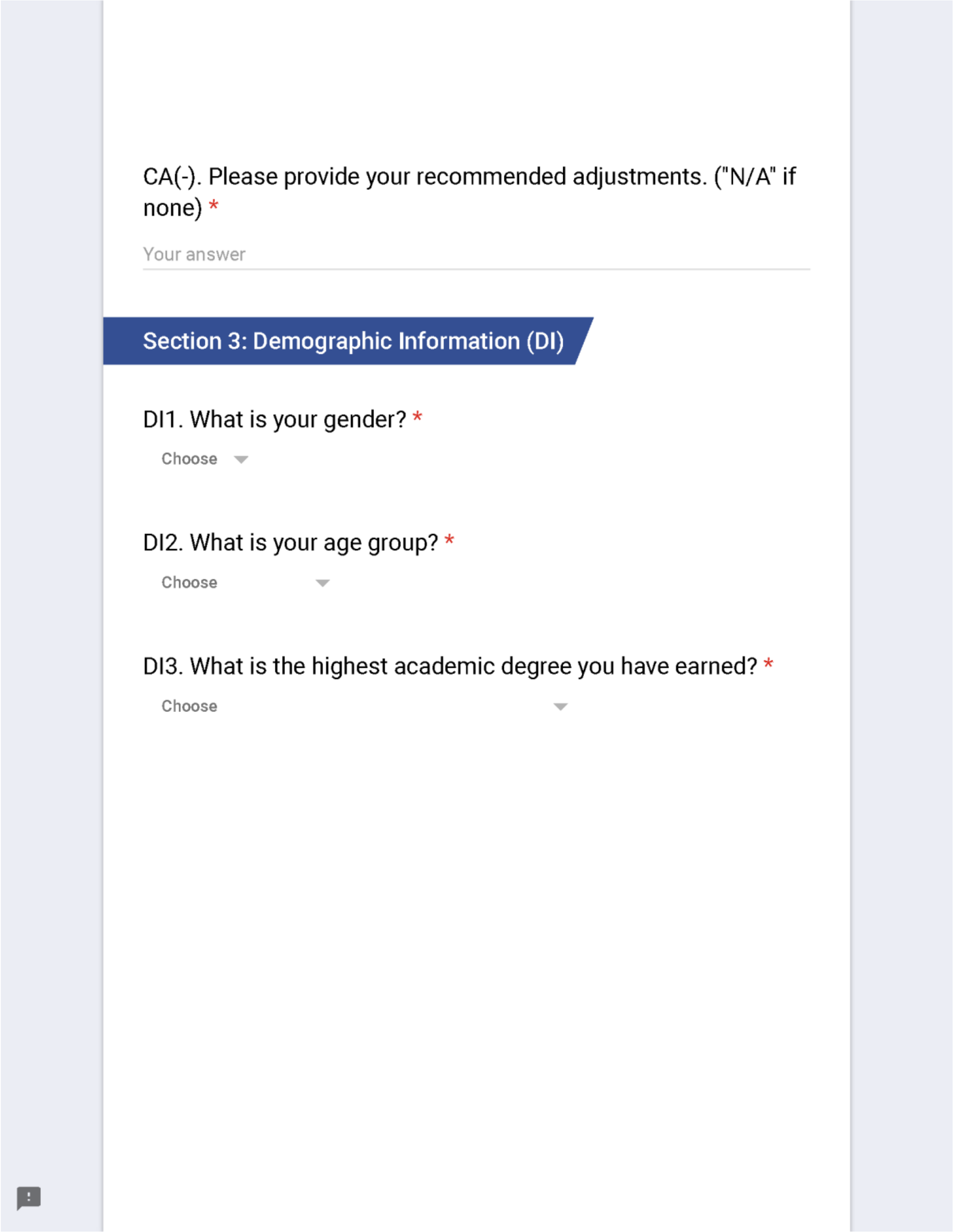
CA6. Malicious insider: A malicious attack perpetrated by a person within the organization, such as employees, former employees, contractors or business associates, who have access to privileged information.

CA7. Phishing / Social Engineering: Phishing is a type of social engineering attempting gain sensitive information from individuals, usually by posing as a trustworthy entity. Social engineering is the use of human interaction to obtain information about a user, an organization, or its computer systems.

CA8. SQL Injection – Targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database then extracting the content.

CA9. Web-Based Attack - Sabotaging websites, probing vulnerabilities through web connected resources, and exploiting Internet connected devices to gain unauthorized access to a system or network.

CA10. Other - Any other cyber-attack not listed above (e.g., cyber extortion/espionage, man-in-the-middle attacks, miscellaneous errors, and payment skimmers).



CA(-). Please provide your recommended adjustments. ("N/A" if none) *

Your answer

Section 3: Demographic Information (DI)

DI1. What is your gender? *

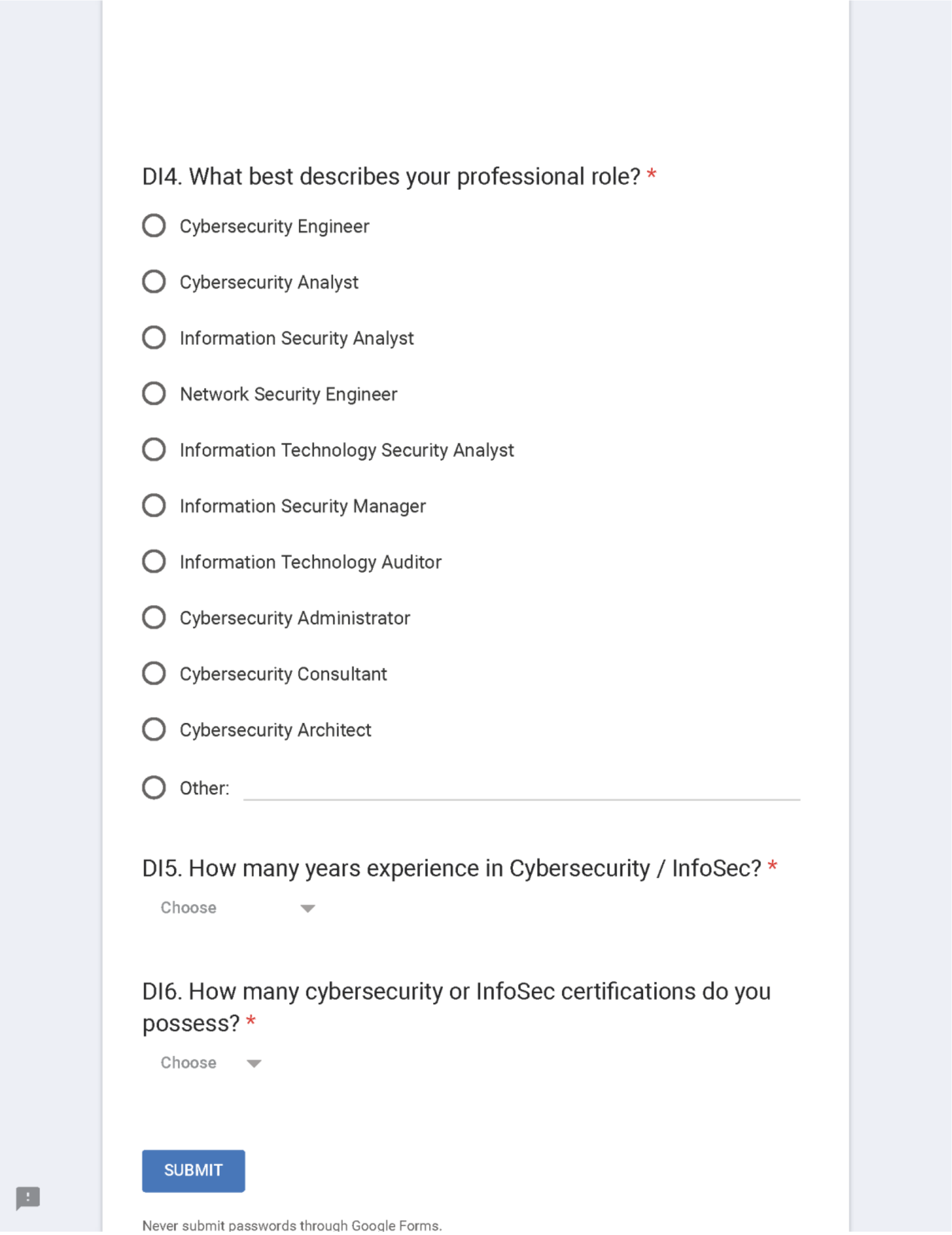
Choose ▾

DI2. What is your age group? *

Choose ▾

DI3. What is the highest academic degree you have earned? *

Choose ▾



DI4. What best describes your professional role? *

○ Cybersecurity Engineer

○ Cybersecurity Analyst

○ Information Security Analyst

○ Network Security Engineer

○ Information Technology Security Analyst

○ Information Security Manager

○ Information Technology Auditor

○ Cybersecurity Administrator

○ Cybersecurity Consultant

○ Cybersecurity Architect

○ Other: ____________________

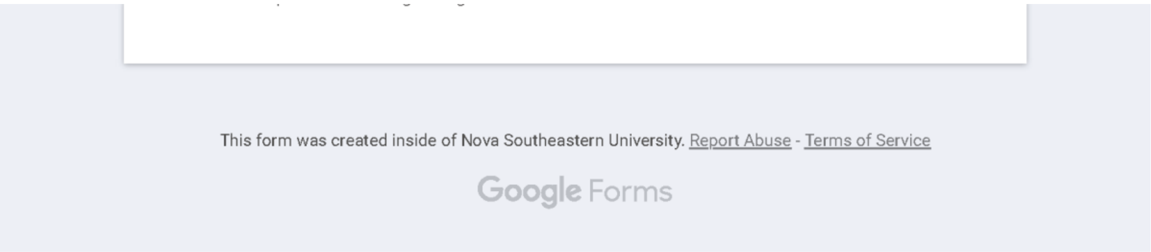
DI5. How many years experience in Cybersecurity / InfoSec? *

Choose ▼

DI6. How many cybersecurity or InfoSec certifications do you possess? *

Choose ▼

Never submit passwords through Google Forms.



This form was created inside of Nova Southeastern University. Report Abuse - Terms of Service

Appendix E

Instrument Questions with SME Assigned Weight

Item	Question	Weight
ID1	Does your business use a framework to manage cybersecurity? (a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets)	6.45
ID2	Does your business evaluate cybersecurity strategies on their alignment with business goals, at least annually?	6.00
ID3	Does your business allocate a budget specifically for cybersecurity?	6.18
ID4	Does your business control who has access to your information? (i.e., systems access policy)	6.77
ID5	Does your business conduct employee background checks? (e.g. level-3 check includes a criminal record search and looks for credentials that are work related)	6.27
ID6	Does your business require individual user accounts for each employee?	6.55
ID7	Does your business assign cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	5.82
ID8	Does your business identify and classify your information types? (e.g., private, public, sensitive, confidential, & proprietary)	6.50
ID9	Does your business maintain an inventory of computer hardware assets? (e.g. servers, workstations)	6.23
ID10	Does your business maintain an inventory of approved software?	6.14
ID11	Does your business have a cybersecurity risk management strategy? (e.g. defined risk tolerances to protect the confidentiality, integrity, and availability of information)	6.45
ID12	Does your business assign risk values to information resources?	6.14
ID13	Does your business assess the likelihood of cyber threats?	6.32
ID14	Does your business identify cybersecurity vulnerabilities?	6.55
ID15	Does your business identify costs (monetary or otherwise) associated with cyber risk impacts?	6.14
ID16	Does your business prioritize actions based on potential impacts of a cybersecurity incident?	6.27

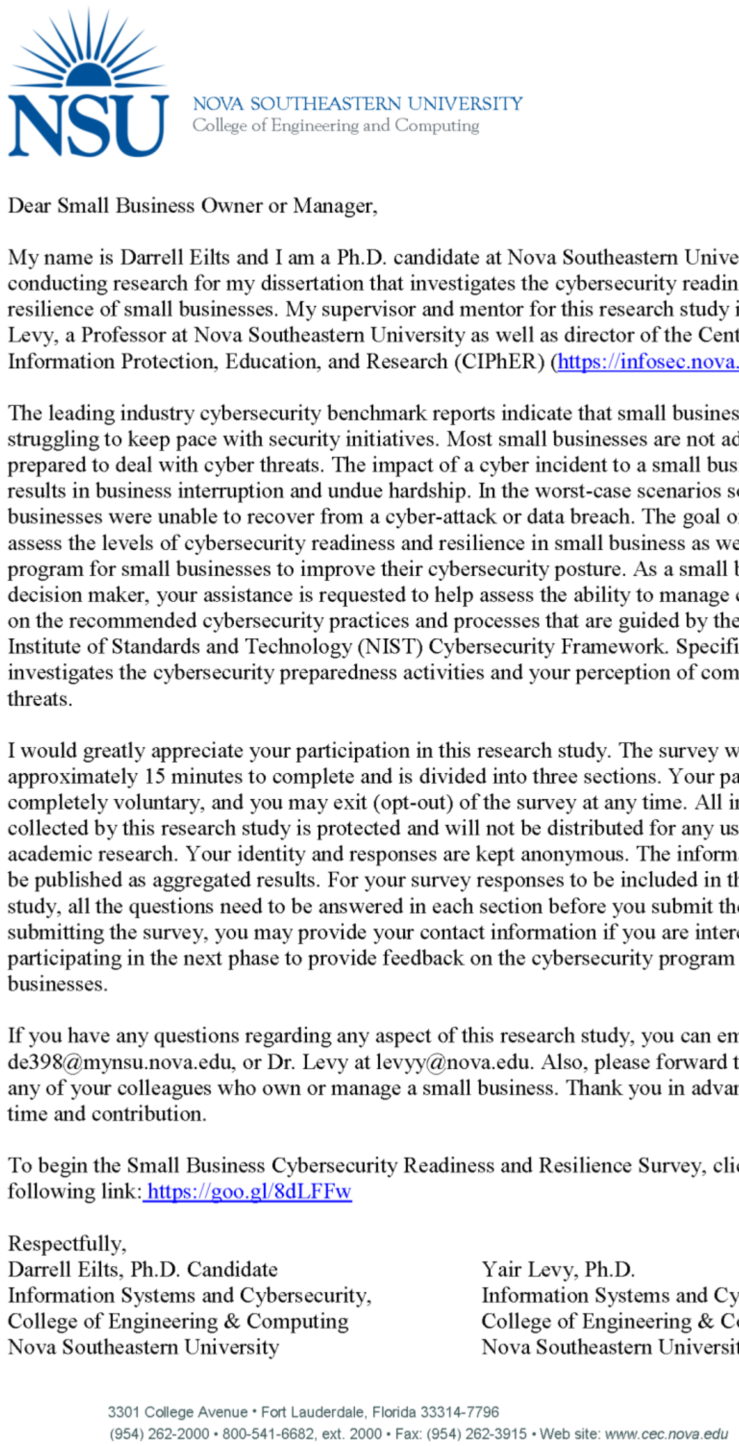
ID17	Does your business conduct cybersecurity analysis to determine what controls need to be implemented?	6.32
ID18	Does your business have a plan for implementing new cybersecurity controls over time?	6.18
ID19	Does your business identify cyber supply chain risks associated with the products and services that it provides and uses?	5.64
ID20	Does your business require service level agreements (SLAs) with technology service providers?	6.18
PR1	Does your business regularly patch your operating systems and applications, at least monthly?	6.77
PR2	Does your business use software and/or hardware firewalls?	6.73
PR3	Does your business have a privacy policy?	6.45
PR4	Does your business have an insider threat management program?	6.09
PR5	Does your business use encryption for sensitive information?	6.77
PR6	Does your business limit employee access to data and information through access controls?	6.64
PR7	Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	6.64
PR8	Does your business restrict downloading and installing software by non-administrators?	6.41
PR9	Does your business disable access when an employee leaves the business?	6.82
PR10	Does your business protect information assets from physical intrusion?	6.68
PR11	Does your business enforce password management? (e.g., password policy with strong passwords, expirations, changing all default administrative passwords)	6.64
PR12	Does your business use multi-factor authentication?	6.14
PR13	Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	6.36
PR14	Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	6.77
PR15	Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	6.18
PR16	Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	6.82

PR17	Does your business restrict the use of web browser, such as email client plugins or add-on applications?	5.86
PR18	Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (e.g., acceptable use policy)	5.82
PR19	Does your business have a data disposal policy?	5.82
PR20	Does your business safely dispose of old computers and media by scrubbing information from drives?	6.50
DE1	Does your business use anti-virus software? (also known as anti-malware)	6.55
DE2	Does your business update anti-virus software, at least daily?	6.50
DE3	Does your business use endpoint security software? (endpoint devices include mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network – endpoint software typically includes anti-virus software)	6.41
DE4	Does your business use an intrusion detection and prevention system (IDPS)?	6.09
DE5	Does your business baseline network utilization and detect anomalies in traffic patterns?	5.68
DE6	Does your business maintain and analyze cybersecurity event logs? (either in-house or managed security service provider)	6.32
DE7	Does your business perform test procedures at discrete intervals to identify cybersecurity events?	5.91
DE8	Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	6.23
DE9	Does your business perform vulnerability assessments, at least quarterly?	6.23
DE10	Does your business perform penetration testing, at least annually?	5.73
RS1	Does your business require training for employees to recognize cybersecurity events?	6.59
RS2	Does your business analyze notifications of suspicious cyber activities reported from employees?	6.68
RS3	Does your business have a roster of support contacts & vendors in the case of cybersecurity events?	6.32
RS4	Does your business have an incident response plan with established roles and responsibilities? (IR plan focuses on an immediate response to an incident)	6.59

RS5	Does your business review incident response procedures, at least annually?	6.05
RS6	Does your business coordinate cyber incident response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	5.95
RS7	Does your business have a disaster recovery / business continuity plan? (DR/BC plan focuses on establishing business operations at the primary or an alternate location).	6.55
RS8	Does your business test disaster recovery / business continuity plan, at least annually?	6.50
RS9	Does your business have the ability to quickly stop or contain a cyber-attack? (either in-house or external expertise, such as service provider)	6.23
RS10	Does your business have the ability to collect digital forensic data about a cyber-attack or data breach? (either in-house or external expertise, such as service provider)	5.95
RC1	Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	6.45
RC2	Does your business routinely backup essential computers and servers, at least monthly?	6.77
RC3	Does your business routinely backup important data/information, at least weekly?	6.55
RC4	Does your business use an offsite storage area for backups?	6.27
RC5	Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	5.77
RC6	Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	5.68
RC7	Does your business review backup processes / procedures / technologies, at least twice a year?	6.23
RC8	Does your business make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly?	5.27
RC9	Does your business train employees on data breach reporting requirements for compliance with federal/state and industry regulations?	6.23
RC10	Does your business have cyber insurance?	5.59

Appendix F

Phase 2 Invitation Letter to Small Business Decision Owners and Managers



NOVA SOUTHEASTERN UNIVERSITY
College of Engineering and Computing

Dear Small Business Owner or Manager,

My name is Darrell Eilts and I am a Ph.D. candidate at Nova Southeastern University. I am conducting research for my dissertation that investigates the cybersecurity readiness and resilience of small businesses. My supervisor and mentor for this research study is Dr. Yair Levy, a Professor at Nova Southeastern University as well as director of the Center for Information Protection, Education, and Research (CIPhER) (https://infosec.nova.edu).

The leading industry cybersecurity benchmark reports indicate that small businesses are struggling to keep pace with security initiatives. Most small businesses are not adequately prepared to deal with cyber threats. The impact of a cyber incident to a small business often results in business interruption and undue hardship. In the worst-case scenarios some small businesses were unable to recover from a cyber-attack or data breach. The goal of this study is to assess the levels of cybersecurity readiness and resilience in small business as well as develop a program for small businesses to improve their cybersecurity posture. As a small business decision maker, your assistance is requested to help assess the ability to manage cyber risk based on the recommended cybersecurity practices and processes that are guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Specifically, this study investigates the cybersecurity preparedness activities and your perception of common cyber threats.

I would greatly appreciate your participation in this research study. The survey will take approximately 15 minutes to complete and is divided into three sections. Your participation is completely voluntary, and you may exit (opt-out) of the survey at any time. All information collected by this research study is protected and will not be distributed for any use other than academic research. Your identity and responses are kept anonymous. The information will only be published as aggregated results. For your survey responses to be included in the research study, all the questions need to be answered in each section before you submit the survey. After submitting the survey, you may provide your contact information if you are interested in participating in the next phase to provide feedback on the cybersecurity program for small businesses.

If you have any questions regarding any aspect of this research study, you can email me at de398@mynsu.nova.edu, or Dr. Levy at levyy@nova.edu. Also, please forward this invitation to any of your colleagues who own or manage a small business. Thank you in advance for your time and contribution.

To begin the Small Business Cybersecurity Readiness and Resilience Survey, click on the following link: https://goo.gl/8dLFFw

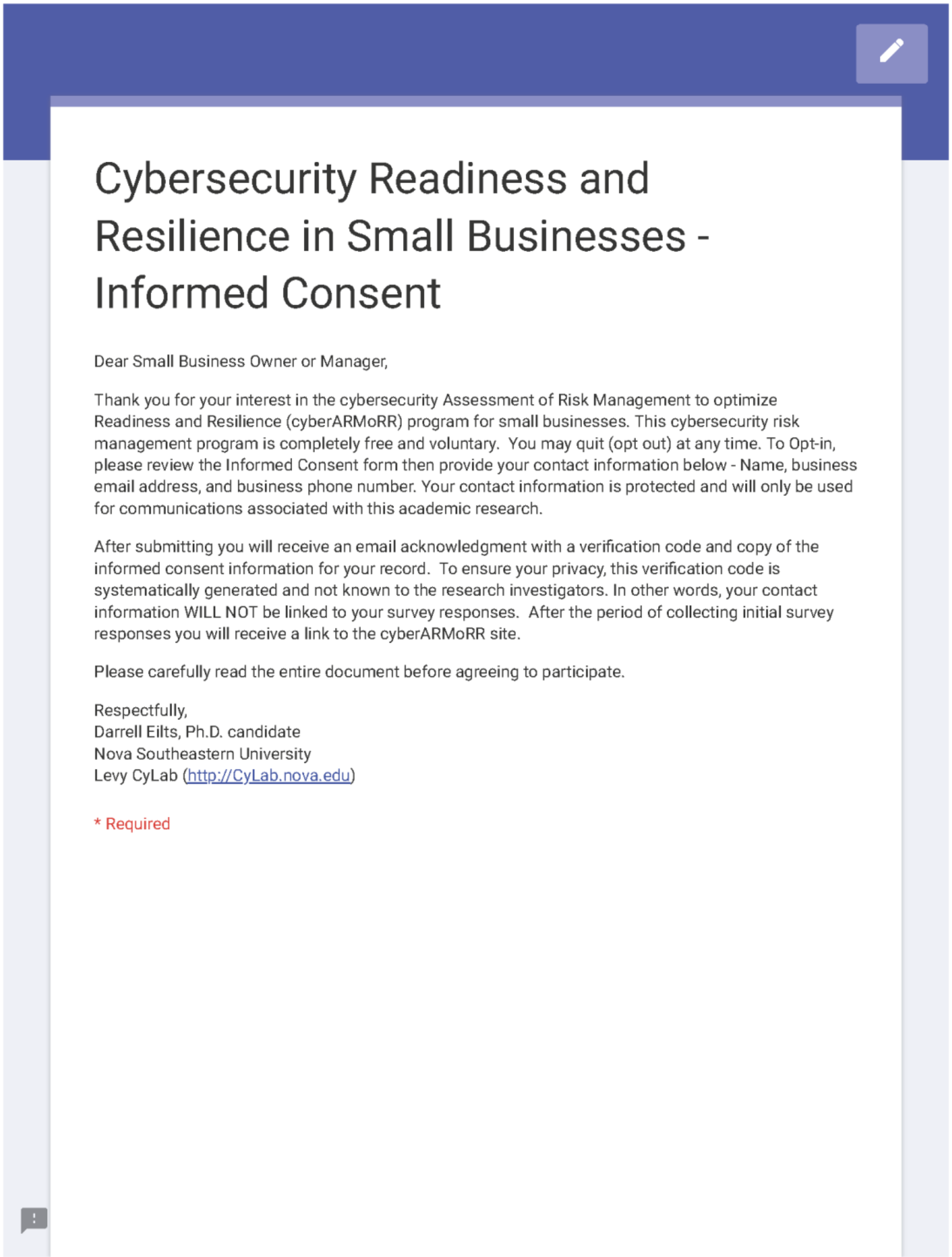
Respectfully,
Darrell Eilts, Ph.D. Candidate
Information Systems and Cybersecurity,
College of Engineering & Computing
Nova Southeastern University

Yair Levy, Ph.D.
Information Systems and Cybersecurity,
College of Engineering & Computing
Nova Southeastern University

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-2000 • 800-541-6682, ext. 2000 • Fax: (954) 262-3915 • Web site: *www.cec.nova.edu*

Appendix G

Phase 2 Online Consent to Participate in a Research Study



Cybersecurity Readiness and Resilience in Small Businesses - Informed Consent

Dear Small Business Owner or Manager,

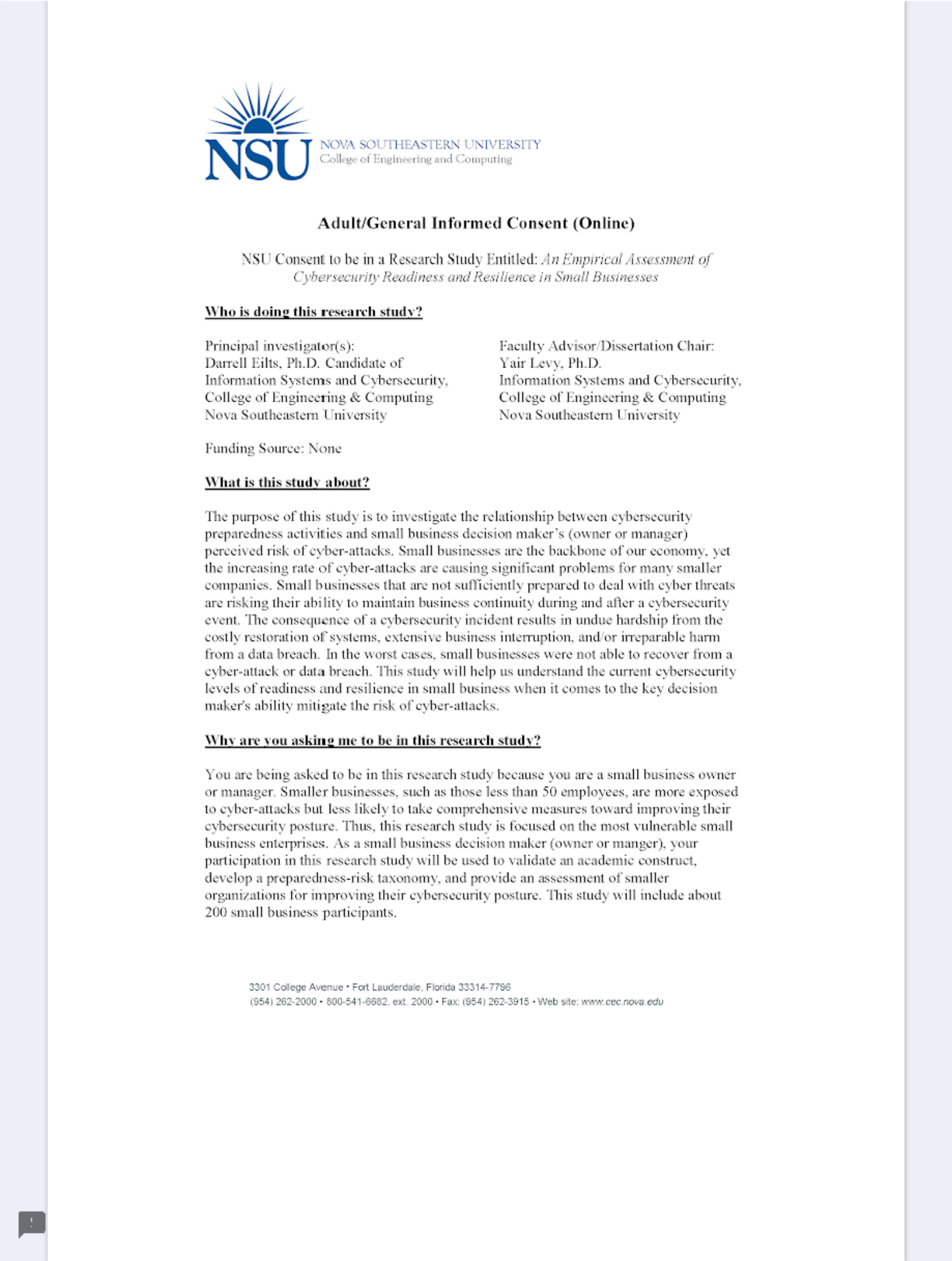
Thank you for your interest in the cybersecurity Assessment of Risk Management to optimize Readiness and Resilience (cyberARMoRR) program for small businesses. This cybersecurity risk management program is completely free and voluntary. You may quit (opt out) at any time. To Opt-in, please review the Informed Consent form then provide your contact information below - Name, business email address, and business phone number. Your contact information is protected and will only be used for communications associated with this academic research.

After submitting you will receive an email acknowledgment with a verification code and copy of the informed consent information for your record. To ensure your privacy, this verification code is systematically generated and not known to the research investigators. In other words, your contact information WILL NOT be linked to your survey responses. After the period of collecting initial survey responses you will receive a link to the cyberARMoRR site.

Please carefully read the entire document before agreeing to participate.

Respectfully,
Darrell Eilts, Ph.D. candidate
Nova Southeastern University
Levy CyLab (http://CyLab.nova.edu)

* Required



NSU NOVA SOUTHEASTERN UNIVERSITY
College of Engineering and Computing

Adult/General Informed Consent (Online)

NSU Consent to be in a Research Study Entitled: *An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses*

Who is doing this research study?

Principal investigator(s):
Darrell Eilts, Ph.D. Candidate of
Information Systems and Cybersecurity,
College of Engineering & Computing
Nova Southeastern University

Faculty Advisor/Dissertation Chair:
Yair Levy, Ph.D.
Information Systems and Cybersecurity,
College of Engineering & Computing
Nova Southeastern University

Funding Source: None

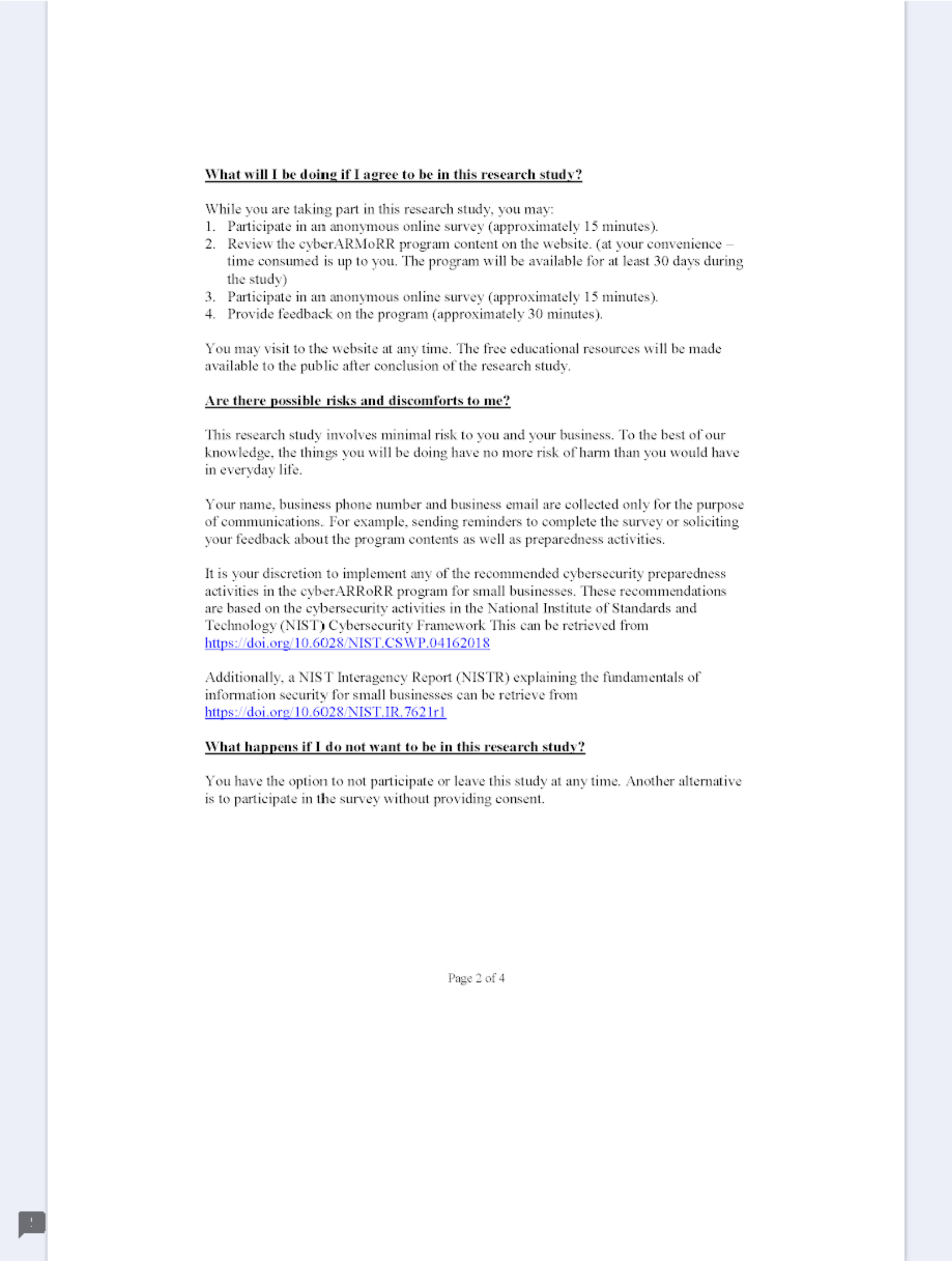
What is this study about?

The purpose of this study is to investigate the relationship between cybersecurity preparedness activities and small business decision maker's (owner or manager) perceived risk of cyber-attacks. Small businesses are the backbone of our economy, yet the increasing rate of cyber-attacks are causing significant problems for many smaller companies. Small businesses that are not sufficiently prepared to deal with cyber threats are risking their ability to maintain business continuity during and after a cybersecurity event. The consequence of a cybersecurity incident results in undue hardship from the costly restoration of systems, extensive business interruption, and/or irreparable harm from a data breach. In the worst cases, small businesses were not able to recover from a cyber-attack or data breach. This study will help us understand the current cybersecurity levels of readiness and resilience in small business when it comes to the key decision maker's ability mitigate the risk of cyber-attacks.

Why are you asking me to be in this research study?

You are being asked to be in this research study because you are a small business owner or manager. Smaller businesses, such as those less than 50 employees, are more exposed to cyber-attacks but less likely to take comprehensive measures toward improving their cybersecurity posture. Thus, this research study is focused on the most vulnerable small business enterprises. As a small business decision maker (owner or manger), your participation in this research study will be used to validate an academic construct, develop a preparedness-risk taxonomy, and provide an assessment of smaller organizations for improving their cybersecurity posture. This study will include about 200 small business participants.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-2000 • 800-541-6682, ext. 2000 • Fax: (954) 262-3915 • Web site: *www.cec.nova.edu*



What will I be doing if I agree to be in this research study?

While you are taking part in this research study, you may:

1. Participate in an anonymous online survey (approximately 15 minutes).
2. Review the cyberARMoRR program content on the website. (at your convenience – time consumed is up to you. The program will be available for at least 30 days during the study)
3. Participate in an anonymous online survey (approximately 15 minutes).
4. Provide feedback on the program (approximately 30 minutes).

You may visit to the website at any time. The free educational resources will be made available to the public after conclusion of the research study.

Are there possible risks and discomforts to me?

This research study involves minimal risk to you and your business. To the best of our knowledge, the things you will be doing have no more risk of harm than you would have in everyday life.

Your name, business phone number and business email are collected only for the purpose of communications. For example, sending reminders to complete the survey or soliciting your feedback about the program contents as well as preparedness activities.

It is your discretion to implement any of the recommended cybersecurity preparedness activities in the cyberARRoRR program for small businesses. These recommendations are based on the cybersecurity activities in the National Institute of Standards and Technology (NIST) Cybersecurity Framework This can be retrieved from https://doi.org/10.6028/NIST.CSWP.04162018

Additionally, a NIST Interagency Report (NISTR) explaining the fundamentals of information security for small businesses can be retrieve from https://doi.org/10.6028/NIST.IR.7621r1

What happens if I do not want to be in this research study?

You have the option to not participate or leave this study at any time. Another alternative is to participate in the survey without providing consent.

Page 2 of 4

Are there any benefits for taking part in this research study?

The main benefit to you is the access to the online educational resources to help improve the cybersecurity posture of your small business. There are many resources publicly available through government sites. However, cybersecurity information can be technically overwhelming and sometimes difficult to know what is important for smaller size businesses. The cyberARMoRR program aims to provide easy to follow guidance to help you prioritize your cybersecurity preparedness activities based on the input of cybersecurity subject matter experts.

There is no guarantee or promise that you will receive a direct benefit as a participant in this research study. However, we hope the information learned from this research study will benefit the you as well as other small business decision makers in the future.

Will I be paid or be given compensation for being in the study?

You will not be given any payments or compensation for being in this research study.

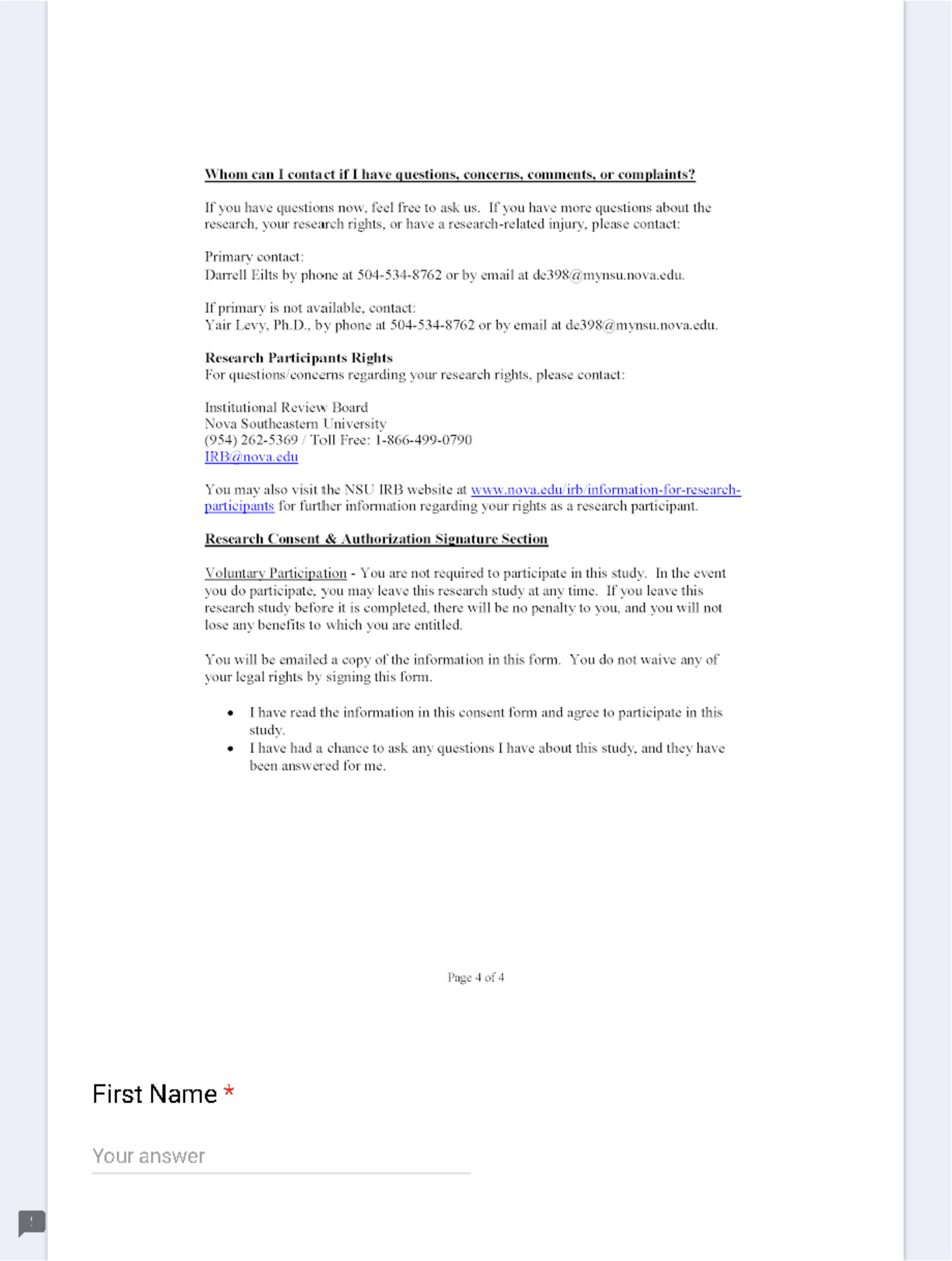
Will it cost me anything?

There are no costs to you for being in this research study.

How will you keep my information private?

Information about you or your business collected in this research study will be handled in a confidential manner, within the limits of the law, and will be limited to people who have a need to review this information. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not include any information that will make it possible to identify you or your business. All confidential data will be kept securely. All data will be kept for 36 months from the end of the study and deleted after that time.

Page 3 of 4



Whom can I contact if I have questions, concerns, comments, or complaints?

If you have questions now, feel free to ask us. If you have more questions about the research, your research rights, or have a research-related injury, please contact:

Primary contact:
Darrell Eilts by phone at 504-534-8762 or by email at de398@mynsu.nova.edu.

If primary is not available, contact:
Yair Levy, Ph.D., by phone at 504-534-8762 or by email at de398@mynsu.nova.edu.

Research Participants Rights
For questions/concerns regarding your research rights, please contact:

Institutional Review Board
Nova Southeastern University
(954) 262-5369 / Toll Free: 1-866-499-0790
IRB@nova.edu

You may also visit the NSU IRB website at www.nova.edu/irb/information-for-research-participants for further information regarding your rights as a research participant.

Research Consent & Authorization Signature Section

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

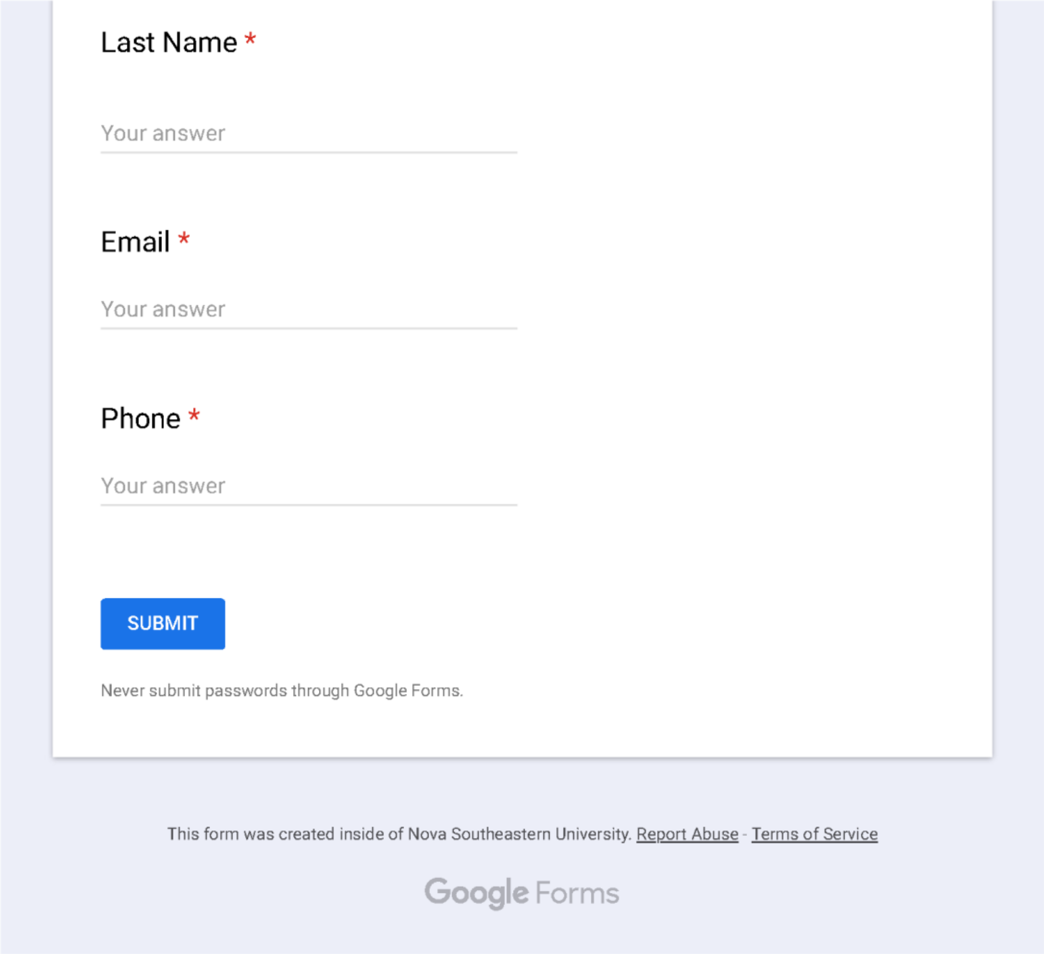
You will be emailed a copy of the information in this form. You do not waive any of your legal rights by signing this form.

- I have read the information in this consent form and agree to participate in this study.
- I have had a chance to ask any questions I have about this study, and they have been answered for me.

Page 4 of 4

First Name *

Your answer



Last Name *

Your answer

Email *

Your answer

Phone *

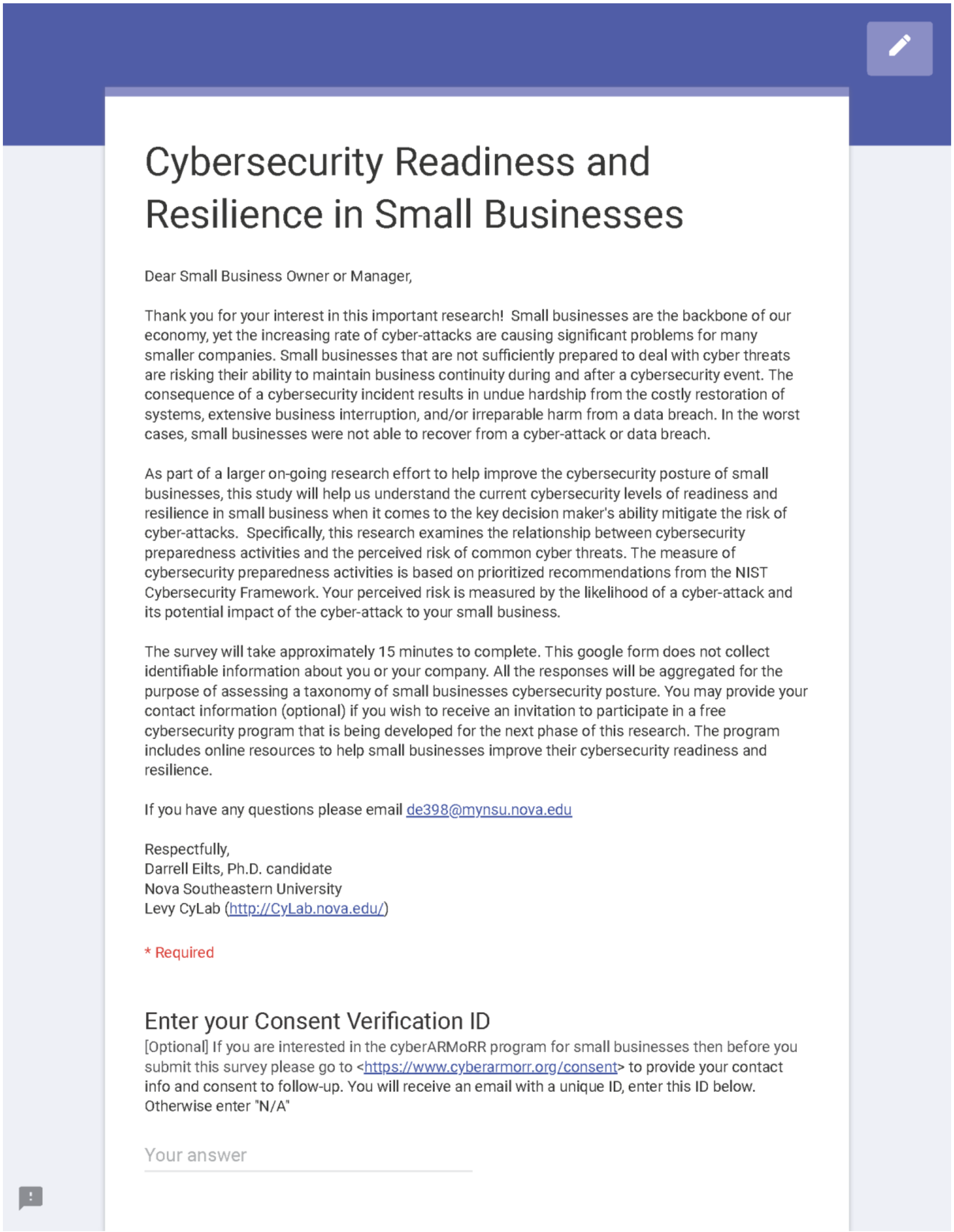
Your answer

Never submit passwords through Google Forms.

This form was created inside of Nova Southeastern University. Report Abuse - Terms of Service

Appendix H

Phase 2 Survey for Participants (Pretest measure)



Cybersecurity Readiness and Resilience in Small Businesses

Dear Small Business Owner or Manager,

Thank you for your interest in this important research! Small businesses are the backbone of our economy, yet the increasing rate of cyber-attacks are causing significant problems for many smaller companies. Small businesses that are not sufficiently prepared to deal with cyber threats are risking their ability to maintain business continuity during and after a cybersecurity event. The consequence of a cybersecurity incident results in undue hardship from the costly restoration of systems, extensive business interruption, and/or irreparable harm from a data breach. In the worst cases, small businesses were not able to recover from a cyber-attack or data breach.

As part of a larger on-going research effort to help improve the cybersecurity posture of small businesses, this study will help us understand the current cybersecurity levels of readiness and resilience in small business when it comes to the key decision maker's ability mitigate the risk of cyber-attacks. Specifically, this research examines the relationship between cybersecurity preparedness activities and the perceived risk of common cyber threats. The measure of cybersecurity preparedness activities is based on prioritized recommendations from the NIST Cybersecurity Framework. Your perceived risk is measured by the likelihood of a cyber-attack and its potential impact of the cyber-attack to your small business.

The survey will take approximately 15 minutes to complete. This google form does not collect identifiable information about you or your company. All the responses will be aggregated for the purpose of assessing a taxonomy of small businesses cybersecurity posture. You may provide your contact information (optional) if you wish to receive an invitation to participate in a free cybersecurity program that is being developed for the next phase of this research. The program includes online resources to help small businesses improve their cybersecurity readiness and resilience.

If you have any questions please email de398@mynsu.nova.edu

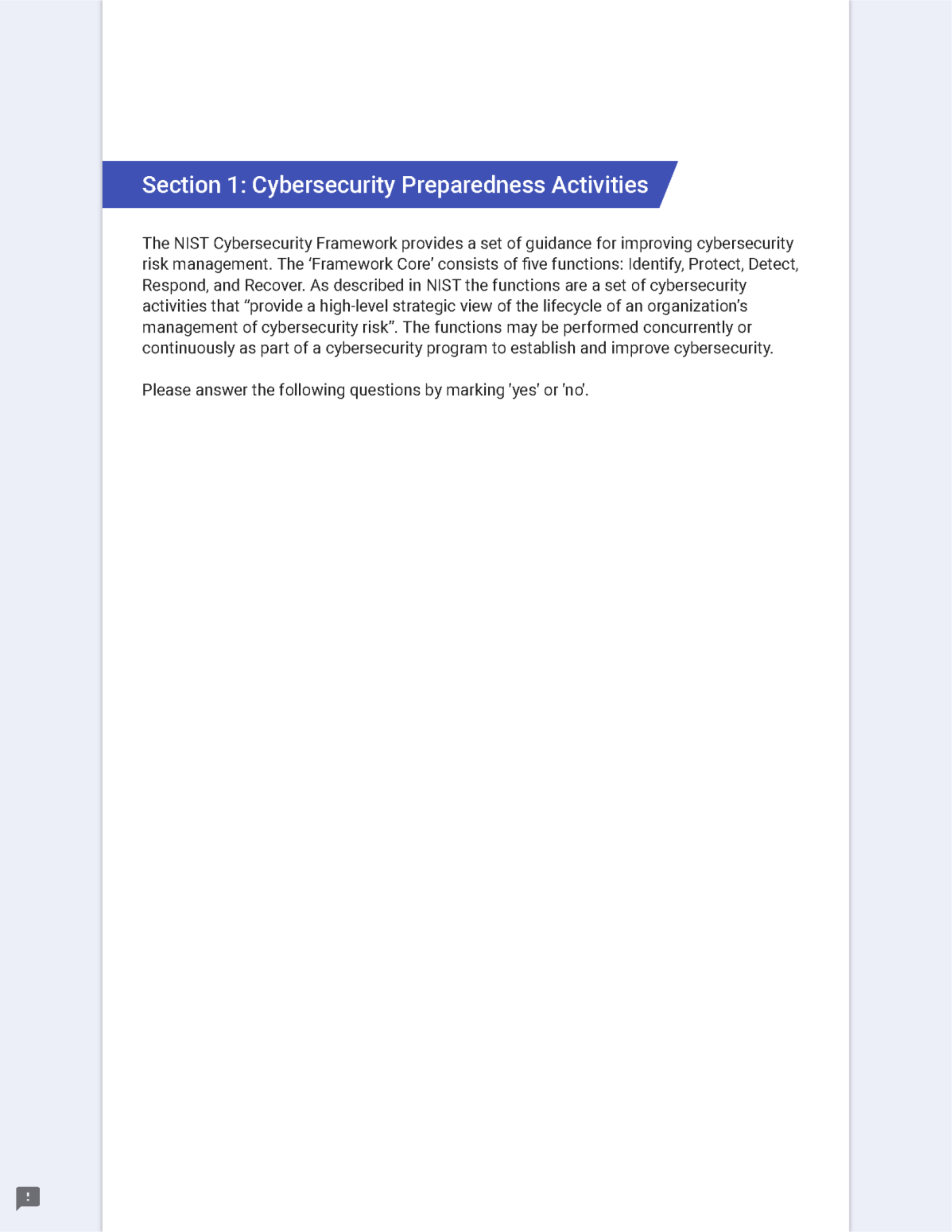
Respectfully,
Darrell Eilts, Ph.D. candidate
Nova Southeastern University
Levy CyLab (http://CyLab.nova.edu/)

* Required

Enter your Consent Verification ID

[Optional] If you are interested in the cyberARMoRR program for small businesses then before you submit this survey please go to <https://www.cyberarmorr.org/consent> to provide your contact info and consent to follow-up. You will receive an email with a unique ID, enter this ID below. Otherwise enter "N/A"

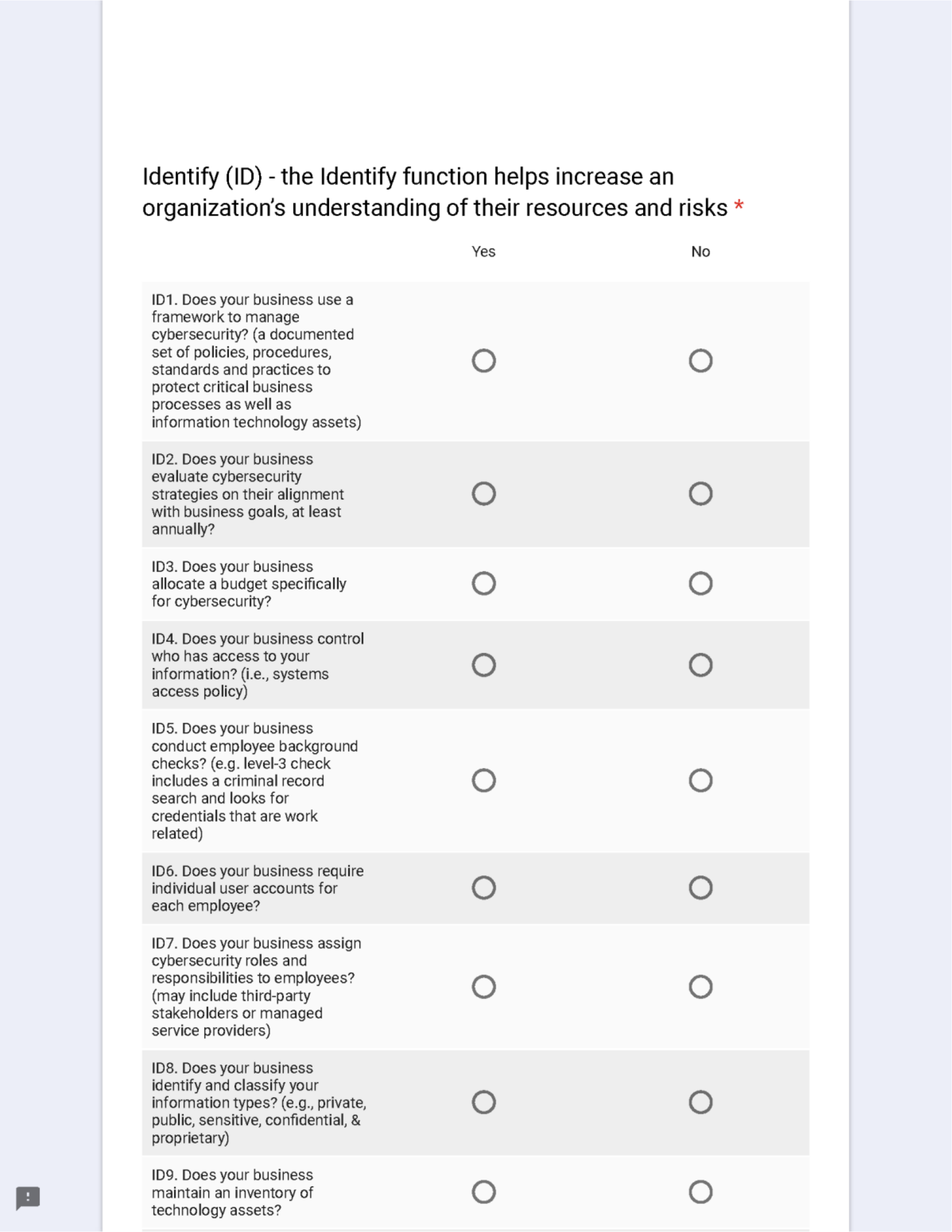
Your answer



Section 1: Cybersecurity Preparedness Activities

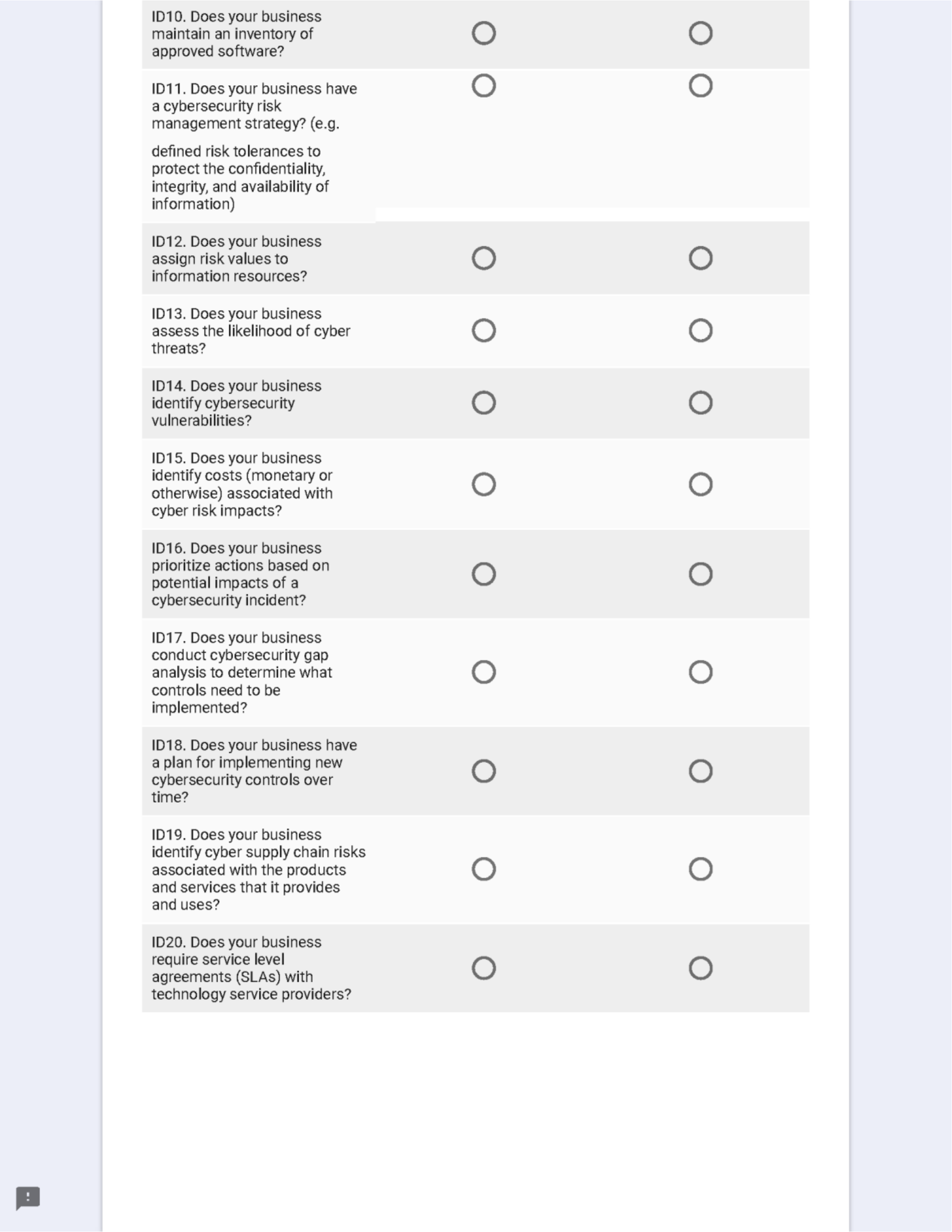
The NIST Cybersecurity Framework provides a set of guidance for improving cybersecurity risk management. The 'Framework Core' consists of five functions: Identify, Protect, Detect, Respond, and Recover. As described in NIST the functions are a set of cybersecurity activities that "provide a high-level strategic view of the lifecycle of an organization's management of cybersecurity risk". The functions may be performed concurrently or continuously as part of a cybersecurity program to establish and improve cybersecurity.

Please answer the following questions by marking 'yes' or 'no'.

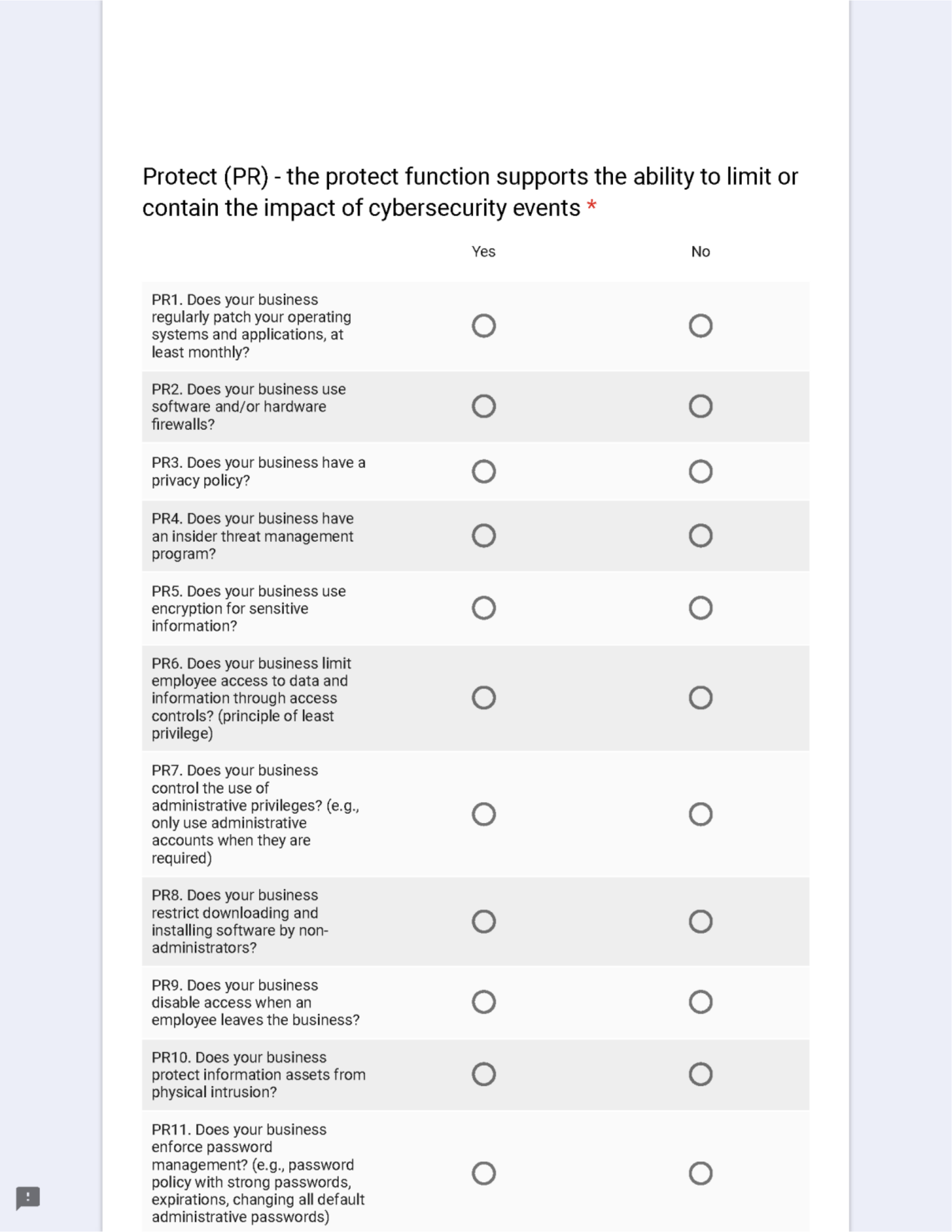


Identify (ID) - the Identify function helps increase an organization’s understanding of their resources and risks *

	Yes	No
ID1. Does your business use a framework to manage cybersecurity? (a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets)	○	○
ID2. Does your business evaluate cybersecurity strategies on their alignment with business goals, at least annually?	○	○
ID3. Does your business allocate a budget specifically for cybersecurity?	○	○
ID4. Does your business control who has access to your information? (i.e., systems access policy)	○	○
ID5. Does your business conduct employee background checks? (e.g. level-3 check includes a criminal record search and looks for credentials that are work related)	○	○
ID6. Does your business require individual user accounts for each employee?	○	○
ID7. Does your business assign cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	○	○
ID8. Does your business identify and classify your information types? (e.g., private, public, sensitive, confidential, & proprietary)	○	○
ID9. Does your business maintain an inventory of technology assets?	○	○

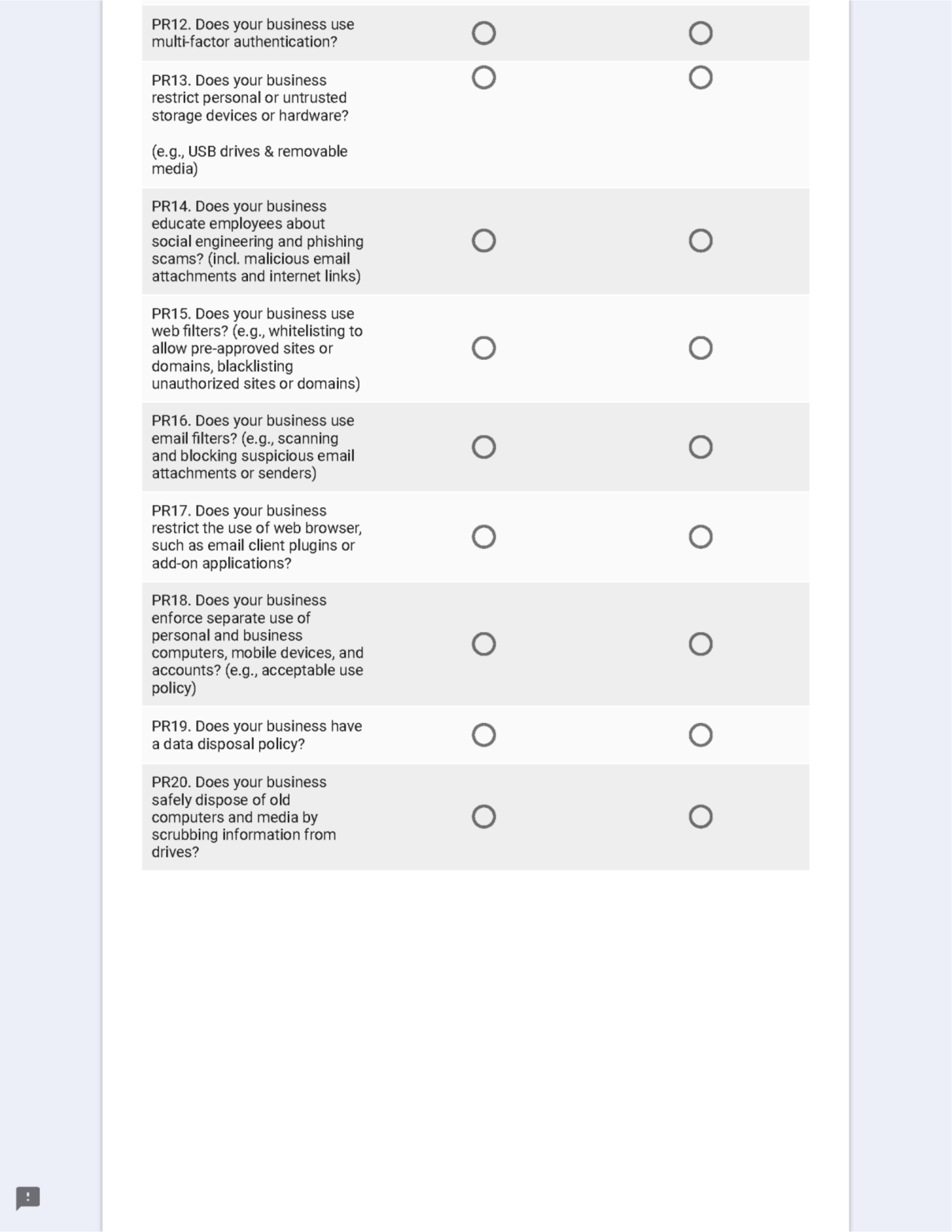


ID10. Does your business maintain an inventory of approved software?	○	○
ID11. Does your business have a cybersecurity risk management strategy? (e.g. defined risk tolerances to protect the confidentiality, integrity, and availability of information)	○	○
ID12. Does your business assign risk values to information resources?	○	○
ID13. Does your business assess the likelihood of cyber threats?	○	○
ID14. Does your business identify cybersecurity vulnerabilities?	○	○
ID15. Does your business identify costs (monetary or otherwise) associated with cyber risk impacts?	○	○
ID16. Does your business prioritize actions based on potential impacts of a cybersecurity incident?	○	○
ID17. Does your business conduct cybersecurity gap analysis to determine what controls need to be implemented?	○	○
ID18. Does your business have a plan for implementing new cybersecurity controls over time?	○	○
ID19. Does your business identify cyber supply chain risks associated with the products and services that it provides and uses?	○	○
ID20. Does your business require service level agreements (SLAs) with technology service providers?	○	○

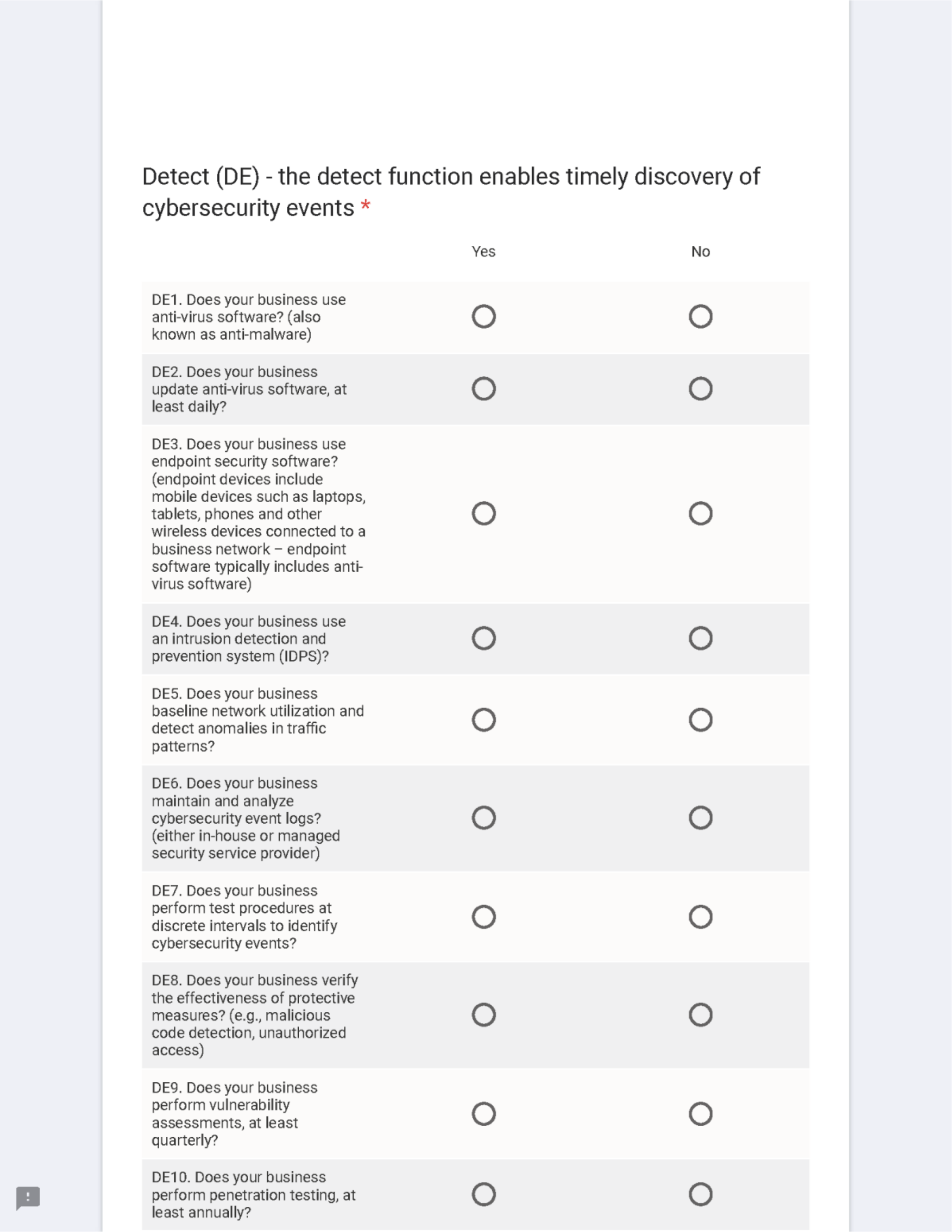


Protect (PR) - the protect function supports the ability to limit or contain the impact of cybersecurity events *

	Yes	No
PR1. Does your business regularly patch your operating systems and applications, at least monthly?	○	○
PR2. Does your business use software and/or hardware firewalls?	○	○
PR3. Does your business have a privacy policy?	○	○
PR4. Does your business have an insider threat management program?	○	○
PR5. Does your business use encryption for sensitive information?	○	○
PR6. Does your business limit employee access to data and information through access controls? (principle of least privilege)	○	○
PR7. Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	○	○
PR8. Does your business restrict downloading and installing software by non-administrators?	○	○
PR9. Does your business disable access when an employee leaves the business?	○	○
PR10. Does your business protect information assets from physical intrusion?	○	○
PR11. Does your business enforce password management? (e.g., password policy with strong passwords, expirations, changing all default administrative passwords)	○	○

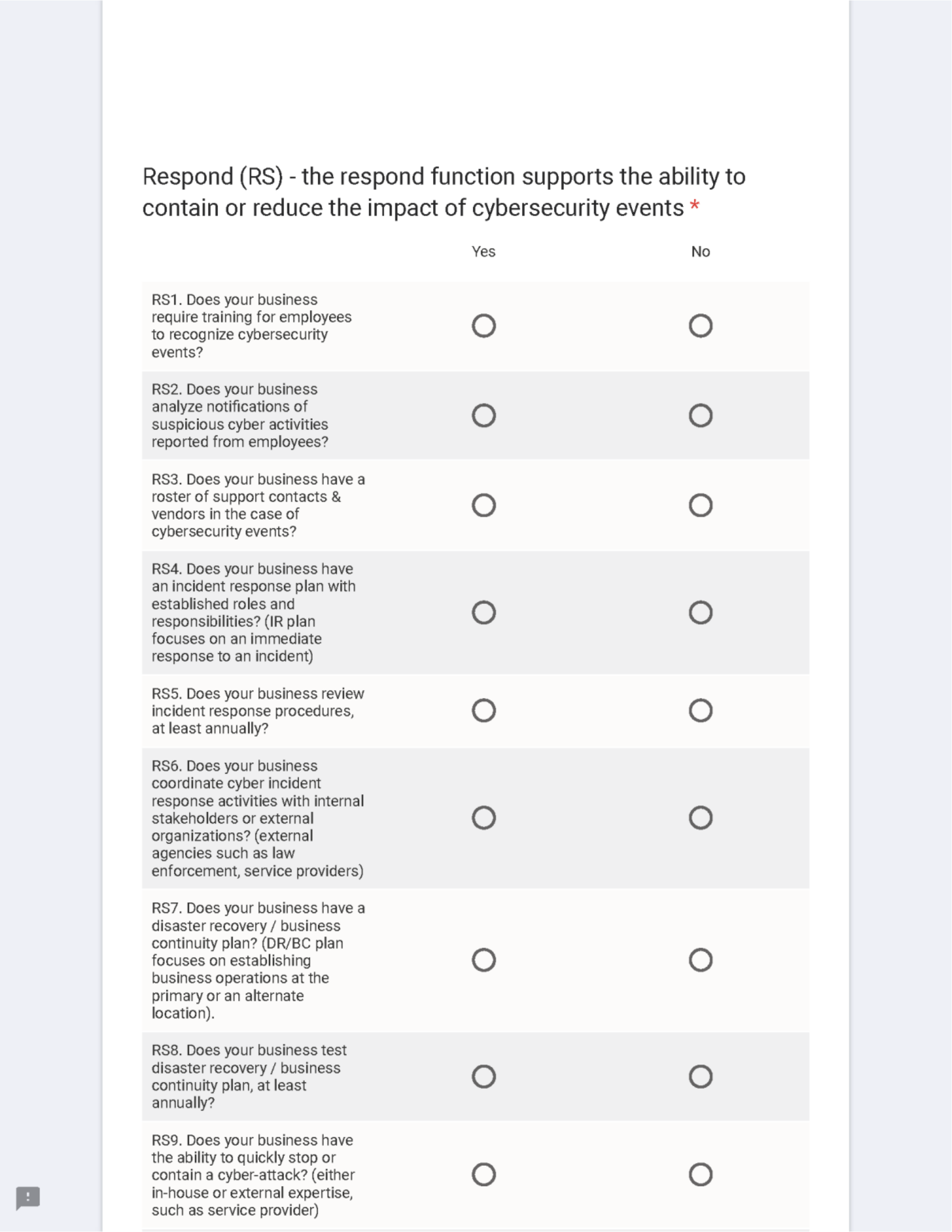


PR12. Does your business use multi-factor authentication?	○	○
PR13. Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	○	○
PR14. Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	○	○
PR15. Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	○	○
PR16. Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	○	○
PR17. Does your business restrict the use of web browser, such as email client plugins or add-on applications?	○	○
PR18. Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (e.g., acceptable use policy)	○	○
PR19. Does your business have a data disposal policy?	○	○
PR20. Does your business safely dispose of old computers and media by scrubbing information from drives?	○	○



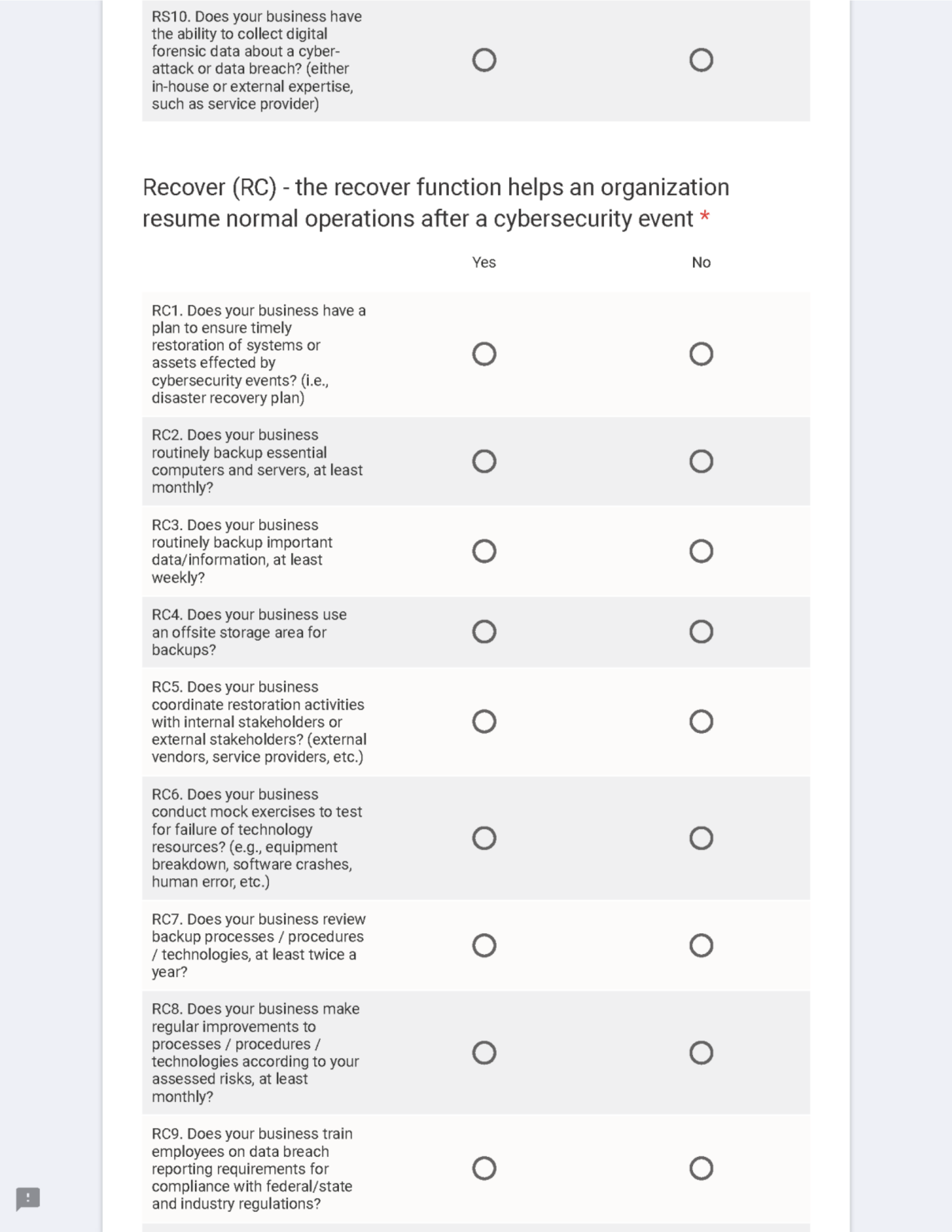
Detect (DE) - the detect function enables timely discovery of cybersecurity events *

	Yes	No
DE1. Does your business use anti-virus software? (also known as anti-malware)	○	○
DE2. Does your business update anti-virus software, at least daily?	○	○
DE3. Does your business use endpoint security software? (endpoint devices include mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network – endpoint software typically includes anti-virus software)	○	○
DE4. Does your business use an intrusion detection and prevention system (IDPS)?	○	○
DE5. Does your business baseline network utilization and detect anomalies in traffic patterns?	○	○
DE6. Does your business maintain and analyze cybersecurity event logs? (either in-house or managed security service provider)	○	○
DE7. Does your business perform test procedures at discrete intervals to identify cybersecurity events?	○	○
DE8. Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	○	○
DE9. Does your business perform vulnerability assessments, at least quarterly?	○	○
DE10. Does your business perform penetration testing, at least annually?	○	○



Respond (RS) - the respond function supports the ability to contain or reduce the impact of cybersecurity events *

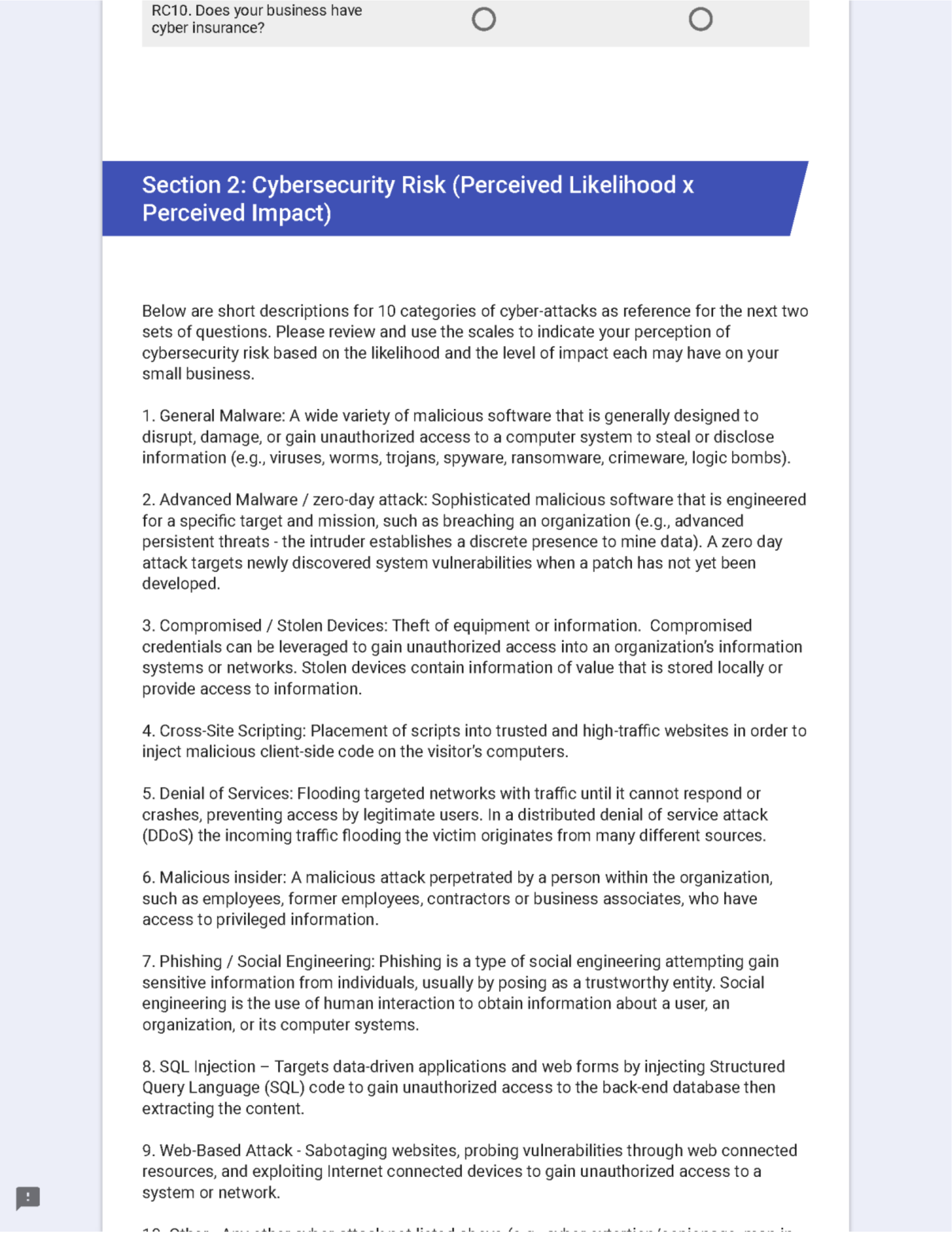
	Yes	No
RS1. Does your business require training for employees to recognize cybersecurity events?	○	○
RS2. Does your business analyze notifications of suspicious cyber activities reported from employees?	○	○
RS3. Does your business have a roster of support contacts & vendors in the case of cybersecurity events?	○	○
RS4. Does your business have an incident response plan with established roles and responsibilities? (IR plan focuses on an immediate response to an incident)	○	○
RS5. Does your business review incident response procedures, at least annually?	○	○
RS6. Does your business coordinate cyber incident response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	○	○
RS7. Does your business have a disaster recovery / business continuity plan? (DR/BC plan focuses on establishing business operations at the primary or an alternate location).	○	○
RS8. Does your business test disaster recovery / business continuity plan, at least annually?	○	○
RS9. Does your business have the ability to quickly stop or contain a cyber-attack? (either in-house or external expertise, such as service provider)	○	○



RS10. Does your business have the ability to collect digital forensic data about a cyber-attack or data breach? (either in-house or external expertise, such as service provider)	○	○

Recover (RC) - the recover function helps an organization resume normal operations after a cybersecurity event *

	Yes	No
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	○	○
RC2. Does your business routinely backup essential computers and servers, at least monthly?	○	○
RC3. Does your business routinely backup important data/information, at least weekly?	○	○
RC4. Does your business use an offsite storage area for backups?	○	○
RC5. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	○	○
RC6. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	○	○
RC7. Does your business review backup processes / procedures / technologies, at least twice a year?	○	○
RC8. Does your business make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly?	○	○
RC9. Does your business train employees on data breach reporting requirements for compliance with federal/state and industry regulations?	○	○



RC10. Does your business have cyber insurance? ○ ○

Section 2: Cybersecurity Risk (Perceived Likelihood x Perceived Impact)

Below are short descriptions for 10 categories of cyber-attacks as reference for the next two sets of questions. Please review and use the scales to indicate your perception of cybersecurity risk based on the likelihood and the level of impact each may have on your small business.

1. General Malware: A wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system to steal or disclose information (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs).

2. Advanced Malware / zero-day attack: Sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats - the intruder establishes a discrete presence to mine data). A zero day attack targets newly discovered system vulnerabilities when a patch has not yet been developed.

3. Compromised / Stolen Devices: Theft of equipment or information. Compromised credentials can be leveraged to gain unauthorized access into an organization's information systems or networks. Stolen devices contain information of value that is stored locally or provide access to information.

4. Cross-Site Scripting: Placement of scripts into trusted and high-traffic websites in order to inject malicious client-side code on the visitor's computers.

5. Denial of Services: Flooding targeted networks with traffic until it cannot respond or crashes, preventing access by legitimate users. In a distributed denial of service attack (DDoS) the incoming traffic flooding the victim originates from many different sources.

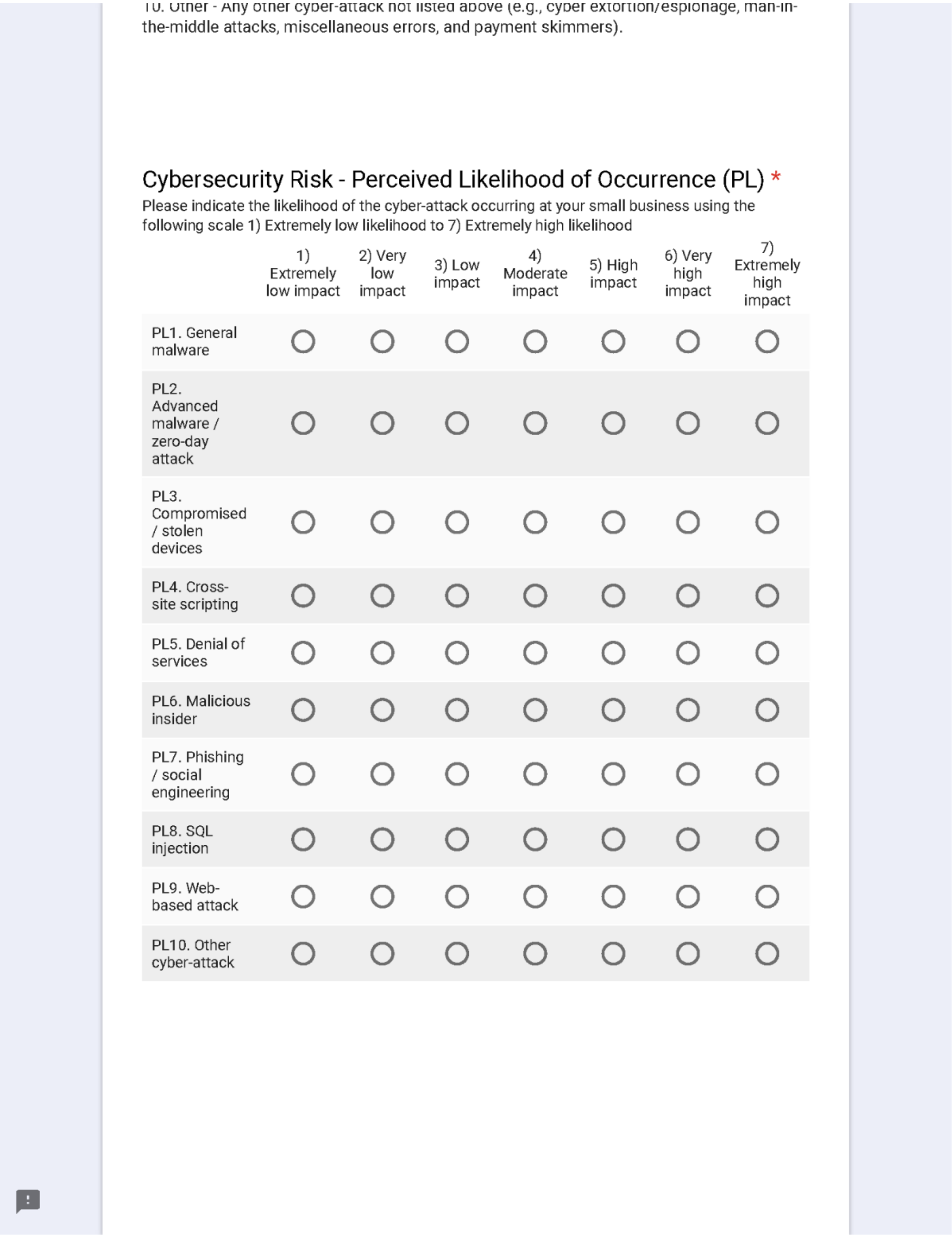
6. Malicious insider: A malicious attack perpetrated by a person within the organization, such as employees, former employees, contractors or business associates, who have access to privileged information.

7. Phishing / Social Engineering: Phishing is a type of social engineering attempting gain sensitive information from individuals, usually by posing as a trustworthy entity. Social engineering is the use of human interaction to obtain information about a user, an organization, or its computer systems.

8. SQL Injection – Targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database then extracting the content.

9. Web-Based Attack - Sabotaging websites, probing vulnerabilities through web connected resources, and exploiting Internet connected devices to gain unauthorized access to a system or network.

10. Other - Any other cyber attack not listed above (e.g., cyber extortion/espionage, man in

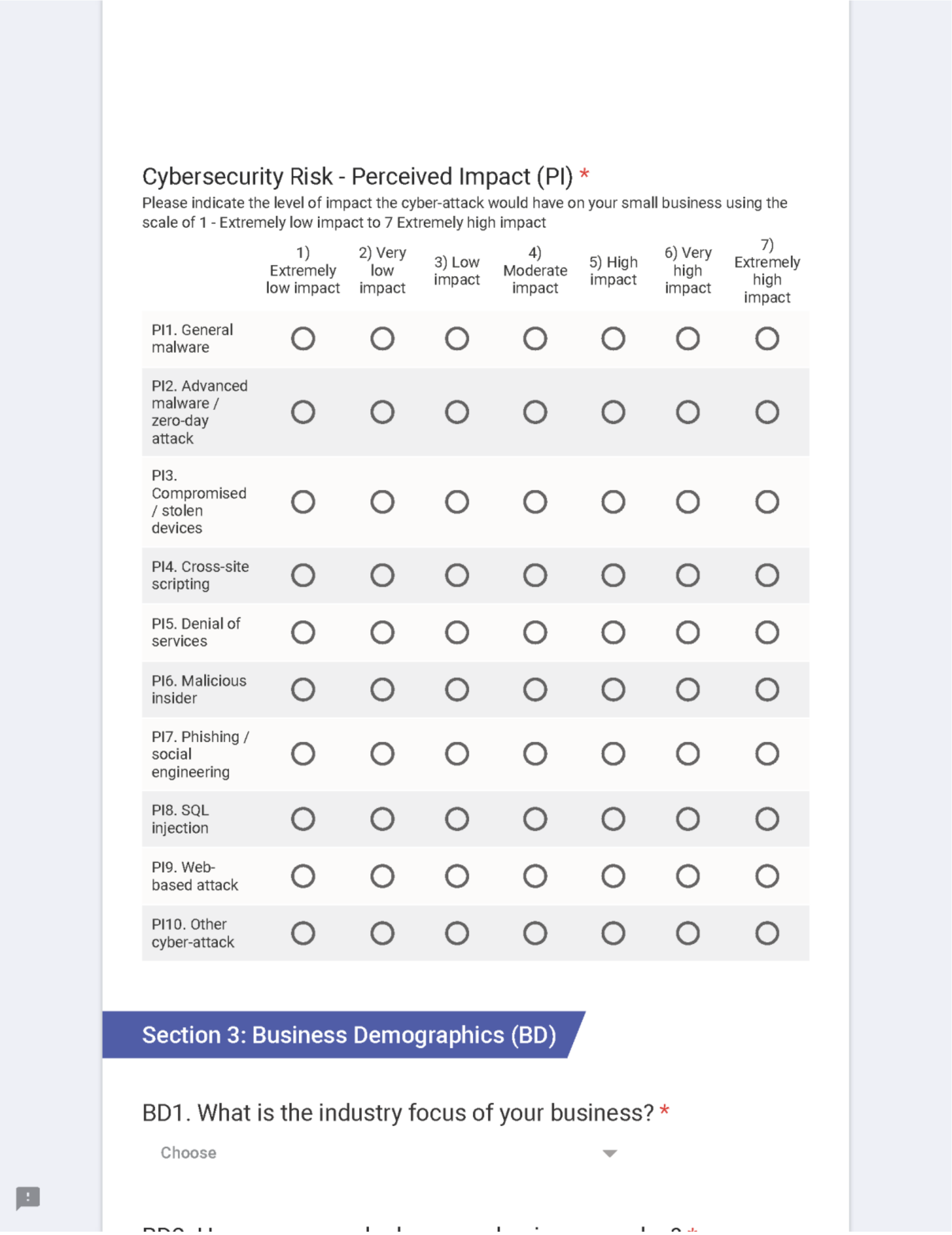


10. Other - Any other cyber-attack not listed above (e.g., cyber extortion/espionage, man-in-the-middle attacks, miscellaneous errors, and payment skimmers).

Cybersecurity Risk - Perceived Likelihood of Occurrence (PL) *

Please indicate the likelihood of the cyber-attack occurring at your small business using the following scale 1) Extremely low likelihood to 7) Extremely high likelihood

	1) Extremely low impact	2) Very low impact	3) Low impact	4) Moderate impact	5) High impact	6) Very high impact	7) Extremely high impact
PL1. General malware	○	○	○	○	○	○	○
PL2. Advanced malware / zero-day attack	○	○	○	○	○	○	○
PL3. Compromised / stolen devices	○	○	○	○	○	○	○
PL4. Cross-site scripting	○	○	○	○	○	○	○
PL5. Denial of services	○	○	○	○	○	○	○
PL6. Malicious insider	○	○	○	○	○	○	○
PL7. Phishing / social engineering	○	○	○	○	○	○	○
PL8. SQL injection	○	○	○	○	○	○	○
PL9. Web-based attack	○	○	○	○	○	○	○
PL10. Other cyber-attack	○	○	○	○	○	○	○



Cybersecurity Risk - Perceived Impact (PI) *

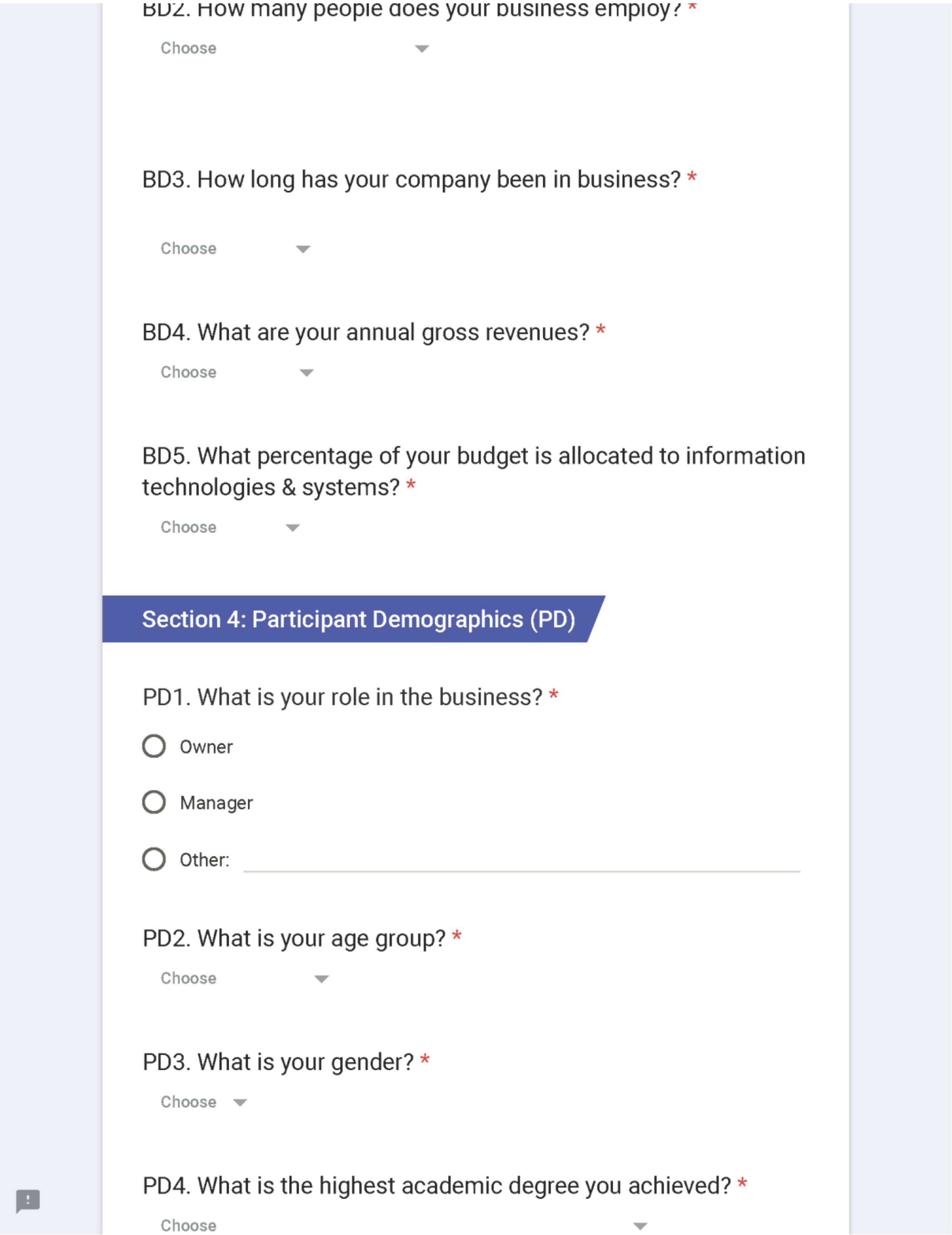
Please indicate the level of impact the cyber-attack would have on your small business using the scale of 1 - Extremely low impact to 7 Extremely high impact

	1) Extremely low impact	2) Very low impact	3) Low impact	4) Moderate impact	5) High impact	6) Very high impact	7) Extremely high impact
PI1. General malware	○	○	○	○	○	○	○
PI2. Advanced malware / zero-day attack	○	○	○	○	○	○	○
PI3. Compromised / stolen devices	○	○	○	○	○	○	○
PI4. Cross-site scripting	○	○	○	○	○	○	○
PI5. Denial of services	○	○	○	○	○	○	○
PI6. Malicious insider	○	○	○	○	○	○	○
PI7. Phishing / social engineering	○	○	○	○	○	○	○
PI8. SQL injection	○	○	○	○	○	○	○
PI9. Web-based attack	○	○	○	○	○	○	○
PI10. Other cyber-attack	○	○	○	○	○	○	○

Section 3: Business Demographics (BD)

BD1. What is the industry focus of your business? *

Choose ▾



BD2. How many people does your business employ? *

Choose ▾

BD3. How long has your company been in business? *

Choose ▾

BD4. What are your annual gross revenues? *

Choose ▾

BD5. What percentage of your budget is allocated to information technologies & systems? *

Choose ▾

Section 4: Participant Demographics (PD)

PD1. What is your role in the business? *

○ Owner

○ Manager

○ Other: ____________________

PD2. What is your age group? *

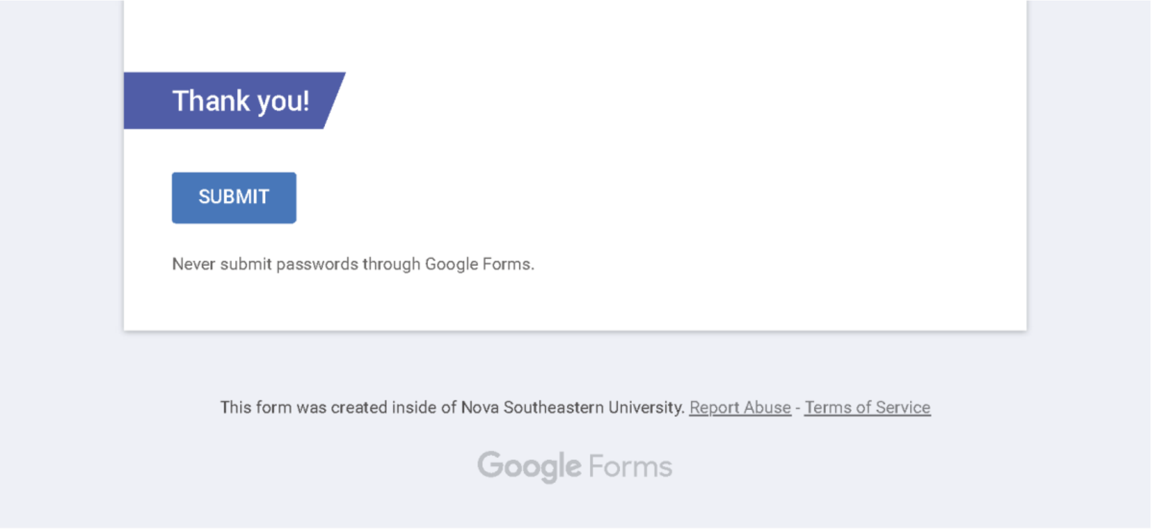
Choose ▾

PD3. What is your gender? *

Choose ▾

PD4. What is the highest academic degree you achieved? *

Choose ▾



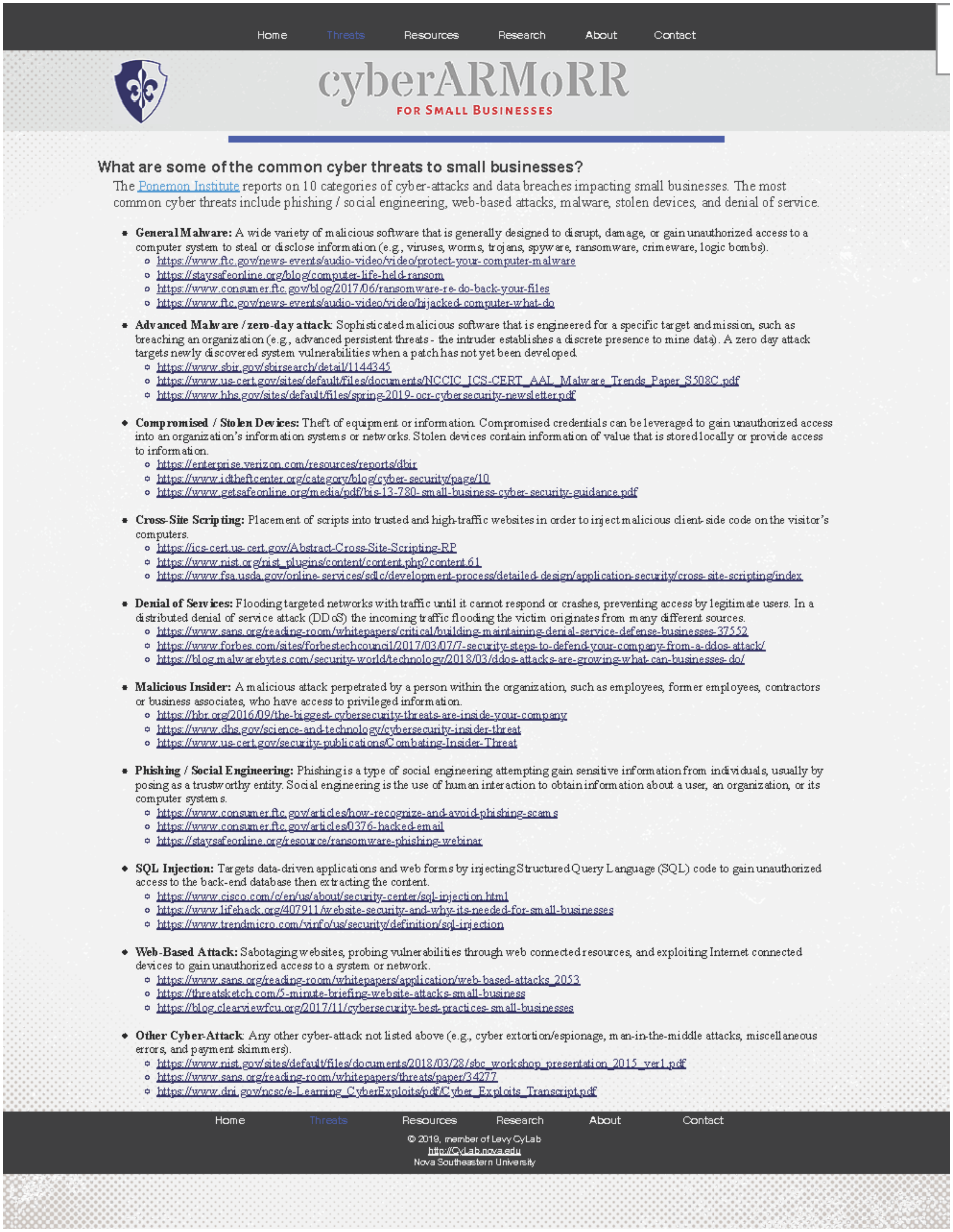
Thank you!

Never submit passwords through Google Forms.

This form was created inside of Nova Southeastern University. Report Abuse - Terms of Service

Appendix I

CyberARMoRR for Small Businesses - Threats



What are some of the common cyber threats to small businesses?

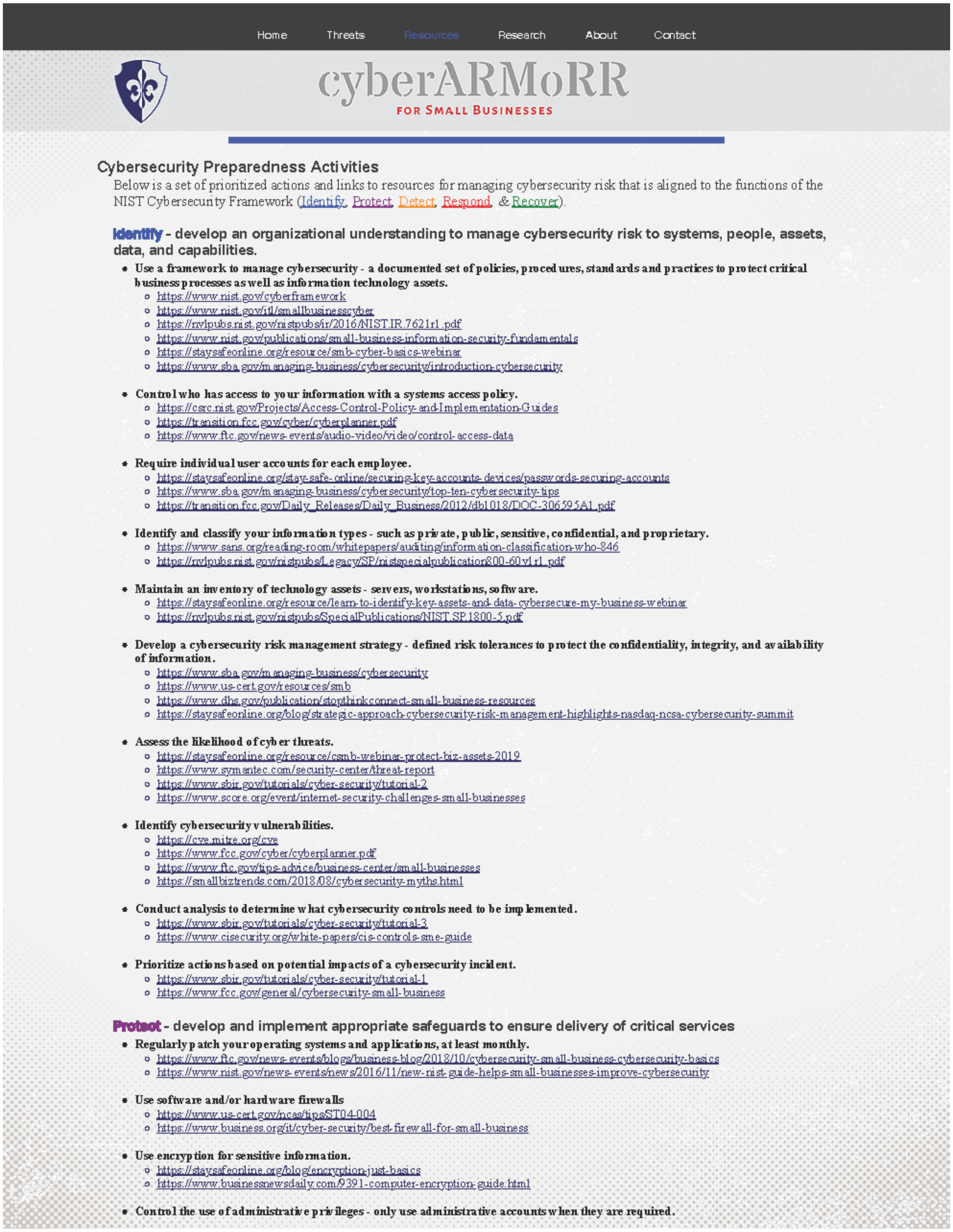
The Ponemon Institute reports on 10 categories of cyber-attacks and data breaches impacting small businesses. The most common cyber threats include phishing / social engineering, web-based attacks, malware, stolen devices, and denial of service.

- **General Malware:** A wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system to steal or disclose information (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs).
  - https://www.ftc.gov/news-events/audio-video/video/protect-your-computer-malware
  - https://staysafeonline.org/blog/computer-life-held-ransom
  - https://www.consumer.ftc.gov/blog/2017/06/ransomware-re-do-back-your-files
  - https://www.ftc.gov/news-events/audio-video/video/hijacked-computer-what-do
- **Advanced Malware / zero-day attack**: Sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats - the intruder establishes a discrete presence to mine data). A zero day attack targets newly discovered system vulnerabilities when a patch has not yet been developed.
  - https://www.sbir.gov/sbirsearch/detail/1144345
  - https://www.us-cert.gov/sites/default/files/documents/NCCIC_ICS-CERT_AAL_Malware_Trends_Paper_S508C.pdf
  - https://www.hhs.gov/sites/default/files/spring-2019-ocr-cybersecurity-newsletter.pdf
- **Compromised / Stolen Devices:** Theft of equipment or information. Compromised credentials can be leveraged to gain unauthorized access into an organization's information systems or networks. Stolen devices contain information of value that is stored locally or provide access to information.
  - https://enterprise.verizon.com/resources/reports/dbir
  - https://www.idtheftcenter.org/category/blog/cyber-security/page/10
  - https://www.getsafeonline.org/media/pdf/bis-13-780-small-business-cyber-security-guidance.pdf
- **Cross-Site Scripting:** Placement of scripts into trusted and high-traffic websites in order to inject malicious client-side code on the visitor's computers.
  - https://ics-cert.us-cert.gov/Abstract-Cross-Site-Scripting-RP
  - https://www.nist.org/nist_plugins/content/content.php?content.61
  - https://www.fsa.usda.gov/online-services/sdlc/development-process/detailed-design/application-security/cross-site-scripting/index
- **Denial of Services:** Flooding targeted networks with traffic until it cannot respond or crashes, preventing access by legitimate users. In a distributed denial of service attack (DDoS) the incoming traffic flooding the victim originates from many different sources.
  - https://www.sans.org/reading-room/whitepapers/critical/building-maintaining-denial-service-defense-businesses-37552
  - https://www.forbes.com/sites/forbestechcouncil/2017/03/07/7-security-steps-to-defend-your-company-from-a-ddos-attack/
  - https://blog.malwarebytes.com/security-world/technology/2018/03/ddos-attacks-are-growing-what-can-businesses-do/
- **Malicious Insider:** A malicious attack perpetrated by a person within the organization, such as employees, former employees, contractors or business associates, who have access to privileged information.
  - https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company
  - https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat
  - https://www.us-cert.gov/security-publications/Combating-Insider-Threat
- **Phishing / Social Engineering:** Phishing is a type of social engineering attempting gain sensitive information from individuals, usually by posing as a trustworthy entity. Social engineering is the use of human interaction to obtain information about a user, an organization, or its computer systems.
  - https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
  - https://www.consumer.ftc.gov/articles/0376-hacked-email
  - https://staysafeonline.org/resource/ransomware-phishing-webinar
- **SQL Injection:** Targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database then extracting the content.
  - https://www.cisco.com/c/en/us/about/security-center/sql-injection.html
  - https://www.lifehack.org/407911/website-security-and-why-its-needed-for-small-businesses
  - https://www.trendmicro.com/vinfo/us/security/definition/sql-injection
- **Web-Based Attack:** Sabotaging websites, probing vulnerabilities through web connected resources, and exploiting Internet connected devices to gain unauthorized access to a system or network.
  - https://www.sans.org/reading-room/whitepapers/application/web-based-attacks_2053
  - https://threatsketch.com/5-minute-briefing-website-attacks-small-business
  - https://blog.clearviewfcu.org/2017/11/cybersecurity-best-practices-small-businesses
- **Other Cyber-Attack**: Any other cyber-attack not listed above (e.g., cyber extortion/espionage, man-in-the-middle attacks, miscellaneous errors, and payment skimmers).
  - https://www.nist.gov/sites/default/files/documents/2018/03/28/sbc_workshop_presentation_2015_ver1.pdf
  - https://www.sans.org/reading-room/whitepapers/threats/paper/34277
  - https://www.dni.gov/ncsc/e-Learning_CyberExploits/pdf/Cyber_Exploits_Transcript.pdf

© 2019, member of Levy CyLab
http://CyLab.nova.edu
Nova Southeastern University

Appendix J

CyberARMoRR for Small Businesses - Resources



Cybersecurity Preparedness Activities

Below is a set of prioritized actions and links to resources for managing cybersecurity risk that is aligned to the functions of the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, & Recover).

Identify - develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.

- **Use a framework to manage cybersecurity - a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets.**
  - https://www.nist.gov/cyberframework
  - https://www.nist.gov/itl/smallbusinesscyber
  - https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf
  - https://www.nist.gov/publications/small-business-information-security-fundamentals
  - https://staysafeonline.org/resource/smb-cyber-basics-webinar
  - https://www.sba.gov/managing-business/cybersecurity/introduction-cybersecurity

- **Control who has access to your information with a systems access policy.**
  - https://csrc.nist.gov/Projects/Access-Control-Policy-and-Implementation-Guides
  - https://transition.fcc.gov/cyber/cyberplanner.pdf
  - https://www.ftc.gov/news-events/audio-video/video/control-access-data

- **Require individual user accounts for each employee.**
  - https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/passwords-securing-accounts
  - https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips
  - https://transition.fcc.gov/Daily_Releases/Daily_Business/2012/db1018/DOC-306595A1.pdf

- **Identify and classify your information types - such as private, public, sensitive, confidential, and proprietary.**
  - https://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

- **Maintain an inventory of technology assets - servers, workstations, software.**
  - https://staysafeonline.org/resource/learn-to-identify-key-assets-and-data-cybersecure-my-business-webinar
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-5.pdf

- **Develop a cybersecurity risk management strategy - defined risk tolerances to protect the confidentiality, integrity, and availability of information.**
  - https://www.sba.gov/managing-business/cybersecurity
  - https://www.us-cert.gov/resources/smb
  - https://www.dhs.gov/publication/stopthinkconnect-small-business-resources
  - https://staysafeonline.org/blog/strategic-approach-cybersecurity-risk-management-highlights-nasdaq-ncsa-cybersecurity-summit

- **Assess the likelihood of cyber threats.**
  - https://staysafeonline.org/resource/csmb-webinar-protect-biz-assets-2019
  - https://www.symantec.com/security-center/threat-report
  - https://www.sbir.gov/tutorials/cyber-security/tutorial-2
  - https://www.score.org/event/internet-security-challenges-small-businesses

- **Identify cybersecurity vulnerabilities.**
  - https://cve.mitre.org/cve
  - https://www.fcc.gov/cyber/cyberplanner.pdf
  - https://www.ftc.gov/tips-advice/business-center/small-businesses
  - https://smallbiztrends.com/2018/08/cybersecurity-myths.html

- **Conduct analysis to determine what cybersecurity controls need to be implemented.**
  - https://www.sbir.gov/tutorials/cyber-security/tutorial-3
  - https://www.cisecurity.org/white-papers/cis-controls-sme-guide

- **Prioritize actions based on potential impacts of a cybersecurity incident.**
  - https://www.sbir.gov/tutorials/cyber-security/tutorial-1
  - https://www.fcc.gov/general/cybersecurity-small-business

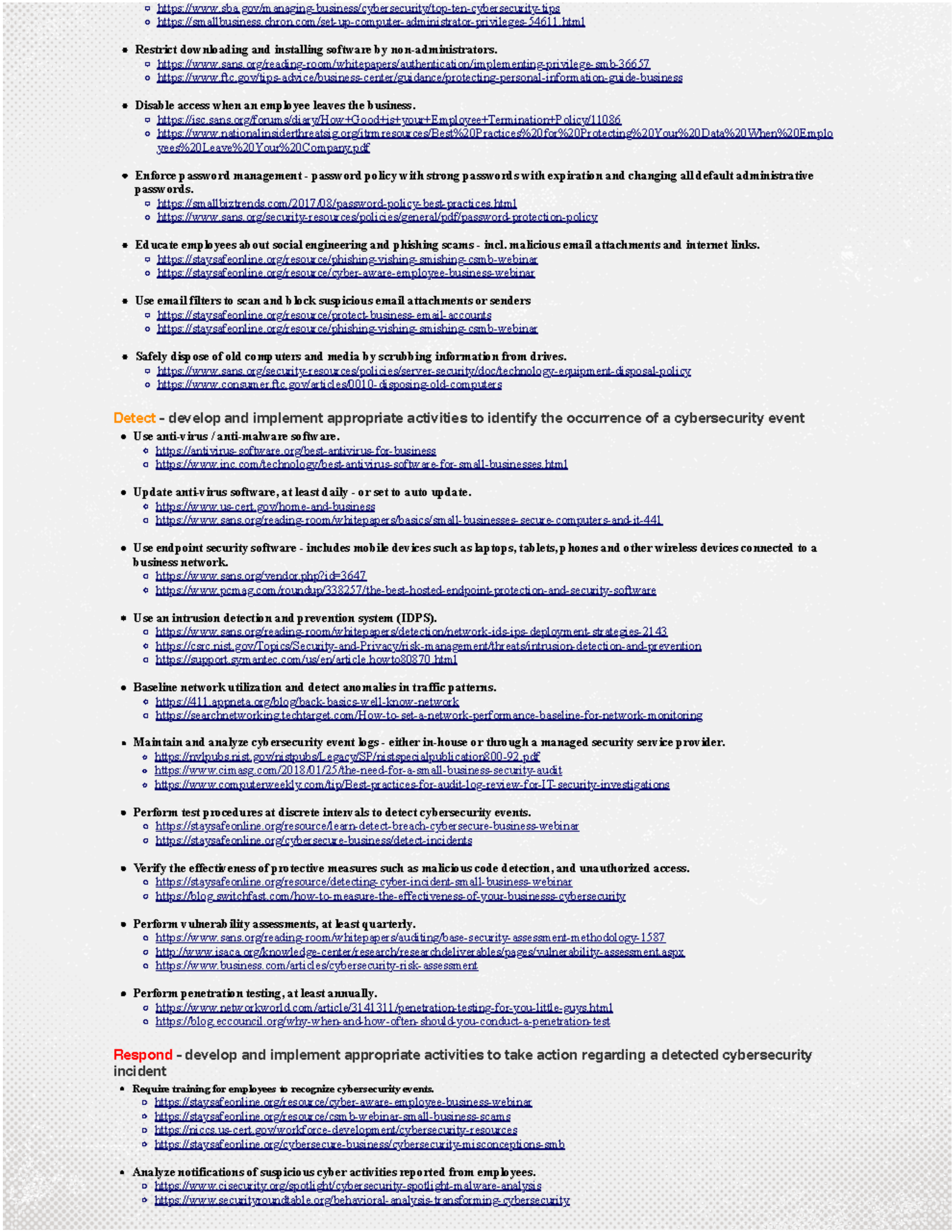
Protect - develop and implement appropriate safeguards to ensure delivery of critical services

- **Regularly patch your operating systems and applications, at least monthly.**
  - https://www.ftc.gov/news-events/blogs/business-blog/2018/10/cybersecurity-small-business-cybersecurity-basics
  - https://www.nist.gov/news-events/news/2016/11/new-nist-guide-helps-small-businesses-improve-cybersecurity

- **Use software and/or hardware firewalls**
  - https://www.us-cert.gov/ncas/tips/ST04-004
  - https://www.business.org/it/cyber-security/best-firewall-for-small-business

- **Use encryption for sensitive information.**
  - https://staysafeonline.org/blog/encryption-just-basics
  - https://www.businessnewsdaily.com/9391-computer-encryption-guide.html

- **Control the use of administrative privileges - only use administrative accounts when they are required.**



- https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips
- https://smallbusiness.chron.com/set-up-computer-administrator-privileges-54611.html

- **Restrict downloading and installing software by non-administrators.**
  - https://www.sans.org/reading-room/whitepapers/authentication/implementing-privilege-smb-36657
  - https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

- **Disable access when an employee leaves the business.**
  - https://isc.sans.org/forums/diary/How+Good+is+your+Employee+Termination+Policy/11086
  - https://www.nationalinsiderthreatsig.org/itmresources/Best%20Practices%20for%20Protecting%20Your%20Data%20When%20Employees%20Leave%20Your%20Company.pdf

- **Enforce password management - password policy with strong passwords with expiration and changing all default administrative passwords.**
  - https://smallbiztrends.com/2017/08/password-policy-best-practices.html
  - https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

- **Educate employees about social engineering and phishing scams - incl. malicious email attachments and internet links.**
  - https://staysafeonline.org/resource/phishing-vishing-smishing-csmb-webinar
  - https://staysafeonline.org/resource/cyber-aware-employee-business-webinar

- **Use email filters to scan and block suspicious email attachments or senders**
  - https://staysafeonline.org/resource/protect-business-email-accounts
  - https://staysafeonline.org/resource/phishing-vishing-smishing-csmb-webinar

- **Safely dispose of old computers and media by scrubbing information from drives.**
  - https://www.sans.org/security-resources/policies/server-security/doc/technology-equipment-disposal-policy
  - https://www.consumer.ftc.gov/articles/0010-disposing-old-computers

Detect - develop and implement appropriate activities to identify the occurrence of a cybersecurity event

- **Use anti-virus / anti-malware software.**
  - https://antivirus-software.org/best-antivirus-for-business
  - https://www.inc.com/technology/best-antivirus-software-for-small-businesses.html

- **Update anti-virus software, at least daily - or set to auto update.**
  - https://www.us-cert.gov/home-and-business
  - https://www.sans.org/reading-room/whitepapers/basics/small-businesses-secure-computers-and-it-441

- **Use endpoint security software - includes mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network.**
  - https://www.sans.org/vendor.php?id=3647
  - https://www.pcmag.com/roundup/338257/the-best-hosted-endpoint-protection-and-security-software

- **Use an intrusion detection and prevention system (IDPS).**
  - https://www.sans.org/reading-room/whitepapers/detection/network-ids-ips-deployment-strategies-2143
  - https://csrc.nist.gov/Topics/Security-and-Privacy/risk-management/threats/intrusion-detection-and-prevention
  - https://support.symantec.com/us/en/article.howto80870.html

- **Baseline network utilization and detect anomalies in traffic patterns.**
  - https://411.appneta.org/blog/back-basics-well-know-network
  - https://searchnetworking.techtarget.com/How-to-set-a-network-performance-baseline-for-network-monitoring

- **Maintain and analyze cybersecurity event logs - either in-house or through a managed security service provider.**
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf
  - https://www.cimasg.com/2018/01/25/the-need-for-a-small-business-security-audit
  - https://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations

- **Perform test procedures at discrete intervals to detect cybersecurity events.**
  - https://staysafeonline.org/resource/learn-detect-breach-cybersecure-business-webinar
  - https://staysafeonline.org/cybersecure-business/detect-incidents

- **Verify the effectiveness of protective measures such as malicious code detection, and unauthorized access.**
  - https://staysafeonline.org/resource/detecting-cyber-incident-small-business-webinar
  - https://blog.switchfast.com/how-to-measure-the-effectiveness-of-your-businesss-cybersecurity

- **Perform vulnerability assessments, at least quarterly.**
  - https://www.sans.org/reading-room/whitepapers/auditing/base-security-assessment-methodology-1587
  - http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/vulnerability-assessment.aspx
  - https://www.business.com/articles/cybersecurity-risk-assessment

- **Perform penetration testing, at least annually.**
  - https://www.networkworld.com/article/3141311/penetration-testing-for-you-little-guys.html
  - https://blog.eccouncil.org/why-when-and-how-often-should-you-conduct-a-penetration-test

Respond - develop and implement appropriate activities to take action regarding a detected cybersecurity incident

- **Require training for employees to recognize cybersecurity events.**
  - https://staysafeonline.org/resource/cyber-aware-employee-business-webinar
  - https://staysafeonline.org/resource/csmb-webinar-small-business-scams
  - https://niccs.us-cert.gov/workforce-development/cybersecurity-resources
  - https://staysafeonline.org/cybersecure-business/cybersecurity-misconceptions-smb

- **Analyze notifications of suspicious cyber activities reported from employees.**
  - https://www.cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis
  - https://www.securityroundtable.org/behavioral-analysis-transforming-cybersecurity

- **Create a roster of support contacts & vendors in the case of cybersecurity events.**
  - https://www.us-cert.gov/ncas
  - https://www.dhs.gov/cisa/protective-security-advisors

- **Create an incident response plan with established roles and responsibilities that focuses on an immediate response to an incident.**
  - https://staysafeonline.org/resource/put-a-response-plan-in-place-cybersecure-my-business-webinar
  - https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

- **Review incident response procedures, at least annually.**
  - https://www.sans.org/reading-room/whitepapers/incident/paper/32979
  - https://www.ready.gov/sites/default/files/documents/ files/sampleplan.pdf

- **Coordinate cyber incident response activities with internal stakeholders and external agencies such as law enforcement, service providers.**
  - https://www.ic3.gov/default.aspx
  - https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center
  - https://fraudsupport.org

- **Create a disaster recovery / business continuity plan to focus on establishing business operations at the primary or an alternate location.**
  - https://www.ready.gov/business/implementation/IT
  - https://www.ready.gov/business/implementation/continuity
  - https://www.sba.gov/blog/seven-ways-start-your-business-continuity-plan

- **Test disaster recovery / business continuity plan, at least annually.**
  - https://staysafeonline.org/cybersecure-business/respond
  - https://www.disasterrecoveryplantemplate.org/download/disaster-recovery-plan-template-basic

- **Test your plan to ensure you can quickly stop or contain a cyber-attack using either in-house or external expertise, such as service provider.**
  - https://www.sba.gov/sites/default/files/Disaster%20Recovery%20Plan%202012.pdf
  - https://www.nist.gov/itl/smallbusinesscyber/planning-guides

- **Evaluate your ability to collect digital forensic data about a cyber-attack or data breach using either in-house or external expertise, such as service provider.**
  - https://biztechmagazine.com/article/2011/03/protect-your-business-computer-forensics
  - https://blog.malwarebytes.com/security-world/2017/08/explained-digital-forensics
  - https://blog.eccouncil.org/4-mistakes-that-can-sink-a-cyber-forensic-investigation

Recover - develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

- **Create a plan to ensure timely restoration of systems or assets effected by cybersecurity events.**
  - https://www.nist.gov/sites/default/files/documents/2017/12/01/recovery-webinar.pdf
  - https://staysafeonline.org/resource/know-what-recovery-looks-like-cybersecure-my-business-webinar
  - https://staysafeonline.org/resource/business-hacked-csmb-webinar-sep19

- **Routinely backup essential computers and servers, at least monthly.**
  - https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf
  - https://www.cio.com/article/2378019/how-to-build-a-storage-and-backup-strategy-for-your-small-business.html
  - https://www.techadvisory.org/2015/06/4-data-backup-methods

- **Routinely backup important data/information, at least weekly.**
  - https://www.score.org/blog/back-it-up
  - https://www.techsoup.org/support/articles-and-how-tos/your-organizations-backup-strategy

- **Use an offsite storage area for backups.**
  - https://staysafeonline.org/stay-safe-online/online-safety-basics/back-it-up
  - https://www.sba.gov/blog/cloud-storage-thumb-drive-or-disk-drive-pros-cons
  - https://www.disasterrecovery.org/small-business-disaster-recovery-in-the-cloud

- **Coordinate restoration activities with internal stakeholders or external stakeholders, such as vendors, service providers, etc.**
  - https://www.us-cert.gov/sites/default/files/c3vp/CISCP_20140523.pdf
  - http://dhs.gov/enhanced-cybersecurity-services

- **Conduct mock exercises to test for failure of technology resources. (e.g., equipment breakdown, software crashes, human error, etc.)**
  - http://www.fema.gov/emergency-planning-exercises
  - https://www.sans.org/reading-room/whitepapers/recovery/paper/564

- **Review backup processes / procedures / technologies, at least twice a year.**
  - https://www.iii.org/article/developing-small-business-disaster-recovery-plan-0
  - https://www.ready.gov/business/implementation/continuity

- **Make regular improvements to processes / procedures / technologies according to your assessed risks.**
  - http://www.fcc.gov/cyberforsmallbiz
  - https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business

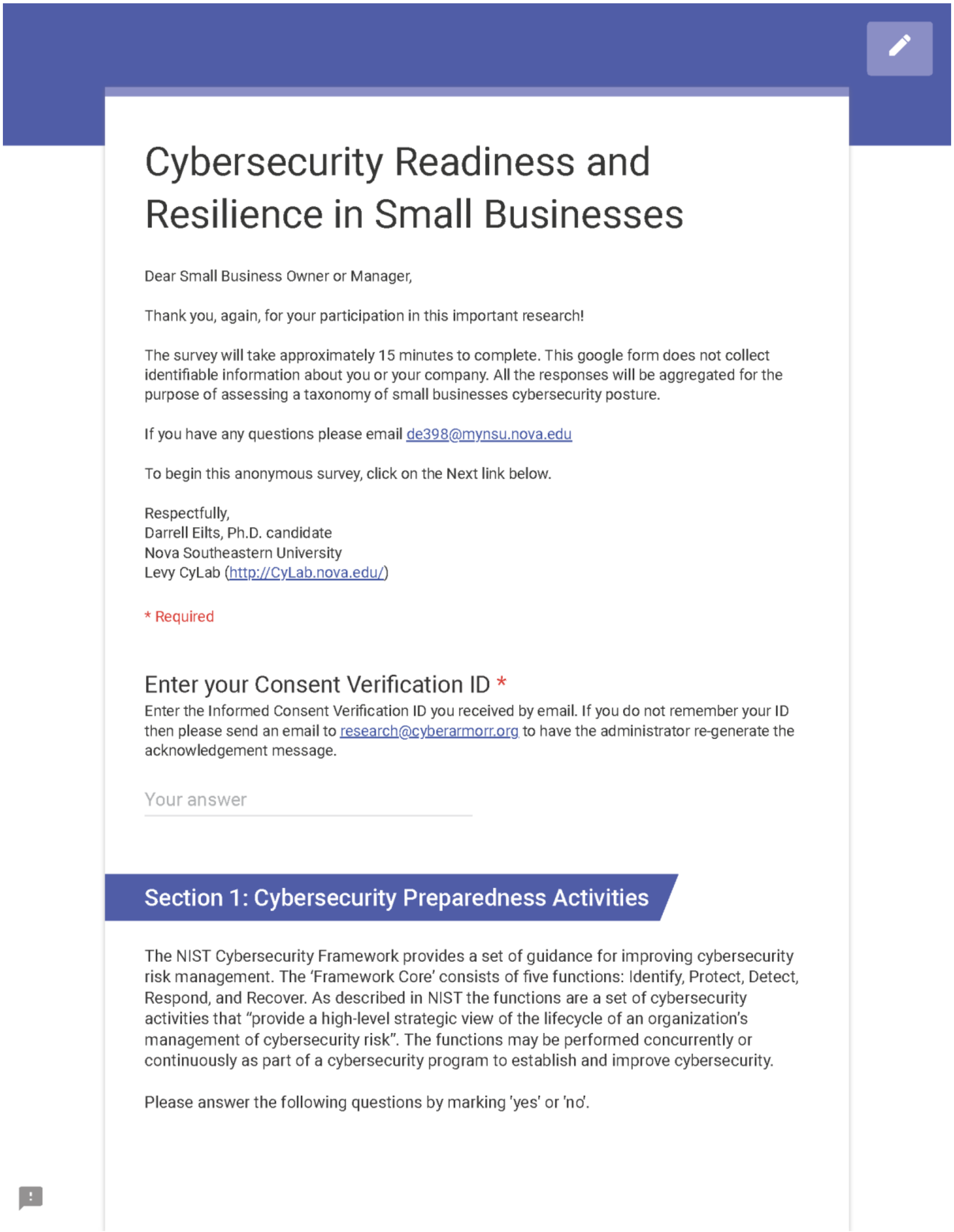
- **Train employees on data breach reporting requirements for compliance with federal/state and industry regulations.**
  - https://www.dhs.gov/how-do-i/report-cyber-incidents
  - https://www.sans.org/reading-room/whitepapers/incident/paper/32979

- **Consider purchasing cyber insurance.**
  - https://staysafeonline.org/blog/cyber-insurance-101-basics-need-know
  - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/cyber-insurance

© 2019, member of Levy CyLab
http://CyLab.nova.edu

Appendix K

Phase 3 Survey for Participants (Posttest measure)



Cybersecurity Readiness and Resilience in Small Businesses

Dear Small Business Owner or Manager,

Thank you, again, for your participation in this important research!

The survey will take approximately 15 minutes to complete. This google form does not collect identifiable information about you or your company. All the responses will be aggregated for the purpose of assessing a taxonomy of small businesses cybersecurity posture.

If you have any questions please email de398@mynsu.nova.edu

To begin this anonymous survey, click on the Next link below.

Respectfully,
Darrell Eilts, Ph.D. candidate
Nova Southeastern University
Levy CyLab (http://CyLab.nova.edu/)

* Required

Enter your Consent Verification ID *

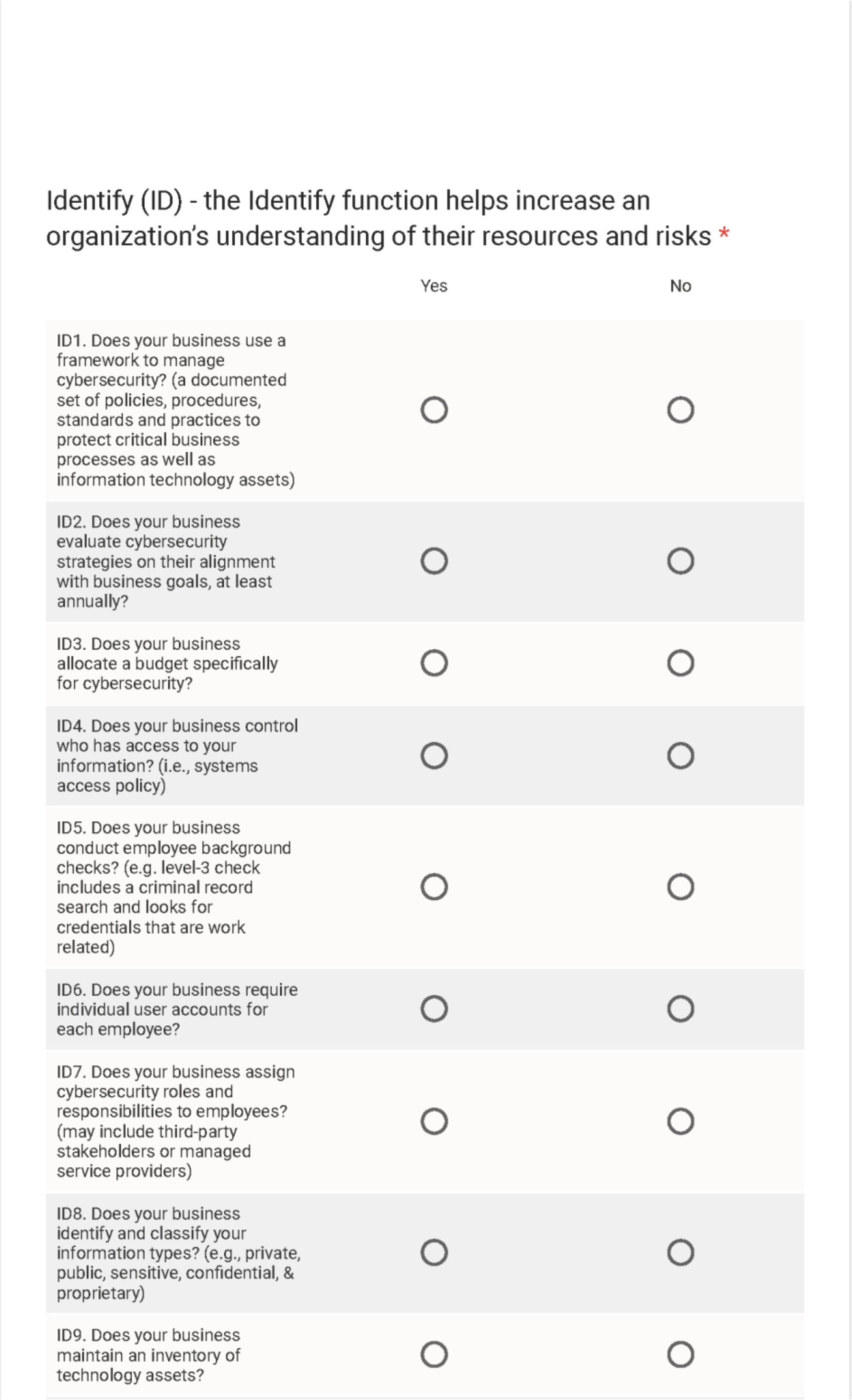
Enter the Informed Consent Verification ID you received by email. If you do not remember your ID then please send an email to research@cyberarmorr.org to have the administrator re-generate the acknowledgement message.

Your answer

Section 1: Cybersecurity Preparedness Activities

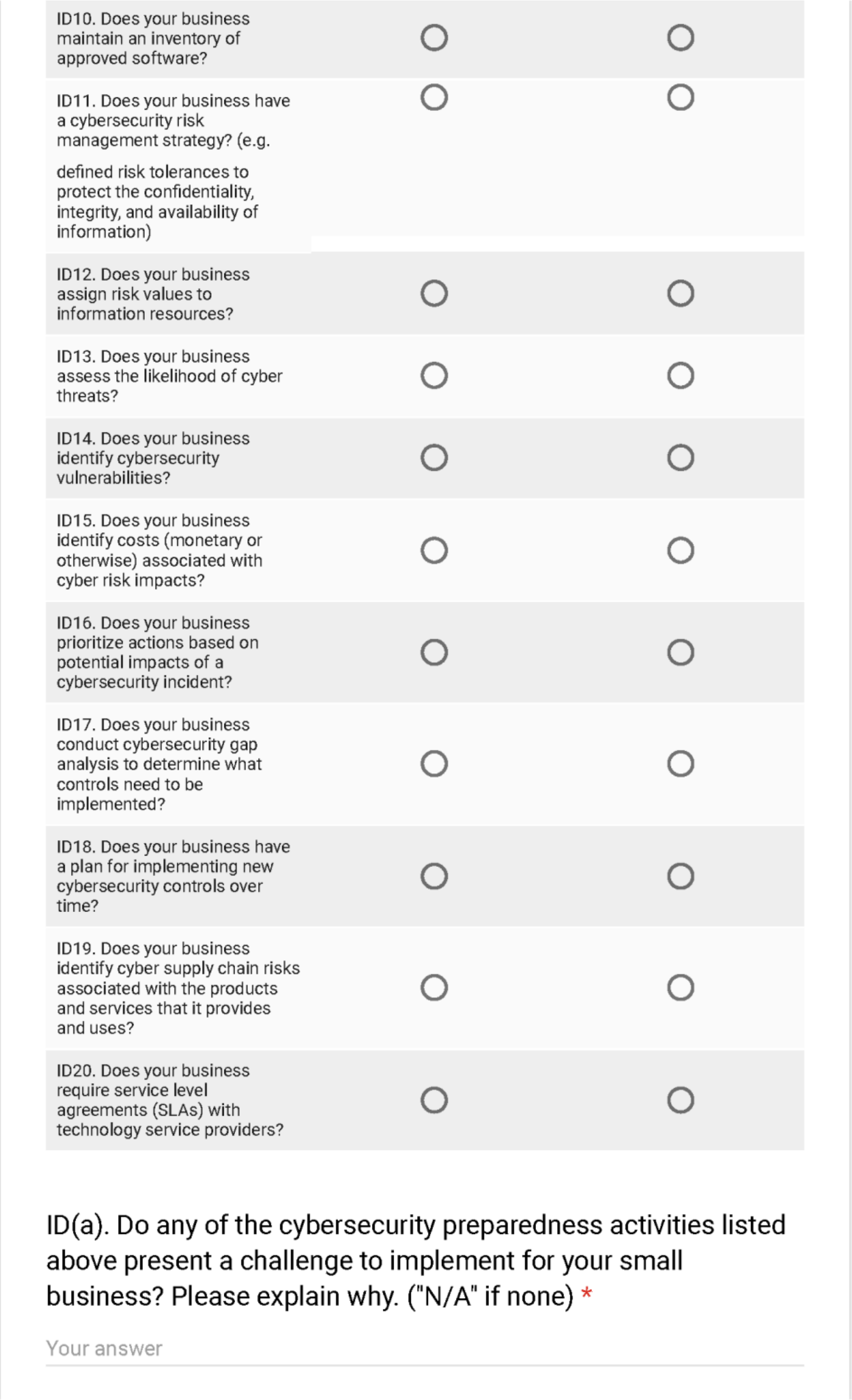
The NIST Cybersecurity Framework provides a set of guidance for improving cybersecurity risk management. The ‘Framework Core’ consists of five functions: Identify, Protect, Detect, Respond, and Recover. As described in NIST the functions are a set of cybersecurity activities that “provide a high-level strategic view of the lifecycle of an organization’s management of cybersecurity risk”. The functions may be performed concurrently or continuously as part of a cybersecurity program to establish and improve cybersecurity.

Please answer the following questions by marking 'yes' or 'no'.



Identify (ID) - the Identify function helps increase an organization’s understanding of their resources and risks *

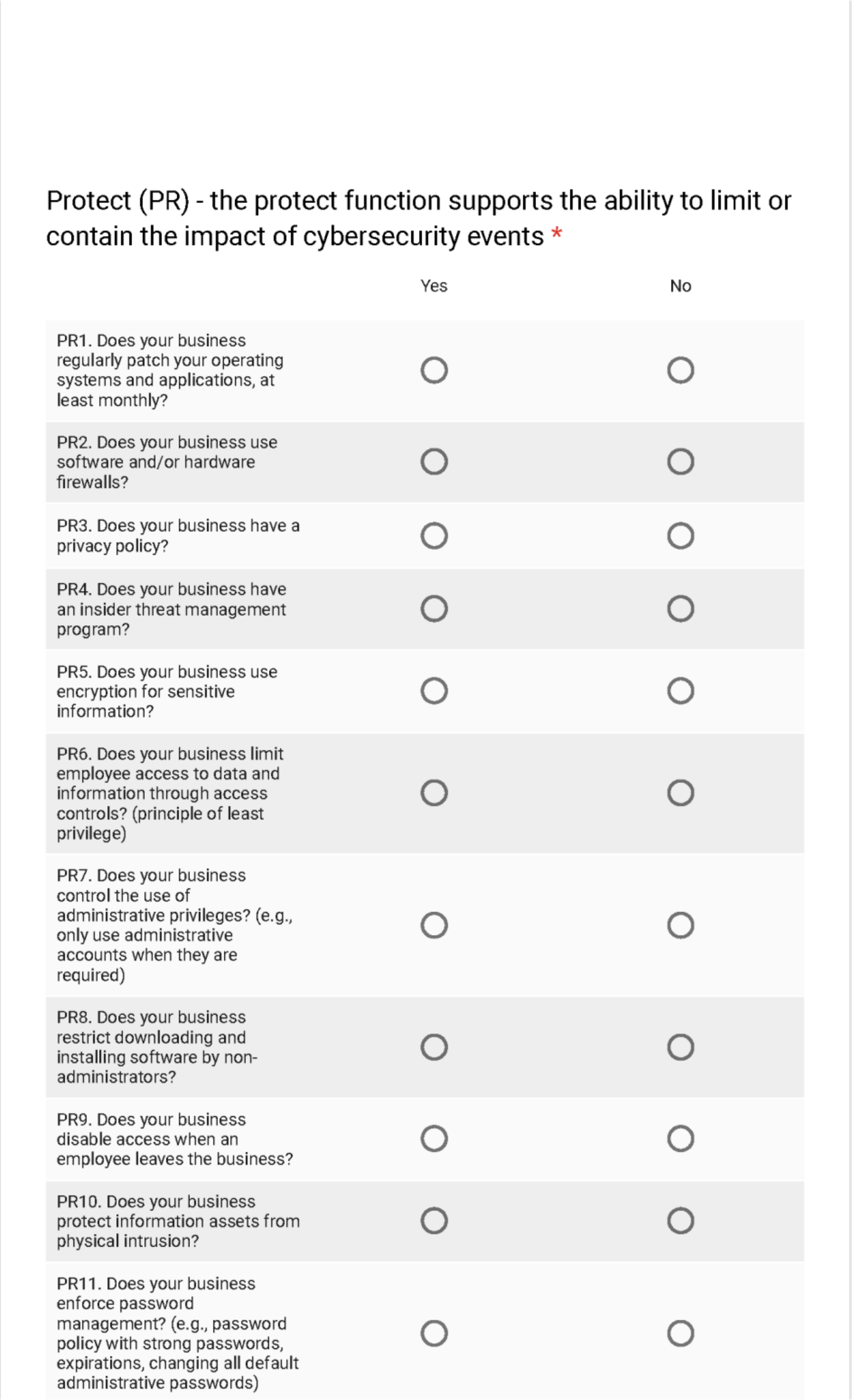
	Yes	No
ID1. Does your business use a framework to manage cybersecurity? (a documented set of policies, procedures, standards and practices to protect critical business processes as well as information technology assets)	○	○
ID2. Does your business evaluate cybersecurity strategies on their alignment with business goals, at least annually?	○	○
ID3. Does your business allocate a budget specifically for cybersecurity?	○	○
ID4. Does your business control who has access to your information? (i.e., systems access policy)	○	○
ID5. Does your business conduct employee background checks? (e.g. level-3 check includes a criminal record search and looks for credentials that are work related)	○	○
ID6. Does your business require individual user accounts for each employee?	○	○
ID7. Does your business assign cybersecurity roles and responsibilities to employees? (may include third-party stakeholders or managed service providers)	○	○
ID8. Does your business identify and classify your information types? (e.g., private, public, sensitive, confidential, & proprietary)	○	○
ID9. Does your business maintain an inventory of technology assets?	○	○



ID10. Does your business maintain an inventory of approved software?	○	○
ID11. Does your business have a cybersecurity risk management strategy? (e.g. defined risk tolerances to protect the confidentiality, integrity, and availability of information)	○	○
ID12. Does your business assign risk values to information resources?	○	○
ID13. Does your business assess the likelihood of cyber threats?	○	○
ID14. Does your business identify cybersecurity vulnerabilities?	○	○
ID15. Does your business identify costs (monetary or otherwise) associated with cyber risk impacts?	○	○
ID16. Does your business prioritize actions based on potential impacts of a cybersecurity incident?	○	○
ID17. Does your business conduct cybersecurity gap analysis to determine what controls need to be implemented?	○	○
ID18. Does your business have a plan for implementing new cybersecurity controls over time?	○	○
ID19. Does your business identify cyber supply chain risks associated with the products and services that it provides and uses?	○	○
ID20. Does your business require service level agreements (SLAs) with technology service providers?	○	○

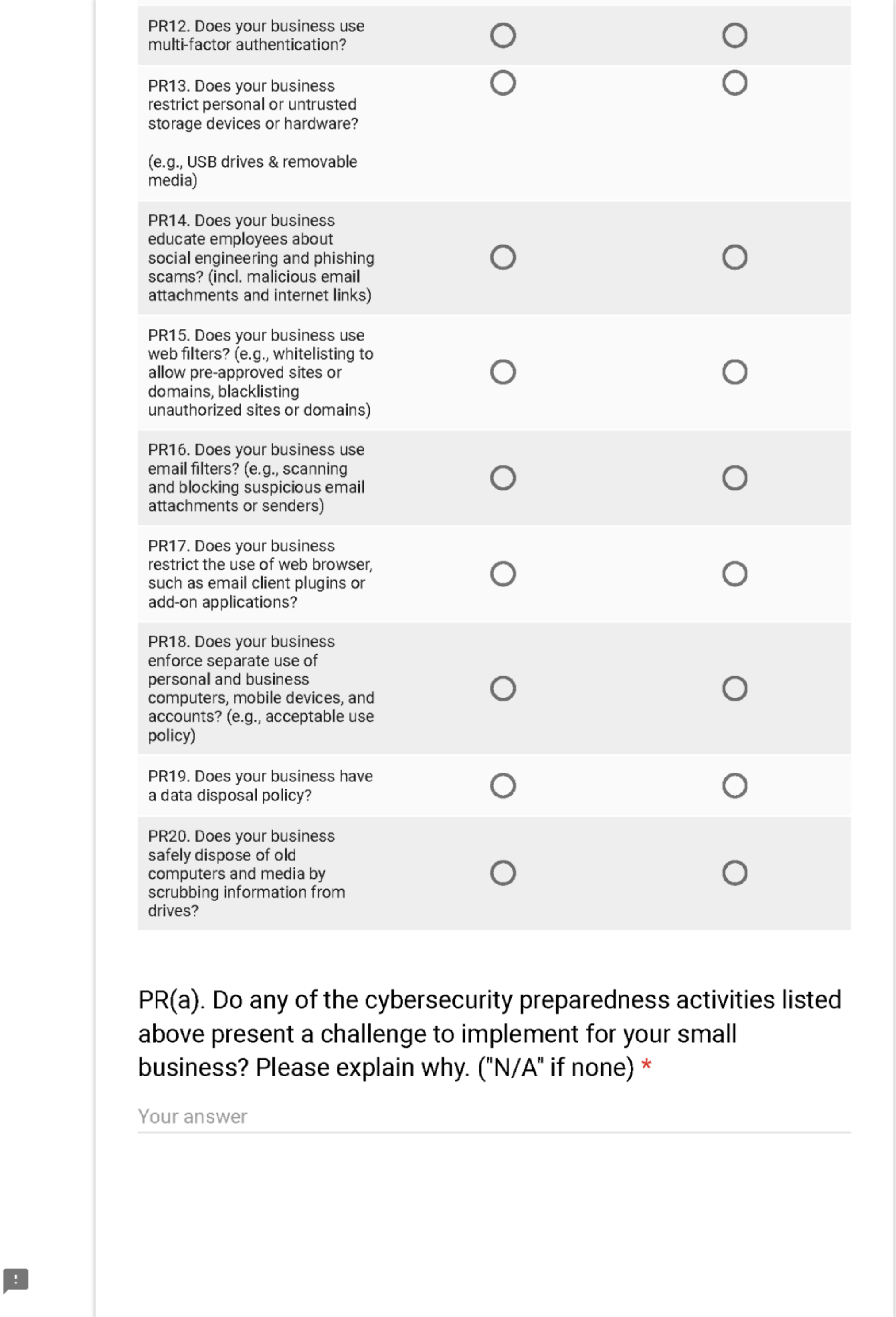
ID(a). Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. ("N/A" if none) *

Your answer



Protect (PR) - the protect function supports the ability to limit or contain the impact of cybersecurity events *

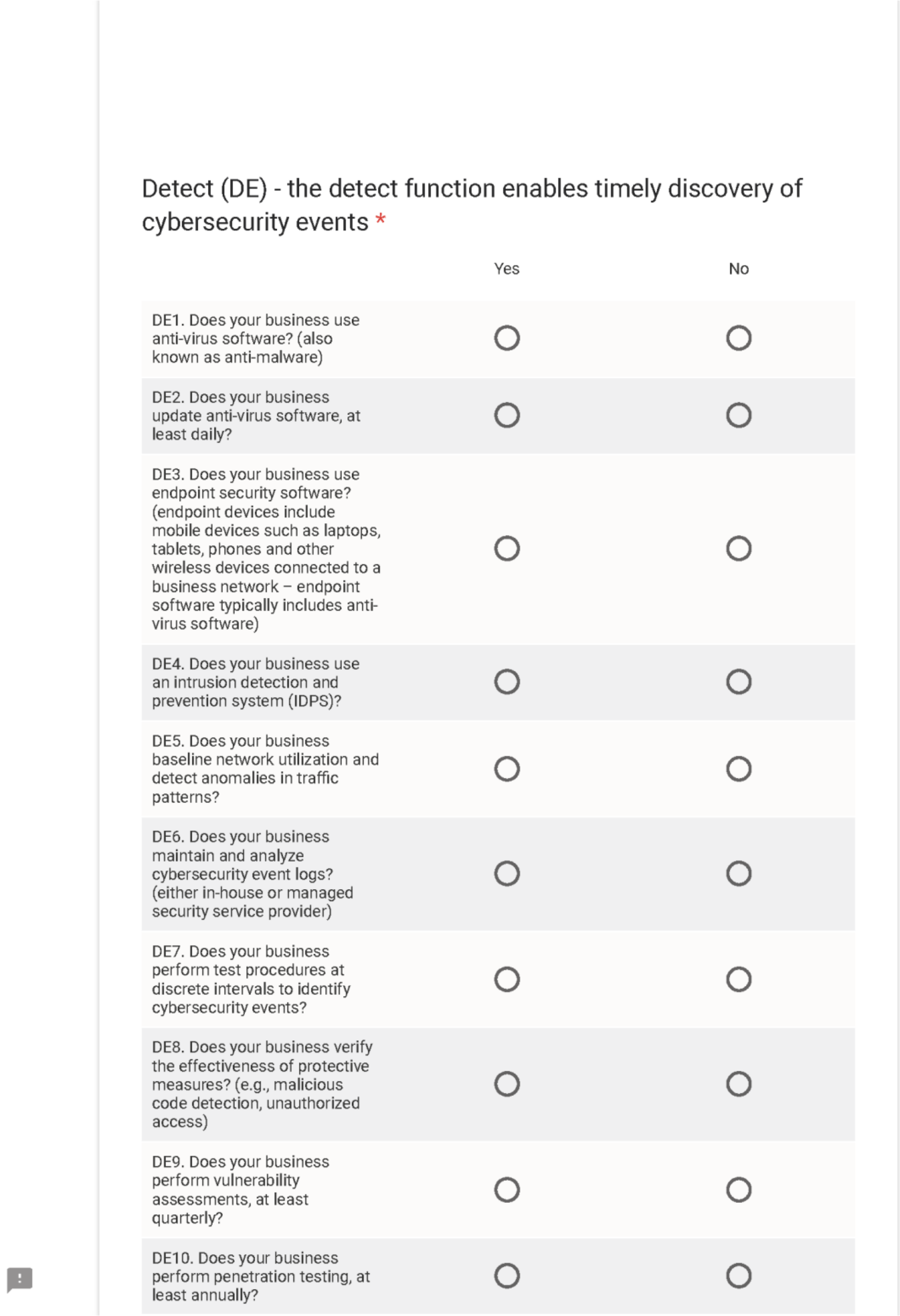
	Yes	No
PR1. Does your business regularly patch your operating systems and applications, at least monthly?	○	○
PR2. Does your business use software and/or hardware firewalls?	○	○
PR3. Does your business have a privacy policy?	○	○
PR4. Does your business have an insider threat management program?	○	○
PR5. Does your business use encryption for sensitive information?	○	○
PR6. Does your business limit employee access to data and information through access controls? (principle of least privilege)	○	○
PR7. Does your business control the use of administrative privileges? (e.g., only use administrative accounts when they are required)	○	○
PR8. Does your business restrict downloading and installing software by non-administrators?	○	○
PR9. Does your business disable access when an employee leaves the business?	○	○
PR10. Does your business protect information assets from physical intrusion?	○	○
PR11. Does your business enforce password management? (e.g., password policy with strong passwords, expirations, changing all default administrative passwords)	○	○



PR12. Does your business use multi-factor authentication?	○	○
PR13. Does your business restrict personal or untrusted storage devices or hardware? (e.g., USB drives & removable media)	○	○
PR14. Does your business educate employees about social engineering and phishing scams? (incl. malicious email attachments and internet links)	○	○
PR15. Does your business use web filters? (e.g., whitelisting to allow pre-approved sites or domains, blacklisting unauthorized sites or domains)	○	○
PR16. Does your business use email filters? (e.g., scanning and blocking suspicious email attachments or senders)	○	○
PR17. Does your business restrict the use of web browser, such as email client plugins or add-on applications?	○	○
PR18. Does your business enforce separate use of personal and business computers, mobile devices, and accounts? (e.g., acceptable use policy)	○	○
PR19. Does your business have a data disposal policy?	○	○
PR20. Does your business safely dispose of old computers and media by scrubbing information from drives?	○	○

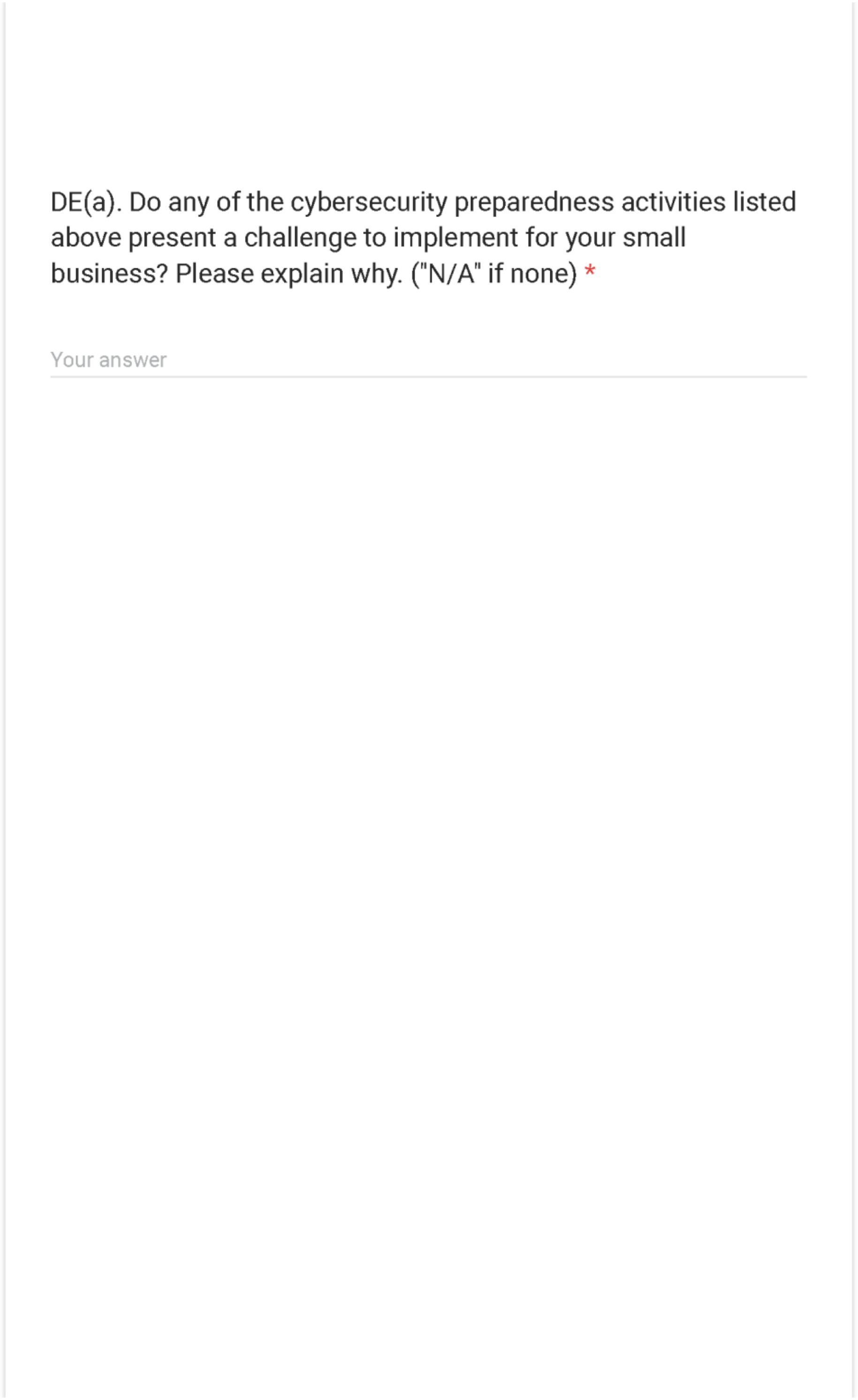
PR(a). Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. ("N/A" if none) *

Your answer



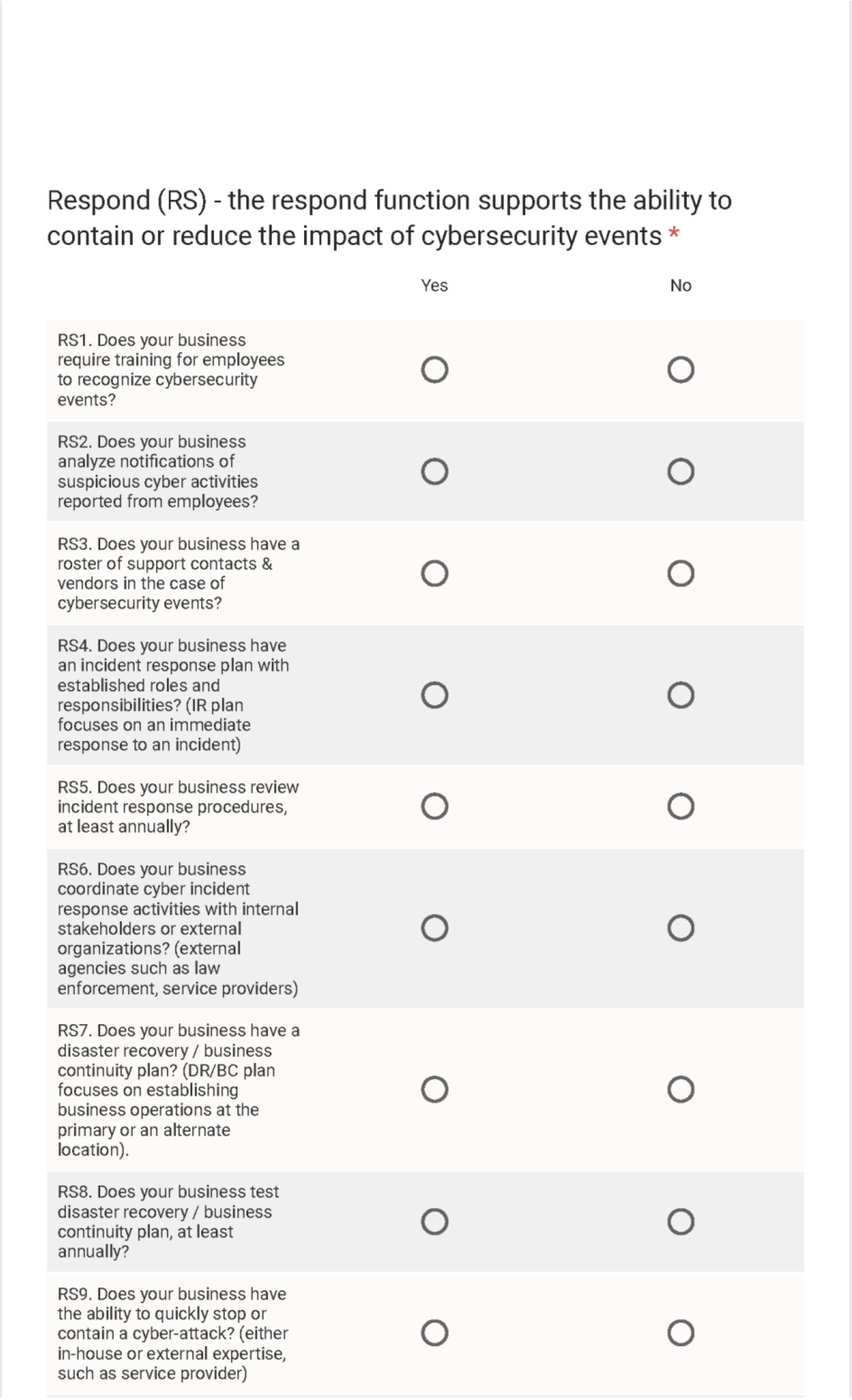
Detect (DE) - the detect function enables timely discovery of cybersecurity events *

	Yes	No
DE1. Does your business use anti-virus software? (also known as anti-malware)	○	○
DE2. Does your business update anti-virus software, at least daily?	○	○
DE3. Does your business use endpoint security software? (endpoint devices include mobile devices such as laptops, tablets, phones and other wireless devices connected to a business network – endpoint software typically includes anti-virus software)	○	○
DE4. Does your business use an intrusion detection and prevention system (IDPS)?	○	○
DE5. Does your business baseline network utilization and detect anomalies in traffic patterns?	○	○
DE6. Does your business maintain and analyze cybersecurity event logs? (either in-house or managed security service provider)	○	○
DE7. Does your business perform test procedures at discrete intervals to identify cybersecurity events?	○	○
DE8. Does your business verify the effectiveness of protective measures? (e.g., malicious code detection, unauthorized access)	○	○
DE9. Does your business perform vulnerability assessments, at least quarterly?	○	○
DE10. Does your business perform penetration testing, at least annually?	○	○



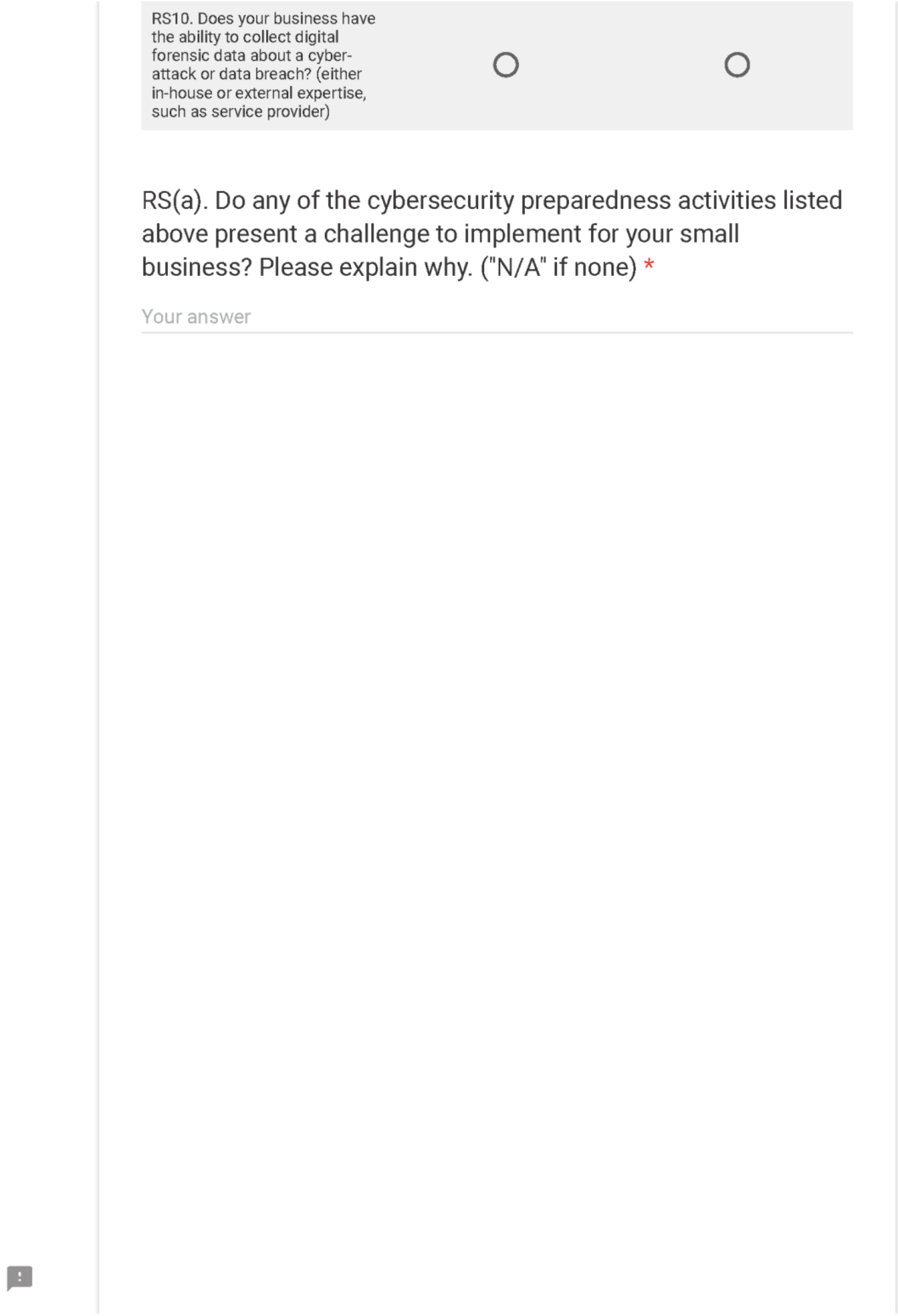
DE(a). Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. ("N/A" if none) *

Your answer



Respond (RS) - the respond function supports the ability to contain or reduce the impact of cybersecurity events *

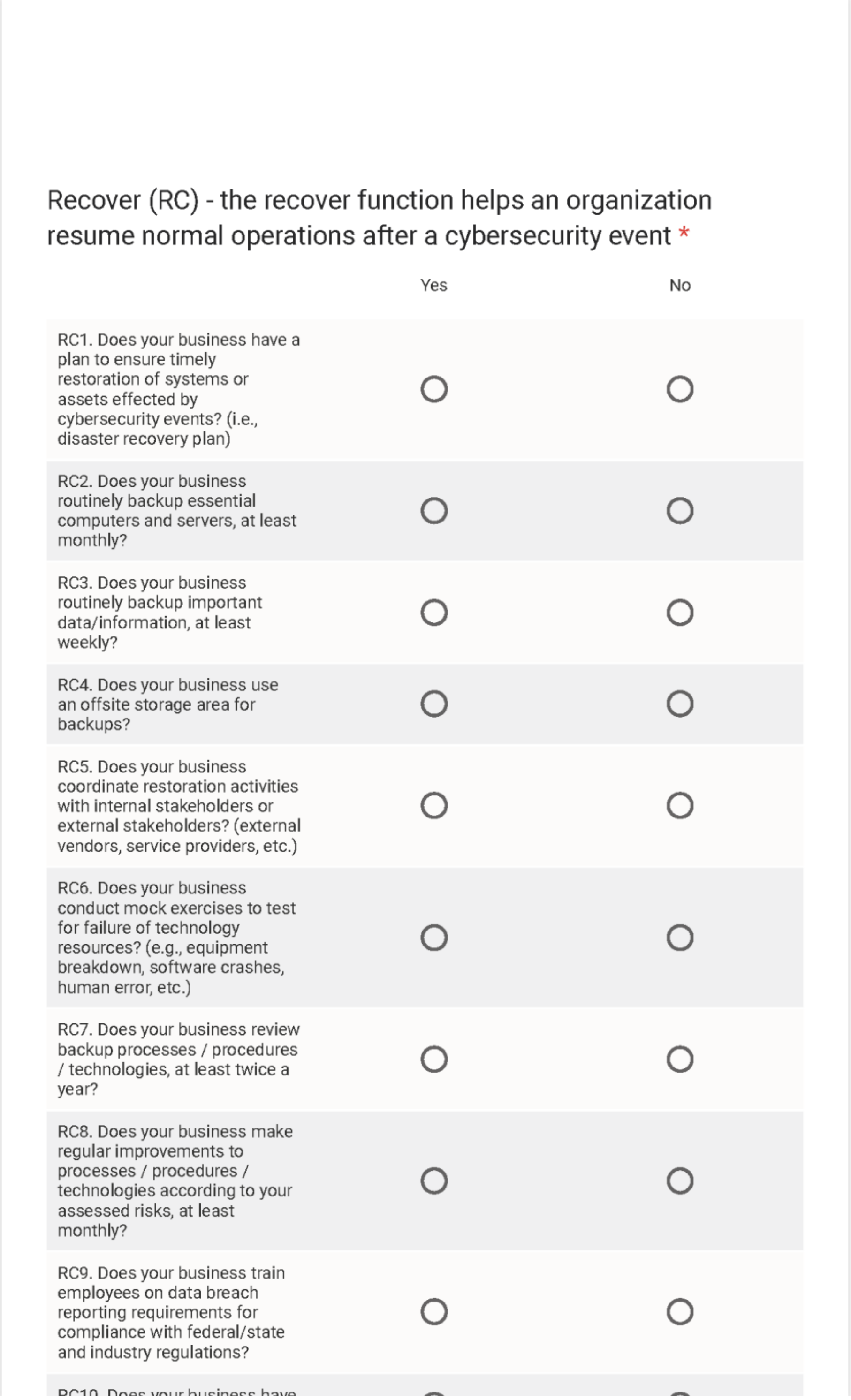
	Yes	No
RS1. Does your business require training for employees to recognize cybersecurity events?	○	○
RS2. Does your business analyze notifications of suspicious cyber activities reported from employees?	○	○
RS3. Does your business have a roster of support contacts & vendors in the case of cybersecurity events?	○	○
RS4. Does your business have an incident response plan with established roles and responsibilities? (IR plan focuses on an immediate response to an incident)	○	○
RS5. Does your business review incident response procedures, at least annually?	○	○
RS6. Does your business coordinate cyber incident response activities with internal stakeholders or external organizations? (external agencies such as law enforcement, service providers)	○	○
RS7. Does your business have a disaster recovery / business continuity plan? (DR/BC plan focuses on establishing business operations at the primary or an alternate location).	○	○
RS8. Does your business test disaster recovery / business continuity plan, at least annually?	○	○
RS9. Does your business have the ability to quickly stop or contain a cyber-attack? (either in-house or external expertise, such as service provider)	○	○



RS10. Does your business have the ability to collect digital forensic data about a cyber-attack or data breach? (either in-house or external expertise, such as service provider)	○	○

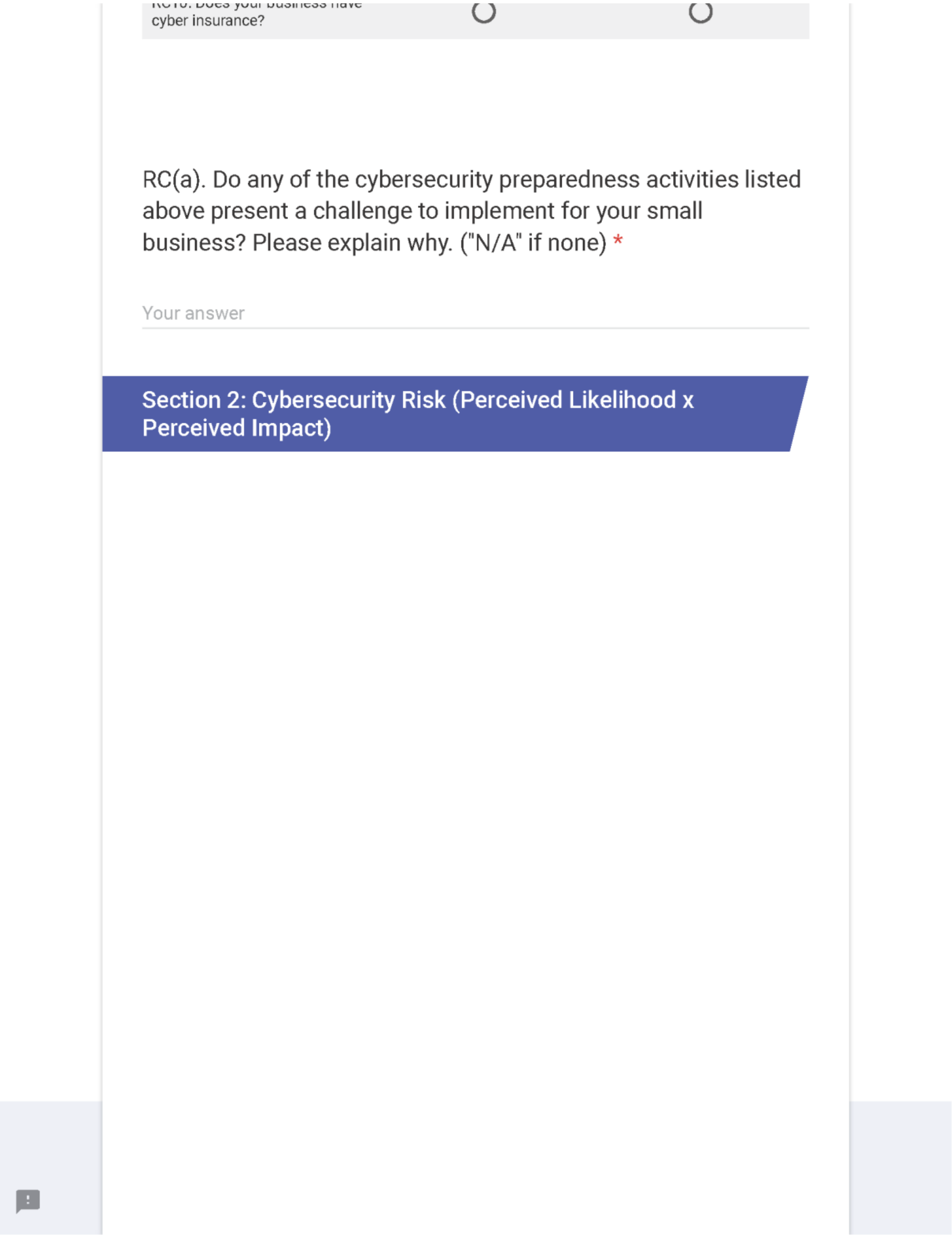
RS(a). Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. ("N/A" if none) *

Your answer



Recover (RC) - the recover function helps an organization resume normal operations after a cybersecurity event *

	Yes	No
RC1. Does your business have a plan to ensure timely restoration of systems or assets effected by cybersecurity events? (i.e., disaster recovery plan)	○	○
RC2. Does your business routinely backup essential computers and servers, at least monthly?	○	○
RC3. Does your business routinely backup important data/information, at least weekly?	○	○
RC4. Does your business use an offsite storage area for backups?	○	○
RC5. Does your business coordinate restoration activities with internal stakeholders or external stakeholders? (external vendors, service providers, etc.)	○	○
RC6. Does your business conduct mock exercises to test for failure of technology resources? (e.g., equipment breakdown, software crashes, human error, etc.)	○	○
RC7. Does your business review backup processes / procedures / technologies, at least twice a year?	○	○
RC8. Does your business make regular improvements to processes / procedures / technologies according to your assessed risks, at least monthly?	○	○
RC9. Does your business train employees on data breach reporting requirements for compliance with federal/state and industry regulations?	○	○
RC10. Does your business have	○	○

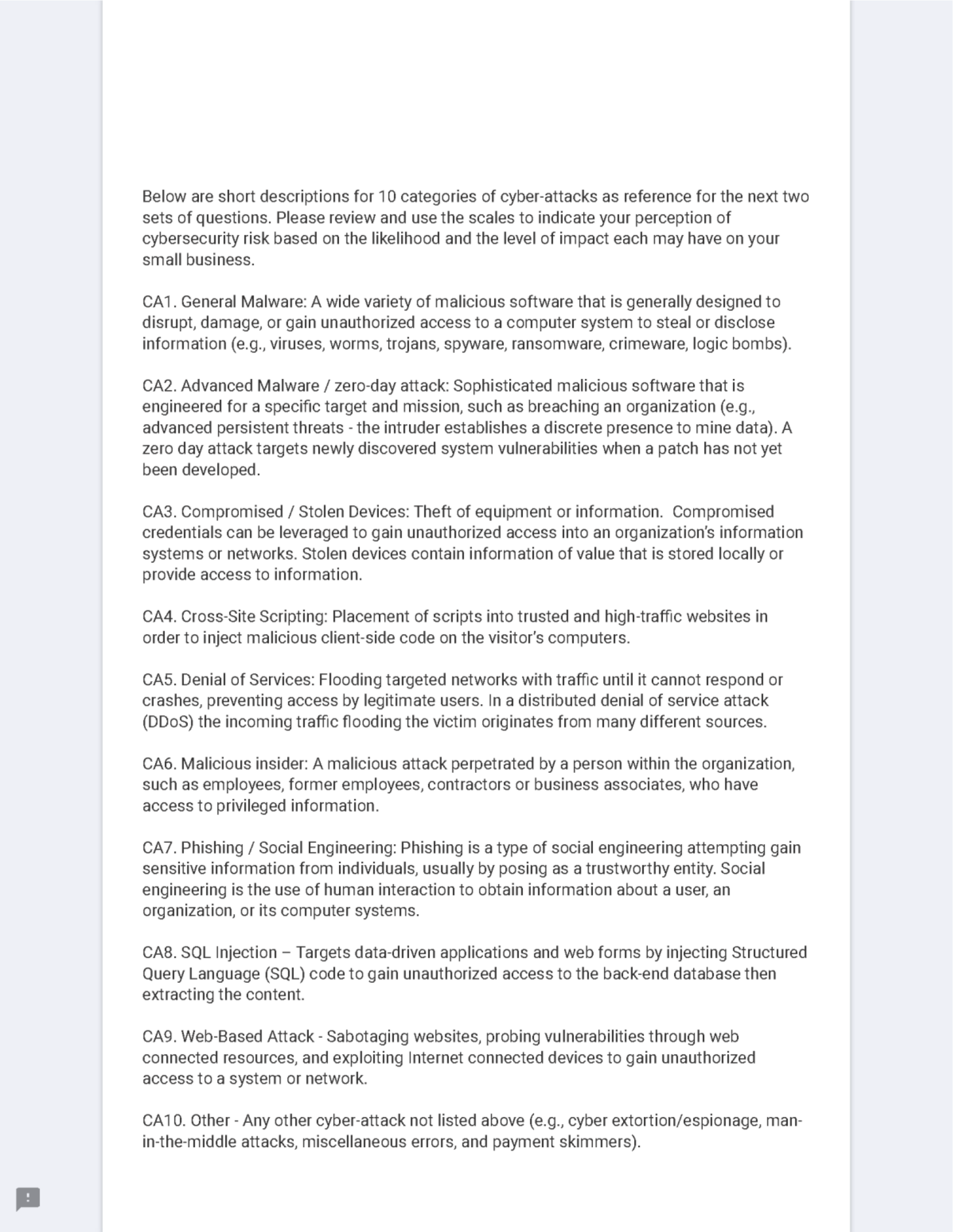


RC10. Does your business have cyber insurance?	○	○

RC(a). Do any of the cybersecurity preparedness activities listed above present a challenge to implement for your small business? Please explain why. ("N/A" if none) *

Your answer

Section 2: Cybersecurity Risk (Perceived Likelihood x Perceived Impact)



Below are short descriptions for 10 categories of cyber-attacks as reference for the next two sets of questions. Please review and use the scales to indicate your perception of cybersecurity risk based on the likelihood and the level of impact each may have on your small business.

CA1. General Malware: A wide variety of malicious software that is generally designed to disrupt, damage, or gain unauthorized access to a computer system to steal or disclose information (e.g., viruses, worms, trojans, spyware, ransomware, crimeware, logic bombs).

CA2. Advanced Malware / zero-day attack: Sophisticated malicious software that is engineered for a specific target and mission, such as breaching an organization (e.g., advanced persistent threats - the intruder establishes a discrete presence to mine data). A zero day attack targets newly discovered system vulnerabilities when a patch has not yet been developed.

CA3. Compromised / Stolen Devices: Theft of equipment or information. Compromised credentials can be leveraged to gain unauthorized access into an organization's information systems or networks. Stolen devices contain information of value that is stored locally or provide access to information.

CA4. Cross-Site Scripting: Placement of scripts into trusted and high-traffic websites in order to inject malicious client-side code on the visitor's computers.

CA5. Denial of Services: Flooding targeted networks with traffic until it cannot respond or crashes, preventing access by legitimate users. In a distributed denial of service attack (DDoS) the incoming traffic flooding the victim originates from many different sources.

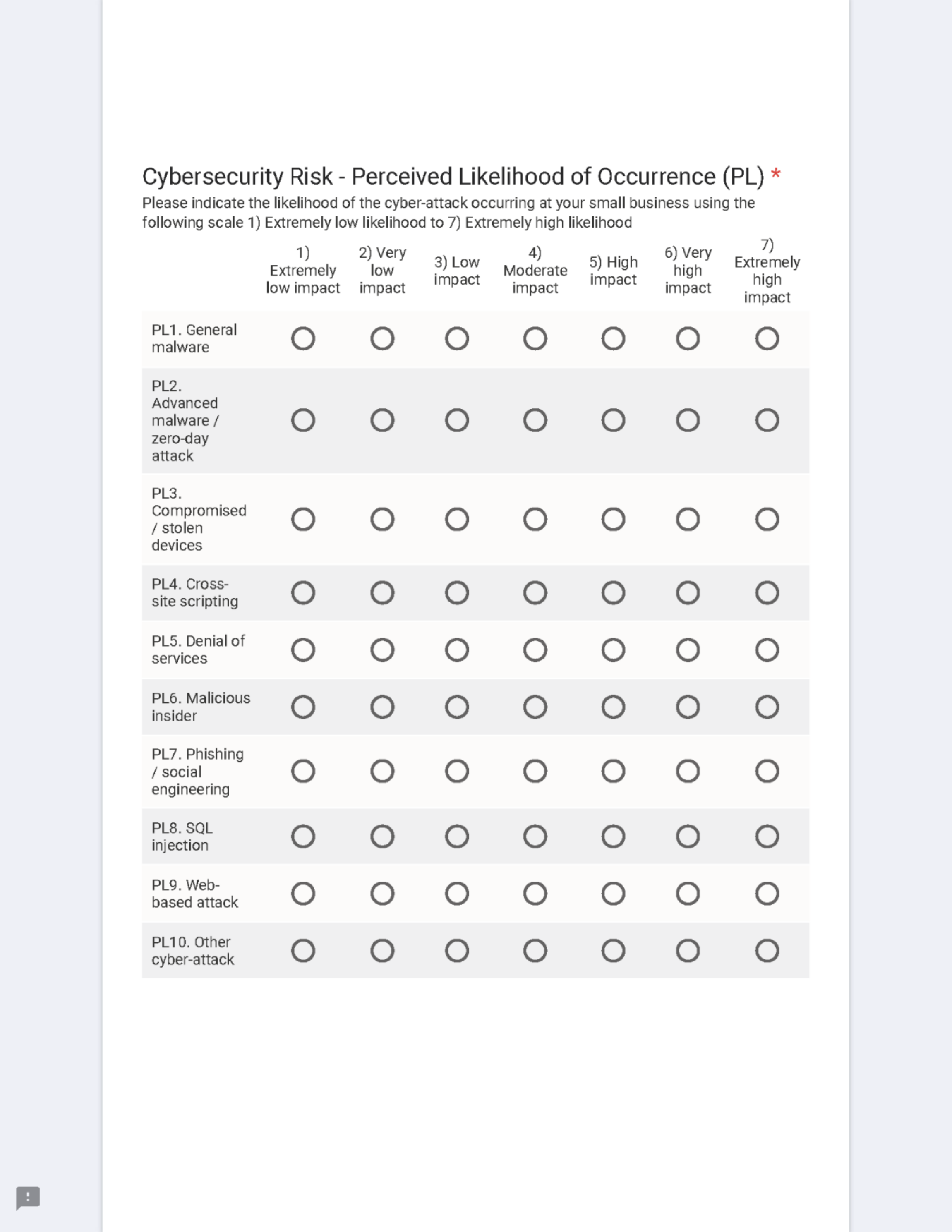
CA6. Malicious insider: A malicious attack perpetrated by a person within the organization, such as employees, former employees, contractors or business associates, who have access to privileged information.

CA7. Phishing / Social Engineering: Phishing is a type of social engineering attempting gain sensitive information from individuals, usually by posing as a trustworthy entity. Social engineering is the use of human interaction to obtain information about a user, an organization, or its computer systems.

CA8. SQL Injection – Targets data-driven applications and web forms by injecting Structured Query Language (SQL) code to gain unauthorized access to the back-end database then extracting the content.

CA9. Web-Based Attack - Sabotaging websites, probing vulnerabilities through web connected resources, and exploiting Internet connected devices to gain unauthorized access to a system or network.

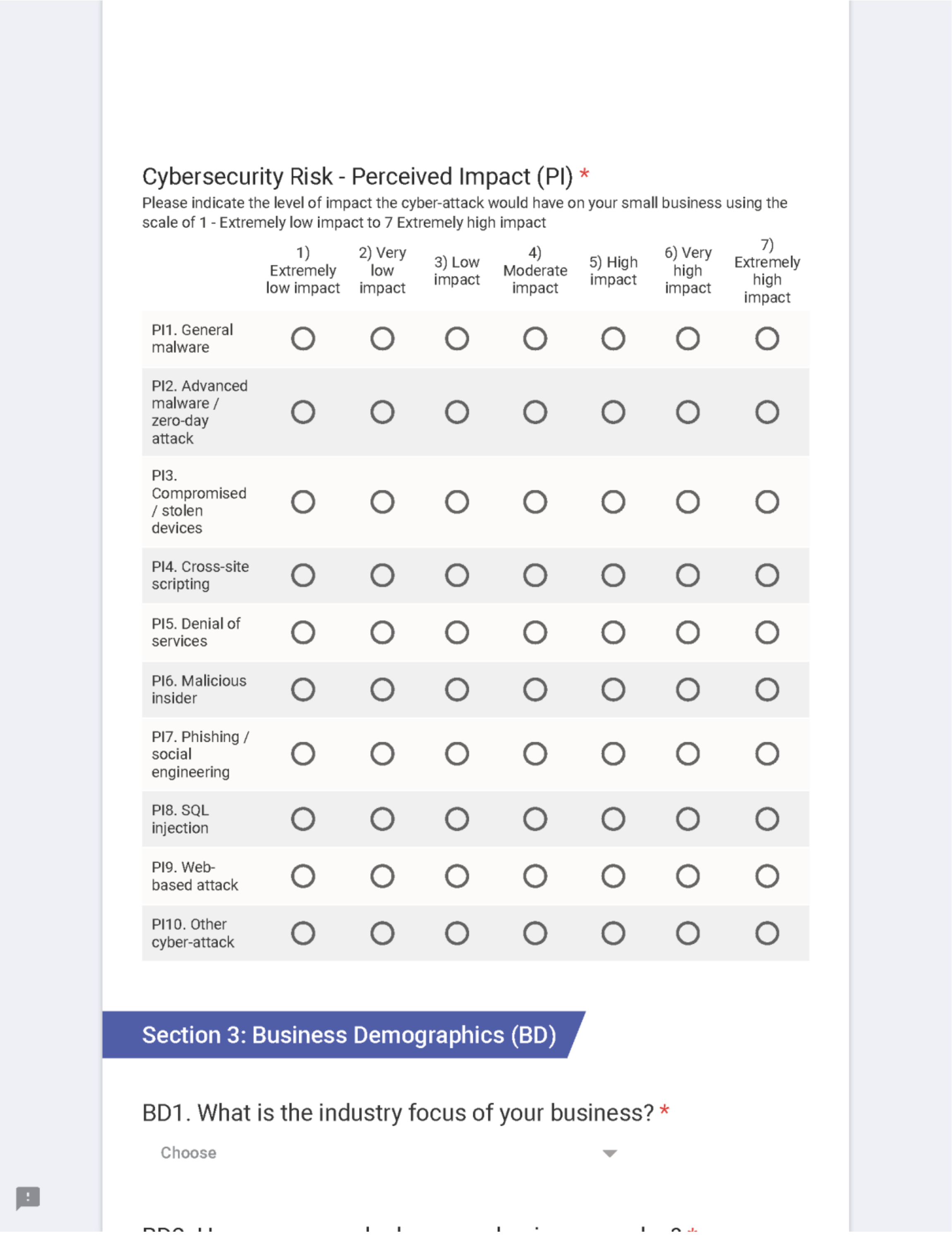
CA10. Other - Any other cyber-attack not listed above (e.g., cyber extortion/espionage, man-in-the-middle attacks, miscellaneous errors, and payment skimmers).



Cybersecurity Risk - Perceived Likelihood of Occurrence (PL) *

Please indicate the likelihood of the cyber-attack occurring at your small business using the following scale 1) Extremely low likelihood to 7) Extremely high likelihood

	1) Extremely low impact	2) Very low impact	3) Low impact	4) Moderate impact	5) High impact	6) Very high impact	7) Extremely high impact
PL1. General malware	○	○	○	○	○	○	○
PL2. Advanced malware / zero-day attack	○	○	○	○	○	○	○
PL3. Compromised / stolen devices	○	○	○	○	○	○	○
PL4. Cross-site scripting	○	○	○	○	○	○	○
PL5. Denial of services	○	○	○	○	○	○	○
PL6. Malicious insider	○	○	○	○	○	○	○
PL7. Phishing / social engineering	○	○	○	○	○	○	○
PL8. SQL injection	○	○	○	○	○	○	○
PL9. Web-based attack	○	○	○	○	○	○	○
PL10. Other cyber-attack	○	○	○	○	○	○	○



Cybersecurity Risk - Perceived Impact (PI) *

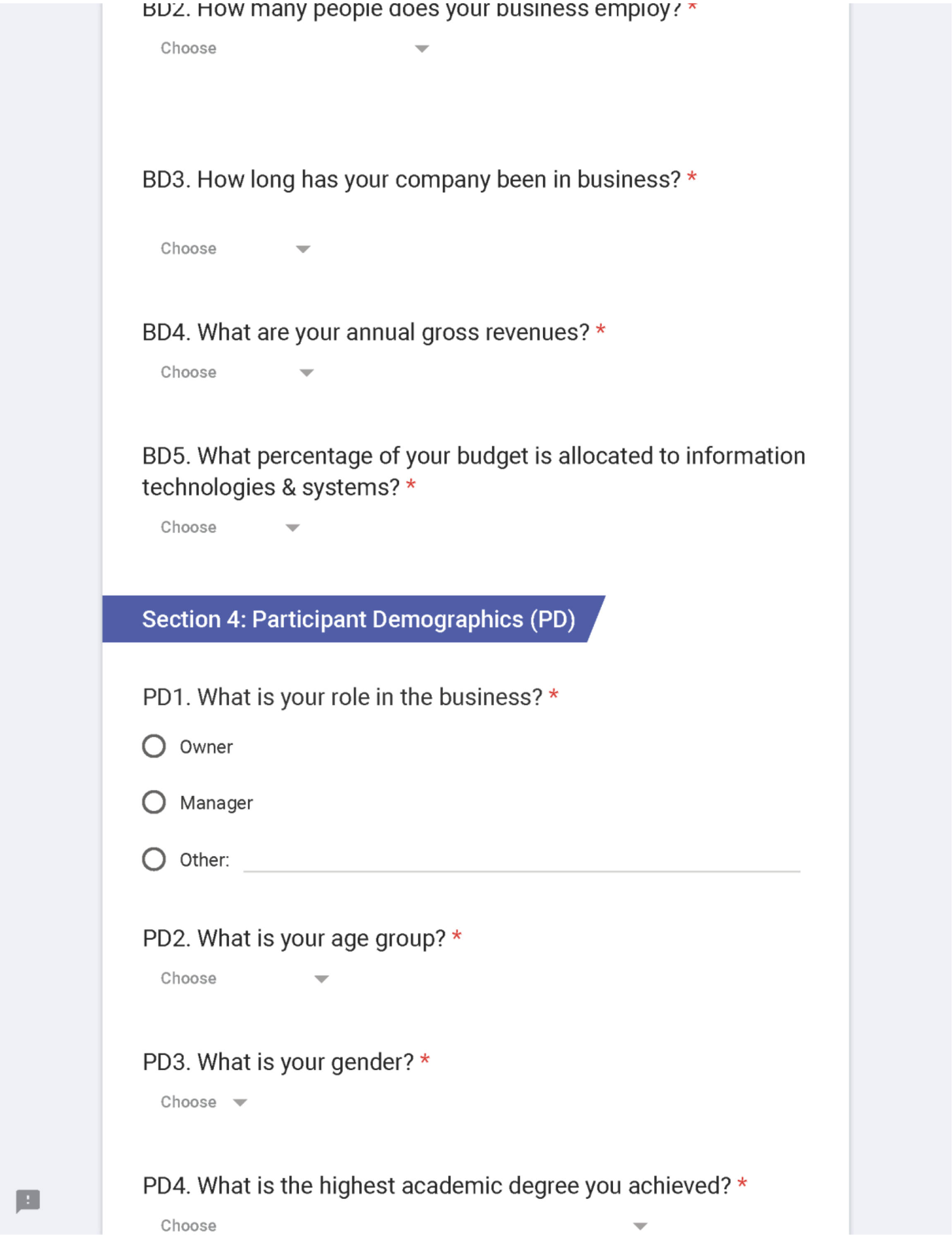
Please indicate the level of impact the cyber-attack would have on your small business using the scale of 1 - Extremely low impact to 7 Extremely high impact

	1) Extremely low impact	2) Very low impact	3) Low impact	4) Moderate impact	5) High impact	6) Very high impact	7) Extremely high impact
PI1. General malware	○	○	○	○	○	○	○
PI2. Advanced malware / zero-day attack	○	○	○	○	○	○	○
PI3. Compromised / stolen devices	○	○	○	○	○	○	○
PI4. Cross-site scripting	○	○	○	○	○	○	○
PI5. Denial of services	○	○	○	○	○	○	○
PI6. Malicious insider	○	○	○	○	○	○	○
PI7. Phishing / social engineering	○	○	○	○	○	○	○
PI8. SQL injection	○	○	○	○	○	○	○
PI9. Web-based attack	○	○	○	○	○	○	○
PI10. Other cyber-attack	○	○	○	○	○	○	○

Section 3: Business Demographics (BD)

BD1. What is the industry focus of your business? *

Choose ▾



BD2. How many people does your business employ? *

Choose ▾

BD3. How long has your company been in business? *

Choose ▾

BD4. What are your annual gross revenues? *

Choose ▾

BD5. What percentage of your budget is allocated to information technologies & systems? *

Choose ▾

Section 4: Participant Demographics (PD)

PD1. What is your role in the business? *

○ Owner

○ Manager

○ Other: ______________________________

PD2. What is your age group? *

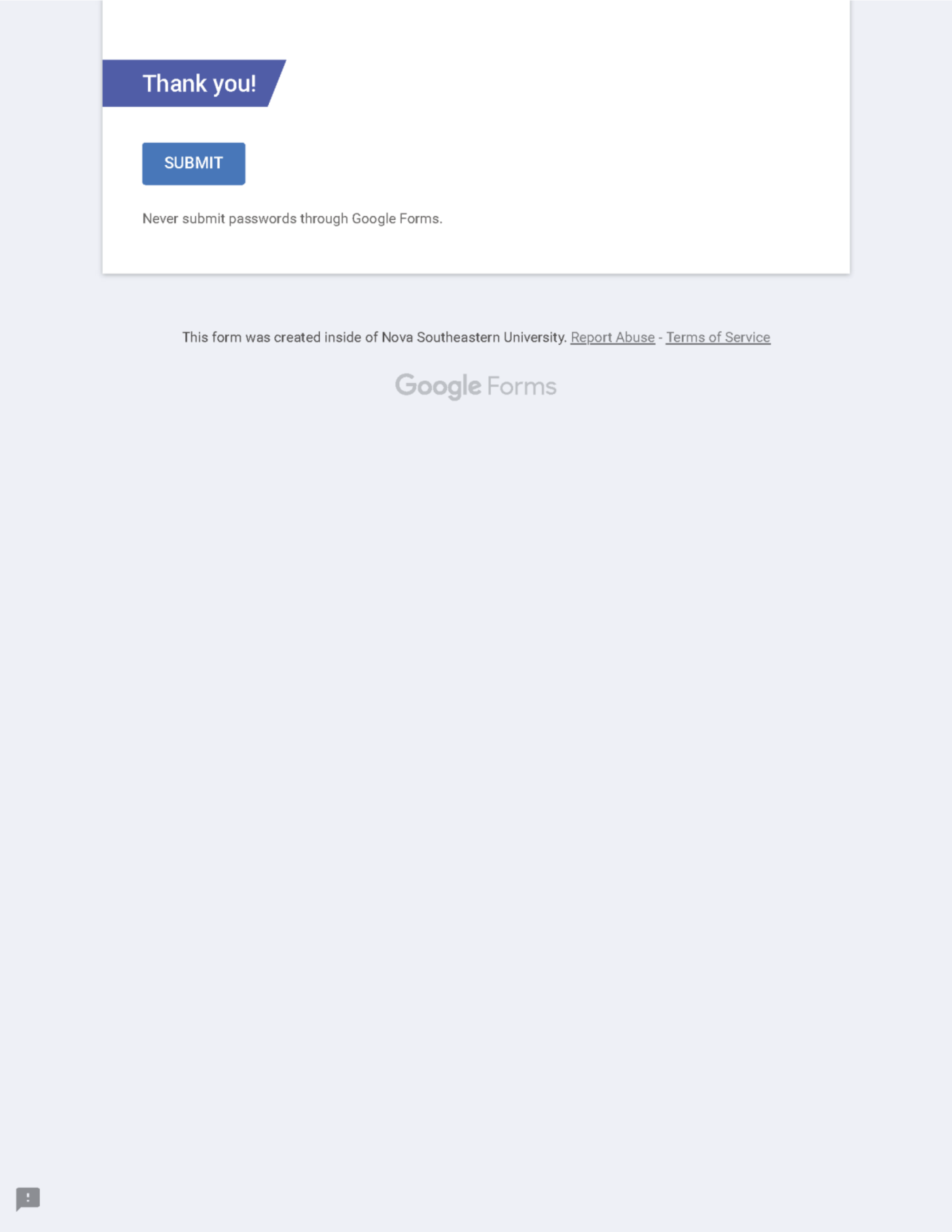
Choose ▾

PD3. What is your gender? *

Choose ▾

PD4. What is the highest academic degree you achieved? *

Choose ▾



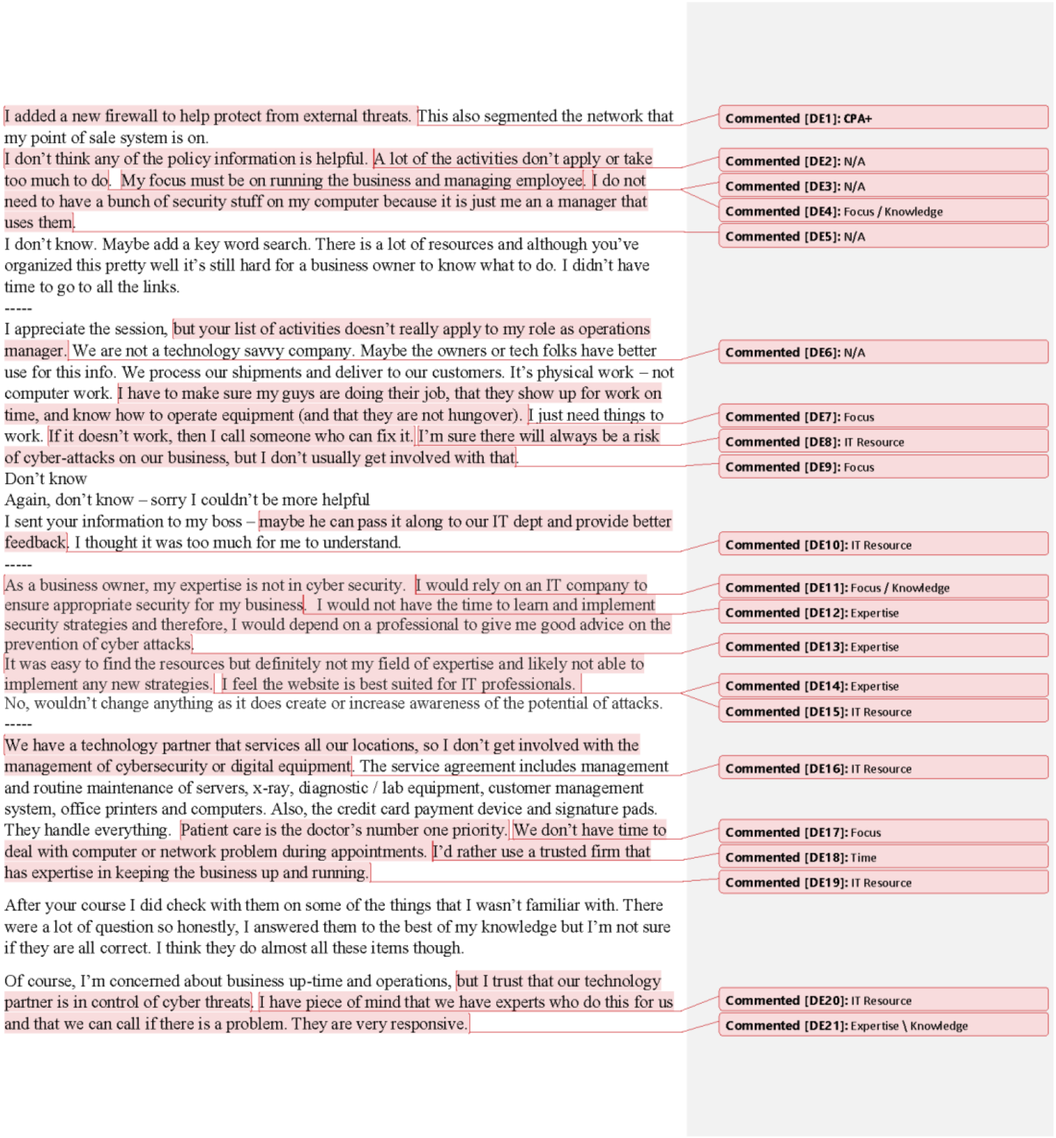
Thank you!

Never submit passwords through Google Forms.

This form was created inside of Nova Southeastern University. Report Abuse - Terms of Service

Appendix L

Phase 3 Qualitative Analysis (Manual Coding)



I added a new firewall to help protect from external threats. This also segmented the network that my point of sale system is on.

Commented [DE1]: **CPA+**

I don't think any of the policy information is helpful. A lot of the activities don't apply or take too much to do. My focus must be on running the business and managing employee. I do not need to have a bunch of security stuff on my computer because it is just me an a manager that uses them.

Commented [DE2]: N/A

Commented [DE3]: N/A

Commented [DE4]: Focus / Knowledge

Commented [DE5]: N/A

I don't know. Maybe add a key word search. There is a lot of resources and although you've organized this pretty well it's still hard for a business owner to know what to do. I didn't have time to go to all the links.

I appreciate the session, but your list of activities doesn't really apply to my role as operations manager. We are not a technology savvy company. Maybe the owners or tech folks have better use for this info. We process our shipments and deliver to our customers. It's physical work – not computer work. I have to make sure my guys are doing their job, that they show up for work on time, and know how to operate equipment (and that they are not hungover). I just need things to work. If it doesn't work, then I call someone who can fix it. I'm sure there will always be a risk of cyber-attacks on our business, but I don't usually get involved with that.

Commented [DE6]: N/A

Commented [DE7]: Focus

Commented [DE8]: IT Resource

Commented [DE9]: Focus

Don't know

Again, don't know – sorry I couldn't be more helpful

I sent your information to my boss – maybe he can pass it along to our IT dept and provide better feedback. I thought it was too much for me to understand.

Commented [DE10]: IT Resource

As a business owner, my expertise is not in cyber security. I would rely on an IT company to ensure appropriate security for my business. I would not have the time to learn and implement security strategies and therefore, I would depend on a professional to give me good advice on the prevention of cyber attacks.

Commented [DE11]: Focus / Knowledge

Commented [DE12]: Expertise

Commented [DE13]: Expertise

It was easy to find the resources but definitely not my field of expertise and likely not able to implement any new strategies. I feel the website is best suited for IT professionals.

Commented [DE14]: Expertise

Commented [DE15]: IT Resource

No, wouldn't change anything as it does create or increase awareness of the potential of attacks.

We have a technology partner that services all our locations, so I don't get involved with the management of cybersecurity or digital equipment. The service agreement includes management and routine maintenance of servers, x-ray, diagnostic / lab equipment, customer management system, office printers and computers. Also, the credit card payment device and signature pads. They handle everything. Patient care is the doctor's number one priority. We don't have time to deal with computer or network problem during appointments. I'd rather use a trusted firm that has expertise in keeping the business up and running.

Commented [DE16]: IT Resource

Commented [DE17]: Focus

Commented [DE18]: Time

Commented [DE19]: IT Resource

After your course I did check with them on some of the things that I wasn't familiar with. There were a lot of question so honestly, I answered them to the best of my knowledge but I'm not sure if they are all correct. I think they do almost all these items though.

Of course, I'm concerned about business up-time and operations, but I trust that our technology partner is in control of cyber threats. I have piece of mind that we have experts who do this for us and that we can call if there is a problem. They are very responsive.

Commented [DE20]: IT Resource

Commented [DE21]: Expertise \ Knowledge

I don't think I would change anything. I think the information is targeted for business owners that are more hands-on, DYI.

For my business we run our banking and accounting systems on dedicated computers. I don't do anything else on these and there is no reason for my employees to use our computers. We email and text a lot, and because my name & email is open to the public, I get a lot of spam. I've learned to be very diligent in what I open. I probably delete messages that could have been good business leads, but I don't get a virus. I don't know that I need to backup because all my email is on gmail. I use a strong password and don't give it to anyone. I don't need to follow a formal approach of managing our security. The framework doesn't apply to me – it too complex I appreciate the training, but I didn't check all the links. It was too much for my small business. Although It looks like it could be useful for other companies.

Commented [DE22]: N/A

Commented [DE23]: Knowledge

Commented [DE24]: N/A

Commented [DE25]: Complexity

Commented [DE26]: N/A

I don't think any of the policy information is helpful. A lot of the activities don't apply or take too much to do. My focus must be on running the business and managing employee. I do not need to have a bunch of security stuff on my computer because it is just me an a manager that uses them.

Commented [DE27]: N/A

Commented [DE28]: N/A

Commented [DE29]: N/A

Commented [DE30]: Focus

I don't know. Maybe add a key word search. There is a lot of resources and although you've organized this pretty well it's still hard for a business owner to know what to do. I didn't have time to go to all the links.

The funny thing is that we work in support of the technology space for [top companies] as project consultants, but we honestly don't do a very good job of protecting ourselves from cyber threats. We work onsite – our customers have their own governance and controls. I know we need to mature as a company and do a better job. The information you provided was helpful, but I don't have the time and to dedicate our systems because we focus on providing value to our customers. Sure, we are just getting started. I know at some point I'll have to hire some experts to put controls in place. But, right now, we are working on business development. We all work and communicate on our own personal machines that I make sure we have anti-virus and basic security, but we do not have a central office and infrastructure, so all the overhead is not really necessary.

Commented [DE31]: Time

Commented [DE32]: Expertise \ Knowledge

Commented [DE33]: CPA+

Commented [DE34]: N/A

Our challenge is growing the business – not really setting up security procedures.

Commented [DE35]: Focus

They were all very basic. It can be a good checklist to follow but I think there needs to be more information on how to conduct vulnerability assessment and costs analysis. Equipment can be replaced easily, and we do most of our work in the online.

Commented [DE36]: Expertise \ Knowledge

Commented [DE37]: Cloud

There needs to be more of a cloud focus. Not all of your preparedness activities apply to small companies. Like firewall. I connect to the internet from various locations, so why do I need a firewall. I think your activities assume a physical location.

Commented [DE38]: N/A

You provided good advice and I can see how some of these activities can improve security for businesses. However, I am mainly focused on day-to-day business operations. I cannot be an expert of every computer technology that we use for our business and I don't have the time to learn every type of cyberattack. Most of our computers and software have support services that we can contact. Sure, we certainly can make some improvements in security, but I really have not had any time to change anything that we are doing in the last month.

I don't know that any of them are challenging or maybe all of them. Again, I'm focused on running the business. I think there are way too many activities that I didn't have time to work on upgrading our computers. My website is hosted by someone else so it's on them. Otherwise, if something happens to my computers then we'll deal with it, but I spend more than 10 hours a day on running the business. I'm generating sales, processing orders, making repairs, on the road to service my clients, and directing my staff, etc.

Not that I can tell, but I didn't look at all of them. Most of the links were to articles that were way over my head.

I think your website should focus on providing links to small business service providers. I have used best buy for computer repairs, but they are not that good. Most of the time I don't know who to contact for an issue and if they are reputable. I ask for recommendation from my staff or from family and friends.

I started limiting access to files by updating permission to shared folders. I also update our password rules. There were things that I could easily take care of myself. I don't know how to do many of these things but I'm going to talk to Jeff. He is normally the one who takes care of all the technical matters. I also shared some information so that I can start training my team on some of the threats like phishing and ransomware.

I think the detect and recover are most challenging. I really don't understand what is needed for these so I will have to see we can do. These two seem require more technical expertise.

There are good resources but some of them that I looked at had more information that I was looking for – it wasn't always specific to the topic.

It would be nice if there were videos on how to do some of this stuff. I think it would be easier to understand. I'll keep looking at it and let you know if I have questions – I'm sure that I will

-----

Our IT Mgr. handles all of the network and office equipment but I'm happy to answer any questions that I can. Your presentation was good, and it definitely raised my awareness of cyber-attacks. Generally, we follow normal practices but I'm not sure how well we follow the NIST. We protect what we can as best we can, but I know we are never going to be 100% secure. We don't need to constantly detect all the threats. We have a lot of equipment, but client information

Commented [DE39]: Focus

Commented [DE40]: Expertise \ Knowledge

Commented [DE41]: IT Resources

Commented [DE42]: Time

Commented [DE43]: Focus

Commented [DE44]: Time

Commented [DE45]: IT Resources

Commented [DE46]: Focus

Commented [DE47]: Focus

Commented [DE48]: Expertise \ Knowledge

Commented [DE49]: IT Resources

Commented [DE50]: Knowledge

Commented [DE51]: Trust

Commented [DE52]: **CPA+**

Commented [DE53]: **CPA+**

Commented [DE54]: Knowledge

Commented [DE55]: IT Resource

Commented [DE56]: **CPA+**

Commented [DE57]: knowledge

Commented [DE58]: Expertise

Commented [DE59]: N/A

Commented [DE60]: Knowledge

Commented [DE61]: IT Resource

Commented [DE62]: **DMPRCA+**

Commented [DE63]: Doubt

Commented [DE64]: N/A

is protected on a few systems. We some of the best anti-virus security, My manager informed me that we update these every day. Also, he told me that we recently upgraded to a unified threat management system. Don't ask me to explain what that is but it sounds like we are taking our security seriously. Your information did help me to have better conversation about some of the things we do and don't do.

I'm not sure which ones are a challenge. I guess I'd have to say the Detect function because we don't have the time or resources to constantly monitor our systems. Most of our equipment has service contracts so if we run into a problem, we'll call their support (for example PACS Imaging).

The resources were not something that I know much about. I'd have to defer you to my technology manager.

Same

--

We specialize in repair of cryogenic tanks and trailers. Most of our work is mechanical fabrication, welding and inspections. I don't have too many computers around the shop. In the front office we have a couple systems that I use as well as my general manager. I have those computers well locked down. We are not that sophisticated, computers are just used for basic work tasks like taking orders, printing reports/certification, invoicing and delivery. I tried putting together a risk plan but I think we are too small of a company, with few people who use the computers, to do anything formally. We hired a company to setup our computers and network. If we have problems, then we will call them to troubleshoot. We would like to do a better job with managing cyber risk but it's hard to keep up with all that.

[referring to the list] I think in Identify, knowing what to do (prioritizing) is the most challenging. In Protect, we don't educate the employee because they don't use the computers. I guess we could educate ourselves better on phishing scams. Detect, we don't analyze traffic patterns or event logs – that would take to much time. For Respond, I don't see any reason why we'd try to coordinate with local police or collect forensic data. We are not some high-tech, high value company. I was a little confused by some of the questions. And for Recover, the most challenging would be same thing – don't see a need to coordinate recovery with external agencies or buy cyber insurance.

I started looking at some of the resources, but it was information overload. I may use them if I'm trying to figure out how to solve a specific problem but otherwise, I wouldn't have time to read through them all.

No sir, nothing I can think of. It was a good – helped me understand that criminal are targeting small companies so I'll more careful with our emails.

Commented [DE65]:

Commented [DE66]: IT Resource

Commented [DE67]: **CPA+**

Commented [DE68]: **CPA+**

Commented [DE69]: **CPA+**

Commented [DE70]: CPA-

Commented [DE71]: IT Resource

Commented [DE72]: **CPA+**

Commented [DE73]: **CPA+**

Commented [DE74]: N/A

Commented [DE75]: Complexity

Commented [DE76]: IT Resource

Commented [DE77]: **CPA+**

Commented [DE78]: Expertise

Commented [DE79]: Knowledge - Expertise

Commented [DE80]: N/A

Commented [DE81]: **CPA+**

Commented [DE82]: Time

Commented [DE83]: N/A

Commented [DE84]: Knowledge

Commented [DE85]: Knowledge

Commented [DE86]: N/A

Commented [DE87]: **CPA+**

Commented [DE88]: Time

Commented [DE89]: **CPA+**

When I filled out the survey, I didn't know what was really applied to my business, since our IT team handles this stuff, I don't know if I skewed your results?

Commented [DE90]: Knowledge

Commented [DE91]: IT Resource

I don't feel I have challenges with cyber security.

I didn't find the resources difficult to follow.

I don't have any suggestions for improvement. Sorry I can't be of more help.

As you know I mostly work on the database and application development. You raised my awareness of security attacks of small business. I did recommend to our team that we start using the NIST framework but I'm not sure that we need to follow a formal process. It's been a long time since we did a full risk analysis. I mean of course we administer our accounts and protect the systems but we typically don't asses our own vulnerabilities outside of the development. For example. I'll make sure that my apps are not exposed to sql injection by using validation scripts – I don't have many open input fields but if I use them then I will not allow SQL syntax like select or update statements. The rest is a responsibility of the administrators for the client. I think we already have pretty good protection from phishing and malware in house so not much changed there. We just need to figure out how we can work within our development lifecycle to provide better security. That is not usually our most important concern. We look at requirements then design and build what has been requested. Although we do protect our intellectual property. Access to our code is limited to just our Dev team.

Commented [DE92]: **CPA+**

Commented [DE93]: N/A

Commented [DE94]: Complexity

Commented [DE95]: CPA-

Commented [DE96]: **CPA+**

Commented [DE97]: IT Resource

Commented [DE98]: N/A

Commented [DE99]: **CPA+**

Commented [DE100]: Focus

Commented [DE101]: **CPA+**

For Identify, I'd say assessing likelihood of vulnerabilities and costs.

Commented [DE102]: Cost

For Protect, I'd say protection of personal devices because its hard to control what others own

Commented [DE103]: CPA-

Commented [DE104]: Control

For Detect, I think IDPS. I'm not sure if a small business would know what that is. Also, most of our stuff if cloud based.

Commented [DE105]: Knowledge

Commented [DE106]: IT Resource

Commented [DE107]: Cloud

For Respond, I'd say training. We have some canned training package, but it is very basic. I don't find it very useful. It's really a check in the box to say that we have satisfied our security training.

Commented [DE108]: CPA-

For Recover, testing we do backups but don't really to mock exercises to recover our systems. It's mostly cloud environment, so we have our provider do this through their controls.

Commented [DE109]: **CPA+**

Commented [DE110]: IT Resource

No, it's organized and easy to follow. I didn't check every link though.

I'd add a search option. That way if I'm looking up how to do something specifically. Also, I don't think I'd have that many resources listed. You are going to get broken links after a while.

I answered the survey questions as best I could, but I don't know if it was all right.

Well to be honest all of it is very difficult for the average small business owner to even understand. We are not computer savvy in any way. We rely solely on our local IT guy. We have our own server here. We are always worried about the possibility of some sort of cyber security happening. This is one of the reasons we don't do any online banking, automatic withdrawals, direct deposit, etc. We have some machinery in our packing shed that can be hooked into our network for trouble shooting, updating, and programming. We don't hook it up until we need to be online. I know this is probably not the answer you were looking for but this is what I have for now. The simple answer to all this is we don't have a clue on any part of it. I guess sometimes we don't worry too much until it happens. The possibility of some sort of issue is why we have been reluctant to do anything more then what we have to.

Commented [DE111]: Knowledge

Commented [DE112]: Expertise

Commented [DE113]: IT Resource

Commented [DE114]: DMPRCA+

Commented [DE115]: DMPRCA+

Commented [DE116]: CPA+

Commented [DE117]: Knowledge

Commented [DE118]: CPA-

Commented [DE119]: CPA-

The site is good. I sent it over to my IT guy

We are a small agency, but our systems are controlled by the realty partner and strictly governed. We don’t have any control of the system. From what I could tell we do most of your activities. I really don’t have much say in what the company does for IT security.

Commented [DE120]: N/A

They made sense but I don’t know which ones would be most challenging for our IT department.

Commented [DE121]: Knowledge

Not really

Looks good – I don’t have any recommendations.

I’m not the cybersecurity professional but our company provides IT consulting for all kinds of businesses. I’m certain everything on your list is done for our clients. I know we follow the NIST CyberSecurity Framework and recommend to our clients. I’ve answered the survey for our company. We do have a dedicated IT department and security consultants. It would look very bad if we were breached – I don’t think we would want to lose a bunch of clients so I know they are at the top of their game.

Commented [DE122]: Experiance

Commented [DE123]: CPA+

Commented [DE124]: IT Resources

No challenges that I know of. We are strictly regulated and have strong level of security for our computers. We do a lot of training on phishing and information privacy and have annual information security training requirements. The protection of clients’ information is very critical. Although I do pay attention to threats, I’m not too worried because we have a good reputation of being a secure company.

Commented [DE125]: Regulatoin/Laws

Commented [DE126]: Training & Guidance

Really great presentation. The website looks good. Nice job and good luck

ID(a)

None

IT does all this

Commented [DE127]: IT Resources

none: we have great security controls

Excellent info, will try using the NIST cybersecurity framework

Commented [DE128]: CPA+

Use a service provider

The Nist is way to complex

Commented [DE129]: CPA-

We have expensive lab equipment. Vendors are responsible for securing their own software

Commented [DE130]: CPA+

Too many questions

Trying to use the NiST framework, will try to allocate budget for Information Security needs

Commented [DE131]: CPA+

Commented [DE132]: CPA+

I don't know what Q2 means

Commented [DE133]: Knowledge

not sure about 17

good to go

Same as before

nothing changed

Could be useful for other companies

Commented [DE134]: N/A

COBIT

PR(a)

IT does all this

Commented [DE135]: IT Resource

none: we have great security

Most of these are part of our normal process

Commented [DE136]: CPA+

We have a techology service

I dont have time

Commented [DE137]: Time

I protect what I can

a privacy policy protect does not protect my business

Commented [DE138]: N/A

Still the same

nothing changed

DE(a)

IT department does all this

Commented [DE139]: IT Resource

I dont have time

Commented [DE140]: Time

I don't think detecting is needed. Will have our IT manager do this

Commented [DE141]: N/A

Commented [DE142]: IT Resource

how do you verify effectiveness

discrete intervals?! How does verify effectiveness differ from test?

Same

nothing changed

RS(a)

IT does it all

Commented [DE143]: IT Resource

same

I dont have time

Commented [DE144]: Time

If there is a problem our IT manager will respond.

Commented [DE145]: IT Resource

I can hire a company to collect forensic data if attacked

Commented [DE146]: IT Resource

Same

nothing changed

RC(a)

IT does all this

I dont have time

Commented [DE147]: Time

If there is a problem our IT manager will recover

Commented [DE148]: IT Resource

what is the difference between essential computers and non-essential computers?

Same

nothing changed

References

Alharthi, S., Levy, Y., Wang, L., & Hur, I. (2019). Employees’ mobile cyberslacking and their commitment to the organization. *Journal of Computer Information Systems*, 1-13. doi: 10.1080/08874417.2019.1571455

Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems, 17*(5), 448-469.

Association for Computing Machinery (ACM), Joint Task Force on Cybersecurity Education. (2017). *Cybersecurity curricula 2017: Curriculum guidelines for post-secondary degree programs in cybersecurity (CSEC2017 v1.0)*. Retrieved from http://cybered.acm.org/

Barberis, N. C. (2013). Thirty years of prospect theory in economics: A review and assessment. *Journal of Economic Perspectives*, *27*(1), 173-196.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems, 17*(4), 37-69.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138-151.

Bazerman, M. H. (1984). The relevance of Kahneman and Tversky's concept of framing to organizational behavior. *Journal of Management*, *10*(3), 333-343.

Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1-10.

Better Business Bureau (BBB). (2017). *State of cybersecurity among small businesses in North America*. Retrieved from https://www.bbb.org/stateofcybersecurity

Bettman, J. R. (1973). Perceived risk and its components: A model and empirical test. *Journal of Marketing Research*, *10*(2), 184-190.

Bhattacharya, D. (2011). Leadership styles and information security in small businesses. *Information Management & Computer Security, 19*(5), 300-312.

Bhattacharya, D. (2015). Evolution of cybersecurity issues in small businesses. *Proceedings of the 4th Annual ACM Conference on Research in Information Technology, Chicago, Illinois, 11*. doi:10.1145/2808062.2808063

Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber resilience -- fundamentals for a definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), *New contributions in information systems and technologies* (pp. 311-316). Springer International Publishing. doi: 10.1007/978-3-319-16486-1_31

Bobko, P., Roth, P. L., & Buster, M. A. (2007). The usefulness of unit weights in creating composite scores: A literature review, application to content validity, and meta-analysis. *Organizational Research Methods, 10*(4), 689-709.

Bodeau, D., & Graubart, R. (2017). *Cyber resiliency design principles* (Case No. 17-0103). Retrieved from The MITRE Corporation website: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf

Boss, S. R. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior* (Doctoral dissertation, University of Pittsburgh). Retrieved from ProQuest Central; ProQuest Dissertations & Theses Global. (Order No. 3284534)

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Carlton, M., & Levy, Y. (2017). Cybersecurity skills: Foundational theory and the cornerstone of Advanced Persistent Threats (APTs) mitigation. *Online Journal of Applied Knowledge Management, 5*(2), 16-28.

Cerullo, V., & Cerullo, M. J. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management, 21*(3), 70-78.

Chan, D. (2009). So why ask me? Are self-report data really that bad? In Charles E. Lance & Robert J. Vandenberg (Eds.), *Statistical and methodological myths and urban legends: Doctrine, verity and fable in the organizational and social sciences* (pp. 309-335). New York, NY: Routledge.

Chen, P., Kataria, G., & Krishnan, R. (2011). Correlated failures, diversification, and information security risk management. *MIS Quarterly, 35*(2), 397-422.

Chenail, R. J. (2012). Conducting qualitative data analysis: Reading line-by-line, but analyzing by meaningful qualitative units. *The Qualitative Report, 17*(1), 266-269. Retrieved from http://www.nova.edu/ssss/QR/QR17-1/chenail-line.pdf

Chittister, C. G., & Haimes, Y. Y. (2011). The role of modeling in the resilience of cyberinfrastructure systems and preparedness for cyber intrusions. *Journal of Homeland Security and Emergency Management, 8*(1), 1-19.

Cisco. (2018). Small and mighty - how small and midmarket businesses can fortify their defenses against today's threats. *CISCO Cybersecurity Special Report*. Retrieved from https://www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

Clark, V. L. P., & Ivankova, N. V. (2015). *Mixed methods research: A guide to the field* (Vol. 3). Thousand Oaks, CA: Sage Publications, Inc.

Cragg, P., Caldeira, M., & Ward, J. (2011). Organizational information systems competences in small and medium-sized enterprises. *Information & Management, 48*(8), 353-363.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Creswell, J. W., & Clark, V. L. P. (2017). *Designing and conducting mixed methods research* (3rd ed.). Thousand Oaks, CA: Sage Publications, Inc.

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced mixed methods research designs. In A. Tashakkori & C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp. 209-240). Thousand Oaks, CA: Sage Publications, Inc.

Committee on National Security Systems (CNSS). (2015, April 6). *National information assurance (IA) glossary* (Instruction No. 4009). Retrieved from https://www.cnss.gov/CNSS/

Cook, T. D., & Campbell, D. T. (1979). *Quasi-experimentation: Design and analytical issues for field settings*. Chicago, IL: Rand McNally.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334.

Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). Retrieved from https://www.cisa.gov/publication/cisa-cyber-essentials

Department of Homeland Security. (2017). *What is security and resilience?* Retrieved from https://www.dhs.gov/what-security-and-resilience

Dilger, R. J. (2019). *Small business size standards: A historical analysis of contemporary issues*. Washington, DC: Congressional Research Service 7.5700. Retrieved from https://fas.org/sgp/crs/misc/R40860.pdf

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61-80.

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. *Issues in Informing Science and Information Technology, 6*, 323-337.

Ellis, T. J., & Levy, Y. (2010). A guide for novice researchers: Design and development research methods. *Proceedings of Informing Science & IT Education Conference, InSITE,* Cassino, Italy, (pp. 107-118). Retrieved from http://proceedings.informingscience.org/InSITE2010/InSITE10p107-118Ellis725.pdf

Experian-CSID. (2016). *Survey: Small business security*. Retrieved from https://www.csid.com/wp-content/uploads/2017/01/WP_SmallBizSecurity_2016.pdf

Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. *International Journal of Human-Computer Studies, 59*(4), 451-474.

Fisher, R., Norman, M., & Klett, M. (2017). Enhancing infrastructure resilience through business continuity planning. *Journal of Business Continuity & Emergency Planning, 11*(2), 163-173.

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM), 7*(1), 14-26.

Gibson, W. J. & Brown, A. (2009). Generating data through questions and observations. In Gibson, W. J., & Brown, A. *Working with qualitative data* (pp. 84-108). London: SAGE Publications, Ltd doi: 10.4135/9780857029041

Given, L. M. (Ed.). (2008). *The Sage encyclopedia of qualitative research methods*. Thousand Oaks, CA: Sage Publications, Inc.

Goel, S., Williams, K., & Dincelli, E. (2017). Got phished: Internet security and human vulnerability. *Journal of the Association for Information Systems, 18*(1), 22-44.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355.

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security, 13*(4), 297-310.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis*, *29*(4), 498-501.

Harrop, W., & Matteson, A. (2015). Cyber resilience: A review of critical national infrastructure and cyber-security protection measures applied in the UK and USA. In F. Lemieux (Ed.), *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice* (pp. 149–166). London: Palgrave Macmillan UK. doi:10.1057/9781137455550_10

Hayes, T., Tanner, M., & Schmidt, G. (2012). Computer security threats: Small business professionals' confidence in their knowledge of common computer threats. *Advances in Business Research, 3*(1), 107-112.

Hess, M. F., & Cottrell, J. H. (2015). Fraud risk management: A small business perspective. *Business Horizons*, *59*(1), 13-18.

Hevner, A. R. (2007). A three cycle view of design science research. *Scandinavian Journal of Information Systems, 19*(2), 87-92.

Hiscox. (2017). 2017 *Hiscox cyber readiness report*. Retrieved from http://www.hiscox.com/cyber-readiness-report

Hiscox. (2018a). 2018 *Hiscox cyber readiness report*. Retrieved from http://www.hiscox.com/cyber-readiness-report

Hiscox. (2018b). 2018 *Hiscox small business cyber risk report*. Retrieved from https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Hovav, A., & Gray, P. (2014). The ripple effect of an information security breach event: A stakeholder analysis. *Communications of the Associations for Information Systems, 34*(50), 893-912.

Hunker, J., & Probst, C. W. (2011). Insiders and insider threats-an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2*(1), 4-27.

Hurley, J. S., McGibbon, H. M., & Everetts, R. (2014). Cyber readiness: Are we there yet? *International Journal of Cyber Warfare and Terrorism, 4*(3), 11-26.

Ivankova, N. V., Creswell, J. W., & Stick, S. L. (2006). Using mixed-methods sequential explanatory design: From theory to practice. *Field Methods, 18*(1), 3-20.

Itai, Y., & Onwubiko, E. (2018). Impact of ransomware on cybersecurity. *International Journal of Computers & Technology, 17*(1), 7077-7080.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed-methods research: A research paradigm whose time has come. *Educational Researcher, 33*(7), 14-26.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science, 32*, 489-496.

Kahan, J. H., Allen, A. C., & George, J. K. (2009). An operational framework for resilience. *Journal of Homeland Security and Emergency Management, 6*(1), 1-48.

Kahneman, D., Knetsch, J. L., & Thaler, R. H. (1991). Anomalies: The endowment effect, loss aversion, and status quo bias. *Journal of Economic perspectives, 5*(1), 193-206.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society, 47*(2), 263-291.

Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist, 39*(4), 341-350.

Kim, H. W., & Kankanhalli, A. (2009). Investigating user resistance to implementation: A status quo bias perspective. *MIS Quarterly, 33*(3), 567-582.

Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information & Management, 41*, 597-607.

Kumar, R. L., Park, S., & Subramaniam, C. (2017). Understanding the value of countermeasure portfolios in information systems security. *Journal of Management Information Systems, 25*(2), 241-280.

Lee, A. S., Thomas, M., & Baskerville, R. L. (2015). Going back to basics in design science: From the information technology artifact to the information systems artifact. *Information Systems Journal, 25*(1), 5–21.

Lee, K., & Joshi, K. (2016). Examining the use of status quo bias perspective in IS research: Need for re-conceptualizing and incorporating biases. *Information Systems Journal, 27*(6), 733-752.

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leedy, P. D., & Ormrod, J. E. (2016). *Practical research: Planning and design* (11th ed.). Upper Saddle River, NJ: Prentice Hall.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science.

Levy, Y., & Ellis, T. J. (2011). A guide for novice researchers on experimental and quasi-experimental studies in information systems research. *Interdisciplinary Journal of Information, Knowledge, and Management, 6*, 151-161.

Li, J., Liu, M., & Liu, X. (2016). Why do employees resist knowledge management systems? An empirical study from the status quo bias and inertia perspectives. *Computers in Human Behavior, 65*, 189-200.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly, 16*(2), 173-186.

Martinsons, M., Davison, R., & Tse, D. (1999). The balanced scorecard: A foundation for the strategic management of information systems. *Decision Support Systems, 25*(1), 71-88.

Mejias, R. J., & Balthazard, P. A. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Information Privacy and Security, 10*(4), 160-185.

Merriam-Webster. (n.d.). Retrieved from https://www.merriam-webster.com/dictionary

Mertler, C. A., & Reinhart, R. V. (2017). *Advanced and multivariate statistical methods (6th ed.): Practical application and interpretation*. New York, NY: Routledge.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2-26.

National Cyber Security Alliance (NCSA). (n.d.). *StaySafeOnline – CyberSecure my business*. Retrieved from https://staysafeonline.org/cybersecure-business

National Initiative for Cybersecurity Careers and Studies (NICCS). (2017). *Cyber glossary*. Retrieved from http://niccs.us-cert.gov/glossary#cybersecurity

National Institute of Standards and Technology (NIST). (2011). *Managing information security risk* (NIST SP 800-39). Retrieved from https://csrc.nist.gov/publications/detail/sp/800-39/final

National Institute of Standards and Technology (NIST). (n.d.-a). *Cybersecurity framework*. Retrieved from https://www.nist.gov/cyberframework

National Institute of Standards and Technology (NIST). (n.d.-b). *Small business cybersecurity*. Retrieved from https://www.nist.gov/itl/smallbusinesscyber

National Institute of Standards and Technology (NIST). (2014, February 12). *Framework for improving critical infrastructure cybersecurity* (version 1.0). Retrieved from https://www.nist.gov/file/20011

National Institute of Standards and Technology (NIST). (2018, April 16). *Framework for improving critical infrastructure cybersecurity* (version 1.1). Retrieved from https://doi.org/10.6028/NIST.CSWP.04162018

Nussbaum, B., & Lewis, C. (2017). Sizing up people and process: A conceptual lens for thinking about cybersecurity in large and small enterprises. *Journal of Cyber Policy, 2*(3), 389-404.

Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & management, 42*(1), 15-29.

Onwuegbuzie, A. J., Bustamante, R. M., & Nelson, J. A. (2010). Mixed research as a tool for developing quantitative instruments. *Journal of Mixed Methods Research, 4*(1), 56-78.

Osborn, E., & Simpson, A. (2017). Risk and the small-scale cyber security decision making dialogue – a UK case study. *The Computer Journal, 61*(4), 1-24.

Osiyevskyy, O., & Dewald, J. (2015). Inducements, impediments, and immediacy: Exploring the cognitive drivers of small business managers' intentions to adopt business model change. *Journal of Small Business Management, 53*(4), 1011-1032.

Oxford Dictionary. (n.d.). Retrieved from https://en.oxforddictionaries.com/definition/programme

Paulsen, C. (2016). Cybersecuring small businesses. *Computer, 49*(8), 92-97.

Paulsen, C., & Toth, P. (2016). Small business information security: The fundamentals. *National Institute of Standards and Technology Interagency Report (NISTIR). 7621 Revision 1*. Retrieved from https://doi.org/10.6028/NIST.IR.7621r1

Peiro, A., Cook, P., & Beydoun, H. (2005). Small business information security readiness. *Small Business Technology Institute, Santa Jose, California* 1-16.

Pfleeger, S. L., Predd, J. B., Hunker, J., & Bulford, C. (2010). Insiders behaving badly: Addressing bad actors and their actions. *IEEE Transactions on Information Forensics and Security, 5*(1), 169-179.

Polites, G. L., & Karahanna, E. (2012). Shackled to the status quo: The inhibiting effects of incumbent system habit, switching costs, and inertia on new system acceptance. *MIS Quarterly, 36*(1), 21-42.

Ponemon Institute. (2016). *2016 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

Ponemon Institute. (2017). *2017 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html

Ponemon Institute. (2018). *2018 State of cybersecurity in small & medium-sized businesses (SMB)*. Retrieved from https://keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Ramim, M. M., & Lichvar, B. T. (2014). Eliciting expert panel perspective on effective collaboration in system development projects. *Online Journal of Applied Knowledge Management, 2*(1), 122-136.

Rees, L. P., Deane, J. K., Rakes, T. R., & Baker, W. H. (2011). Decision support for cybersecurity risk planning. *Decision Support Systems, 51*(3), 493-505.

Renaud, K. (2016). How smaller businesses struggle with security advice. *Computer Fraud and Security, 8*, 10-18.

Richey, R. C., & Klein, J. D. (2014). *Design and development research: Methods, strategies, and issues.* New York, NY: Routledge.

Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business infosec posture using social theories. *Information & Computer Security, 24*(5), 534-556.

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121-135.

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Salkind, N. J. (2010). *Encyclopedia of research design*. Thousand Oaks, CA: Sage Publications, Inc.

Samuelson, W., & Zeckhauser, R. (1988). Status quo bias in decision making. *Journal of Risk and Uncertainty*, *1*(1), 7-59.

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica, 16*(2), 58.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Education*, *57*, 14-30.

Shefrin, H., & Statman, M. (2003). The contributions of Daniel Kahneman and Amos Tversky. *The Journal of Behavioral Finance, 4*(2), 54-58.

Simon, M. K. (2011). *Dissertation and scholarly research: Recipes for success* (2011 ed.). Seattle, WA: Dissertation Success, LLC.

Simon, M. K., & Goes, J. (2013). *Dissertation and scholarly research: Recipes for success* (2013 ed.). Seattle, WA: Dissertation Success, LLC.

Skinner, R., Nelson, R., Chin, W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems, 37*(2), 31–63.

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

Spillan, J. E. (2003). The difference between survival and disaster: Crisis planning in small business. *Journal of Small business Strategy*, *14*(1), 20-31.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Stewart, A. (2004). On risk: Perception and direction. *Computers & Security*, *23*(5), 362-370.

Sumner, M. (2009). Information security threats: A comparative analysis of impact, probability, and preparedness. *Information Systems Management*, *26*(1), 2-12.

Sun, J., Ahluwalia, P., & Koong, K. S. (2011). The more secure the better? A study of information security readiness. *Industrial Management & Data Systems, 111*(4), 570–588.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information security challenge and breaches: Novelty approach on measuring ISO 27001 readiness level. *International Journal of Engineering and Technology*. *IJET Publications UK, 2*(1), 67-75.

Symantec Corporation. (2016). *Internet security threat report (ISTR)*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec Corporation. (2017). *Internet security threat report (ISTR)*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Symantec Corporation. (2018). *Internet security threat report (ISTR)*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science, 211*(4481), 453-458.

Tversky, A., & Kahneman, D. (1991). Loss aversion in riskless choice: A reference-dependent model. *The Quarterly Journal of Economics, 106*(4), 1039-1061.

Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and uncertainty, 5*(4), 297-323.

United States Census Bureau. (2015). *2015 U.S. Statistics of U.S. Business (SUSB)*. Retrieved from https://www.census.gov/programs-surveys/susb.html

United States Computing Emergency Readiness Team (US-CERT). (n.d.). Retrieved from https://www.us-cert.gov/ccubedvp/smb

United States Small Business & Entrepreneurship Council (SBE Council). (n.d.). Retrieved from http://sbecouncil.org/about-us/facts-and-data

Verizon Enterprise. (2016). *Verizon 2016 data breach investigations report (DBIR)*. Retrieved from www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

Verizon Enterprise. (2017). *Verizon 2017 data breach investigations report (DBIR)*. Retrieved from www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Verizon Enterprise. (2018). *Verizon 2018 data breach investigations report (DBIR)*. Retrieved from www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Williams, P., & Manheke, R. J. (2010). Small business - a cyber resilience vulnerability. *Proceedings of International Cyber Resilience Conference.* Edith Cowan University, Perth Western Australia.

Whitman, M. E. (2003). Enemy at the gate: Threats to information security. *Communications of the ACM, 46*(8), 91.

Whitman, M., & Mattord, H. (2015). Ongoing threats to information protection. *Proceedings of the 2015 Information Security Curriculum Development Conference*. New York, NY: Association for Computing Machinery. doi: 10.1145/2885990.2885994

Whyte, G. (1986). Escalating commitment to a course of action: A reinterpretation. *Academy of Management Review*, *11*(2), 311-321.

Zobel, C. W., & Khansa, L. (2012). Quantifying cyberinfrastructure resilience against multi-event attacks. *Decision Science*, *43*(4), 687-710.