Mind the Gap: Revealing Security Barriers through Situational Awareness of Small and Medium Business Key Decision-Makers

Yuanhaur Chang[†], Oren Heller[†], Yaniv Shlomo[†]
Iddo Bar-Noy[§], Ella Bokobza[†], Michal Grinstein-Weiss[†], Ning Zhang[†]
[†] *Washington University in St. Louis, MO, USA*
[§] *Israel National Cyber Directorate*

Abstract

Key decision-makers in small and medium businesses (SMBs) often lack the awareness and knowledge to implement cybersecurity measures effectively. To gain a deeper understanding of how SMB executives navigate cybersecurity decision-making, we deployed a mixed-method approach, conducting semi-structured interviews (n=21) and online surveys (n=322) with SMB key decision-makers. Using thematic analysis, we revealed SMB decision-makers' perceived risks in terms of the digital assets they valued, and found reasons for their choice of defense measures and factors impacting security perception. We employed the situational awareness model to characterize decision-makers based on cybersecurity awareness, identifying those who have comparatively low awareness in the fight against adversaries. We further explored the relationship between awareness and business attributes, and constructed a holistic structural equation model to understand how awareness can be improved. Finally, we proposed interventions to help SMBs overcome potential challenges.

1 Introduction

Small and medium businesses (SMBs) contribute significantly to the global economy. According to the World Bank, SMBs represent 90% of businesses and over 50% of employment worldwide [3]. However, cybersecurity poses significant challenges for SMBs, which often lack the resources and expertise to combat sophisticated cyber threats. With limited budgets and no dedicated IT security teams, these businesses struggle to keep up with evolving security protocols, increasing their vulnerability to data breaches and financial losses. This not only impacts their own operations but also poses risks to larger organizations they may be connected with. In Israel, SMBs are responsible for 39% of national employment [32], though they are mostly unprepared against cyber-crimes. In 2023, 33,000 SMBs have fallen victim to cyber incidents, with 21% of those suffering major or irrecoverable damage [37].

Gap in Existing Work and Our Focus. Recognizing the importance of the topic, there has been a significant amount of attention to understand the security practice of SMBs [1, 9, 11, 13, 23]. However, the focus has been either on understanding cybersecurity policy and implementations from both employees' perspectives [26, 38] and the IT counselors' perspectives [41], but not from the key decision-makers themselves. While prior studies provide important information on the current state-of-the-art cybersecurity practices in SMBs, there are still gaps in translating from the measurement of security hygiene to understanding the key obstacles for maximizing the appropriate cybersecurity protection for business operations. Therefore, an in-depth understanding of decision-makers' perceptions and decisions in the context of different business characteristics is essential, particularly for implementing effective interventions to fundamentally shift the posture of SMB cybersecurity at a societal scale.

Key Research Questions. To facilitate the development of interventions and motivate key decision-makers to adopt a security-aware mindset, we aim to develop an in-depth understanding of how decision-makers make cybersecurity decisions. We constructed four research questions that drove the measurement process and the corresponding analysis:

- **RQ1:** What are key decision-makers' perceived cyber threats and risks for SMBs?
- **RQ2:** How do key decision-makers perceive cyber defenses and their impact on company operations?
- **RQ3:** What factors influence key decision-makers' security perception?
- **RQ4:** What perceived roadblocks hinder better security?

Contribution 1: Specific assets, protections, and factors of influence from semi-structured interviews. Through our semi-structured interviews with 21 key decision makers, we identified the actions implemented and the potential challenges faced by SMBs. We inductively coded these responses, reporting themes and factors they kept in mind when directing cybersecurity implementations. The findings also served as a foundation for the quantitative study.

Contribution 2: Correlation between business attributes and situational awareness. Building on the understanding

from the interviews, we used quantitative analysis to further verify how the identified elements and challenges can affect situational awareness. We recruited 322 decision-makers to understand how they perceive cyber threats in the real world. We closely examined whether and how decision-makers' perceptual awareness of cybersecurity issues is correlated with the characteristics of their businesses. We predicted the awareness issues that a business with certain characteristics would likely face, and characterized decision-makers according to their situational awareness.

Contribution 3: Holistic SEM modeling SMB decision-making. We constructed a structural equation model (SEM) [22] that helps to visualize the causality between factors impacting decision-maker's security mindset, drawing forth a connection between reasons and eventual cybersecurity awareness. This mapping can help future researchers develop effective interventions that tackle the obstacles faced by SMBs, enable informed decision-making, and facilitate usable business management.

Contribution 4: Root causes and roadblocks towards secure SMB. Reflecting on the semi-structured interviews as well as the findings from the survey studies and the SEM, we identified the potential roadblocks that prevent key decision-makers from reaching comprehensive situational awareness. We discussed several interventions that may be deployed to address these roadblocks, and hope to mitigate the perceptual biases and increase awareness of SMB key decision-makers.

2 Background and Related Work

Situational Awareness (SA). Understanding the factors affecting SMB decisions can be invaluable for creating incentives that reinforce secure behavior while dismissing misconceptions regarding cybersecurity. To this end, Renaud et al. [36] extended Endsley's theory of SA [17] to build a framework in the cybersecurity domain. In our work, we thoroughly examined SMB key decision-makers' security awareness, delving deeper into understanding the "what" and the "why" that causes low awareness while also drawing correlations between awareness and eventual cybersecurity installment. To the best of our knowledge, our work is the first to systematically study the relationship between perceptual beliefs and business actions of SMB key decision-makers.

Endsley's SA theory, widely used to model human decision-making in critical situations [18, 39], suits this study because cybersecurity threat operations require SMB decision-makers to contextualize threats/vulnerabilities according to current situations to actively defend their business. Previous studies have used SA models to analyze security perception and propose solutions in the context of eHealth [4], network security [24, 42], scamming scenarios [25], or mixed reality systems [10], though none focused on SMBs. As shown in Figure 1, our RQs can be mapped to the three levels of SA. The first level of Endsley's theory is *perception of elements in the current situation*, which from the perspective of cybersecurity, involves both the threat model and security mechanisms. Therefore, RQ1 and RQ2 are designed to gain a better understanding of business decision-makers' perceptions of these two important elements. Building on the perception of elements, the second level is the *comprehension of the current situation*, which puts together the perceptions of all the elements in the context of SMBs. Therefore, RQ3 targets the decision-making process, which requires comprehension and composition of all the key elements in the current cybersecurity situation. The last level focuses on the *projection of future status*. Understanding the gap is important, but coming up with actionable steps to improve the status quo is the ultimate goal. RQ4 focuses on understanding the challenges and plausible paths forward to address SMB's security challenges.

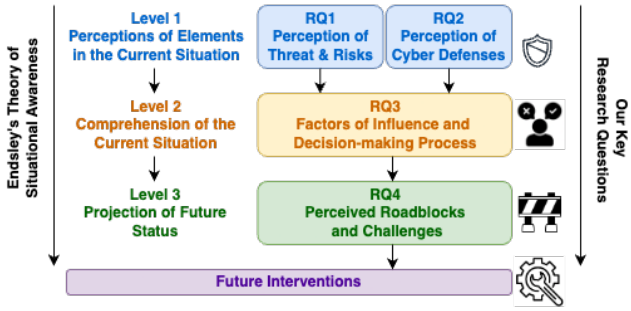


Figure 1: SMB cybersecurity with Endsley's theory of SA.

SMB Cybersecurity. Prior work often stresses the stringent need for cybersecurity research in SMBs, pointing out that it is imperative for SMBs to have the ability to detect, respond, and recover from cyberattacks [1, 11]. For instance, Chen et al. [9] discussed the current state of SMBs and how they interact with emerging cyber threats, as well as various regulations currently in place and the changes necessary to ensure compliance among businesses. De Smale et al. [13] studied how organizations condensed and filtered known vulnerability information. Unfortunately, the result was that no organization tried to acquire a comprehensive view of published vulnerabilities, but relied on a single source. While these works offered a view of the security practices of SMBs, they did not consider the diverse intrinsic characteristics of the businesses under study. Meanwhile, our work bridged the gap by investigating the panoply of SMBs in the full spectrum of technology exposure and business attributes.

One line of existing work studied SMB cybersecurity through the perspective of a single stakeholder [2, 26, 38, 40, 41]. For example, Wolf et al. [41] uncovered security obstacles from the perspective of Chief Information Security Officers (CISOs), regarding them as third-party observers of the actions of SMBs. On the other hand, Stegman et al. [38] surveyed employees' concerns over ambiguous data collection through enterprise security software. Recognizing that SMB executives often juggle multiple issues that could affect the fate of the company [34], an in-depth understanding

Table 1: Demographics of SMB Key Decision-Makers and Business Characteristics

Business Characteristics				Interviewee Info.			Operational Aspect				Technological Aspect			
#	Economic Sector	*Size	Digital Assets	Yrs. of Exp.	Gender	IT Exp.	Activity Abroad	Regulation Requirements	Outsourced Sec. Consult	WFH	Website	Ecommerce	Cloud Storage	CRM
P1	Accommodation and food services	M	Employee Data	6	M				✓		Informational		✓	✓
P2	Manufacturing	S	Operational Data	22	F				✓		Informational			✓
P3	Administrative and support service activities	S	Customer Data / Operational Data	6	M				✓		-		✓	
P4	Financial and insurance activities	S	Customer Data / Operational Data	-	F				✓	✓	-		✓	✓
P5	Financial and insurance activities	S	Customer Data	9	M				✓		-		✓	✓
P6	Construction	M	Intellectual Property / Operational Data	-	F				✓		-		✓	
P7	Information and communication	S	Intellectual Property / Customer Data	-	M		✓			✓	Informational / Online Service		✓	✓
P8	Manufacturing	S	Operational Data	29	M		✓		✓		Informational / Online Service	✓		
P9	Information and communication	S	Intellectual Property	-	M	✓	✓			✓	Informational		✓	
P10	Wholesale and retail trade	S	Operational Data	20	F				✓	✓	Online Services	✓	✓	
P11	Information and communication	S	Customer Data	-	F		✓	✓		✓	Online Services		✓	
P12	Professional, scientific and technical	S	Operational Data	16	M		✓		✓	✓	Online Services		✓	
P13	Accommodation and food services	S	Customer Data	10	M			✓	✓		Online Reservations	✓	✓	
P14	Professional, scientific and technical	M	Employee Data / Operational Data	5	F	✓				✓	Informational		✓	
P15	Accommodation and food services	S	Customers data	25	F				✓	✓	Online Reservations	✓	✓	
P16	Professional, scientific and technical	S	Customer Data	20	M	✓				✓	-		✓	✓
P17	Information and communication	S	Customer Data	18	M	✓		✓		✓	Informational		✓	✓
P18	Manufacturing	M	Operational Data	15	M	✓	✓			✓	Informational		✓	✓
P19	Professional, scientific and technical	S	Intellectual Property / Operational Data	4	M	✓	✓	✓	✓	✓	Informational		✓	✓
P20	Information and communication	M	Intellectual Property / Operational Data	2	M	✓		✓	✓	✓	Online Services		✓	✓
P21	Manufacturing	M	Operational Data	23	M				✓		Commercial	✓		✓

*Size: Small (S) - 6 to 50 employees, Medium (M) - 51 to 100 employees; WFH: Work from home

of SMB cybersecurity efforts from the key decision-maker's perspectives is essential. However, findings from previous research lack context for cybersecurity decision-making and their impact on decision-makers' responses to cyberthreats is unknown [2,21,23,40]. To this end, our work explored factors and challenges influencing decision-makers' perceptions of their cybersecurity status. We addressed the lack of adequate sample size in prior work by conducting large-scale studies with a diverse set of SMBs and key decision-makers.

3 Interview Study

To understand how decisions are made in SMBs and to obtain a framework for the main survey development, we conducted an interview study exploring how SMB executives navigate cybersecurity decision-making. Our study was formally approved by the Institutional Review Board (IRB).

Recruitment Method. Our study was conducted in Israel. To capture a representative sample of key decision-makers whose business belongs to different economic sectors as defined by ISIC Rev 4 classification [29] of the United Nations, we recruited through commercial records while meeting the definition of SMBs [1]. We define key decision-makers as people who hold the mandate for cybersecurity policies in the business, including owners, CEOs, CTOs, Vice Presidents, and managers who report directly to the CEO or the owner of the business. We carefully selected the key decision-makers and businesses, ensuring that our sample was diverse and representative in terms of SMB characteristics. Businesses that are not privately owned were excluded. In the end, 21 key decision-makers were recruited. Participants were happy to volunteer and were not compensated. Demographics of decision-makers and their businesses are shown in Table 1.

Interview Process. We followed a semi-structured interview protocol for the study, allowing the interviewer and the interviewees to raise and explore new issues when possible. After obtaining the participant's informed consent, the interviewer would ask questions using the interview guide in Appendix A.

Limitations. Participants may be subjected to self-selection bias. There may also be potential self-report bias, where discrepancies may exist between the decision-makers' perception and the actual situation. Social desirability bias may also cause decision-makers to report better security practices than they actually have to make their business look better.

Ethical Considerations. Before the interview, participants were given the research description and signed a consent form. All interviews were conducted in Hebrew and recorded. The recordings were then transcribed and translated by the research team for analytical purposes. Confidentiality and anonymity were given careful attention, and each participant in the study received a unique research ID number. We refrained from including identifiable information in our results.

Thematic Coding. We deployed thematic analysis [6] to identify themes that help answer our research questions. Two coders independently went over the transcripts, noting and refining the initial set of themes and codes. The themes and codes were then discussed iteratively and the differences were resolved until all coders reached an agreement on the final codebook, which is presented in Appendix D and used to code all responses. We use this categorization in the second part of the study for survey development and quantitative analysis.

4 Interview Results

In this section, we summarize key decision-makers' perceived risks based on digital assets (§ 4.1) and defense deployment (§ 4.2), which are important elements to discuss for level 1 situational awareness. We summarize key decision-makers reasons for the chosen defenses, as well as the factors influencing their security perceptions (§ 4.3, § 4.4). Through these,

[1] Businesses with 6-100 employees and 10M-100M NIS annual revenue.

we identify various root causes of insecure SMBs.

4.1 What digital assets are SMB key decision-makers concerned about?

Security is ultimately a process of risk minimization, since there is no perfectly secure system. As a result, the first step towards helping SMB decision-makers achieve better security is to understand what are the essential assets they deem valuable and wish to protect. This gives us a perspective of how decision-makers perceive their current cybersecurity threats.

Customer data for secure services. The most prevalent information SMB executives deem as important digital assets are customer profiles and data. For individual customers, SMBs may need to securely preserve *"delivery certificates and the contract of the services (P3)"* up to a certain time. In addition, for SMBs working in the healthcare sector, the security of personal health information is of great concern. P11 noted, *"Theoretically, someone could break into our system and change the instructions for the patient and cause the patient to be treated incorrectly."* For customers who are companies, sensitive financial information may leak out due to malpractice or attacks. For instance, P4 expressed concern in handling customer bank credentials for tax purposes, *"I have 300 clients, most of them companies. I need to log into the bank account. I received a password, and some of them gave access not only to viewing but also to making transactions. Even if not maliciously something can happen."*

Employee data for efficient management. P1, who owns a restaurant, indicated that he heavily relies on apps to manage his restaurant. The apps allow him to efficiently manage employees, shifts, and salaries, helping him minimize managerial costs. *"For me, the data is a major asset. In the first years before I had this data gathered things were more challenging."*

Operational data for service availability and safety. Some decision-makers stated that assets essential to company service should be protected since the lack or leakage of those can cause major operational issues. Many participants mentioned having a website to promote their business or as a means of communication with customers. The availability of websites is particularly vital for SMBs who utilize them as major channels for customer interaction. For P12, who runs a survey company, *"A server crash in our company in the past silenced my activity for a few hours. In our world, this is critical because usually within 24 hours the survey needs to be closed and the information received."* Meanwhile, in a factory setting, P18 is worried about the access control of their operational technology. *"There are quite a few things here, from sophisticated machines to raw materials. It definitely needs to be protected and if someone gets into [the system] they can activate a lot of things."*

Intellectual properties for business competitiveness. Besides the digital assets mentioned above, SMBs often have intellectual properties or business secrets that they need to protect. P6, who is the owner of a construction company, worried that their engineering plans will be stolen. In addition, owners who work in the information and communication sector expressed more concerns over the algorithms in their software development projects than customer information, stating *"Mainly the code [should be protected] because we don't have customer information that could expose us to lawsuits. The fact that you work with a client is no secret." (P9)*

Discussion: These four major categories mentioned in participants' responses point out the different concerns decision-makers have according to different types of assets. These assets are seen to be directly related to the working and availability of company services, and if compromised, may lead to significant financial loss. A key observation is that a business with more diverse digital assets may face a larger threat surface. In other words, the *technological intensity* of a business can affect decision-makers' perception of threats and risks.

4.2 What defensive measures do SMB key decision-makers choose (not) to deploy?

Also related to decision-makers' level 1 situational awareness is the perception of security mechanisms and the reasons behind deployment decisions. Understanding the thought process behind defense decisions can help identify where potential misconceptions may need to be corrected, as well as where knowledge may be lacking to improve security defenses.

Backups are important for operation. When asked about how the company protects its digital assets, almost all the participants reflected on either having local and remote backups or hosting all of their services on the cloud. P3 said, *"[Everything] is saved on local drives and on the cloud. Everything is also printed and saved in binders."* However, other than stating this defensive measure, we observed that most decision-makers do not care to understand the details of the operation. In general, participants tend to have a false sense of security about hosting their service on the cloud, believing that whatever is on the cloud is backed up and secure. P14 shared his strategic consulting experience and concurred, *"Even when it is possible to negotiate terms of backup from the providers, customers are not aware of their options."*

Divided opinion on employee training. Some SMB executives require their employees to receive training or follow certain rules while handling business operations. For instance, P18's company conducted "mock attacks" to familiarize employees with phishing scams. *"Lectures are quite boring, in my opinion, you don't take anything from it, at best you remember some nice gimmick. That's why what we do is send scams from an external email and then check who fails."* In addition, P14 spends a great effort raising security awareness among the employees, sending out monthly newsletters to employees to update them on recent incidents and requiring employees to provide comments and feedback.

On the other hand, some business owners adopted a more fatalistic viewpoint and believed there was no value in implementing employee training, as it was too difficult even to identify the source of the issue. Owners who made this decision are eager to "get back to normal". P5 reasoned, *"Security is always delegated to professionals. We didn't see any point [to do training] because we can't help and the attack already happened. We just wanted to return the office to function."*

Minimal effort on firewall, antivirus software, and guideline implementation. Only decision-makers who are more tech-savvy or have a higher security awareness would allocate budgets annually for cyber defenses, such as setting up firewalls and renewing antivirus software licenses, while following security standards if the nature of their company demands so. P20, who runs a software company, mentioned having developed incident response plans with scenarios that allow all employees and management to understand what to do if the company is being attacked. Moreover, P16 shared his opinion as to why some SMBs neglect to renew their antivirus licenses, *"They are not stingy. They simply save every shekel because small businesses in Israel are suffocating from the economic burden. They want to see the security people work because otherwise, they don't feel comfortable paying."*

Discussion: While decision-makers understand that some degree of defensive measures needs to be deployed, they tend to only do the bare minimum to save the already strained budget and time. There also exist large misconceptions about the extent or the effectiveness of the employed protections, such as cloud services are guaranteed to be safe and secure. The root cause of this oversight could be largely due to the *lack of technological orientation and innovation*.

4.3 What sources of information do SMB key decision-makers rely on?

Apart from digital assets and security measures, sources of decision-makers' cybersecurity knowledge can influence how they comprehend SMB's security status and make decisions, which is captured by Endsley's level 2 situational awareness. As seen in § 4.1 and § 4.2, much of the decisions on defense and their effectiveness rely on accurate comprehension of threats by the key decision-makers. Therefore, it is imperative to identify sources that may be unreliable.

Expert Guidance. Some key decision-makers seek advice from or outsource the task to dedicated agencies specializing in computer services. We observed that the frequency of interaction between SMB and the agency is surprisingly low, mostly reporting to be *"once every six months (P10)"* or on-demand: *"From time to time I pester them with some question at the request of a client regarding their security systems. (P12)"* Instead of large consulting agencies, many would choose to hire individual technicians whom someone else recommended. They expressed complete trust in the technicians, agreeing to whatever they advised. For example, *"He sends me an email and I don't understand but I tell him yes. These are amounts like 30 or 50 Shekels per month. (P4)"*

Others suggested that when the company merged with another institution, they get to know how the other party implements defensive measures. Mainly, *"We have merged with a strong tax consultancy headed by the "Institute of Tax Consultants in Israel". The senior partners in the institute accumulated lots of security know-how. We can consult on all kinds of questions such as where to improve the cyber defenses. (P5)"*

Structured Information Source. A few SMB executives rely on structured sources to obtain the security knowledge necessary for company operations. When asked if there are other information sources beyond meetings with IT personnel, P21 mentioned conferences and lectures, *"The Association of Manufacturers had a lecture on information security, also in business forums."* Meanwhile, some said that they will *"go over the journals that are published in this field (P14)"* or *"hear about other businesses in the media* (P6)" to update themselves on the current status of their business ecosystem.

Due to the business's specific economic sector, decision-makers may be required to become familiar with related standards such as the ISO 27001 Standard. For instance, *"I adopt an ISO information security standard so that the basis of the cyber requirements are familiar to us and we try to preserve and comply with them. I also use the 9001 standard which is also a quality standard (P17)."* However, P21 mentioned that sometimes he needed to *"route between all the advice that exists in the market, which can be contradictory to one another."* He noted that *"someone should make some characterizations of several levels of companies and explain what each level should do for cybersecurity."* Furthermore, P12 believed that having stricter regulation and enforcement could help raise awareness. *"If there was an orderly definition of regulation and even tests and penalties by government bodies, then I would be more committed to it. I would have a guide that I would follow and know if I am working correctly."*

Personal Background and Experience. Some key decision-makers we interviewed have educational backgrounds in IT, and they mentioned using personal expertise as a source for security judgment. Interestingly, three key decision-makers attribute their IT knowledge to their time during military service. As P16 said, *"All my life I studied and worked in the field of computers, not in academia, graduated from a computer unit in the army, both at the programming level and at the IT level. I learned everything from zero."*

Others said they gradually become familiar with cybersecurity through years of experience in operating the business, especially after their first encounter with cyberattacks. P8 said, *"We went through a ransomware attack, the computers were locked, they asked for money, 30 bitcoins. At the time I didn't understand what Bitcoin was at all. As far as we were concerned, we understood that we had entered into a war with terrorists."* P16, who owns a company that provides IT ser-

vices, also said, *"I don't go to courses or further training, we learn while working, while dealing with problematic activities that have been identified with the customers."*

Discussion: Due to the lack of credible sources of consultation, *difficulty in information navigation* can be one of the root causes for SMB's cybersecurity barrier. Surprisingly, most SMB decision-makers prefer individual technicians over consulting agencies to cut personnel expenses, and even when they have invested in large agencies, the interaction is infrequent. Too much information can overwhelm key decision-makers as they lack the means to effectively filter and identify useful ones. It is also noted that many choose to rely on their own experiences in cybersecurity, particularly as a victim of an incident.

4.4 What factors impact SMB key decision-makers' security decision?

Finally, we look into the decision-making process after all elements are jointly considered, in which we disclose the reasons key decision-makers give for whether security measures are implemented. Understanding the rationale behind these decisions can help policy-makers and stakeholders devise suitable strategies that promote cyber defense installments.

Whether risks are covered by another entity. From our interviews, we observed that executives tend to be more indifferent toward security issues when the risk can be offloaded to or mitigated by another agency or institution. While this includes hiring third-party consultants to assist the process as described in § 4.3, responsibilities in the case of an attack can also be completely shifted. P1 argued, *"I don't think about cyber risks. The financial risk of payments is taken care of by the credit card company. The credit card company gives us insurance."* Also, as P5 said, *"We would contact the Israeli IRS and tell them that we lost information in a ransom attack. We would continue to work and not close the business."*

Whether losing/leaking data entails inconvenience. When data leakage can cause inconvenience to business operations, participants are more likely to implement defensive measures. *"The biggest headache is to restore documents and for that purpose, there are backups in all places so that if they take over or steal the backup there will be a backup somewhere else. (P2)"* Some would choose to focus on other parts of the business because there are no foreseeable risks. P8 added, *"I know there is no complete solution and I don't want to bother with the issue either. Jams will always be produced, the information is not secret. There will be no harm."*

Whether attacks hinder company operation. In addition to financial losses that may be the result of service downtime, a business' reputation can also be affected by cyberattacks, indirectly motivating decision-makers to allocate more resources for defense. P13 shared, *"If a rumor gets out that we were attacked, then customers will stop believing in us and give us their details."* On the other hand, when the data is evaluated to be "non-critical", there is a significant drop in willingness to adopt security measures: *"I don't see a financial risk. Regarding my operational data, I don't think they can wipe out information that is important to me. (P1)"*

Whether other companies experienced attacks. While many key decision-makers failed to see the likelihood of being attacked, news of incidents from other businesses (particularly of the same niche) can remind them to implement defense for their own company. P4 viewed this as a defining moment for her to be more aware of cybersecurity, *"I have clients, lawyers, who went through a cyber-attack, tried to fix the computers for 3 days and without success. In the end, they paid a ransom in Bitcoin. That day I moved to the cloud."*

Discussion: These factors suggested that SMB decision-makers may have *inadequate risk management* skills, as they tend to rely on other larger entities to mitigate cyber risks or believe that cyberattacks will not cause any damage to business operations. Others may perceive their digital assets as unimportant without having a proper risk evaluation, eventually neglecting to install necessary protection due to the *lack of constructive decision-making*.

5 Online Survey

To understand how business factors and root causes observed from the interview may impact SMB key decision-maker's situational awareness, and to understand in which area decision-makers may be less aware, we developed and conducted an online survey study to explore how SMB executives navigate cybersecurity decision-making. Our study was formally approved by the Institutional Review Board (IRB).

5.1 Survey Protocol

Pilot. We piloted the survey with 20 SMB executives in batches, addressing feedback by removing redundant questions and clarifying question statements. The final survey instrument is included in Appendix B.

Participant Recruitment. We recruited key decision-makers in Israel through Panel4All [35]. Similar to the interview study, we excluded businesses that are not privately owned, as well as those that do not fit the definition of small and medium businesses. We surveyed only owners/CEOs/Vice Presidents/department managers who report directly to the CEO or the owner of the business. The survey took 20 minutes on average to complete and participants were compensated 10 NIS. Distribution of participant and business demographics are presented in Table 2.

Data Analysis. We excluded responses that selected "Don't know/Refuse to response" to more than 70% of the questions, resulting in a total of 322 responses. For the purpose of the analysis, economic sectors were categorized into five

Table 2: Demographic of Survey Participants and Businesses (N=322)

Business				Decision-makers					
# of Employees	6-10	26.70%	50%*	Position	Owner	7.80%	Gender	Male	54.00%
	11-50	55.00%	44%*		CEO	7.80%		Female	46.00%
	51-100	18.30%	6%*		Vice President	12.70%	Seniority (years)	1-4	12.70%
Economic Sector	Services	31.40%	39%*		Manager	71.70%		5-9	18.60%
	Professional services	28.00%	18%*	Age	25-34	25.20%		10-14	20.20%
	Trade	9.30%	27%*		35-44	28.60%		15-19	12.10%
	Information and communication	18.90%	7%*		45-54	26.70%		20+	35.10%
	Production	12.40%	9%*		55+	19.30%		Refuse to answer	1.20%
Annual Revenue (NIS)	Up to 1 million	9.60%	-		Refuse to answer	0.30%	Technology Knowledge	Basic knowledge	8.10%
	1-5 million	18.60%	-	Education	High school diploma or less	25.50%		Intermediate-level knowledge	44.70%
	5-10 million	13.00%	-		Certificate	14.00%		Advanced	32.00%
	10+ million	18.00%	-		Bachelor's degree	37.00%		Professional	13.40%
	Refuse to answer	40.70%	-		Master's degree or higher	23.00%		Refuse to answer	1.90%
					Refuse to answer	0.60%			

*Real-world distribution of SMBs with the corresponding attribute

major groups. We measured a company's *technological intensity* by the ownership of different types of digital assets and the digital technologies deployed. We referenced the Digital Intensity Index (DII) from Eurostat [14] with some modifications. Specifically, SMB received one point each time one of the following is true: 1) Company employs ICT experts, 2) 50% of the employees use the Internet for work purposes, 3) Company has a website, 4) Company's website has advanced functions (order tracking, personalization, etc.), 5) Company purchases advanced cloud services (CRM, computing power, software, etc.), and 6) Company has online trading. We then took the average of the scores as the threshold. If a business's score is above average, it relies heavily on digital technology and is said to have high technological intensity. We describe our survey analysis methods in more detail in §5.2.

Limitations. As with other survey studies, our sample distribution is limited by the participants we recruited, and there may also be self-reporting biases. Although our sample is not fully aligned with the real-world distribution of business sizes and economic sectors as indicated by the Israeli National Bureau of Statistics [28], each business size and economic sector still has an adequate representation in our studied samples. The alignment of business revenue between our sample and the real-world is unknown, as these are considered trade secrets and businesses often refuse to provide them.

Ethical Considerations. Participants were asked for their consent as part of the survey before starting. All responses were collected through self-report measures and anonymized, and participants were not required to disclose any information they did not want to share.

5.2 Survey Analysis

5.2.1 Situational Awareness (SA)

The bulk of our survey was designed with situational awareness model in mind [17]. We referenced the five-level framework for cyber situational awareness [36], and developed methodologies to measure and identify low awareness. Each level of SA maps to specific questions to examine how perceptions and barriers affect SMB cybersecurity. Since survey responses are self-reported, we lack objective information on the potential damage to SMBs in the case of cyberattacks. However, our data enables us to infer this damage. For instance, the more digital assets an SMB possesses and the more sensitive the website functionalities, the higher the damage can be as a result of cyberattacks [19]. We relate SMBs' attributes and decision-makers' perceived potential damage, leveraging crowd wisdom in management [7, 31] to identify those whose self-assessments were substantially lower than others at each level. With this population of low-SA SMBs, we performed a logistic regression to predict the probability of low SA if certain business attributes are present (Figure 3).

Level 1: Not being aware of the importance of cybersecurity to business continuity. This level characterizes a lack of basic understanding of cybersecurity matters. Executives lacking level 1 SA tend to underestimate possible damages faced by their company. To assess SMB key decision-makers' level 1 SA, we compared their self-assessments of their business's potential damage and the projected potential damage due to cyberattacks. If the decision-maker anticipates low damage but the business may face severe damage, then it is implied that the decision-maker exhibits low awareness. It should be noted that this projected potential damage is regardless of the precautions taken by the SMB.

To do so, we estimated this logistic regression model:

$$logit(pr(Damage_i = 1)) = \beta_0 + \sum \beta_j X_{ij}^{Level\ 1} + \varepsilon_i \quad (1)$$

where, $Damage_i = 1$ if the answer to *"In your opinion, what is the greatest possible damage that could occur in the event of the loss or theft of all the digital assets of your business?"* is either "Bankruptcy" or "Significant decrease in income/revenue" (42%), and $Damage_i = 0$ for other responses (medium/minor damage: 53%; no damage at all: 5%). The variable $X_{ij}^{Level\ 1}$ includes all business attributes (number of digital assets, website functionality, number of employees, etc.) A detailed variable and coefficient table is included in Appendix E. The residual term ε_i represents business i's deviation from the average relationship. Given a business attribute, a larger value of ε_i implies an overestimation of the damage and a smaller value implies an underestimation of the damage compared to

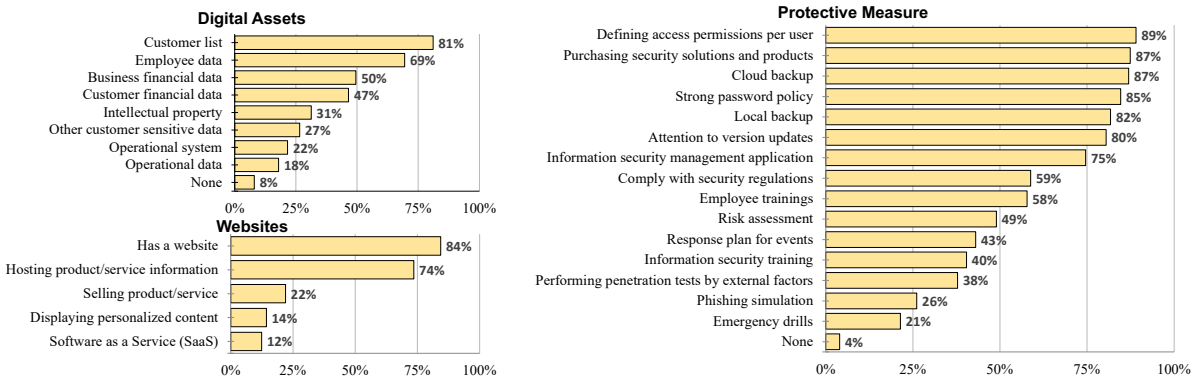


Figure 2: Percentage of SMBs owning digital assets, websites, and protective measures deployed (N = 322).

other businesses. We standardized ε_i and used it as a measure for level 1 awareness. We defined a key decision-maker as having low level 1 awareness if its ε_i is of the lowest 20%. [2]

Level 2: Not being aware of the risk of being exposed to a cyber-attack. This level entails having misconceptions about the probability of being attacked. We asked, *"On a scale of 1 to 10, what is the likelihood that a business like yours will be attacked in the coming year?"* This variable was standardized and used as a level 2 SA measure. Those whose self-assessment falls below the 23% threshold (1: 12.8% or 2: 10.6%) were grouped as low level 2 SA.

Level 3: Not being aware of cyber security precautions and controls. This level is characterized as lacking knowledge and understanding regarding the actions that need to be taken. We asked, *"From a scale of 1 to 10, to what extent do you think the knowledge you have in the field of cybersecurity is sufficient?"* This variable was standardized and used as a level 3 SA measure. Those whose self-assessment falls below the 27% threshold (1: 13.8%; 2: 13.4%) were grouped as having low level 3 SA.

Level 4: Not being aware of the need to act. Decision-makers who have low awareness at this level may overestimate the level of protection their business has due to the misconception that the necessary defense measures have already been taken. To find out the group of decision-makers who exhibit such misconception, we first assessed to what extent are SMB precautions adequate to its needs. We estimated the following linear regression model [3]:

$$Precautions_i = \beta_0 + \sum \beta_j \, X_{ij}^{Level\ 4} + u_i \qquad (2)$$

where $Precautions_i$ is the number of protective measures of the SMB. The variable $X_{ij}^{Level\ 4}$ includes SMB attributes such as the type of digital assets, website functionalities, etc. Detailed regression variables and coefficients are included in Appendix E. The residual term u_i represents business i's deviation from the average number of precautions over our population sample. A large u_i stands for over-cautiousness, and a low u_i stands for under-cautiousness relative to other SMBs. We refer to the standardized u_i as *relative cautiousness*.

We next associated relative cautiousness with the subjective perception of risk. This allowed us to address decision-makers whose risk perception did not fit its cautiousness. Specifically, we wished to identify under-cautious decision-makers who believe their business is safe. We stressed a 45° line between participants' answers to the question, *"On a scale of 1 to 10, what is the level of cyber protection in your business?"* (y-axis) and relative cautiousness (x-axis), both being standardized measures. Level 4 SA equals the distance from the 45° line, where decision-makers above the line show low awareness and those below show high awareness. We defined those at the lowest 20% as having low level 4 SA.

Level 5: Lack of resources. Decision-makers at this level face challenges related to the lack of resources for cybersecurity, even though they understand what needs to be done. We asked if they had encountered a lack of social influence over company personnel, or a lack of organizational resources such as the required budgets and time. Likewise, those are standardized and used as a scale for having sufficient resources. Decision-makers who reported lacking one or more resources (among budget, personnel, and time) were grouped as having low level 5 SA, which took up 25% of the sample (lacking 1 item: 16%; 2 items: 7%; 3 items: 2%).

5.2.2 Root Causes

In addition to evaluating the specific SA issues businesses face when implementing security measures, the survey studies whether the potential root causes identified in the interview significantly impact SA. These were asked on a 5-point scale. The responses are aggregated and the average is reported.

Inadequate Risk Management. We evaluated the adequacy of SMB risk management by asking decision-makers to rate

[2] Those who assessed no damage at all in case of losing all digital assets were also included as having low level 1 SA, even if they were not defined as such by the described mechanism. Those who self-assessed as anticipating severe damage were not included as low level 1 SA, even if they were defined as such by the described mechanism.

[3] Theoretically, Poisson regression would be a better model for count data; however, linear regression yielded the same results as Poisson regression in this case. For simplicity, we report results from the basic linear model.

themselves regarding the following: having a clear understanding of risks, taking active actions to reduce risks, having contingency plans, and prioritizing risk management.

Difficulty in Information Navigation. We asked participants whether they felt overwhelmed or confused by the abundant cybersecurity information and whether they had difficulty staying up-to-date due to the constantly evolving threats.

Lack of Technological Orientation. For technological orientation, we inquired about participants' tendency to act when implementing new technologies in the business. We also asked whether their business has explored innovative security solutions in the past three years, as well as the extent of their exposure to such solutions made by business competitors.

Lack of Constructive Decision-making. We evaluated whether business executives make constructive decisions by asking what information they base their decisions on (personal management experience, employee experiences, intuitions, external consultants, and statistical insights).

6 Quantitative Analysis Result

Digital Assets and Defense Distribution. Figure 2 shows participating SMB's current status in terms of valuable digital assets and deployed protective measures. Based on our survey, the type of data that most SMBs own regardless of business attributes are personal data of the customers and employees. In addition, a majority of SMBs have websites available, and most use them as a means to communicate business information, such as for product viewing and service advertisements. For protective measures, 89% of the SMBs claimed they define access permissions for individual employees. Specifically, every employee is assigned a username, and their security clearances are adjusted accordingly. This is followed by purchasing security solutions from third parties and practicing regular backup to cloud storage. Interestingly, we found that SMBs in Israel tend to choose technical measures (such as backups and access control) over training and simulations, which is similar to SMBs in Germany [23]. Note that around 4% and 8% of the SMBs shared that they do not have any digital assets or protective measures, respectively.

6.1 Awareness vs. Business Characteristics

Figure 3 shows the marginal probabilities for low SA based on a logistic regression with business attributes (number of employees, business sector, annual revenue level, technological intensity, and cyber-attack experience). The corresponding coefficients, standard errors, and statistical significance are included in Appendix F. We describe our findings below.

Level 1. Our analysis did not reveal statistically significant variables that are directly correlated with level 1 SA. However, we observed several interesting tendencies. We found that SMBs with less than 1M annual revenues are most likely to ignore the importance of cybersecurity, while SMBs that are in the Professional Service sector or have more employees can be more aware. Interestingly, those who have high technological intensity are more likely to be at low level 1 SA than others who have relatively lower technological intensity.

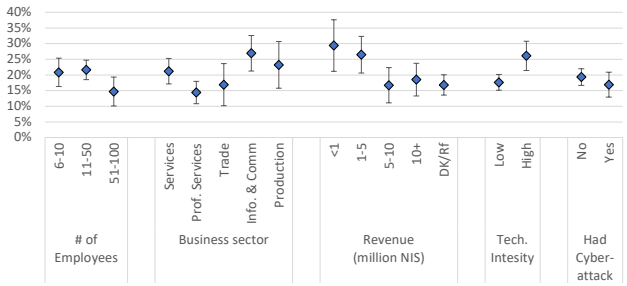
Level 2. The average assessment given by all interviewees is 3.4, meaning a majority of decision-makers do not believe that they are easily exposed to attacks. Meanwhile, decision-makers in the Information and Communication sector are more aware of the risks of attacks ($\beta = -1.075, p < 0.05$), making them more prepared in case of cyber incidents. Decision-makers whose businesses have experienced attacks before generally perceive a higher risk of attacks than those who did not ($\beta = -1.19, p < 0.01$), indicating that decision-makers may learn from past experiences to raise awareness. In addition, businesses with 6-10 employees are more likely to overlook the risk of cyberattacks ($\beta = 0.576, p < 0.1$).

Level 3. Based on our survey, more than half (54%) of the respondents reported that they are familiar with official cybersecurity guidelines. Surprisingly, participants generally expressed a lower confidence score despite their claim on cyber guideline familiarity. This is especially evident in businesses with 6-10 employees, in which over half of the interviewees (53%) claimed guideline familiarity but had an average confidence rating of only 3.8. This is also reflected in Figure 3c, where businesses with less than 10 employees are the most likely to be at low awareness ($\beta = 1.023, p < 0.01$). Greater confidence in cybersecurity knowledge sufficiency is seen in those from the Information and Communication sector ($\beta = -1.045, p < 0.05$), and those from technology-intensive businesses ($\beta = -0.868, p < 0.05$). Experience with cyberattacks may also prompt decision-makers to understand security precautions more ($\beta = -0.720, p < 0.05$).

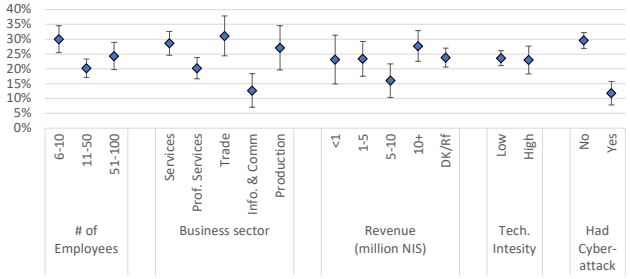
Level 4. Referring to Figure 3d, we see that SMBs from the Trade sector are the least likely to be ignorant about level 4 SA, though this is not statistically significant. We found that most decision-makers who are not aware of the high risk come from businesses with more than 50 employees ($\beta = 1.15, p < 0.05$). Businesses that have no prior attack experiences also tend to overlook the need to act ($\beta = -0.618, p < 0.1$).

Level 5. Around one in five decision-makers reported that their available budgets and human resources prevent them from implementing better cyber precautions, while one in ten indicated the lack of time as a barrier. It is worth noting that businesses with more than 50 employees are more likely to experience resource shortage ($\beta = -0.775, p < 0.1$). As for the difference between economic sectors, the Professional Service sector ($\beta = -0.651, p < 0.1$) and the Production sector ($\beta = -1.026, p < 0.1$) are less likely to indicate a lack of resources. Revenue level, technological intensity, and past attack experiences do not significantly affect level 5 SA.

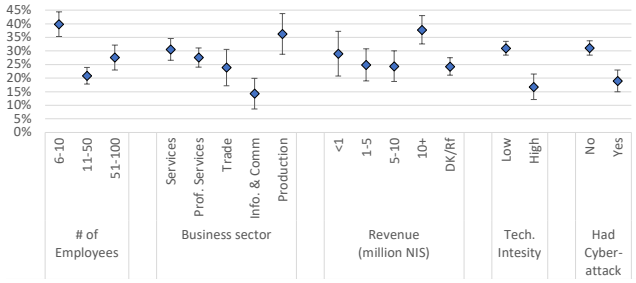
Multiple Low Awareness. Figure 3f shows which type of business may have low SA on multiple levels. Professional Service sector ($\beta = -0.857, p < 0.05$) and businesses that make 5M-10M NIS annually ($\beta = -1.103, p < 0.05$) are



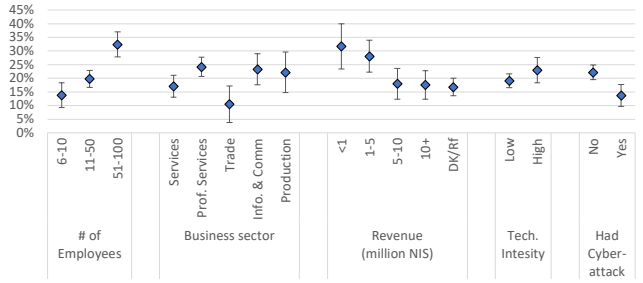
(a) Low SA Level 1



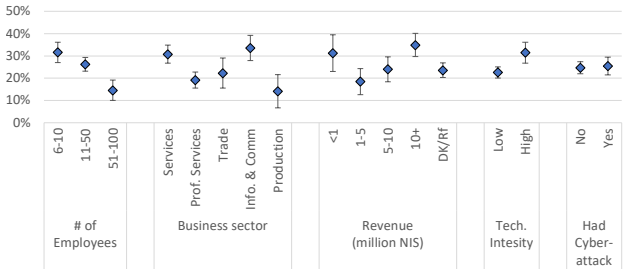
(b) Low SA Level 2



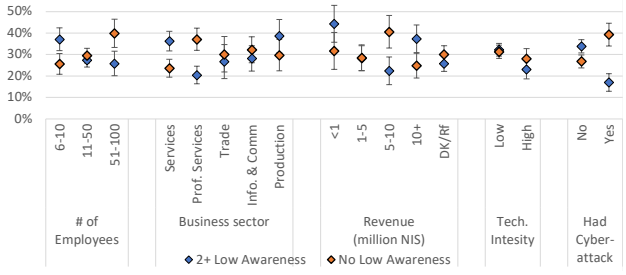
(c) Low SA Level 3



(d) Low SA Level 4



(e) Low SA Level 5



(f) Multiple Low SA vs. No Low SA

Figure 3: Margins from logistic regressions predicting the probabilities of decision-makers having low awareness.

more likely to be aware of cybersecurity. Those who have experienced cyberattacks before are less likely to have multiple awareness issues ($\beta = -0.967, p < 0.01$).

No Low Awareness. Figure 3f shows which type of business are likely to be free of any awareness issues. Businesses with more than 50 employees ($\beta = 0.729, p < 0.1$) and businesses with attack experiences ($\beta = 0.617, p < 0.05$) are likely to be more aware. Those with high technological intensity are less likely to have no low awareness issues ($\beta = -0.524, p < 0.1$).

Takeaway: Our results show that revenue level does not significantly impact individual situational awareness, though companies having 5-10 million NIS annually are less likely to have multiple awareness issues. We also see a positive impact of attacked experiences on awareness. In addition, being in the Information and Communication sector allows decision-makers to become familiar with awareness levels 2 and 3, while high technological intensity mainly increases level 3 awareness. Finally, a larger company size appears to negatively influence awareness level 4, possibly due to overconfidence or difficulty in management. Yet, it suggests sufficient resources to tackle security challenges.

6.2 Holistic Structural Equation Model

We constructed a holistic structural equation model (SEM) [22] from the collected data, showing the correlation of factors impacting key decision-maker's security awareness. The SEM draws relations between root causes, attack experience, relative cautiousness, and different levels of SA among all kinds of businesses, as shown in Figure 4. Only the statistically significant arrows are shown.

Correlation among SA Levels. While level 1 is positively correlated with level 2, and level 2 is positively correlated with level 3, level 3 is negatively correlated with level 4. This implies that greater perceived knowledge of precautions can lead to false beliefs that there's no further need to act. In addition, level 4 is negatively correlated with level 5, indicating that resources such as time, budget, and personnel are essential and lacking for businesses that wish to actively defend against cyberattacks. The estimated correlations between SA levels indicate that the SA model is a maturity model [30], as it is implied that each level influences the next, and thereby indirectly influences relative cautiousness. The model also suggests that levels 2, 3, and 4 directly influence relative cautiousness.

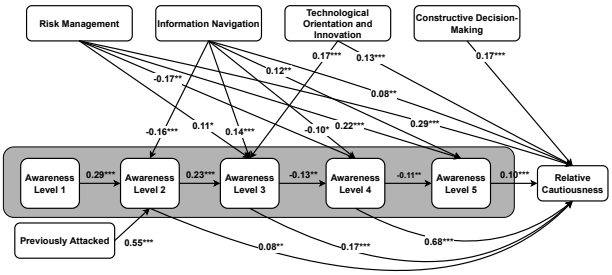


Figure 4: Structural equation model of situational awareness, root causes, and relative cautiousness.

Correlation with Other Factors. Except for awareness level 1, all SA levels are positively correlated with relative cautiousness. This shows that relative cautiousness can be improved by increasing SA. Moreover, experience with cyberattacks influences the perceived risk of attack exposure, which in turn motivates decision-makers to improve cybersecurity knowledge and readiness. It is also shown that root causes are strongly related to SA and relative cautiousness. Therefore, they are critical when considering interventions for SMBs. We discuss the role of root causes in our model and the respective interventions in § 6.3. Besides the root causes' influence, SA is directly correlated with relative cautiousness. The correlation implies that other factors besides SA link root causes to security readiness. Such factors could be due to cultural tendencies or influences from other positions besides decision-makers, and should be further explored in future work.

6.3 Impact of Root Causes

Inadequate Risk Management. According to Table 3, most SMBs facing this obstacle are from the Trade and Service sector. Our holistic model suggested that risk management is highly correlated with SA and also directly correlated with relative cautiousness. Inadequate risk management affects decision-maker's level 3 and level 4 SA, making them under/over-estimate the urgency and failing to correctly allocate available resources. For these businesses, allocating resources effectively according to the situation is the key.

Difficulty in Information Navigation. Except for SA level 1, the ability to navigate abundant information can also impact SA and relative cautiousness. Note that the perception of information navigation difficulty is negatively correlated with SA level 2 and level 4, meaning the harder it is to navigate information, the more likely there is for an overestimation of risks. The average rating from decision-makers is 2.6, which is the lowest of the root causes. For these businesses, improved information sources are needed to mitigate biased awareness.

Lack of Technological Orientation and Innovation. According to the holistic model, the lack of technological innovation directly affects SA level 3. This is also where decision-makers believe they need the most guidance. For these businesses, a way to facilitate discussion about available software or tactics is needed. The Information and Communication sector, whose businesses presumably engage more with technology, rates the highest in their technological knowledge (3.1).

Table 3: Root Causes vs. Business Characteristics

		R.M.	I.N.	T.I.	C.D.M
Total		3.0	2.6	2.6	3.6
Business Size (# of Employees)	6-10	3.1	2.4	2.6	3.7
	11-50	2.9	2.6	2.5	3.5
	51-100	3.3	2.9	2.8	3.8
Business Sector	Services	2.8	2.8	2.4	3.4
	Prof. Services	3.1	2.4	2.6	3.8
	Trade	2.7	2.3	2.7	3.6
	Info. & Comm.	3.4	2.8	3.1	3.7
	Production	3.1	2.9	2.3	3.6
Revenue (million NIS)	<1	2.9	2.6	2.6	3.7
	1-5	3.1	2.7	2.5	3.5
	5-10	2.8	2.8	2.7	3.2
	10+	3.8	2.4	2.6	3.6
	Refuse to answer	3.1	2.6	2.6	3.8
Technological Intensity	Low	3.0	2.6	2.5	3.6
	High	3.1	2.6	2.8	3.6
Experienced Cyberattack	No	3.0	2.6	2.6	3.6
	Yes	3.2	2.6	2.7	3.5

R.M.: Risk Management, I.N.: Information Navigation, T.I.: Technology Innovation, C.D.M: Constructive Decision Making

Lack of Constructive Decision-Making. Finally, while constructive decision-making is related to a business's relative cautiousness, it does not seem to correlate with any of the SAs. According to Table 3, this is where decision-makers think they perform best and have the least issues comparatively.

7 Discussion

7.1 Answers to Research Questions

With both qualitative and quantitative analysis, we have a glimpse of the security mindsets of SMB key decision-makers. Modeling SA into different levels and accounting for the root causes of low awareness shed light on the way SA could be improved. We finally answer our research questions.

RQ1. We identified key decision-makers' perceived cyber threats based on the digital assets they valued. Alongside company data such as customer data, employee data, operational data, and intellectual property, many companies stated that they host websites for advertisement or customer communication, and are concerned with service disruption due to server downtime. Yet, comparing businesses with others showed that 23% believed that they would not get attacked. To motivate security actions among SMBs, key decision-makers first need to be able to accurately evaluate their business's organizational risks. As prior attack experiences greatly influence risk perception, red team exercises may help guide the evaluation, identifying where false risk perceptions exist.

RQ2. We observed a tendency for executives to mention more technical measures than employee training, which coincides with the findings from [23]. Interestingly, almost all participants unanimously agreed that backup to cloud storage is important for company operation. However, other forms of defense are mostly seen as redundant, with organizational measures receiving mixed preferences, and only minimal efforts are spent to enforce secure behaviors. We found 27% of the businesses in our sample to have insufficient knowledge

regarding security defenses. Like risk perceptions, accurate deployment and evaluation of defenses are also needed to enforce security cost-effectively, as the deployed defense may not necessarily mitigate risk and has its own set of harms. For instance, common industrial practice to combat phishing attacks was found to be ineffective by prior study [27]. Figure 4 shows several ways this perception can be improved, including adequate risk management and getting familiar with both security knowledge and available defense technologies.

RQ3. The capability to acknowledge and comprehend elements in the current situation to draw informative decisions marks level 2 maturity in Endsley's SA model. Third-party consultants, lectures, news, and past security experiences are common information sources that SMB executives consider when making decisions. The impact of security incidents is two-sided. On the one hand, decision-makers would be motivated to implement more defense if the impact is costly. On the other, some would only view them as inconveniences and focus more on recovery but not defense. The status of other businesses may also influence how decision-makers perceive their own risks. Meanwhile, whether the company has cyber-attack experiences is a critical indicator of low SA regarding security. Businesses that have experienced attacks before are more likely to be free of any awareness issues. Having a larger business size seems to negatively affect decision-maker's awareness of the need to act, though resources are also more readily available. For economic sectors, businesses in the technology domain are usually more aware of the risks. For those who neglect the need to take cybersecurity actions, the issue can be addressed by assisting in risk management or easing information navigation, such as using channels familiar to decision-makers to convey concrete security suggestions.

RQ4. We draw correlations between root causes and the level of awareness that they have an impact on. In general, decision-makers consider the navigation of security information and the adoption of innovative technology as major roadblocks in business operations. They perform averagely in terms of risk management, and consider the lack of constructive decision-making as a less critical problem. Except for SA level 1, these root causes can affect decision-maker's SA significantly.

7.2 Interventions

We aim to make our findings on SA and practical challenges broadly applicable despite this study being conducted in Israel. Though our results indicate universal problems faced by SMBs, the corresponding solutions for these issues may depend on a country's cultural, economic, and technological context. Based on this work, we have collaborated with Israeli government officials to devise actionable interventions to address the challenges and barriers accordingly.

Networking and Institutional Guidance. Given that lectures were mentioned as one of the vital information sources, networking opportunities such as government-led conferences and workshops should be catered to provide educational lectures on how best to manage company resources, as well as providing a space to help build personal connections between SMB executives and government officials [5]. Since most SMBs facing the obstacle of inadequate risk management are from the Trade and Service sector (Table 3), policies regarding tax credits and guidance from financial institutions, such as the Small Business Lending Fund [33], may also help SMBs budget their capital.

SMB-friendly Information Source. From the policy point of view, actionable standards and guidelines may help inform SMBs' legal obligation in matters of cybersecurity. In addition, a mix of information pulling and pushing leveraging intelligent agents, such as a central hub dedicated to the curation and sharing of cybersecurity knowledge, may be extremely useful in improving key decision-makers' experience during information navigation, helping them combat information overload [16]. Subsidies on counseling services may offer extra aid in offloading some of the decision-making to dedicated information specialists [8].

Identify Security Solutions through Technical Exchange. One way to tackle the issue with technological orientation is to host venues where merchants of security solutions can showcase their products. Such means of open-system orchestration help facilitate technical exchange between software companies, which can foster innovations that combat cyber criminals more effectively [15, 20]. This will also allow SMB executives to understand what is currently available on the market, while letting them experience the products first-hand and communicate with the representatives about potential customization to fit their business.

Preventive Assessment and Detection. It is recommended that decision-makers assess their business resiliency and find out potential vulnerabilities in advance, since organizations that practice regular security assessments experienced 40% less unplanned downtime [12]. There is also a need to encourage organizational measures such as employee training, emergency drills, or attack simulations. These help familiarize decision-makers with incidental situations and prepare them to make more informed decisions under urgency.

8 Conclusion

We conducted an initial semi-structured interview with 21 key decision-makers to understand what they consider when dictating a company's course of action regarding cybersecurity. Using the situational awareness model, we surveyed 322 key decision-makers to identify important factors influencing company executives' decision-making process, as well as find out the current awareness status of cybersecurity among Israeli SMBs. Based on our findings, we developed a holistic structural equation model considering potential root causes and relative cautiousness. In light of our results, we suggested interventions to overcome the identified barriers.

References

[1] Abdulmajeed Alahmari and Bob Duncan. Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, pages 1–5. IEEE, 2020.

[2] Abdulmajeed Abdullah Alahmari and Robert Anderson Duncan. Investigating potential barriers to cybersecurity risk management investment in SMEs. In *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, pages 1–6. IEEE, 2021.

[3] World Bank. World Bank SME finance: Development news, research, data. *World Bank*, 2022.

[4] Xavier Bellekens, Andrew Hamilton, Preetila Seeam, Kamila Nieradzinska, Quentin Franssen, and Amar Seeam. Pervasive ehealth services a security and privacy risk awareness survey. In *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*, pages 1–4. IEEE, 2016.

[5] Leo Billington, Robyn Neeson, and Rowena Barrett. The effectiveness of workshops as managerial learning opportunities. *Education+ Training*, 51(8/9):733–746, 2009.

[6] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2):77–101, 2006.

[7] David V Budescu and Eva Chen. Identifying expertise to extract the wisdom of crowds. *Management science*, 61(2):267–280, 2015.

[8] Helen Butcher et al. Meeting managers' information needs. 1998.

[9] Jane Chen. Cyber security: Bull's-eye on small businesses. *J. Int'l Bus. & L.*, 16:97, 2016.

[10] Kaiming Cheng, Jeffery F Tian, Tadayoshi Kohno, and Franziska Roesner. Exploring user reactions and mental models towards perceptual manipulation attacks in mixed reality. In *USENIX Security*, volume 18, 2023.

[11] Alladean Chidukwani, Sebastian Zander, and Polychronis Koutsakis. A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access*, 10:85701–85719, 2022.

[12] CloudIBN. Benefits of regular cloud security assessments for your business!, 2023.

[13] Stephanie de Smale, Rik van Dijk, Xander Bouwman, Jeroen van der Ham, and Michel van Eeten. No one drinks from the firehose: How organizations filter and prioritize vulnerability information. In *2023 IEEE Symposium on Security and Privacy (SP)*, 2023.

[14] dimodim. Digital intensity index description. https://circabc.europa.eu/ui/group/89577311-0f9b-4fc0-b8c2-2aaa7d3ccb91/library/30b83b9c-3d0c-4086-bf52-77905e19b4eb/details, 2022.

[15] Nilanjana Dutt, Olga Hawn, Elena Vidal, Aaron Chatterji, Anita McGahan, and Will Mitchell. How open system intermediaries address institutional failures: The case of business incubators in emerging-market countries. *Academy of Management Journal*, 59(3):818–840, 2016.

[16] Angela Edmunds and Anne Morris. The problem of information overload in business organisations: a review of the literature. *International journal of information management*, 20(1):17–28, 2000.

[17] Mica R Endsley. Toward a theory of situation awareness in dynamic systems. *Human factors*, 37(1):32–64, 1995.

[18] Mica R Endsley, Daniel J Garland, et al. Theoretical underpinnings of situation awareness: A critical review. *Situation awareness analysis and measurement*, 1(1):3–21, 2000.

[19] Fortinet. Why are smbs most vulnerable to cyberattacks? https://www.fortinet.com/resources/cyberglossary/smb-cyberattacks, 2023.

[20] Alessandro Giudici, Patrick Reinmoeller, and Davide Ravasi. Open-system orchestration as a relational source of sensing capabilities: Evidence from a venture association. *Academy of Management Journal*, 61(4):1369–1402, 2018.

[21] 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*, 21:1285–1305, 2019.

[22] Rick H Hoyle. *Structural equation modeling: Concepts, issues, and applications*. Sage, 1995.

[23] Nicolas Huaman, Bennet von Skarczinski, Christian Stransky, Dominik Wermke, Yasemin Acar, Arne Dreißigacker, and Sascha Fahl. A large-scale interview study on information security in and attacks against small and medium-sized enterprises. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1235–1252, 2021.

[24] Martin Husák, Tomáš Jirsík, and Shanchieh Jay Yang. Sok: contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ARES '20, New York, NY, USA, 2020. Association for Computing Machinery.

[25] Lennart Jaeger and Andreas Eckhardt. Eyes wide open: The role of situational information security awareness for security-related behaviour. *Information Systems Journal*, 31(3):429–472, 2021.

[26] Dilara Keküllüoğlu and Yasemin Acar. "We are a startup to the core": A qualitative interview study on the security and privacy development practices in turkish software startups. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 2015–2031. IEEE, 2023.

[27] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859. IEEE, 2022.

[28] The Israeli National Bureau of Statistics. Survey of economic sectors. https://www.cbs.gov.il/he/mediarelease/DocLib/2023/247/29_23_247b.pdf, 2019.

[29] United Nations. Statistical division and others. *International Standard Industrial Classification of All Economic Activities (ISIC) Revision 4*, 2008.

[30] Tobias Mettler. Maturity assessment models: a design science research approach. *International Journal of Society Systems Science*, 3(1-2):81–98, 2011.

[31] Johannes Müller-Trede, Shoham Choshen-Hillel, Meir Barneron, and Ilan Yaniv. The wisdom of crowds in matters of taste. *Management Science*, 64(4):1779–1803, 2018.

[32] OECD. *Financing SMEs and Entrepreneurs 2022*. 2022.

[33] U.S. Department of the Treasury. Small business programs, Mar 2024.

[34] Emma Osborn and Andrew Simpson. Risk and the small-scale cyber security decision making dialogue—a uk case study. *The Computer Journal*, 61(4):472–495, 2018.

[35] Panel4All. https://www.panel4all.co.il/, 2023.

[36] Karen Renaud and Jacques Ophoff. A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. *Organizational Cybersecurity Journal: Practice, Process and People*, 1(1):24–46, 2021.

[37] Small and Medium Business Agency. Small and medium business status report in 2023, 2023.

[38] Jonah Stegman, Patrick J Trottier, Caroline Hillier, Hassan Khan, and Mohammad Mannan. "My privacy for their security": Employees' privacy perspectives and expectations when using enterprise security software. *arXiv preprint arXiv:2209.11878*, 2022.

[39] Sarah Vieweg, Amanda L Hughes, Kate Starbird, and Leysia Palen. Microblogging during two natural hazards events: what twitter may contribute to situational awareness. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 1079–1088, 2010.

[40] Mahmoud Watad, Sal Washah, and Cesar Perez. IT security threats and challenges for small firms: Managers' perceptions. *International journal of the academic business world*, 12(1):23–30, 2018.

[41] Flynn Wolf, Adam J Aviv, and Ravi Kuber. Security obstacles and motivations for small businesses from a CISO's perspective. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 1199–1216, 2021.

[42] Fangfang Zhou, Ronghua Shi, Ying Zhao, Yezi Huang, and Xing Liang. Netsecradar: A visualization system for network security situational awareness. In *Cyberspace Safety and Security: 5th International Symposium, CSS 2013, Zhangjiajie, China, November 13-15, 2013, Proceedings 5*, pages 403–416. Springer, 2013.

A Interview Guide

1. Please start by telling me about yourself, including your education and familiarity with computer technology.
2. Please tell me about your company, what it does, how long it has been operating, and the annual turnover.
3. What kind of systems do you use and what information is stored? What is something you think has a high risk of losing and needs to be protected?
4. Who is in charge of IT information security? If a third party is in charge, is there any specific reason that you hired him/them?
5. What are the risks and consequences of your business being attacked? Have you heard talk of cyberattacks in your field?
6. What are the protective measures that the company is using? Was there some cyber defense that you were unable to implement?
7. Has the company experienced attacks before? What did you do after the attack?
8. Can you share with me your sources of information for learning about cyber protection?
9. Is there anything else you would like to share?

B Survey Instrument

Screening

Q1. Which of the following best describes your business ownership?

◯ Privately Owned ◯ Cooperative Owned ◯ Government Owned
◯ Publicly Owned ◯ Non-profit

Q2. How many employees are in your business?

Q3. What is your position in the business? (Select all that apply)

◯ Business Owner ◯ Vice President ◯ CEO
◯ Department/Division Manager ◯ Non-management Role

Q4. What type of business do you own?

Q5. What is the economic sector of the business?

◯ Activities in real estate (Service)
◯ Management and support services (Service)
◯ Wholesale and retail trade and repair of motor vehicles (Trade)
◯ Industry, mining and quarrying (Production)
◯ Electricity and water supply, sewage services and waste treatment (Service)
◯ Professional, scientific and technical services (Professional Service)
◯ Information and communication
◯ Hospitality and food services (Service)
◯ Transportation, storage, mail and courier services (Service)
◯ Financial services and insurance services (Professional Service)
◯ Other:____ ◯ DK/RF

Q6. What was your company's annual revenue (in NIS) for 2022? Your answers will not be transferred to any business entity.

◯ Up to 1 million ◯ 1-5 million ◯ 5-10 million
◯ 10-50 million ◯ 50+ million ◯ DK/RF

Business Background

Q7. In what year was your business established?

Q8. How many of your employees use a computer when they work?

Q9. Are there standards and/or regulations for information security that your company implements?

◯ Yes, please specify ◯ No ◯ DK/RF

Q10. Does the business operate outside of Israel?

◯ Yes ◯ No

Q11. Where is your business located?

◯ Located at one site ◯ Located at several sites

Q12. Are you a member of a business association?

◯ Yes, please specify ◯ No ◯ DK/RF

Q13. In which city do most of your business's activity take place?

Risk Exposure

Q14. Does your business have an employee who is in charge of computing?

◯ Yes ◯ No ◯ DK/RF
◯ No, an external party/person provides my business with computing services

Q15. [If Q14 == Yes] Who is in charge of overseeing all aspects of computing matters for your business, including information security?

◯ CIO ◯ ICT ◯ CISO
◯ Other:____ ◯ DK/RF

Q16. [If Q14 == external party/person] How would you best describe the relationship you have with your computing services company/person? (Select all that apply)

◯ We are in touch when there are technical problems.
◯ We hold regular periodic meetings at least once a year.
◯ We receive from him/them general updates on new technologies.
◯ We receive recommendations from them to buy cybersecurity products.
◯ Other:____ ◯ DK/RF

Q17. Do the employees in your business have the choice of working remotely?

◯ Yes, all of our employees can work remotely.
◯ Yes, some of our employees can work remotely.
◯ No ◯ DK/RF

Q18. Is software installed on local servers in the business or are they on the cloud?

◯ All our software is on the cloud only
◯ Some of the software is located on the cloud and some on local servers
◯ All our software is located local server only
◯ DK/RF

Q19. Does your business use Customer relationship management (CRM)?

◯ Local CRM ◯ Cloud CRM ◯ No ◯ DK/RF

Q20. Does your business use Enterprise resource planning (ERP)?

◯ Local ERP ◯ Cloud ERP ◯ No ◯ DK/RF

Q21. Does your business have a website?

◯ Yes ◯ No ◯ DK/RF

Q22. [If Q21 == Yes] How is the website managed?

◯ Independent management from our business.
◯ Webpage on other websites such as Amazon, Etsy, Ebay, etc.
◯ Other:____ ◯ DK/RF

Q23. [If Q21 == Yes] What is the purpose of the website? (Select all that apply)

◯ For business information: viewing products/services offered by the business
◯ For selling products or services, and charging the customer for the purchase
◯ For individualized use, where each user can sign in with a personal account
◯ The service provided by the business is located on the website (SaaS)
◯ Other ◯ DK/RF

Q24. How are the payments completed?

◯ Charged directly on our website ◯ Payment applications
◯ Charged on an external website ◯ Bank transfer
◯ Check/Cash ◯ Other ◯ DK/RF

Q25. Which of the following digital assets does your business have? (Select all that apply)

◯ Customer data (customer names, personal details)
◯ Customer financial information (credit cards, bank accounts, etc.)
◯ Customer sensitive data (medical information)
◯ Employee data (personal data, shifts, salaries, etc.)
◯ Operational data (details pertaining to machines, materials, etc.)
◯ Intellectual property (software projects, engineering plans, etc.)
◯ Company financial data ◯ DK/RF

Q26. A cyberattack has the potential to harm the digital assets of the business, including their destruction or theft. Please assess the severity of potential damage or loss for each of the digital assets on a scale of 1 (minimal damage) to 10 (most significant damage). *[Use list of digital assets selected in the previous question.]*

Situational Awareness

Q27. In your opinion, what is the greatest possible damage that could occur in the event of the loss or theft of all the digital assets of your business?

◯ Bankruptcy
◯ A significant decrease in income/revenue
◯ There will be a cost to restore the information
◯ There will be a decrease in business productivity
◯ Harm to the motivation levels of the business team
◯ Harm to the business reputation ◯ Other:____
◯ Fines ◯ There will be no damage/harm

Q28. In your estimation, what is the likelihood that a business like yours will be attacked in the next year? On a scale of 1 to 10, with 1 indicating not likely at all, and 10 indicating extremely likely that an attack will occur.

Q29. Do you know the guidelines on cyber-related issues from official sources in Israel and worldwide?

◯ Yes, fully ◯ No
◯ Yes, partially ◯ Refuse to answer

Q30. What are your sources of information in cybersecurity? (Select all that apply)

◯ Newsletter and magazines ◯ Lectures and conferences
◯ Conversations with colleagues, other business owners
◯ Government websites (Agency for Small and Medium Businesses, the National Cyber Array, etc.)

◯ Internet forums ◯ Other:____

Q31. To what extent do you think the knowledge you have in the field of cybersecurity is sufficient? On a scale of 1 to 10, with 1 indicating not at all sufficient, and 10 indicating extremely sufficient.

Q32. How does your business protect itself from cyberattacks? (Select all that apply)
◯ Purchasing security products (antivirus, firewall, and more)
◯ Everyone has a username and their security settings are adjusted accordingly
◯ Implementing information security procedures
◯ Compliance with information security standards and authorization as a regulatory requirement
◯ Conducting penetration tests by external parties
◯ Requiring a password ◯ Employee training
◯ Information security training ◯ Keeping all software up to date
◯ Incident response plan ◯ Local backup
◯ Routine risk assessment ◯ Cloud backup
◯ Emergency drills ◯ Other:____
◯ Phishing simulation ◯ Don't know

Q33. To the best of your knowledge, what is the level of cyber protection in your business? On a scale of 1 to 10, with 1 indicating a very low level of cybersecurity protection and 10 indicating a very high level of cybersecurity protection.

Q34. What are the reasons you chose this score?

Q35. What is the maximum amount in NIS you would be willing to invest annually to ensure cybersecurity measures?
◯ No need to invest at all ◯ 20,000-50,000
◯ up to 5,000 ◯ 50,000-100,000
◯ 5,000-10,000
◯ 10,000-20,000 ◯ Over 100,000

Q36. In your opinion, what is the annual budget in NIS that a business like yours should invest in cybersecurity?
◯ No need to invest at all ◯ 20,000-50,000
◯ up to 5,000 ◯ 50,000-100,000
◯ 5,000-10,000
◯ 10,000-20,000 ◯ Over 100,000

Q37. In your opinion, does the business invest enough budget for cybersecurity?
◯ Much more than necessary ◯ A little more than necessary
◯ Approximately the amount needed
◯ A little less than necessary ◯ Much less than necessary
◯ DK/RF

Q38. In your opinion, how many monthly hours (meetings, reading material, consultations, etc.) should a manager like you devote to cybersecurity?
◯ No need to spend time at all ◯ 20-30
◯ up to 5 hours ◯ 30-50
◯ 5-10 ◯ More than 50
◯ 10-20 ◯ DK/RF

Q39. Are you devoting enough time to cybersecurity?
◯ Much more than necessary ◯ A little more than necessary
◯ Approximately the amount needed
◯ A little less than necessary ◯ Much less than necessary
◯ DK/RF

Q40. Please indicate whether you agree with the following statements. On a scale of 1 to 5, with 1 indicating strongly disagree and 5 indicating strongly agree.
◯ My competitors have implemented or are in the process of implementing cybersecurity measures.
◯ My customers want my business to implement cybersecurity measures.
◯ Businesses I interact with believe we need to adopt cybersecurity measures.

Q41. Has your business experienced cyberattacks?
◯ No ◯ Yes, more than a year ago
◯ Yes, once in the last year
◯ Yes, several times in the last year ◯ DK/RF

Q42. Has your business faced the following due to security problems?
◯ Attempt to cause unavailability of the information and communication systems (such as ransomware)
◯ Attempt to cause destruction or corruption of information
◯ Attempt to cause disclosure of confidential data (e.g. phishing)

Q43. What was the extent of the damage? (Select all that apply)
◯ No damage at all ◯ Damage to reputation
◯ Ransom payment ◯ Damage to employee morale
◯ Money for additional computing services ◯ Man-hours for fixing
◯ Other:____
◯ Damage to hardware ◯ DK/RF

Q44. Do you know of a business that experienced a cyber-attack? (Select all that apply)
◯ Yes, a close colleague/acquaintance of mine experienced a cyber-attack
◯ Yes, I heard business in the same sector as mine experienced cyber-attack
◯ Yes, there are businesses that I do not know personally being attacked.
◯ I never heard of cyberattacks occurring to others.
◯ Refuse to answer

Q45. How much do the following statements limit your implementation of cyber defense measures in your business? On a scale of 1 to 5, with 1 indicating limits very much and 5 indicating does not limit at all.
◯ I have no contact with a security expert
◯ No clear instructions from reliable sources regarding the required actions
◯ I don't have a suitable technological understanding
◯ The employees are not involved in this matter
◯ The management team is not involved in this matter
◯ Lack of budget to implement the guidelines
◯ There is a lack of personnel who can implement the guidelines
◯ I have no one to consult in my social circle
◯ I have no time

Q46. Does your business hold executive meetings regarding cybersecurity?
◯ Never ◯ Once a year or less
◯ More than once a year - once every quarter
◯ At least once a quarter – once a month
◯ More than once a month ◯ Refuse to answer

Q47. In the case that you would want to implement new cybersecurity guidelines that will require changing work habits, to what extent do you think the employees will cooperate in implementing the guidelines?
◯ Extremely ◯ Slightly ◯ Refuse to answer
◯ Very much ◯ Not at all

Root Causes

Q48. Which of the following statements best conveys your tendency to act when it comes to implementing new technologies in the business?
◯ New technology is implemented in the business only if the existing technology is no longer possible
◯ New technology is implemented in the business only if it has an external demand from customers, suppliers, or regulators.
◯ New technology is implemented in the business only after we see that it proves itself in businesses similar to mine
◯ We strive to be ahead of our competitors when it comes to implementing new technologies that have just been released

Q49. The following statements refer to your personal attitudes regarding cybersecurity. There are no right or wrong answers. Please provide your opinion on the following statements using a scale of 1 to 5, with 1 indicating strongly disagree and 5 indicating strongly agree.
◯ Cybersecurity is an important issue that should concern all businesses.
◯ My business is at risk of experiencing a cyber-attack.
◯ Cybersecurity threats are constantly evolving, so it's hard to stay up-to-date.
◯ I believe that the existing cybersecurity measures implemented in the business effectively safeguard against cyberattacks.
◯ I believe that cybersecurity measures are too expensive and are not worth the investment.

Q50. During the last three years, has your business invested any resources in exploring new ideas for innovation? (For example, through participation in conferences, fairs, or exhibitions, following scientific/technical journals or commercial publications, information from professional organizations, social networks, or online business platforms)
◯ Did not invest resources at all ◯ Invested few resources
◯ Invested a moderate amount of resources
◯ Invested several resources ◯ Invested much resources
◯ DK/RF

Q51. To what extent is your business exposed to information about innovations made by similar companies? (Information regarding product development, production technologies, marketing methods, etc.)

- ◯ Not exposed to this information
- ◯ Exposed a little
- ◯ Exposed moderately
- ◯ Exposed to a great extent
- ◯ Extremely exposed
- ◯ DK/RF

Q52. The following set of questions are related to the ways in which you make decisions. There are no right or wrong answers. Please rate how strongly you agree with the following statements on a scale from 1 (strongly disagree) to 5 (strongly agree).

- ◯ We rely on the personal experience of the management team
- ◯ We rely on the experience of the employees in the organization
- ◯ We rely on intuition and gut feelings
- ◯ We rely on information from external consultants
- ◯ We rely on data, facts, and insights

Q53. Does your business implement a risk management program?

- ◯ Yes
- ◯ No
- ◯ DK/RF

Q54. On a scale from 1 (strongly disagree) to 5 (strongly agree), please indicate your level of agreement with the following statements.

- ◯ We have a clear understanding of the risks the business can face
- ◯ We take actions to reduce risks
- ◯ We have contingency plans in the case that potential risks actually do occur
- ◯ Other issues in business management take priority over risk management

Q55. Which of the following types of insurance does your business have? (Select all that apply)

- ◯ Building insurance
- ◯ Content insurance
- ◯ Third-party insurance
- ◯ Professional liability insurance
- ◯ Employers liability insurance
- ◯ Product liability insurance
- ◯ Loss of profits insurance
- ◯ Cyber insurance
- ◯ Other:____
- ◯ DK/RF

Q56. The following statements refer to your attitudes regarding cybersecurity. There are no right or wrong answers. Please rate the following from 1 (strongly disagree) to 5 (strongly agree).

- ◯ cyberattacks are a growing threat to businesses.
- ◯ My business is too small for hackers to bother attacking it.
- ◯ There is too much information circulating around cyberattacks that it overwhelms and confuses me.
- ◯ My business was not attacked so what we are doing is probably good enough.
- ◯ Small and medium-sized companies do not have the means to follow and implement all the guidelines in the field of cybersecurity.

Interviewee Demographics

Q57. How old are you? (in years)

Q58. What is your gender?

- ◯ Male
- ◯ Female
- ◯ Other:____
- ◯ RF

Q59. What is the highest level of education you completed?

- ◯ Primary or middle school graduation certificate
- ◯ Matriculation (without certificate)
- ◯ Matriculation certificate
- ◯ Vocational certificate (secondary studies)
- ◯ Certificate that is not an academic degree such as technician or engineer
- ◯ Bachelor's degree or equivalent
- ◯ Master's degree or equivalent, including M.D.
- ◯ Ph.D. or equivalent
- ◯ Yeshiva
- ◯ Other:____
- ◯ Refuse to answer

Q60. How long have you held your *current position* in the business?

Q61. How long have you been in this profession?

Q62. How would you describe your level of technological knowledge?

- ◯ No knowledge: I don't use a computer.
- ◯ Basic knowledge: I can use a computer for basic purposes, such as working with Microsoft Word.
- ◯ Intermediate level of knowledge: I feel comfortable using a computer and can solve problems on my computer if necessary.
- ◯ Advanced: I have advanced ability to install programs/solve related problems.
- ◯ Professional: I have professional background and the ability to program; professional knowledge of advanced technologies; relevant formal education
- ◯ Refuse to answer

Q63. Where did you acquire your technological knowledge and skills? (Select all that apply)

- ◯ I never acquired technological skills
- ◯ High school studies/engineer
- ◯ Academia (Bachelor's and Master's degrees)
- ◯ Professional training
- ◯ Military service
- ◯ Work experience
- ◯ Personal experience / Self-taught
- ◯ Other:____
- ◯ Refuse to answer

C Expected Damage from Cyber-Attacks from Interview Participants

#	Data Recovery Cost	*Operational Damage	*Financial Fines	IP Leakage	Reputational Damage	Bankruptcy	Aggregated Damage Severity
P1	✓	✓					⊙
P2	✓						○
P3	✓						○
P4	✓	✓	✓		✓	✓	◉
P5	✓	✓	✓		✓	✓	◉
P6	✓		✓	✓			◉
P7		✓	✓	✓	✓	✓	◉
P8	✓						○
P9				✓			◉
P10	✓	✓	✓				◉
P11			✓	✓	✓	✓	◉
P12		✓	✓		✓		◉
P13	✓	✓	✓		✓		◉
P14	✓						○
P15	✓	✓	✓		✓		◉
P16	✓	✓	✓	✓	✓	✓	●
P17	✓	✓	✓		✓	✓	◉
P18	✓	✓				✓	◉
P19	✓	✓	✓	✓	✓	✓	●
P20	✓	✓	✓	✓	✓	✓	●
P21	✓	✓		✓			◉

*Operational Damage: No access to the business computers temporarily
*Financial Fines: Due to failure to comply with regulations

● - Very Highly, ◉ - Highly, ⊙ - Medium, ⊙ - Low, ○ - Very Low

D Interview Qualitative Analysis Codebook

Digital Asset	Customer data		list of customers	**Awareness Impact**	Risk covered by	consulting agency
			financial data			insurance
			other sensitive data			government agency
	Business data		list of employee		Level of inconvenience	restoring lost data
			financial data			perceive no inconvenience
	Operational data		website availability		Hinder operation	financial lost
			operational system access			reputation damage
	Intellectual property					perceive no harm
					Attack experienced by others	
Defense	Technical		cloud/local backup	**Information Source**	External human	other institution	
			version updates/ renew license			IT consultant	consulting agency
							individual
			security products		External non-human	policy	security standards
			firewall				security regulations
	Organizational	policy	security regulation/ security standard			conference & lectures	
						journals	
		training	incident response plan			news	
			employee training		Personal	education	
			phishing simulation			military service	
			emergency drills			cyberattack experience	

E Awareness Level 1 and Level 4 Regression Coefficients

Level 1 Variables	Coefficients	Standard Errors	Level 4 Variables	Coefficients	Standard Errors
Has Cyber Insurance	**0.432***	(0.194)	Has Cyber Insurance	**25.68*****	(15.75)
Revenue: 1-5	0.188	(0.195)	Digital Assets: Customer list	2.177	(1.171)
Revenue: 5-10	**0.120***	(0.144)	Digital Assets: Customer financial data	1.438	(0.597)
Revenue: 10+	**0.086****	(0.105)	Digital Assets: Other customer sensitive data	**4.264*****	(2.048)
Revenue: undisclosed	**0.09*****	(0.084)	Digital Assets: Employee data	-0.577	(0.282)
Sector: Professional Services	0.516	(0.399)	Digital Assets: Operational system	1.135	(0.609)
Sector: Trade	**4.976***	(4.734)	Digital Assets: Operational data	1.754	(1.036)
Sector: Info. and Comm.	1.064	(0.869)	Digital Assets: Intellectual property	**2.724****	(1.291)
Sector: Production	1.677	(1.579)	Digital Assets: Business financial data	0.571	(0.255)
# of Digital Assets	0.881	(0.247)	Website: Hosting product or service information	1.675	(1.078)
Has a Website	1.370	(0.771)	Website: Selling product or service	0.800	(0.398)
Website: Hosting product or service information	0.896	(0.392)	Website: Displaying personalized content	2.405	(1.443)
Website: Selling product or service	**2.203****	(0.765)	Website: Software as a service (SaaS)	2.337	(1.463)
Website: Displaying personalized content	1.135	(0.481)	Uses CRM or ERP	**5.443*****	(2.816)
Website: Software as a service (SaaS)	**2.360****	(1.032)	Uses CRM or ERP: undisclosed	**4.701*****	(2.669)
Uses CRM or ERP	**2.250****	(0.822)	Remote Work: Yes	0.832	(0.414)
Uses CRM or ERP: undisclosed	**2.527****	(1.055)	Remote Work: No	**0.384***	(0.221)
Revenue (1-5) X # of Digital Assets	1.374	(0.432)	Program Installation: Cloud	0.607	(0.456)
Revenue (5-10) X # of Digital Assets	**1.896***	(0.680)	Program Installation: Cloud & Local	**1.832***	(0.837)
Revenue (10+) X # of Digital Assets	1.514	(0.489)	Program Installation: Local	**0.310***	(0.201)
Revenue (undisclosed) X # of Digital Assets	**1.662***	(0.47)	Program Installation: undisclosed	**0.117*****	(0.0772)
Sector (Prof. Service) X # of Digital Assets	1.280	(0.261)	Constant	**215.9*****	(185.8)
Sector (Trade) X # of Digital Assets	**0.489****	(0.146)			
Sector (Info. & Comm.) X # of Digital Assets	1.151	(0.242)			
Sector (Production) X # of Digital Assets	0.774	(0.166)			
Constant	0.607	0.574			

*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$

F Business Characteristics Impacting Awareness of SMB Decision-Makers

Variables	Low Awareness 1	Low Awareness 2	Low Awareness 3	Low Awareness 4	Low Awareness 5	2+ Low Awareness	No Low Awareness
Size: 6-10	-0.0522	**0.576***	**1.023****	0.449	0.272	0.491	0.481
	(0.356)	(0.343)	(0.330)	(0.395)	(0.323)	(0.317)	(0.327)
Size: 51-100	-0.491	0.256	0.402	**1.150****	**-0.775***	-0.0893	**0.729***
	(0.429)	(0.385)	(0.374)	(0.481)	(0.408)	(0.364)	(0.422)
Sector: Professional Services	-0.488	-0.492	-0.159	0.457	**-0.651***	**-0.857****	0.428
	(0.394)	(0.356)	(0.335)	(0.385)	(0.352)	(0.346)	(0.339)
Sector: Trade	-0.289	0.131	-0.369	-0.587	-0.457	-0.479	0.606
	(0.565)	(0.479)	(0.508)	(0.682)	(0.498)	(0.485)	(0.463)
Sector: Info. & Comm.	0.332	**-1.075****	**-1.045****	0.401	0.135	-0.403	0.315
	(0.402)	(0.477)	(0.473)	(0.425)	(0.369)	(0.385)	(0.382)
Sector: Production	0.123	-0.0811	0.285	0.339	**-1.026***	0.111	0.0508
	(0.513)	(0.446)	(0.419)	(0.509)	(0.545)	(0.416)	(0.447)
Revenue: 1-5	-0.155	0.0228	-0.231	-0.183	-0.731	-0.765	0.153
	(0.516)	(0.537)	(0.527)	(0.543)	(0.512)	(0.486)	(0.535)
Revenue: 5-10	-0.766	-0.484	-0.261	-0.792	-0.384	**-1.103****	0.747
	(0.598)	(0.643)	(0.599)	(0.625)	(0.549)	(0.561)	(0.560)
Revenue: 10+	-0.637	0.268	0.454	-0.822	0.176	-0.318	-0.313
	(0.567)	(0.563)	(0.558)	(0.583)	(0.518)	(0.505)	(0.579)
Revenue: Undisclosed	-0.765	0.0436	-0.269	**-0.885***	-0.411	**-0.903****	0.287
	(0.488)	(0.493)	(0.487)	(0.521)	(0.450)	(0.442)	(0.492)
Tech. Intensity: High	0.532	-0.0366	**-0.868****	0.250	0.481	-0.495	**-0.524***
	(0.324)	(0.330)	(0.348)	(0.331)	(0.296)	(0.316)	(0.309)
Experienced Cyberattack	-0.166	**-1.190*****	**-0.720****	**-0.618***	0.0456	**-0.967*****	**0.617****
	(0.348)	(0.382)	(0.343)	(0.374)	(0.312)	(0.343)	(0.287)
Constant	**-0.920***	-0.783	-0.665	**-1.405****	-0.636	-1.780**	0.362
	(0.515)	(0.525)	(0.518)	(0.551)	(0.482)	(0.517)	(0.473)
Total Percentage	20%	23%	27%	20%	25%	34%	29%

Standard errors in parentheses
*** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$