Security Obstacles and Motivations for Small Businesses from a CISO's Perspective

Flynn Wolf, *University of Maryland, Baltimore County;* Adam J. Aviv, *The George Washington University;* Ravi Kuber, *University of Maryland, Baltimore County*

https://www.usenix.org/conference/usenixsecurity21/presentation/wolf

This paper is included in the Proceedings of the
30th USENIX Security Symposium.

August 11–13, 2021

978-1-939133-24-3

Security Obstacles and Motivations for Small Businesses from a CISO's Perspective

Flynn Wolf
University of Maryland, Baltimore County

Adam J. Aviv
The George Washington University

Ravi Kuber
University of Maryland, Baltimore County

Abstract

Small businesses (SBs) are often ill-informed and under-resourced against increasing online threats. Chief Information Security Officers (CISOs) have a key role in contextualizing trade-offs between competing costs and priorities for SB management. To explore the challenges CISOs face when guiding SBs towards improved security we conducted two interview studies. Firstly, an exploratory study with CISOs with SB experience to identify themes related to their work (n=8). Secondly, we refined our methods and conducted broader structured interviews with a larger non-overlapping group of similarly qualified SB CISOs (n=19) to validate those themes and extend outcomes. We found CISOs confirmed common observations that SBs are generally unprepared for online threats, and uninformed about issues such as insurance and regulation. We also found that despite perceived usability problems with language and formatting, the effectiveness of government-authored guidance (a key reference source for CISOs and SBs) was deemed on par with commercial resources. These observations yield recommendations for better formatting, prioritizing, and timing of security guidance for SBs, such as better tailoring checklists, investment suggestions, and scenario-based exercises.

1 Introduction

Small business (SB) information security is a mounting concern. As large and medium-sized businesses have recognized online threats and tightened their security, research suggests that targeting by criminals has shifted to smaller companies [32]. These businesses generally have fewer resources to direct at their information technology (IT) and security, and are often simply focused on financial survival. Although many SBs may assume they have "security through obscurity," many ransomware, data theft, and fraud threats can scale to include smaller businesses as targets [32, 36]. The impact of cybersecurity incidents to SBs is of particular concern. Malicious damage to information systems can decrease productivity, siphon away revenue and intellectual property, impose significant remediation costs, and diminish trust among customers and partners [11]. A 2019 industry survey found as many as 25% of hacked SBs file for bankruptcy, with 10% closing entirely [5]. Research suggests that it is vitally important that each SB understands and manages the risk to information, systems, and networks that support their business [28]. However, limited resources and lack of knowledge often negatively affect their ability to estimate security-related risks and commensurately protect themselves.

Prior work qualitatively examining IT decision makers responsible for guiding *small businesses* through cybersecurity-related challenges is highly limited. We addressed this gap with an exploratory set of studies. Given that SB owners may lack the IT expertise to fully reflect on resource and security trade-offs, we have instead focused on those with a unique vantage point on SB operations and security decisions, namely Chief Information Security Officers (CISOs, or those in an equivalent SB role).

In this paper, we present a two-part qualitative work investigating the perspective of CISOs ($n = 8$, and $n = 19$) that have direct experience working for or consulting with SBs. The interviews focused on challenges CISOs face when motivating smaller enterprises to consider IT security improvements.

We first performed an exploratory open-ended interview-based phase (Study 1) with a small cohort of *SB-focused* IT staff and several local government SB development officials (n=8). This identified themes arising from their work supporting SB IT security decisions. These were mostly individuals with the professional title of CISO or Chief Security Officer (CSO, but we use CISO to refer to both) and direct experience with IT security decision making for SBs (those with less than 500 employees or $5 million USD in annual revenue [3]). In our interviews, we addressed the CISOs' opinions and experiences with cybersecurity problems and effective approaches to motivating at-risk SBs to invest in better security *before adverse IT events occurred.*

We inductively coded those responses, and a number of issues became apparent. Unsurprisingly, perceptions of widespread IT security shortfalls were prevalent, but CISOs also described opportunities to more effectively intervene with SBs. We derived a structured interview from the Study 1 themes to better understand these mental models and validate concepts in Study 2.

We recruited a non-overlapping cohort of similarly SB-exposed CISOs for Study 2, slightly more than doubling the sample size of Study 1. Interview topics included motivations for SBs to make IT improvements, security best practices, sufficiency of IT security education resources, and comparative views on the efficacy of commercial and government guidance (government guidance in these studies being State- and Federal-authored publications in the United States).

Findings Several key findings emerged from the analysis which offer highly actionable insight for those seeking to positively engage with SBs on IT security improvement (see Section 6). These include:

1. **Government-sourced security guidance deemed as effective as commercial guidance**: Security guidance documents are a key resource for CISOs and SBs. A preponderance of Study 2 participants disagreed with the theme from Study 1 that commercially-sourced guidance was simply more effective for SBs than government-sourced guidance.
2. **Government guidance deemed important but hard to use**: Study 2 CISOs confirmed Study 1 themes indicating government guidance was difficult to use but still an important source of direction. They acceded that its language was often too broad and imprecise for definitive interpretation, offering principles rather than best practices. However, the content was still deemed appropriately comprehensive and of comparable value to commercial sources.
3. **Commercial guidance seen as narrow to use**: Study 2 CISOs noted that commercial guidance could often afford to be more clear and prescriptive than government sources because of a narrower focus on product offerings, but could also impose more work on IT managers to filter out profit motives.
4. **SBs lack required IT protections**: Study 2 CISOs confirmed the prevalent view and coded theme from Study 1 that SBs are too resource-constrained to manage information security properly because of cost, complexity and focus on profitability. Participants saw SBs as generally informed about complex or vague regulatory and insurance issues. However, CISO sentiment was divided on whether SBs understood potential financial implications, due to the difficulty of projecting preventative costs.
5. **CISOs divided blame for SB vulnerabilities**: Participants were also divided on responsibility for poor SB security, noting similar problems in medium and large-scale businesses, the well-known challenges guarding numerous IT attack vectors, and the frequency of security flaws in software and hardware.

Recommendations We draw a number of direct implications from these observations that can lead to interventions that more effectively motivate and inform SB security (see Section 7). These include three major points:

1. **Messaging at the right time**: Suggested timing for security advocates to contact SBs, within their short and long-term business processes and tax schedules, to get an optimal response to security guidance.
2. **Priorities for effective IT guidance checklists**: Discussion of factors for effective use of checklists, a key SB security practice, as described by Study 2 participants.
3. **Guidance formats**: Discussion of formats and labeling for IT guidance (e.g., checklists and scenario-based team exercises) based on CISO discussion of effective structural features and content.

2 Related Work

Obstacles to Information Security for Small Businesses Although IT security has been studied within corporate structures (e.g., cybersecurity training, and security operators and developers [2, 14, 17, 25, 34, 38], and local government [24]), examination of perceptions, understandings, and actions related to cybersecurity for SBs are under-explored. Some related studies also predated the widespread proliferation of both network-based business technologies and services and significant online threats [6, 15, 39]. Examples include threat assessments focused on personnel and physical security, access control, and information assurance of networked information systems [39], and examinations of employee practices identifying deficiencies in preventive mechanisms, incident reporting and management, and risk analysis processes [31].

While common obstacles to maintaining IT security faced by SBs (e.g., distraction, limited resources, compliance) have been documented [18, 22, 27, 29], in-depth qualitative inquiry regarding the mindset of SB IT security decision makers is limited, especially considering the breadth of the increasing challenges confronting so many businesses of that type. That outlook has been examined (although not focusing on small businesses exclusively) by Moore et al., who examined CISOs' interaction with management in a variety of private industries. Leadership of those companies was found to be increasingly aware and willing to invest in security, but still struggling to locate important resources, especially trained IT staff [23]. Those constraints and risk complacency often make SBs more susceptible to proliferating cyber threats. As security breaches can quickly devastate a SB, many owners are more likely to pay ransomware attackers to get their data back [30].

More recently, initiatives have been developed to better pool resources for SBs and provide educational opportunities to aid cybersecurity knowledge [19, 33]. These generally included a repository of best practices and security self-assessment tests. However, messaging to SBs about these specific valuable initiatives (e.g., Small Business Big Threat

[33], Cyber Readiness Institute [19]) was often narrowly geographically-targeted and did not fully account for the diversity of SB types and resources.

Government Security Guidance for Small Businesses Several government organizations in the United States have developed enterprise IT security guidance, including the National Institute of Standards and Technology (NIST) [28], Federal Communications Commission (FCC) [7], and public-private, non-profit organizations such as the National Cyber Security Alliance (NCSA) [4]. NIST guidance issued in 2014 [28] focused on cybersecurity fundamentals for SBs, and provided an overview of risks and best practices (e.g., patching computing systems, and employing email filters, encryption, and strong passwords). More broadly, following the Cybersecurity Enhancement Act of 2014 [8], NIST also releases annual cybersecurity reports [26], and published a voluntary framework in 2014. That framework focused on using business drivers to guide cybersecurity activities and risk management processes [10]. More recently, in 2018, the NIST Small Business Cybersecurity Act, S. 770 required NIST to disseminate concise resources to help SBs identify and manage their online risks. The resources were intended to be technology-neutral, and apply to businesses of different sizes storing data of varying sensitivity [9, 37]. Researchers suggest these actions in the United States amount to a patchwork of laws, rather than a cohesive legal framework addressing data security [20].

Motivation While prior work offers valuable insight, research should further explore how to overcome obstacles to SB security improvement. Describing some of these limitations and motivations might not be possible for SB owners who have limited understanding of security or technology. To position ourselves to gather an informed perspective with direct knowledge of SB challenges, we instead targeted CISOs experienced with SBs. Our intent in this research was to hear from those with first hand experience informing SBs about online risks and proposing security investment. Further, we have translated their views into actionable guidance which can be used directly by agencies supporting SBs (see Section 7). We first conducted an exploratory investigation of security themes derived from a group of commercial and county, state, and federal government CISOs, IT security managers, and development officers with direct SB security consulting experience (see Section 3). These findings are presented in this paper, as well as those of our second study, which extended and validated the Study 1 themes with a larger non-overlapping group of similar SB CISOs (see Section 5).

3 Study 1 Methods

Objectives and Recruitment We conducted our first exploratory study (IRB-approved) to gather views on information security issues from eight consultants with direct experience with SBs. Participants were not compensated. From these interviews, we developed a larger survey instrument with broader recruitment in Study 2. We recruited participants through online searches for contacts in county and federal-level SBs organizations and CISO-related organizations, word of mouth at cybersecurity business events, and through snowballing personal referrals once participants were interviewed. Recruitment targeted those in CISO-like roles, who had participated directly in IT security decision making for SBs. All of the participants, due to the nature of their roles, had consulted with multiple SBs and described their views on these interactions. The title of CISO was not an explicit requirement, rather that they had firsthand knowledge of the advising SBs on relevant issues. The participants included commercial and government cybersecurity consultants and SB development consultants (see Table 1 in Appendix A). As is typically the case with harder-to-reach populations, finding SB-specific CISOs proved to be a slow process and yielded a smaller sample size. However, the preliminary themes were intriguing and we extended the results in our second study, described in Section 5.

Interview Instrument We chose semi-structured interviews to allow flexible, open-ended inquiry. Participants were interviewed by phone and audio Skype, after being read a prescribed ethics disclosure and informed participation consent script. A twenty-two question instrument was generated (see Appendix B), initially based upon topics derived from published descriptions of SB information security challenges. The question instrument was also refined several times as interviews were conducted to focus on the emergent themes offered by participants, clarify language, and to group questions by topic for effectiveness. The question topics include how participants assessed SBs' general motivation and obstacles towards better security, the general level of knowledge of online risks for SBs, available IT and education resources, and potential business implications of security incidents. Participants were also asked which guidance formats and security practices had been effective in motivating SBs in their experience.

Inductive Thematic Coding The eight interviews were transcribed and analyzed with open coding with one rater. A second coder performed an inter-rater reliability procedure on 25% of the transcripts. Reliable results were indicated by that procedure (overall Cohen's kappa value of $\kappa = 0.76$). Questioning about themes was added to the instrument as they were identified to test their validity and extend the content under discussion.

4 Study 1 Discussion

Analysis of the Study 1 data revealed four main themes relating to IT security for SBs from the perspective of consultants with direct experience with SBs. These are described below.

Mostly Reactive Motivation for Security Investment Participants in Study 1 related a number of potential reasons for why SBs delay making security upgrades (primarily lack of knowledge and resource limitations), and potential reasons they finally acknowledge network IT risks and make security investments. Primarily, CISOs saw SBs as reacting to threats after-the-fact in response to an adverse IT event, such as a data breach or ransomware attack that compromises customer information and affects business operations.

Participants mentioned other factors that motivated security improvement. These included SBs receiving security upgrades *incidentally* when purchasing new business IT capability, and maintaining compliance with contractually obligated audits if they are a services company. CISOs also described SBs in the software sector realizing risks after publicly releasing intellectual property such as apps or online content involving customer data. These effects could also be modulated by typical physical settings of new SBs. For example, operating from a small business incubator may offer better inhouse IT security support, but consequently not teach caution. Alternatively, working in *"Starbucks and airplanes" (p1.01, participant 1 of Study 1, a CISO consultant to a county-level SB council*) on cloud-based services might induce greater caution from the outset without *"the illusion...* [of being] *apart from the public network somehow protected behind the firewall... The smalls understand that don't have the facilities with locked doors... there's already a recognition that that's the world in which they operate."*

Influence of Business Regulation Study 1 participants had experienced SB security improvements as primarily reactive, motivated by reaction to adverse events. However, those CISOs also acknowledged awareness of online risks and countermeasures driven by business domain-specific regulation, such as finance or medical business rules. They also noted that software outsourcing moderated SBs' reaction to regulation. SBs were deemed to entrust many compliance decisions to their contracted business software providers. This included software for primary business services (e.g. customer billing) that touched sensitive and regulated types of customer information. Also, CISOs pointed out that SB compliance could be limited by the potential return on the effort. For example, SB acceptance of the implementation costs for security improvements stipulated by a contract might be limited by the its potential profitability. *"Might be worth it to comply for ten contracts, but not for one,"* stated p1.01. "[SBs] *do the customer-required ones, and may just omit the ones they can't cost-justify."*

Poor Overall Understanding of Risks CISO participants took a notably dim view of how much the SBs they had interacted with were able to learn and apply with regard to security. Without motivation from regulatory or contractual requirements, and with many facets of data security managed by third-party cloud-based services, SBs were seen as largely uninformed and unprepared. Often this deficit was seen as imposed on SBs, struggling to reach early profitability, by the all-too-familiar lack of resources and funds for security costs. SBs were also seen as struggling to remain informed about potential financial costs, insurance liability, and regulatory exposure imposed by online threats. At the same time, another noted factor in SBs' comprehension and motivation was the increasingly ubiquitous national and international news coverage of data breaches and hacking events, and the negative consequences those events caused for business victims and their customers.

Available Guidance Sources and Their Efficacy Study 1 participants expressed concern that many SBs, once brought to the point of wanting guidance, then struggled to find a cogent course of action prescribed by either industry or government sources. Often guidance was deemed to be too long, confusing, and full of jargon to be helpful, or tainted by an overriding commercial profit motive to sell a security solution.

These observations made it clear that CISOs deemed SBs to be generally at risk, unaware, and unprepared. Further, CISOs were faced with an array of serious challenges when trying to impart their understanding of online risk to SBs. We were therefore motivated to inquire in more detail in Study 2 about the specific issues identified in Study 1, and to assess the sentiment and outlook of a larger but similarly qualified cohort. We next describe the methodological approach taken.

5 Study 2 Methods

Objectives and Recruitment To further explore themes identified in Study 1 we conducted an expanded set of interviews with a larger group of 19 similarly qualified CISOs who had made SB IT security decisions. No Study 1 participants were reused. As with Study 1, no participants were compensated. This sample size is consistent with similar qualitative security research [1, 13, 16]. These participants were asked two-part confirmation questions based closely on themes from Study 1. This approach assessed the validity of emergent themes and enriched our discussion of the related issues. Recruitment was conducted in a similar manner to the initial study, utilizing solicitation in online IT security forums, numerous state SB and cybersecurity organizations, and IT industry events. While the Study 2 cohort ultimately proved well-qualified, recruitment for participants in this role proved slow and challenging, with generally very low response rates to solicitation contacts. Instead, most participants were obtained through snowball or direct word of mouth recruitment.

Low response rates may be attributable to several factors, including typical low survey response behavior, heightened privacy concerns in the target demographic, and the relatively limited number of SB-focused IT consultants in the wider pool of cybersecurity professionals. Despite this we were eventually able to double the sample size from Study 1 with new, SB-qualified CISO participants.

The IRB-approved study was initiated in the Mid-Atlantic region of the United States, which has a concentration of information security organizations and businesses. To counteract assumptions that might be regional, deliberate sampling was carried out through SB development offices in other parts of the United States. In some cases participants noted that we were offering opinions that might be more relevant to SBs in their Midwestern American states than those in the Mid-Atlantic region.

Participant Demographics Participants in Study 2 averaged forty-nine years of age, averaging fifteen years of IT security decision making experience. Notably, the cohort had most recent experience addressing SBs with an average of less than fifty employees, making familiarity with personnel resource constraints more likely (see Table 2 in Appendix A). Two were female, which comports with the unfortunately low female representation found by a 2017 industry survey of comparable cybersecurity professionals [12]. Qualifications included a PhD in cybersecurity, BAs in Electrical Engineering, CISSP certifications, and often extensive self-taught learning and on-the-job training. Their experience in IT security decision making included SBs in finance, healthcare, municipal government, manufacturing, law, and higher education. Several participants were both owner and operators of small cybersecurity consulting businesses, and were asked to identify in their responses whether they were speaking about their own SB experience, or those of SB clients.

Interview Instrument The instrument for Study 2 included 26 two-part questions, based on eight themes and twenty subtopics observed during Study 1 (see Appendix C). Participants were first asked to respond with their *agreement* in terms of a bimodal 5-point Likert scale to a theme expressed as a statement. For example, "The resources of SBs are too limited to properly manage information security responsibilities." Care was taken to include appropriate counterbalancing language in requesting a response, while also offering a clear and nonambiguous statement of the Study 1 theme for participants to evaluate. Secondly, after rating their sentiment towards the statement, participants were asked to explain their rationale in their own words. Follow-up questions, also utilizing counterbalancing language, were employed frequently to evoke further expansion on these explanations. Our discussion of these results differentiates between observations drawn from the sentiment data and the coded follow-up discussions. The combination of both allowed us to directly compare the Study 1 themes against a larger population, while also gathering nuanced rationales for CISO views on those issues. We acknowledge that, despite our best efforts to limit any bias introduced by using the Study 1 themes as prompts for structured questioning, we cannot rule out these effects in the data. These issues are discussed further under *Inductive Thematic Coding* in this section. These discussions were recorded, transcribed, and inductively thematically coded.

Eight Study 1 themes were chosen for validation. These included issues such as SB motivations for IT security improvement, availability of adequate or affordable security education resources, SB understanding of IT risk factors, differences in the efficacy of commercial versus government-authored guidance, and influences on SB willingness to invest in security improvements. We offered clarification and exemplars of terminology at participants' request. Follow up questions were often asked during the rationale to prompt elaboration and examples. Coding of these rationales, more than the Likert sentiment measures, significantly informed our analysis and conclusions.

Participants were also asked to score a list of nine security practices (e.g., updating software, securing physical hardware, implementing employee security training) for their *importance* to SBs, and the *effectiveness* of a list of formats for security guidance (e.g. checklists, whitepapers). As with the other questions, these prompts were based directly on themes and content collected from Study 1 CISOs in order to verify assumptions and reinforce the validity of our conclusions on these topics.

The Study 2 interviews averaged 38 minutes in length and were audio recorded. Participants were contacted by phone or audio Skype. An ethics disclosure was provided, informed consent recorded, and any participant questions answered at the beginning. Written notes were taken concurrently. Audio was software transcribed and manually error corrected. Written notes were used primarily to refine the question instrument and perform a qualitative research memo practice. The transcripts were used to perform inductive thematic coding on the responses.

Inductive Thematic Coding As with Study 1, Study 2 responses to the prompts were analyzed with inductive thematic coding. 117 codes were extracted, averaging about six codes per question, which described different emergent rationales for agreement, neutrality, or disagreement with the prompting statement (see Appendix D). Saturation on thematic codes was reached by the end of the interview sample. Encouragingly, variance in this sentiment data on the prompts, combined with the themes from the coded discussion data collected in parallel, indicates that participants largely were able to freely offer both agreement and disagreement in response to the prompts, suggesting that possible in-person questioning effects were limited. In a limited number of cases, rationales that were conceptually very close were scored differently by the participants (i.e. the same basic opinion on a topic scored by one participant as neutral, and moderate agreement by another). To address this, two researchers coded independently, met together to present and discuss their codes, and were then able to refine to reach agreement on describing the concepts. After multiple iterations with additional transcripts, new codes were rare, suggesting that we reached saturation within the sample.

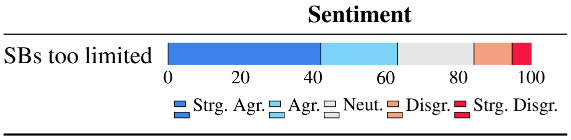

Figure 1: 5-point Likert response distributions regarding SBs being too resource-limited to manage infosec. properly

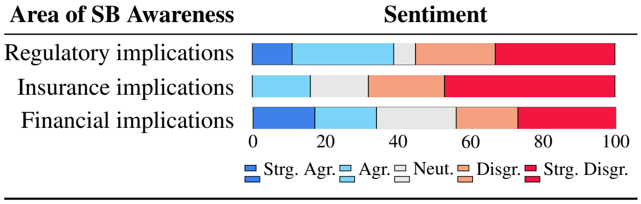

Figure 2: 5-point Likert response distributions regarding SB understanding of implications of three IT security factors

Inter-rater reliability testing was performed on 15% (or 3) of transcripts selected at random with a reliability coder, and an overall Cohen's kappa value of $\kappa = 0.88$ was ascertained, indicating good agreement and a valid code book that well represents the data without needing to compare further transcripts or modifications to the code book. Following, a primary coder proceeded to code the remainder of the data using the coded book. These methods are inline with qualitative coding in the field [21, 35]. High agreement on a subsample of the transcripts may also be attributable in part to the structured nature of the interview instrument, in which a 5-point Likert question (based on a Study 1 theme) was used as a prompt (e.g., Rate and explain your agreement, with this statement: "SBs have adequate education sources for information security."). Open discussion of the CISO's relevant experience and scoring rationale followed (which was coded). This tended to produce non-ambiguous discussion with few tangents, reducing disagreement over coding interpretation.

6 Study 2 Discussion

Reacting to questions derived from Study 1 responses, Study 2 CISOs offered their perspectives on small business IT security issues including motivations for initiating improvements, SBs' understanding of underlying security and business factors, and the suitability of available security guidance. We present assessment of the overall sentiment on the questions, and incorporate comparison to the results of inductive thematic coding of participant follow-up discussion. We also offer comparison to several related studies that have also addressed SB IT security [18, 22, 27, 29].

6.1 SB IT Resources Are Too Limited

A clear preponderance of Study 2 participants agreed with the Study 1 theme asserting that SBs struggle to fully finance and staff their information security responsibilities (see Figure 1). While this is a common observation, hearing it directly from CISOs who have interacted with SBs underscores the importance of effectively communicating tangible risk and value in these relationships.

CISOs attributed this limitation to several familiar factors. SBs were described as often unaware of online risks, and consequently unwilling to deal with the cost and complexity of implementing better security. Others noted that SBs are distracted by everyday business goals (per p2.14, participant fourteen of Study 2): [for SBs] *"the goal is to work on the widget"*). CISOs noted several implications of SBs' limited defense posture. One participant felt that security guidance needed to offer more flexible and simplified suggestions, describing adaptable best practices rather than advocating for brittle tool-based approaches to security (p2.06). Another felt that ultimately greater software-based automation would be required to relieve business owners of complex and time-intensive security decision making and maintenance (p2.05), while others noted that any of those remedies would only find traction if regulatory mandates *forced* more diligence by SBs themselves (p2.01, p2.02).

In their related research, Mierzwa and Scott investigated information security in non-profits and non-governmental organizations (NGOs) using surveys (n=53) [22]. These business models had many features in common with SBs, and both works cite resource constraints, business-oriented distraction, and failure to fully appreciate online risks as obstacles to timely security investment. Mierzwa and Scott also prescribed IT security practices very similar to those nominated and reviewed by SB CISOs in Studies 1 and 2, such as conducting security drills and purchasing insurance [22]. However, our study captured commentary on obstacles to applying these same approaches (such as the lack of SB awareness of cybersecurity insurance). Mitigating factors to these problems nominated by SB CISOs (such as closely tailoring drills to an organization's real-world financial realities and business domain), are described as specific implications of this study (see Section 7).

6.2 SBs Misread Critical Security Factors

Study 2 CISOs largely confirmed that SBs struggle to recognize three important information security factors identified in Study 1 (see Figure 2). These factors included understanding of the *regulatory, insurance,* and *financial implications* of hacking risks. Notably, many Study 2 participants felt SBs misunderstood all three factors (see Figure 2), which could easily affect SB security management and investment decisions. Regulation and insurance were most predominantly deemed to be misunderstood, but CISOs were almost evenly split on whether SBs' understood the financial implications of security risk.

Awareness of Regulatory Implications Regarding regulatory understanding, SBs were deemed to struggle with the confusing nature of the relevant laws (n=4) and legal requirements that might only pertain to certain fields (n=4). Contending with *"regulatory gotchas"* was deemed harder still for business-oriented managers without IT training (n=4), and it was noted that even better-resourced medium and large businesses also struggled to understand the law.

Awareness of Insurance Implications Study 2 CISOs also attributed SBs' limited generally sparse knowledge of insurance coverage for data security events to the same underestimation of online risks, with p2.04 (an IT manager with four years of SB experience) stating, *"The concept is foreign to them."* As with regulation, CISOs saw the *"evolving"* complexity of the insurance offerings as an obstacle for SBs. Several also felt these insurance offerings had loopholes, making it very difficult for SBs to negotiate clauses and make claims (n=4), with p2.16 (20 years of SB experience) stating, *"hope they lawyer'd up."*

Awareness of Financial Implications Similarly, Study 2 CISOs enumerated obvious shortcomings in SBs' understanding of their financial exposure, such as potential lost revenue and reputation damage, fines, and compliance costs. Others (n=4) disputed this, seeing SB managers as actually grasping these potential costs, but feeling they had no choice but to operate at risk because of costs. For example, participants felt that SBs might understand that a data breach could bankrupt their business, but didn't know how to estimate prevention costs, making risk evaluation impossible. p2.18 (a vice president for information security in a legal SB with seven years of experience) offered that the task was hard, stating *"It's hard to know for sure... how do you scope a data breach... Where's the methodology to calculate that?"* Such events could involve, *"just a reputation hit, versus lawsuits, regulatory fines. Hard to even know the factors, and many don't."* As with regulation, CISOs measured SB financial preparedness against larger organizations, pointing out, *"Big companies botch this all the time."*

Renaud conducted a qualitative study with a similar focus on risk perception among Scottish small and medium businesses, and found similar obstacles to improved security [29]. Like the CISO-held view from our study that SBs underestimated online threats, over half of Renaud's SME respondents also saw themselves as never or only remotely likely to be affected, and only 15% were utilizing all items from a basic list of security measures [29].

Renaud noted the puzzling disconnect between business owners knowing there was a risk, but not taking very basic preventative actions. *"They are being overwhelmed by choice,"* Renaud states, leading to confusion and inaction. In particular, the businesses struggled with the quantity and variety of advice, which produced a *"surprisingly high level of uncertainity"* about actions to be taken [29].

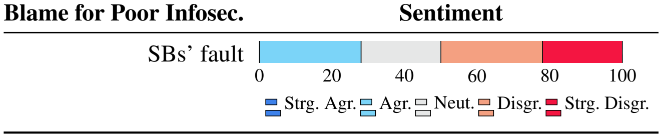

Figure 3: 5-point Likert response distributions regarding responsibility for poor SB infosec.

6.3 Shared Blame for SB Problems

A theme drawn from Study 1 participants was that SBs did not do enough to protect themselves from clear security risks. Study 2 CISOs were asked whether responsibility for perceived SBs' vulnerability was "more their own fault" than that of other parties such as criminals or software vendors (also identified in Study 1). Study 2 CISO participants were overall slightly sympathetic to the plight of SBs, although responses varied (see Figure 3).

Flawed Software and Hardware Also Deemed Culpable As p2.16 stated, *"it's really hard to draw the fault line."* Most felt that the responsibility was at least shared with software and hardware vendors who sold products with security flaws and default configurations that left SB users exposed (n=5). Participants also noted the high cost of well-trained security-qualified IT staff, and that the number of *"vectors"* for assault was simply too high for SBs to realistically protect on their own (n=2). For example, while describing SBs as *"naive"*, p2.01 (supervisor of an IT security organization with 24 years of experience) also felt software companies *"are more interested in getting to deadline and producing the product to get the money to fix the flaws. So they put a product out there that has many flaws in it. Let the world find them. And at the same time that puts all of their customers at risk."* As a result, *"The system doesn't come inherently with security features... not fully locked down,"* and specifically, *"I'll just pick on Windows for a second... if you buy a Windows laptop people have the assumption that it should be somewhat secure, because they just don't read all the news that happens every day."*

SBs Also Seen Falling Short However, others confirmed the original Study 1 theme, blaming SB owners for their own security problems (n=4), which were deemed a result of short sighted focus on profitability over responsibility. p2.19 (CEO of cybersecurity firm that has worked with SBs in finance, healthcare, municipal government, manufacturing, and higher education) summarized this, stating, *"I hate to say it, but there's a lot they could do."*

6.4 SBs Mostly Reactive to Adverse Events

Several Study 1 themes described SB paths to security investment; reacting *after the fact* to an adverse IT event, gaining

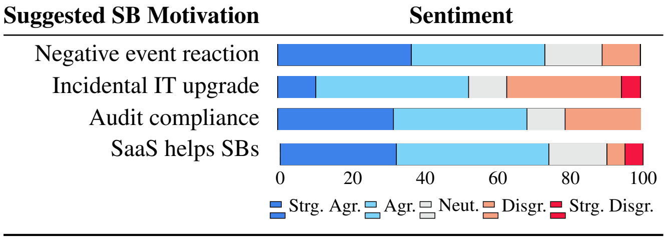

Figure 4: 5-point Likert response distributions for three possible primary motivations for SBs to improve their infosec., and perceived impact of SaaS

better security incidentally when contracting for new IT support, and improving to remain compliant as a sub-contractor. Given that CISOs generally were skeptical of SBs willingness to adequately fund information security management, we inquired if these themes were deemed valid. Study 2 participants mostly affirmed these views (see Figure 4).

Mostly Reactive to Negative IT Events Among the three themes, Study 2 participants slightly favored reactive improvement as the most common motivator for SB IT security improvement. Not surprisingly, CISOs saw this as unfortunate, given that negative reinforcement to improve security could arrive too late to prevent serious data and business losses. Additionally, reaction to second-hand accounts of IT problems, such as news reports, was also often seen as a faulty impulse. For example, CISOs described some popular media accounts of data breaches as sensationalized and distorted, even if they might spur change. p2.05 (a government security architecture lead with 20 years of prior SB experience), for example, felt news reports of data breaches and vulnerabilities, such as the 2014 Heartbleed event, were highly effective motivators. Other participants, however, such as p2.17 (CISO for a university, with thirty years of SB experience), saw this effect as limited and felt SBs instead needed a much more *localized* source of information to incite change. p2.17 felt word-of-mouth accounts of hacking or ransomware losses shared in regional, trade, or SB-specific organizations would have more impact than wider popular media reports, because SBs would more easily relate to the experience and be compelled not be the next victim. Other participants felt security news was ineffectual because business owners would prefer denial, as *"it's human nature not to accept risk"* (p2.08, a cybersecurity consultant with twenty years of SB experience).

Incidental Improvement via IT Upgrades Participants largely agreed that IT upgrades, while often not security-driven in the minds of SB customers, were a primary driver for improvement. Dissenting participants (n=5) mentioned that IT purchases are not always beneficial to security.

SaaS Viewed as Beneficial to Security A separate question, also drawn from a Study 1 theme, inquired if Study 2 participants agreed that third party software-as-a-service (SaaS) offerings were beneficial to SB security. These include common business tools such as payment services, cloud-based storage, or human resources management. Purchasing this type of business software could *"solve operational and security problems at once."* (p2.08). This was overwhelmingly seen to be the case by Study 2 CISOs (see Figure 4). For example, p2.18 (who described once finding new multi-million dollar SB clients lackadaisically co-hosting web and email servers on the same machine) noted, *"way better [for SBs] to use Dropbox than have a file server."* p2.05 concurred, stating, *"But the long and short of it is these* [SaaS] *tools are definitely helping, right? . . . You can just teach people applications and how they work. . . You no longer have to manage the underlying infrastructure. . . "*

However, CISOs also expressed SaaS reservations. While overall deemed safer than homemade software integration, the practice of outsourcing to networked services was felt by some to also inherently increase other types of security exposure (n=5). p2.19 explained, *"The cloud is just someone else's computer."* Data breaches in SaaS vendors were noted, along with the costliness of purchasing more secure business software over *"mom and pop"* offerings, when many SBs *"don't know what to ask for"* (p2.17).

Compliance with Audits Recognized A similar but slightly smaller proportion of Study 2 participants also agreed with the concept from Study 1 that compliance with security audits imposed by sub-contracting relationships would be a primary motivator for SB security improvement (see again Figure 4). The direct impact of a business-to-business requirements, tied to financial *"survival"* was deemed to accelerate acceptance of security improvement, even if imposed externally with a *"you-must-be-this-tall-to-ride"* view (p2.18). Participants noted that the prevalence of contracting requirements varied greatly by industry and region. Potential sampling effects created by this and our methodological responses are addressed in Section 8. While Study 2 sampled participants (partially, but not exclusively) in a region with many federally-funded SB contracting vehicles, many participants also cited examples of contractual security compliance in other fields (e.g., banking, accounting, and healthcare), suggesting this effect should apply broadly.

Other Motivating Factors Participants also cited peer networks such as local business and professional organizations as motivating factors (n=3), given that SBs could accept and learn about risk and solutions directly from those in very similar conditions. Further, relatively close associations would impose keen motivation *not* to be embarrassed as the next victim and suffer damage to a professional reputation, over and above potential business losses from a data breach.

6.5 SBs Influenced by Other Factors

Additional themes were also drawn from Study 1 responses regarding influences that may induce SBs to take action on

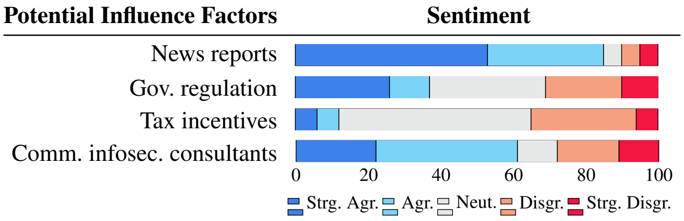

Figure 5: 5-point Likert response distributions regarding influences on SB security motivation

security risk, before adverse events. These included news reports on IT security risks, government regulation, tax incentives, and guidance from commercial information security consultants. Study 2 CISOs sentiment toward these themes as motivating factors was mostly mixed, except for news reports which were clearly deemed influential (see Figure 5).

Heidt and Gerlach also conducted an interview based study with SME IT and business executives (again, like Renaud, not CISO-type security experts) [18]. They described aspects of security decision making by these participants that in some ways differed from our findings. "Low formalization levels" and unorganized, short-term management focus were assessed, similar to the issues our CISO cohort raised. Other factors did not overlap with our findings. For example, the authors note that better SB security support should account for SME managers' age and emotional connection to the value proposition of IT, as well as factors such as "geographical insularity" (i.e., difficulty hiring qualified IT security in rural areas) and "ingrained culture" (i.e., dependence in SMEs on family-based, trust-based personal relationships). Description of these exact constraints on SB security decision making did not appear in our CISO responses, but they may well represent important second-order effects of the problems our cohort did identify. Without access to highly practical security guidance (as our CISOs asserted), SBs may struggle to find local resources and turn instead to less-qualified personal networks, as Heidt and Gerlach suggest [18].

News Reports Seen as Positive Influence Study 2 participants largely agreed that news reports of information security problems were helpful in focusing SBs on limiting their own risks. The few dissenting participants (n=5) cited concerns that negative reporting was often sensationalized and insufficiently informative (similar to limitations described in Section 6.4). Others felt that SBs might misinterpret the focus of news reports on the problems of large businesses to mean that SBs were somehow protected by *"security through obscurity."*

Regulation Seen to Help Slightly Participants only slightly affirmed that regulation could positively influence SBs. Participants noted a number of limitations, including the slowness of creating and applying new regulation (n=3), and sector-specificity that could restrict impacts just to fields like healthcare and finance (n=6).

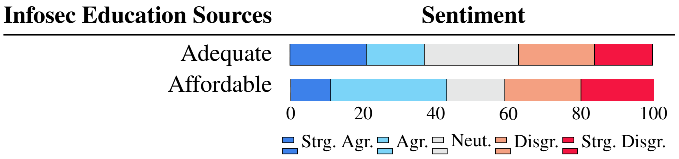

Figure 6: 5-point Likert response distributions regarding condition of infosec. education sources for SBs

Tax Incentives Largely Unfamiliar Participants were essentially neutral on the impact of tax incentives, often because they were unaware of any actually in effect (although the theme was drawn from discussion in Study 1 of existing state-level tax incentive programs). The concept in principle was also met with some skepticism, with CISOs doubting that such incentives could produce widespread impact for SBs (n=5), or be technically comprehensible (n=2).

Commercial Security Consultants Viewed Positively Participants affirmed the view that commercial security consultants influence SBs. In some cases, participants were essentially reflecting on the contribution of their own industry. Very limited dissent was offered, and was restricted to the view that consultants generally don't cater enough to SBs (n=1), and that the information security consulting industry itself generated too much counter-productive advertising *"spam."*

6.6 Mixed View of Guidance Suitability

Security guidance documents are important to SB security because they often suffice as standalone direction for many SBs lacking a CISO functionary, and also serve as references and authority for CISOs recommending actions to SBs. Preliminary themes addressing the *cost* and *adequacy* of guidance available to SBs were observed in Study 1, namely that motivated SBs could both find and afford better security guidance. Study 2 CISOs were divided on the technical sufficiency of guidance that motivated SBs would likely find. However, coded discussion revealed differing reasons for dissent on this theme. Some noted the topic's complexity. Others cited the sheer volume of sources that SBs must interpret. Similarly, for several reasons a dim view was held of guidance affordability. Some Study 2 CISOs noted hidden costs while others regarded free or low-cost sources as less reputable.

SBs Can Find Adequate Security Guidance Response sentiment was essentially mixed regarding the question of whether motivated SBs can find *adequate* education resources to help them improve their security (see Figure 6). However, looking at the coded responses, a slim majority (n=8) described reasons to agree that such resources are available. Dissenters (n=6) included several concepts in their responses, including how unsuitable available guidance is because of

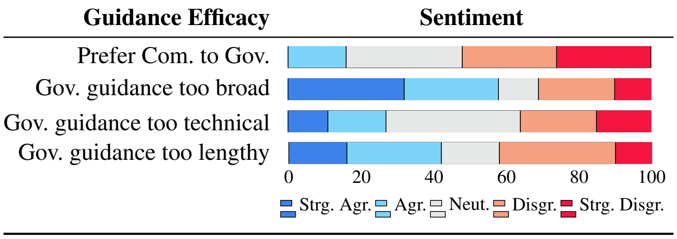

Figure 7: 5-point Likert response distributions regarding efficacy of commercial versus government guidance

its complexity (n=1), how hard it is to know where to start a search for guidance (n=1), and the amount of unhelpful marketing that would encumber a SB starting on the path to better security (n=4). p2.13 (a research organization CISO and former administrator of a government SB security program) expressed frustration with available guidance from government sources, finding it *"so complicated,"* and thus unsuitable. Instead, p2.13 continued, most users needed more simple, intuitive direction akin to *"a 5-star crash rating,"* so interpretation would be more *"clear and easy, like car safety."* p2.17 identified the problem with available guidance, not as its technical adequacy, but locating the right material in a glut of sources. SBs would, *"get a million Google results, and don't know which to use... Most don't know the right place to begin."* Neutral respondents (n=4) alluded to the difficulty of knowing what to do with information that would likely turn up. It was related that SBs would need to *"dig deeper"* and expend resources to plan effective follow-on actions after finding online guidance. Recommendations for effective guidance labelling based upon these observations are offered in Section 7 addressing SBs searching for help. These recommendations may apply to SBs, CISOs, and those authoring guidance.

Effective Guidance Still Viewed as Costly Sentiment among Study 2 CISOs was similarly divided on whether *affordable* guidance was available to motivated SBs, including free online resources from government agencies, Internet security companies, and non-profit organizations. Concepts from the qualitative analysis showed slightly more disagreement with the proposal. CISOs mentioned that free certifications were generally not regarded as seriously by industry (n=2), and that using otherwise free guidance still imposed *"opportunity costs."* Others felt that while acquiring security awareness was affordable, actually implementing countermeasures based on that knowledge was unavoidably costly (n=3).

6.7 Contrasts Seen Between Commercial & Government SB Guidance

Study 1 CISOs related a variety of difficulties with security guidance, both for their own use and for SBs to find and interpret on their own. Commercial and government-authored materials were characterized differently, with contrasting usability challenges that appeared to frustrate those tasked with applying them. However, despite these problems Study 2 CISOs ultimately identified strengths and value in both sources. Those challenges suggest opportunities for security authors trying to reach SBs to fine tune their approach.

When prompted with these Study 1 themes, Study 2 CISOs' sentiment was mostly opposed to the notion that government-authored guidance (i.e., resources authored by United States government agencies such as NIST, FTC, and Department of Homeland Security) is less effective for SBs than commercial guidance (see Figure 7). Notably, government guidance was described as being written in broad, all-encompassing language to address as many circumstances as possible, making interpretation challenging (sentiment also favored the proposal that this is the case). One participant (p2.05, an IT Manager with 10 years of experience) related, *"You have to really extrapolate a lot of what they are trying to say,"* and as a result *"most people really only find out what those* [government standards] *mean when they get audited, right?."*

In contrast, commercial guidance was often seen as tailored to expedite interpretation, but its quality was deemed less consistent and undermined by profit motives. p2.05 noted that filtering out overly-profit motivated advice required comparing multiple sources of information, which imposed extra work on SB IT staff. Also, commercial sources were deemed to benefit from only needing to describe limited types of relationships between software, allowing more specific and practical guidance on configuration. For example, p2.03 and p2.04 described commercial guidance similarly. p04 felt it was helpfully *"broken down in layman's terms,"* but vendors were often overcharging for guidance of limited value that could be *"too sales-y."* p2.03 (a university cybersecurity manager with fourteen years of SB CISO experience) concurred, noting that commercial guidance could be overly profit-driven and self-promoting, and that *"Most* [commercial] *infosec training, for its quality, is overpriced, and the cheap stuff is not worth taking."*

In comparison, p2.03 felt government guidance benefited from not having profit-motivated biases towards specific software or hardware. As a result of having *"no skin in the game"* (p2.03) government guidance offered broad security principles open to interpretation.

Mixed View of Government Guidance Usability Sentiment was evenly mixed on whether government guidance was overly technical or lengthy in its language. Slightly more dissenting concepts were described (n=11), noting that government authors were obligated to be comprehensive (n=8). Other CISOs pointed out that while the government corpus of guidance might be overwhelming to navigate (*"brutality to read,"*, p2.05), documents themselves were often right-sized for the subject matter (n=3). Others felt *"buried in standards"* confusing even for a graduate-level IT professional (p2.04), and struggled with *"ambiguous natural language"* (p2.09, an university cybersecurity trainer), *"grey areas"* (p2.05), and *"gobbeldy goop,"* only readable a few pages at a time (p2.07, a SB manager).

Comparatively, other CISOs felt that commercial sources had to be filtered for cost and profit-motivation, requiring more effort to compare sources. However, it also concisely addresses specific software relationships. p2.05 noted, *"You know they're able to apply it to a framework that has direct examples, right, because they own that intellectual property. . . . So at the end of the day I do think that commercial guidance is definitely better."*

Mierzwa and Scott (referenced previously regarding IT security obstacles) addressed sources for security guidance for non-profits and NGOs with many of the same critiques made by SB CISOs [22]. Mierzwa and Scott state, "The guidelines that do apply or could be implemented (such as NIST 800-53) are all often quite long and comprehensive, and complicated for small and medium-sized business (SMB), Non-Profits, and NGOs to implement. Non-Profits, NGOs and others would greatly benefit from simplifications or short implementation summaries of NIST and other frameworks." These conclusions are well supported by the themes drawn here, but we further qualify this with the expectations and hurdles to interpretation experienced by those applying the standards for SBs [22].

6.8 Favored Practices and Guidance Formats

We present Study 2 CISOs' 5-pt. Likert responses and coded discussion on two topics, IT best practices and guidance formats. Examples within the topics were nominated by Study 1 CISOs, based on what they deemed most effective for SBs in their direct experience. Given the sample size and inherent variation in their experiences, we did not test for significant differences in this data, instead focusing on using the responses for qualitative inquiry. The Study 2 CISOs evaluated and discussed nine SB IT best practices nominated in Study 1 (see Figure 8). The rationale for these responses often included the recognition that SBs could not afford *"to do it all,"* given implementation costs and must therefore prioritize among feasible practices. With the exception of subscribing to security information sharing services, all of the practices were viewed more favorably than unfavorably. Study 2 CISOs were also asked to respond to a similar list of seven IT security guidance formats that Study 1 participants had used with SBs (see Figure 9). Similarly, all except whitepapers were viewed more positively than negatively.

Parkin et al. also conducted a topically related examination of small and medium-sized business IT security implementation costs. Using a list of five recommended IT security practices (e.g., managing firewalls and gateways and patch management) drawn from the UK Cyber Essentials Scheme, indirect financial costs (often overlooked in similar research) were modeled for several SME archetypes (e.g., 1-person, micro, and small businesses) [27]. Several of these practices overlapped with the list of nine SB IT security best practices we gathered from our Study 1 CISO participants and reviewed with Study 2 participants. Interestingly, both lists suggested controls omitted by the other. Our CISOs suggested and rated highly (using a 5-pt Likert scale for SB efficacy) data backups which were not addressed by Parkin et al., while their modeling rated 2FA implementation as the most effective control to include, which was not nominated by our sample. Both studies addressed software patching, which CISOs ranked highly as a practice. Parkin et al. note that modeling of businesses of different sizes reveals that patching costs would increase with the size of the enterprise (and thereby reducing the adoption rate as a consequence) [27].

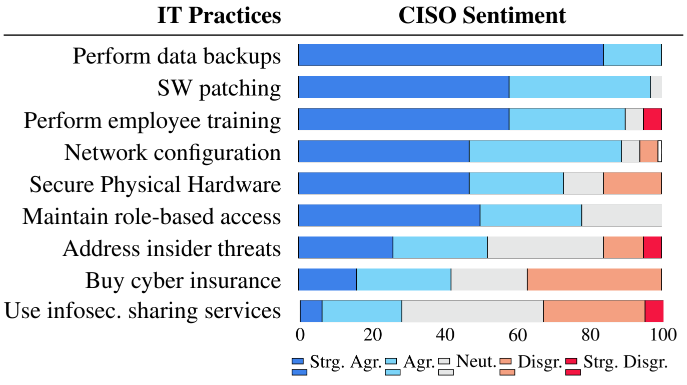

Figure 8: 5-point Likert response distributions from Study 2 CISOs, regarding the efficacy of nine SB IT practices nominated in Study 1

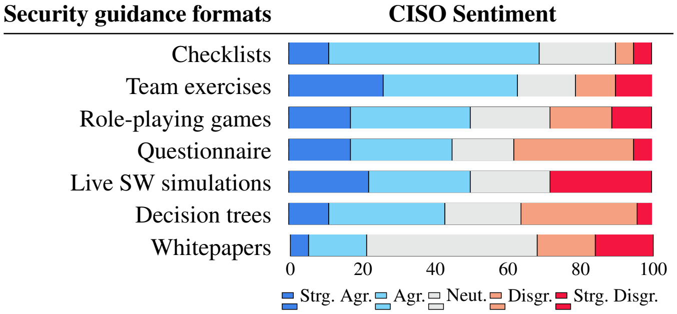

Figure 9: 5-point Likert response distributions from Study 2 CISOs, regarding the efficacy of nine SB IT practices nominated in Study 1

In the following section we further discuss the practical implications of several of the Study 2 responses regarding guidance formats and best practices.

7 Recommendations

These studies indicate several practical recommendations for those supporting SBs that draw on the discussion of IT practices and security guidance formats from Study 1 CISOs and vetted by Study 2 CISOs. This approach served to reinforce the timeliness, validity, and specificity of these implications. The detailed recommendations are also focused on the IT practices and guidance formats that scored highest for efficacy, suggesting these could contribute directly to existing SB CISO practices. The implications could also serve to inform researchers examining security issues of SBs and small-scale organizations (e.g., non-profit organizations) which lack the resources of larger enterprises.

7.1 Actionable Sentiment-Based Guidance Practices

We assessed Study 2 CISOs' sentiment towards a list of security guidance formats for SBs, derived from Study 1 commentary. Sentiment was mixed on all formats, including checklists, decision trees, whitepapers, questionnaires, role-playing games, team exercises, and live software simulations. However, there was slight negative sentiment towards whitepapers (attributed to their length and the limited time and technical knowledge of many SB owners), and slightly positive views on checklists and team exercises.

Checklist Efficacy for SB Security Guidance Participants differed in their view of checklists, a common basis for security auditing. Some favored the highly structured nature of checklists, which they felt helped organize numerous individual tasks. However, others saw the same brevity as a liability. The limited context proffered in a typical checklist item could allow misunderstanding, error, or bias in interpretation, which could in turn introduce risk in implementation. p03 (35 years old, largely self taught, 14 years of IT security experience, cybersecurity director for private company) stated there is *"too much emphasis"* on checklists when performing audits. SB IT staff may not know if a network map is current and correct (i.e., information for confirming checklist items may often be uncertain). Further, p03 stated, *"I'm working with auditors everyday... They'll come in with a checklist and go check-check-check... and I have no idea what they're actually working with. I'll just make sure all those policies are in place. This router's on. This router's off. Check-check-check... It's not actually doing anything except going through a checklist and doesn't really enhance the security beyond "they brought in a checklist." It's very rigid, very overblown... "* Similarly, p05 (30 years old, IT degree and on-the-job training, 10 years of IT security experience, Manager of Professional Services at a private company) felt checklists are *"easy to follow but... don't encapsulate reality."* These views suggest the need for reinforcing the diagnostic basis of security guidance in checklists. Providing examples and references to describe the intent of checklist items would help to alleviate the sort of ambiguity CISOs saw as the format's limitation.

Labeling Guidance's Target Audience To generalize, Study 2 CISOs at times seemed to want contradictory qualities from SB-tailored language. In discussion of themes relating to guidance they suggested SBs needed both highly simplified practical advice of the type proffered by commercial vendors, but also needed all-encompassing security principles of the type found in some government documents. We have endeavored to provide context illustrating that these views are not contradictory. They instead reflect differing needs among the many sizes and types of SBs that our cohort had directly supported. In turn, this suggests that security guidance should include aids to efficiently navigate the inevitable gradient of SB IT experience.

Firstly, security guidance can better serve by identifying who it is directed towards, in terms of resources and IT experience. Clearly, "mom-and-pop flower shop" SBs that self administer their own IT will need security guidance with different language from that of better funded SBs with in-house or consultant IT support. CISOs related that "micro" SBs with limited IT experience internet-searching for guidance face an overwhelming variety of sources. Prefacing advice with a clear declaration of the resources and experience needed for interpretation would allow SBs to more easily zero in on content appropriate to their needs.

Similarly, smaller SBs will need guidance in layman's terms with a clear priority structure, allowing the user to interpret the relative value of suggested security goals, with the assumption that not all will be immediately achievable.

Efficacy of Team-Based Exercises Similarly, Study 2 participants differed on using scenario-based exercises to present information security. Some felt role-playing games provided an effective shortcut to *"turn vague ideas into reality"* (p05), and develop consideration of potential costs and implications of a data breach or loss. Others felt that these type of exercises were simply too costly and time-consuming to be feasible for many SBs, and limited security-allocated resources would often be better spent elsewhere. p03 cited unrealistic terms in exercise scenarios as a common limiting factor in his experience, *"Yeah. Those are just garbage in a lot of instances. They don't even have a computer half the time. And they're just sitting and pretending "Oh, I'm the SOC operator. I would then do this." I have a very negative impression and experience with them. They're pretty ineffective."*

Study 2 CISO participants suggested a number of practices needed for worthwhile team-based exercises. Firstly, these events needed to involve both management and IT staff so that the business context of management decisions could be shared with IT staff, and IT security considerations shared in turn. It was noted that including both groups in exercises would raise personnel costs, but exposing business and security rationales among exercise participants was considered a key outcome of the practice. Additionally, participants in some cases doubted the cost-benefit of the practice if scenario content was not closely tailored to the business domain and financial reality of the participating SB. Without this extra exercise preparation, the value and learning potential of the practice was deemed to be reduced below the operating costs.

7.2 Optimal Timing of Security Messaging

A number of concepts were observed among Study 2 CISO participants regarding when SBs would be most receptive to messaging suggesting they take security more seriously. For example, p12 suggested that guidance and training exercises would be most effective when presented in the second or third financial quarter of the year, when companies typically would have completed tax projections. Potential costs from the security-related lessons learned could then be weighed immediately against available funds. On a longer timescale, p10 identified the second and third round of investor funding, at which point SBs might have achieved enough financial stability *"to breathe,"* and would be willing to finally evaluate needed security investments that were previously ignored to focus on *"staying lean and shipping product."*

Other participants pointed to frequent opportunities within common business processes to successfully insert security guidance. p13 suggested evaluation of IT purchases would be a key point of intervention for inserting the topic, either from within or outside a SB. p17 noted that guidance arriving after a purchase, that would impose further costs to rebuild the IT would be much less likely to succeed. Similarly, p15 saw no optimal point based on internal financial timing, but felt security-related hiring criteria for IT personnel was a valuable way to raise the profile of better security practices.

7.3 Including IT Within Emergency Planning

Several study participants suggested adding network security investment to basic continuity planning. This planning typically would already be both familiar to management and financially commensurate to SB resources. It was pointed out that many SBs are likely more aware of commonplace risk factors such as fire or natural disasters than online threats. Planning for important network security practices such as data backups and network-based continuity of operations could often easily piggyback on this acceptance of known risk factors. Messaging from CISOs to SBs on this practice could also be tailored to local continuity concerns (e.g., weather) and thereby comport with our finding on the efficacy of more *localized* security messaging (see Section 6.4). This was viewed as a way to promote consideration for more abstract and unfamiliar information security-related risks such as malware or ransomware incidents.

8 Limitations

Potential effects of several methodological aspects of these studies warrant review. Firstly, we sampled CISOs primarily in an area of the Mid-Atlantic region of the United States that includes significant activity in the IT security economic sector and government contracting. One participant (p1.01) made reference to the area as the *"cybersecurity Silicon Valley"* in light of this security focus, and others acknowledged that their IT investment outlook was colored by compliance to relatively stringent contracting requirements. As discussed in Section 5, we attempted to balance this feature of the sample by purposefully sampling CISOs from small business development organizations in other parts of the country.

Additionally, we acknowledge the sample sizes of the studies as a limitation. Smaller samples are unfortunately common when dealing with harder-to-reach populations, like small business CISOs. Our sample for Study 1 is, in particular, smaller than desired, but we mitigate this limitation by expanding the study and validating many of the responses (as well as invalidating other themes) as part of Study 2. Unfortunately, samples sizes of $n = 19$ are common for qualitative research [1, 13, 16], and we were able to reach saturation in themes with this sample.

9 Conclusion and Future Work

In this paper we explored obstacles and motivations experienced by IT security decision makers working with SBs. We identified often misunderstood areas of risk, and limits in corresponding IT protections. While SB CISOs depended on government-sourced security guidance, the technicality and size of this key resource was often found to be overwhelming. Insights and resulting implications from the work can be used to motivate and inform SB security, as well as support researchers interested in investigating this subject.

Study 1 and 2 CISOs made several testable assertions about the state of SB preparation and guidance that they use as a basis for suggesting SB security investment. An immediate line of inquiry derived from these findings will be to compare the coded CISO observations about guidance sources to real-world examples. Namely, we will compare those real world examples to coded observed themes regarding the usability and structural qualities of commercial and government guidance with examples. This may include features of those examples including the security subject matter chosen for small business audiences, as well as characteristics such as readability. We would also like to add to these comparisons the perspective of SBs owners themselves. This may be approached by think aloud and observation sessions with small business operators as they read and interpret security guidance sources. These extensions of this research would enhance the validity of the themes coded thus far by including qualitative assessment of the other factors and actors that CISO have proposed for us. This will capitalize upon our existing sentiment and coded discussion as a valuable starting point for understanding the intersection of small businesses and a hard-to-reach population of related security professionals.

References

[1] Noura Abdi, Kopo M Ramokapane, and Jose M Such. More Than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[2] Yasemin Acar, Christian Stransky, Dominik Wermke, Michelle L. Mazurek, and Sascha Fahl. Security developer studies with github users: Exploring a convenience sample. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 81–95, Santa Clara, CA, 2017. USENIX Association.

[3] Small Business Administration. Federal contracting, 2019. https://www.sba.gov/document/support--table-size-standards, 02/2020.

[4] National Cyber Security Alliance. Stay safe online, 2018. https://staysafeonline.org/stay-safe-online/free-online-security-checkups-tools/, 02/2020.

[5] National Cyber Security Alliance. Small business cyber target survey data, Oct 2019. https://staysafeonline.org/small-business-target-survey-data/.

[6] Debasis Bhattacharya. Leadership styles and information security in small businesses. *Information Management & Computer Security*, 19(5):300–312, 2011.

[7] Federal Communications Commission. Cybersecurity for small business, 2018. https://www.fcc.gov/general/cybersecurity-small-business, 02/2020.

[8] US Congress. S.1353 - Cybersecurity Enhancement Act of 2014, Public Law No: 113-274, 2014. https://www.congress.gov/bill/113th-congress/senate-bill/1353/text, 02/2020.

[9] US Congress. S.770 - NIST Small Business Cybersecurity Act, Public Law No: 115-236, 2018. https://www.congress.gov/bill/115th-congress/senate-bill/770, 02/2020.

[10] Critical Infrastructure Cybersecurity. Framework for improving critical infrastructure cybersecurity. *Framework*, 1:11, 2014.

[11] Deloitte. Beneath the surface of a cyberattack, Apr 2020. https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html.

[12] The Center for Cyber Safety, Risk Management Education, Executive Women's Forum on Information Security, Frost Privacy, and Sullivan. The 2017 global information security workforce study: Women in cybersecurity, March 2017.

[13] Kelsey R Fulton, Rebecca Gelles, Alexandra McKay, Yasmin Abdi, Richard Roberts, and Michelle L Mazurek. The effect of entertainment media on mental models of computer security. In *Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019)*, 2019.

[14] Susanne Furman, Mary Frances Theofanos, Yee-Yin Choong, and Brian Stanton. Basing cybersecurity training on user perceptions. *IEEE Security & Privacy*, 10(2):40–49, 2012.

[15] Atul Gupta and Rex Hammond. Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security*, 13(4):297–310, 2005.

[16] Julie M Haney and Wayne G Lutters. The work of cybersecurity advocates. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1663–1670, 2017.

[17] Julie M. Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. "We make it a big deal in the company": Security Mindsets in Organizations that Develop Cryptographic Products. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 357–373, Baltimore, MD, 2018. USENIX Association.

[18] Margareta Heidt, Jin P Gerlach, and Peter Buxmann. Investigating the security divide between sme and large companies: How sme characteristics influence organizational it security investments. *Information Systems Frontiers*, pages 1–21, 2019.

[19] Cyber Readiness Institute. The cyber readiness program, 2019. https://www.cyberreadinessinstitute.org/the-cyber-readiness-program, 02/2020.

[20] Jeff Kosseff. Positive cybersecurity law: Creating a consistent and incentive-based system. *Chap. L. Rev.*, 19:401, 2016.

[21] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–23, 2019.

[22] Stan Mierzwa and James Scott. Cybersecurity in non-profit and non-governmental organizations. *Institute for Critical Infrastructure Technology, February*, 2017.

[23] Tyler Moore, Scott Dynes, and Frederick R Chang. Identifying how firms manage cybersecurity investment. *Southern Methodist University*, 32, 2015. https://blog.smu.edu/research/files/2015/10/SMU-IBM.pdf, 02/2020.

[24] Donald F Norris, Laura Mateczun, Anupam Joshi, and Tim Finin. Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security and Emergency Management*, 2018.

[25] Daniela Seabra Oliveira, Tian Lin, Muhammad Sajidur Rahman, Rad Akefirad, Donovan Ellis, Eliany Perez, Rahul Bobhate, Lois A. DeLong, Justin Cappos, and Yuriy Brun. API blindspots: Why experienced developers write vulnerable code. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 315–328, Baltimore, MD, 2018. USENIX Association.

[26] Patrick O'Reilly, Kristina Rigopoulos, and Larry Feldman. Annual report 2017: NIST/ITL Cybersecurity Program. Technical Report Spec. Publ. 800-203, National Institutes of Standards and Technology, July 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-203.pdf, 02/2020.

[27] Simon Parkin, Andrew Fielder, and Alex Ashby. Pragmatic security: modelling it security management responsibilities for sme archetypes. In *Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats*, pages 69–80. ACM, 2016.

[28] Celia Paulsen and Patricia Toth. Small business information security: The fundamentals. US Department of Commerce, National Institute of Standards and Technology, 2016.

[29] Karen Renaud. How smaller businesses struggle with security advice. *Computer Fraud & Security*, 2016(8):10–18, 2016.

[30] Andreas Rivera. Cybersecurity: A small business guide, 2015. https://www.businessnewsdaily.com/7681-small-business-cybersecurity-issues.html, 02/2020.

[31] Moufida Sadok and Peter M Bednar. Information security management in smes: Beyond the it challenges. In *Human Aspects of Information Security and Assurance*, pages 209–219, 2016.

[32] Nilaykumar Kiran Sangani and Balakrishnan Vijayakumar. Cyber security scenarios and control for small and medium enterprises. *Informatica Economica*, 16(2):58, 2012.

[33] Big Threat Small Business. How protected is your small business?, 2019. https://smallbusinessbigthreat.com, 02/2020.

[34] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. Turning contradictions into innovations or: How we learned to stop whining and improve security operations. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 237–251, Denver, CO, 2016. USENIX Association.

[35] Moin Syed and Sarah Nelson. Guidelines for establishing reliability when coding narrative data. *Emerging Adulthood*, 3, 05 2015.

[36] Anas Tawileh, Jeremy Hilton, and Stephen McIntosh. Managing information security in small and medium sized enterprises: A holistic approach. In *ISSE/SECURE 2007 Securing Electronic Business Processes*, pages 331–339. Springer, 2007.

[37] Kevin Townsend. NIST Small Business Cybersecurity Act Becomes Law, 2018. https://www.securityweek.com/nist-small-business-cybersecurity-act-becomes-law, 02/2020.

[38] Chamila Wijayarathna and Nalin Asanka Gamagedara Arachchilage. Why Johnny Can't Develop a Secure Application? A Usability Analysis of Java Secure Socket Extension API. *Computers & Security*, 80:54–73, 2019.

[39] Patricia AH Williams and Rachel J Manheke. Small Business-A Cyber Resilience Vulnerability. In *International Cyber Resilience Conference*. School of Computer and Information Science, Security Research Centre, Edith Cowan University, Perth, Western Australia, 2010.

Appendix

A Demographic Tables

Study 1 can be found in Table 1, and Study 2 can be found in Table 2.

Table 1: Study 1 participants' demographics

Partic. #	Role
p01	IT consultant to county-level SB council
p02	Federal-level SB IT security manager
p03	Private SB CISO consultant
p04	Private SB CISO consultant
p05	County-level SB development officer
p06	Private CISO consultant to SBs
p07	County-level SB IT security consultant
p08	State-level SB IT security manager

Table 2: Study 2 participants' demographics, including participant number, years of IT information security experience, the employee count of the smallest SB with which they have direct CISO experience, the work domain with which they have most recently had direct CISO experience, and source of their CISO knowledge (BS/MS/PhD = Bachelor/Masters/Doctorate of Science, EE = Electrical Engineering, CS = Computer Science, IS = Information Security, Cyber = Cybsersecurity, Certs. = information security certificate programs, OJT = on the job training, ST = self taught.)

#	Yrs. Exp	Smallest SB Exp.	Recent SB Domain	CISO Training
p01	24	1	Cybersecurity	BS.EE, OJT
p02	5	5	Cybersecurity	BS/MS/PhD.CS, OJT, ST
p03	14	180	CS contracting	OJT
p04	4	40	Education	ST, MA.IS
p05	20	1	Medical	BS.CS, OJT, ST
p06	20	1	Education	ST, Certs.
p07	20	10	Software	OJT, ST
p08	20	300	Cybersecurity	BA/MS.EE, OJT, ST
p09	20	6	Education, cybersecurity	Certs., PhD.IS
p10	2	15	Education, cybersecurity	ST
p11	2.5	NA	Non-profit, education	BA.EE, OJT
p12	20	40	Systems Integration	Certs., OJT, ST
p13	8	NA	Research	OJT
p14	15	15	Education, cybersecurity	MA.Cyber, OJT, ST
p15	3	50	Professional services	OJT
p16	19	20	Cybersecurity	Certs., OJT, ST
p17	30	50	Education	OJT, ST
p18	7	10	Education	Certs., OJT, ST
p19	25	3	Cybersecurity	Certs., OJT, ST
Avg.:	**15 (SD 8.6)**	**44 (SD 78.6)**		

B Study 1: Initial CISO interviews Survey Instrument

1. Can you please tell me a little bit about your background in information security, i.e. how you got into the field, how long you've been doing this, where you learned the essentials?
2. Assuming that the time and financial resources of most SBs are highly constrained, and focused on achieving profitability, how do they manage their infosec responsibilities?
3. In your experience, what are SBs' biggest motivations and biggest obstacles with regard to infosec?
4. How much understanding of infosec risk and privacy implications do SBs typically have?
5. What infosec education sources are there for SBs? How effective are they?
6. In your opinion, what infosec and privacy education gaps are there for SBs?
7. What types of compliance issues do SBs deal with?
8. What's the typical level of legal knowledge in SBs that you

have seen?

9. How does a SB's domain (e.g., "feds, eds, and meds") impact their handling of infosec and privacy issues?
10. How well does existing infosec/privacy guidance (e.g., legal, insurance, administration) help SBs?
11. What difference do you see in the effectiveness of commercial (e.g., industry threat reports) vs. government (e.g., NIST protocols) infosec/privacy guidance for SBs?
12. What do SBs think about risks with using 3rd party services and tools for security and data management (e.g., cloud based SaaS)?
13. What infosec investment areas/gaps are there for SBs?
14. How do insider threats like embezzlement, IP theft, employee poaching/acquisition fit into the threat picture for SBs?
15. What threats do SBs tend to underestimate? Overestimate?
16. What are the insurance implications for SBs?
17. Is there a reference system for classifying SBs by their cybersecurity profile (risk, exposure, domain, etc.)?
18. The news frequently mentions challenges to end users' privacy from large data and social media companies. In your experience, how do business considerations balance making money off of client data and those same clients' privacy and info security?
19. What types of aids would really help inform SBs about infosec/privacy issues? (i.e. checklist, decision-trees, whitepaper, questionnaire, role-playing games, team exercises)
20. What has helped inform SBs on this topic in your experience?
21. What types of help have not worked as well?
22. What types of aid do you use now to inform SBs, either about infosec/privacy or other issues (taxes, insurance, licensing, etc.)?

C Study 2: Follow-up CISO interview instrument

Demographic questions:

1. Can you tell me your age and identified gender please?
2. How many years of IT security management experience do you have?
3. What is the smallest company size, in number of employees, for which you have made IT security decisions?
4. What was the primary source for your IT security-related knowledge (e.g. degree or certificate program, employer training (including military or industry), self-taught, or other (please describe)?
5. What is your current job title?

Agreement questions (Rate agreement on scale 1-5, and explain view if possible):

6. "The resources of SBs are too limited to properly manage information security responsibilities."
7. "The main reason SBs improve their information security is something bad happens with those issues."
8. "The main reason SBs improve their information security when they hire or contract for IT services."
9. "The main reason SBs improve their information security is to comply with security audits as a sub-contractor."
10. "SBs have adequate education sources for information security."
11. "SBs have affordable education sources for information security."
12. "The information security problems suffered by SBs are more their own fault than the fault of outside parties (for example service providers, software vendors, insurers, cyber criminals, law enforcement, government, etc.)."
13. "SBs understand the regulatory implications of information security issues related to their operations."
14. "SBs understand the insurance implications of information security issues related to their operations."
15. "SBs understand the financial implications of information security issues related to their operations."
16. "Commercial guidance on information security for SBs (e.g., industry threat reporting) is more effective than government guidance."
17. "Government guidance on information security (e.g., NIST protocols) is too broadly written to be useful to SBs."
18. "Government guidance on information security is too technical to be useful to SBs."
19. "Government guidance on information security is too lengthy to be useful to SBs."
20. "3rd party data management tools (e.g., cloud-based SaaS) are helpful to the information security practices of SBs."
21. "News reports about information security problems have changed how SBs think about their operations."
22. "Information security regulation from either federal, state, or local government has changed how SBs think about their operations."
23. "Information security tax incentives from either federal or state government have changed how SBs think about their operations."
24. "Commercial information security consultants have changed how SBs think about their operations."

Infosec practices question

25. Please rate each of the following issues or practices for their importance to the information security of SBs (on a 1-5 scale, explain as possible): Securing hardware devices (laptops, phones, etc.), Network configuration, Patching software, Insider threats (embezzlement, theft, etc.), Data backups, Insurance coverage for data loss or hacking events, Employee information security training, Role-based access controls, Subscription based info sharing services

Infosec guidance question

26. Please rate the following formats for information security guidance for SBs for their effectiveness (on a scale from 1-5, explain as possible): Checklists, Decision trees, Whitepapers, Questionnaire, Role-playing game, Team exercises, Live SW simulations

D Study 2 Codebook

1. *Study 1 theme - Causes of SB resource limitations*

   (a) Topic - SB resources are too limited

i. Agree - SBs don't have the resources to do ITsec properly
ii. Agree - SB resources limited by complexity
iii. Agree - SB resources limited by cost
iv. Agree - SB resources limited by SBs being too focused on biz survival
v. Neutral - SBs can overcome limits
vi. Disagree - Just harder for SBs than LMEs
vii. Neutral - Mandate missing/coming to force SB ITsec improvement
viii. Neutral - SBs need best practices not tools
ix. Neutral - SBs need more automation

2. *Study 1 theme - SB reasons to improve (reactive, incidental, compliance)*

(a) Topic - SBs improve reactively to bad news

i. Agree - Are primarily reactive to bad event
ii. Neutral - Depends on events
iii. Disagree - Other reasons

(b) Topic - SBs improve incidentally with new IT

i. Agree - Primarily improve due to IT updates
ii. Neutral - Depends on IT service
iii. Disagree - Going for new SaaS, not security (score as agree)
iv. Disagree - Have other reasons generally
v. Disagree - New IT doesn't automatically improve

(c) Topic - SBs improve to comply with audits

i. Agree - Primarily improve for compliance
ii. Neutral - Not sure
iii. Neutral - True but many examples of fake compliace
iv. Disagree - Doesn't apply to many
v. Disagree - Compliance checklist problem

(d) Topic - Other motivations for SB ITsec improvment

i. Influenced by peer networking
ii. Market trends
iii. Awareness campaigns
iv. Depends on SB's threat model, e.g. has own IP, broker PII
v. Compliance only, customers don't incentivize

3. *Study 1 theme - Available guidance (adequate, affordable)*

(a) Topic - SBs can find adequate guidance

i. Agree - resources are available
ii. Neutral - Resources there but must dig deeper to address issues
iii. Disagree - Most don't know right place to begin
iv. Disagree - More marketing than best practices
v. Disagree - Subject is too complicated
vi. Agree - But have to know where to start and what to ask for first

(b) Topic - SBs can find affordable guidance

i. Agree - resources are affordable
ii. Disagree - Cyber training or hiring is needed, and costly
iii. Neutral - Free cyber certs aren't as well regarded as more expensive accredited ones, which aren't tenable cost-wise for most
iv. Neutral - Free resources still have opportunity costs in time and manpower
v. Neutral - ITsec awareness free, but countermeasures very expensive

4. *Responsibility for SB vulnerability*

(a) Topic - SB infosec trouble is their own fault

i. Shared fault, IT often under funded in SBs, but SW and hardware often flawed, not securely configured OOTB, ITsec personnel hard to find
ii. Agree - Don't pay attention until impacted, just focused on profitability
iii. Agree - SBs must have ITsec knowledge to function with client data
iv. Disagree - Happens to all size orgs not just SBs
v. Disagree - Depends on service agreement
vi. Disagree - So many vectors that can't be up to SBs to manage ITsec
vii. Make money off personal info
viii. Disagree - Threat migrating at scale from harder big targets down to SBs
ix. Affordability of ITsec hurts SB preparation

5. *Study 1 theme - SB understanding of ITsec issues*

(a) Topic - SBs understand ITsec regulation

i. Disagree - Regs are vague and confusing, even for IT personnel
ii. Disagree - Regs only apply to a few fields (med, financial, etc.)
iii. Agree
iv. Neutral
v. Regs confusing for IT personnel
vi. M/LBs struggle also
vii. Speaking for self as cyber co - Agree - drink own Kool Aid

(b) Topic - SBs understand ITsec insurance

i. Disagree - SBs don't understand
ii. Disagree - SBs unaware of cyber ins.
iii. Disagree - Most SBs couldn't negotiate clauses
iv. Agree -
v. Neutral - Not sure
vi. Neutral - Same issues in M/LBs also
vii. Cyber insurance has loopholes, is evolving

(c) Topic - SBs understand ITsec financial costs

i. Neutral - SBs know there are ramifications but limited scope
ii. Agree - Aware of potential damages but not accurate sense of prevention ocsts
iii. Agree - Have to operate at risk anyway
iv. Disagree - Weak link in SB, unaware of risks, fines, costs, GDPR compliance, etc.

6. *Study 1 theme - Com vs gov guidance issues*

(a) Topic - Commercial guidance is more effective than gov

    - i. Agree - Commercial more detailed, better formatted
    - ii. Disagree - Both are ineffective unless SB is motivated by bottom line
    - iii. Disagree - No equivalent to gov in com for breadth and influence
    - iv. Disagree - Varies by industry
    - v. Disagree - no-cost gov guidance is more effective because its where SB will start
    - vi. Disagree - Gov has "no skin in the game" with profit motive, so offers more impartial guidance
    - vii. SBs need to be motivated to use any guidance
    - viii. Neutral - both effective com and gov guidance exists
    - ix. Neutral - both bad

  - (b) Topic - Government guidance is too broad
    - i. Agree - gov guidance states principle, not specific method for a ITsec control
    - ii. Disagree - Gov's guidance method (stating principles over practice) is correct approach
    - iii. Com guidance doesn't cover as many potential issues, is more specific and direct
    - iv. Disagree
    - v. Disagree - Gov guidance broadness varies
    - vi. Neutral - Expected

  - (c) Topic - Government guidance is too technical
    - i. Agree - Too hard for SBs
    - ii. Neutral - technical level varies
    - iii. Commercial guidance more plain English
    - iv. Disagree - Right level

  - (d) Topic - Government guidance is too lengthy
    - i. Disagree - Gov trying to be comprehensive
    - ii. Disagree - Gov corpus is huge, but individual docs can be right-sized
    - iii. Com is more direct and specific
    - iv. Agree - Too long
    - v. Agree - many controls, have to know what applies, can be overwhelming
    - vi. Neutral
    - vii. Neutral - OK length and detail but need wizard to aid security control

7. *SBs helped by outsourcing IT*
  - (a) Topic - 3rd SaaS helps SB ITsec
    - i. Agree - better than in-house
    - ii. Also increases SB exposure if SAS vendor gets hacked
    - iii. Disagree - Hard to know what you're getting and lots of breaches
    - iv. Neutral - Depends on vendor
    - v. Allows more focus on business instead of difficult security solutions
    - vi. Costly for reliable vendors

8. *Study 1 theme - Influences on SB ITsec*
  - (a) Topic - News reports influence SB ITsec
    - i. Agree - don't want to be next victim
    - ii. SBs may feel they're too small to be targeted
    - iii. Disagree - Other reaons
    - iv. Disagree - News is sensationalized
    - v. Primarily motivated by risk to name

  - (b) Topic - Regulation influences SB ITsec
    - i. Agree - regulation making more impact
    - ii. Agree - depends on industry by CC and HIPAA have matured significantly
    - iii. Disagree - Not paying attention if not critical to biz focus
    - iv. Neutral - Takes time to have effect
    - v. Neutral - Don't know
    - vi. Neutral - Depends on industry

  - (c) Topic - Tax incentives influence SB ITsec
    - i. Neutral - Wasn't aware of any
    - ii. Agree -
    - iii. Disagree - Too few to make difference
    - iv. Disagree - Taxes too confusing
    - v. Neutral - Don't know

  - (d) Topic - ITsec consultants influence SBs
    - i. Agree - Might be junk mail but makes impact
    - ii. Disagree - Other reasons
    - iii. Disagree - most don't cater to SBs
    - iv. Neutral - Not sure