Revealing Barriers to Cyber-Protection Among Small and Medium Businesses

Oren Heller, Yuanhaur Chang, Yaniv Shlomo
Ella Bokobza, Ning Zhang, Michal Grinstein-Weiss
Social Policy Institute, Washington University in St. Louis, MO, USA

March 2024

Acknowledgments. The Social Policy Institute thanks Mastercard and its FinSec Innovation Lab for their sponsorship of this research. We also thank the following external members of this study's Advisory Board for their support: Ido Aharoni (former Israel Consul-General to New York), Iddo Bar Noy (Israel National Cyber Directorate), Nir Ben Aharon (Israel Ministry of Economy and Industry), Dadi Gertler (Israel National Cyber Directorate), and Yona Hollander (Architect, Rescana).

1 Introduction

Small and medium businesses (SMBs) contribute significantly to the global economy. According to the World Bank, SMBs represent 90% of businesses and more than 50% of employment worldwide [2]. In addition, SMB ownership helps facilitate upward social mobility by building wealth and assets. However, even though the financial gain of owning a business is high, so too are the risks, especially when the age of digitization has transformed how SMBs manage their digital assets. Like large enterprises, SMBs face risks of being attacked by hackers [21]. But with their fewer resources and a general lack of cybersecurity knowledge, they can be more vulnerable to these attacks [25]. A recent survey conducted on SMBs [1] in Israel found that only 22% of them were aware of the cybersecurity recommendations provided by the Israeli National Cyber Directorate [1], showing the negative impact of resource constraints on the security preparedness of small and medium-sized businesses.

Due to having only a limited number of employees, key decision-makers such as the owner or manager of small and medium businesses often play a principal role in deciding various topics [20], including cybersecurity defense implementations, which could have a great impact on the ultimate fate of the company. However, due to limited knowledge backgrounds, they may base their decision solely on their own perception of the defensive measures' cost-effectiveness, instead of the reliability or strength of the defense measures. It is therefore vital to understand the company's current security status, as well as the extent of decision-makers' misconceptions between perception and the real world when implementing security strategies. Focusing on the human component in this study, including perceptions, attitudes, and behavioral patterns associated with cybersecurity, we can develop insights and recommendations that motivate SMBs toward better cybersecurity and secure management.

[1] Small businesses have 6 to 50 employees and Shekels 10M-25M in revenue; Medium businesses have 51 to 100 employees and Shekels 25M-100M in revenue.

Key Research Questions. To facilitate the development of intervention guidelines and inform policy regulations to support SMB security development, as well as to motivate SMBs to implement securer defense, we aim to develop a deeper understanding of how key decision-makers make cybersecurity decisions. The goal of our project is to answer the following research questions:

- **RQ1:** What are key decision-makers' perceived cyber threats and risks for SMBs?
- **RQ2:** How do SMB key decision-makers weigh the cost and effectiveness of the defenses, as well as their impact on company operation?
- **RQ3:** What factors influence SMB key decision-makers' security perception?
- **RQ4:** What are the perceived roadblocks and interventions toward 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 their actions and decisions in facing challenges including operational damage, financial damage, reputational damage, and more. 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 development of the quantitative study.

Contribution 2: Quantitative analysis on the correlation between situational awareness and business attributes. For the quantitative part of the study, we recruited 322 decision-makers to understand how they perceive real-world cyber threats and their company's own defense. We closely examined if and how business size, business sectors, annual revenue, and technological intensity can impact a decision-maker's situational awareness, which we employed as a guide to evaluate key decision-makers' perceptual misalignment regarding cybersecurity issues. We predict the awareness issues

that a business with certain characteristics would likely face, and we explain the relationship between awareness levels and business attributes, locating businesses on the ladder of situational awareness according to their characteristics.

Contribution 3: Cluster analysis of SMB types and holistic structural equation model. We conducted a cluster analysis and grouped our business sample into 5 major types according to their situational awareness at each level and calculated the *relative cautiousness* of each group, the clusters help generalize the current status of SMB cybersecurity, which is essential in developing effective interventions across SMBs of different characteristics and attributes.

Contribution 4: Root causes and interventions for SMB cybersecurity. Reflecting on the semi-structured interviews as well as the findings from the survey studies and cluster analysis, we formulated recommendations and interventions that can be adopted by SMBs who have different awareness levels, potential root causes, and business attributes, hoping to address the gap in SMB cybersecurity, as well as mitigate the perceptual mistakes and increase awareness of company key decision-makers.

2 Existing Work

Cybersecurity with SMBs. Prior work often stress 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 cyber-attacks [3, 9]. For instance, Chen et al. [8] 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. [10] studied how organizations cope with the myriad of known vulnerabilities. Given the flood of vulnerability information, they focused on how comprehensive such information is condensed and filtered by organizations in critical infrastructures and government services, and found that no organization tried to acquire a comprehensive view of published vulnerabilities but rather relied on a single source. While these offered a holistic view of SMB cybersecurity, they did not consider the intrinsic characteristics of the various enterprises under study. Through the first part of our two-stage interview study, we identified that the level of digitalization, or digital intensity, may be a factor affecting how SMBs direct cybersecurity efforts. The second part of our study investigated the panoply of SMBs in the full spectrum of technology exposure, and considered various economic sectors and business size, involving newly formed and rapidly changing businesses, as well as more established ones.

SMB Cybersecurity with Key Decision-Makers. Several prior works studying security and privacy in a business setting often attempted to understand the issues through the lenses of a single targeted population within the business [4, 16, 23–25]. Wolf et al. [25] studied security obstacles from the perspective of Chief Information Security Officers (CISOs), collecting responses from CISOs and regarded them as third-party observers of the actions of SMBs. On the other hand, Stegman et al. [23] studied employees' concerns over the ambiguous data collection within the enterprise security software. Meanwhile in [5], Bartette et al. studied the factors behind the security protective behaviors based on the protection motivation theory in the diverted focus of two differentiated subgroups of stakeholders, SMB owners and non-owners. The extension of their work [6] took a similar approach of trying to explain the CEO's cybersecurity decisions with social peer pressure. Recognizing that SMB owners or managers often play a principal role in deciding various topics [20] due to having only a limited number of employees operating in a small form factor, our work chooses to study the SMB key decision enablers, as they are often the ones who are in a position to direct the cybersecurity initiative, while needing to consider the bigger picture and trade-off security with business operation at the same time. This positioning is similar to [4, 14, 24]; however, these works overlooked how security is traded off for other operational factors, as well as whether the decision-maker's perception misaligns with the real-world situations. They also suffered from the lack of adequate sample size, which we address by conducting large-scale interviews with decision-makers from a diverse and comprehensive set of SMBs.

Exploring Security Trade-Off and Perception-Action Relationship. In addition, [25] and [15] identified some opportunities to motivate SMBs to make IT improvements, with Huaman et al. [15] conducting computer-assisted telephone interviews to explore the relationship between reported attacks and deployed security measures, as well as how company characteristics such as size and economic sectors affect such decisions. However, how SMB decision-makers weigh the pros and cons of these security measures is yet to be known. Understanding the reasons behind their beliefs can be potentially invaluable for creating incentives that reinforce secure behavior while dismissing misconceptions regarding cybersecurity. To this end, we recognize the work of Renaud et al. [22] as closely related, studying the security controls and precautions regarding Endsley's model of situation awareness. In our work, we take a different perspective of SMB cybersecurity research using the situational awareness model to study SMB key decision-makers' risk perceptions, as well as attempt to draw correlations between perceptions 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.

3 Interview Study

To understand how decisions are made in SMBs and to obtain a framework for the main survey development, we conducted

Table 1: Demographics of key decision-makers and businesses in the interview study.

#	Economic Sector	Yrs Exp	Gender	IT BG	Employees (> 50)
P1	Accommodation and food services	6	M		✓
P2	Manufacturing	22	F		
P3	Administrative and support service activities	6	M		
P4	Financial and insurance activities	-	F		
P5	Financial and insurance activities	9	M		
P6	Construction	-	F		✓
P7	Information and communication	-	M		
P8	Manufacturing	29	M		
P9	Information and communication	-	M	✓	
P10	Wholesale and retail trade	20	F		
P11	Information and communication	-	F		
P12	Professional, scientific and technical	16	M		
P13	Accommodation and food services	10	M		
P14	Professional, scientific and technical	5	F	✓	✓
P15	Accommodation and food services	25	F		
P16	Professional, scientific and technical	20	M	✓	
P17	Information and communication	18	M	✓	
P18	Manufacturing	15	M	✓	✓
P19	Professional, scientific and technical	4	M	✓	
P20	Information and communication	2	M	✓	✓
P21	Manufacturing	23	M		✓
Avg:		**15 (SD 8.4)**			

Yrs Exp: decision-maker's year of experience in the business
IT BG: whether decision-makers have IT background

Table 2: Detailed statistics on company operation, use of technology, and interviewee's age and gender distribution.

	Ratio (n=21)
Company Operation	
Activity abroad	33.3%
Work from home	61.9%
Outsourced security consulting	66.7%
Use of Technology	
Cloud storage	85.7%
Customer relationship management (CRM)	52.4%
Company website	76.2%
Interviewee Age	
< 36	9.5%
36-50	57.1%
> 50	33.3%
Interviewee Gender	
Male	66.7%
Female	33.3%

an initial interview study exploring how SMB executives navigate cybersecurity decision-making. Our study was formally approved as exempt by our university's Institutional Review Board (IRB).

Recruitment Method. We recruited interviewees through personal connections and word-of-mouth while meeting the Israeli definition of small and medium businesses. We aim to recruit a representative sample comprising interviewees whose business belongs to different economic sectors as defined by ISIC Rev 4 classification [18] of the United Nations. In the end, we interviewed 21 key decision-makers who are diverse in both personal and professional backgrounds and have the mandate for cybersecurity policies in the business, including company owners, CEOs, CTOs, and department managers. Moreover, businesses come from different sectors of the economy, with varying company sizes and levels of digitization, ensuring that our sample was diverse in terms of SMB challenges. No participants were compensated. Participant demographic and company information are presented in Table 1, with additional statistics provided in Table 2.

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 will ask questions related to:

- Background information: participants' and the business' general background information, such as the makeup of the team, the digital assets they own, and the operation of the company.
- Knowledge source: participants' source of knowledge regarding IT security in a business setting.
- Business risk and defensive measures: participants' perceived risk of their business being attacked, the defensive measure already in place, and whether they have experienced cyber-attacks before.

Ethical Considerations. All interviews were conducted in Hebrew and were audio-recorded. The recordings were then professionally transcribed and translated for analytic purposes. Confidentiality and anonymity were given careful attention, and we refrained from putting any identifiable information into our results.

Thematic Coding. We deployed thematic analysis [7] to identify themes that help answer our research questions. To avoid the result being biased by one researcher's subjectivity, two coders independently and iteratively went over the transcripts, noting and refining the themes and codes in each iteration. The themes and codes were then discussed and the differences were resolved until all coders reached an agreement on the final codebook, which is presented in Appendix B. By documenting what kind of damage the decision-makers care about, we surface the various challenges that need to be overcome to ensure the survival of SMBs of different characteristics.

4 Interview Results

In this section, we describe our insights gathered from the interviews. We summarize key decision-makers' perceived risks based on digital assets in § 4.1, their reasons for defense deployment in § 4.2, and factors influencing their security perception in § 4.3.

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

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 about 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. (P1)"*

Operational data for service availability and safety. Some SMBs stated that assets essential to company service should be protected since the lack or leakage of those can cause major operational issues. Many interviewees mentioned having a website to promote their business or as a mean of communication with the customers. The availability of the 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 they have more concerns about 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)*

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

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 in the cloud. Everything is also printed and saved in binders."* However, other than stating this defensive measure, we observed that most interviewees 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 considered backed up and secure. P14 shared from 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 awareness 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 refused to implement employee training, even after having encountered ransomware attacks. Owners who made this decision are eager to "get back to normal". As long as the business can continue, they do not seem to care. P5 reasoned, *"We didn't see any point [to do training] because we didn't know the source and also the fact that the attack already happened. We wanted to return the office to function."*

Minimal effort on firewall, antivirus software, and guideline implementation. Only SMB managers 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."*

4.3 Factors of Influence and Challenges

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

External Human Source. Some key decision-makers seek advice from or outsourced 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 that 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)"*

External Non-Human Source. A few SMB executives rely on non-human sources to obtain the security knowledge necessary for company operation. When asked if there are other information sources beyond meetings with IT companies, 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 nature of the business' economic sector, business owners 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)."*

Personal Background and Experience. Some key decision-makers we interviewed have educational backgrounds in IT, and they mentioned using their personal expertise as a source for security judgment. Interestingly, three SMB owners we interviewed 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 cyber-attacks. 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 services 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."*

4.3.2 What external factors impact SMB key decision-makers' security activeness?

Whether risks are covered by another entity. From our interviews, we observed that when the risk can be offloaded to or mitigated by another agency or institution, executives tend to be more indifferent toward security issues. While this includes hiring third-party consultants to assist the process as described in § 4.3.1, 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 in business operations, participants would consider deploying 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)"* Meanwhile, 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, and anyone can do it. There will be no harm."*

Whether attacks hinder company operation. In addition to financial loss that may be the result of service downtime, a business's reputation can also be affected by cyber-attacks, 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, we also discovered that when the data is evaluated to be "non-essential", 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 (par-

ticularly in the same sector) 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."*

Whether clear guidelines/regulations exist. 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 calls for the implementation of a clearer guideline, noting that *"someone should make some characterizations of several levels of companies and explain what each level should do for cyber security."* Furthermore, P9 reinforced the point by saying, *"If I would get some guidance from governmental agencies I would read them and selectively apply their recommendations."*

Similarly, 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."* Demonstrating the demands of governmental guidance and regulation, as well as their importance and potential effect in aiding SMB security.

5 Online Survey

Leveraging the findings from our previous interviews and qualitative analysis, we developed and conducted an online survey study to explore how SMB executives navigate cybersecurity decision-making. Our study was formally approved as exempt by our university's Institutional Review Board (IRB).

5.1 Survey Design

Screening & Background. For screening, we asked several questions regarding some background of the participants and their businesses. We exclude businesses that are not privately owned, as well as those that do not fit the definition of small and medium businesses. We interviewed only owners/CEOs/Vice Presidents/Manager who reports directly to the CEO or the owner of the business. We also recorded the economic sector the businesses belong to, their revenues, and their locations.

Risk Exposure. We also investigated the company's risk exposures characterized by the ownership of different types of digital assets and the digital technologies deployed, which we termed "technological intensity". For the technological intensity of a business, we referenced the Digital Intensity Index (DII) from Eurostat index [11] with some modifications. Specifically, we assigned SMB one point any time one of the following is true:

- Company employs ICT experts
- 50% of the employees use the Internet for work purposes
- Company has a website
- Company's website has advanced functions (order tracking, personalization, etc.)
- Company purchases advanced cloud services (CRM, computing power, software, etc.)
- Company has online trading
- Company analyzes Big Data

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.

Situational Awareness. The bulk of our survey was designed with the situational awareness model in mind, which we detailed in § 5.3. According to this theory [12], awareness can be theoretically broken down into (1) the general acknowledgment and basic understanding of a certain matter, (2) the construction of a coherent and comprehensive knowledge map of a matter, and (3) the obtainment of sufficient information and knowledge to yield the necessary and appropriate actions.

Our model exhibits 5 levels: (1) Not being aware of the importance of cyber security to business continuity, (2) Not being aware of the risk of being exposed to a cyber attack, (3) Not being aware of cyber security precautions and controls, (4) Not being aware of the need to act, and (5) Lack of resources. Each level is coupled with specific questions to collect participant responses, examining how perceptions and barriers affect SMB cybersecurity. In addition to evaluating the specific barriers that businesses face when implementing cyber security measures, the survey studies the core reasons for the barriers. Specifically, we looked at how inadequate risk management, lack of technological orientation, business decision-making style, and difficulty in information navigation can be used to explain the barriers.

Participant Demographics. As the last questions, we asked about participants' general demographic questions, including age, gender, education level, technical background, seniority, etc. Participants can choose to not disclose the information if they do not wish to. We use these data to account for the participants' demographic diversity.

5.2 Survey Methodology

Pilot Study. We piloted the survey with 20 SMB executives to improve question clarity and adjusted the length of the survey to avoid survey fatigue. The final survey instrument is included in Appendix C.

Table 3: Demographic of Survey Participants and Businesses

Business				Interviewee					
# of Employee	6-10	26.70%	50.00%*	Position	Business owner	7.80%	Gender	Male	54.00%
	11-50	55.00%	45.00%*		CEO	7.80%		Female	46.00%
	51-100	18.30%	6.00%*		Vice President	12.70%	Seniority (years)	1-4	12.70%
Economic Sector	Services	31.40%	39.00%*		Manager	71.70%		5-9	18.60%
	Professional services	28.00%	18.00%*	Age	25-34	25.20%		10-14	20.20%
	Trade	9.30%	27.00%*		35-44	28.60%		15-19	12.10%
	Information and communication	18.90%	6.00%*		45-54	26.70%		20+	35.10%
	Production	12.40%	9.00%*		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

Participant Recruitment. We recruited participants via an online survey company during July and August 2023. After filtering out 12 low-quality responses, we have a total of 322 responses from key decision-makers. The survey took about 30 minutes to complete and participants were compensated. Participant and business demographics are presented in Table 3.

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 [17], each business size and economic sector still has an adequate representation in our studied samples. The only attribute that we found difficult to account for is business revenue, as these are often considered trade secrets and were refused to provide.

Ethical Considerations. All responses were collected through self-report measures, and participants were not required to disclose any information they did not want to share. Confidentiality and anonymity were maintained throughout the research. All participants are required to give written consent prior to completing the survey.

5.3 Situational Awareness Model

For each of the situational awareness levels, we defined and calculated a variable indicating the status of SMBs at each level. We further employed these variables to identify SMBs with relatively low values as having low awareness at the corresponding level. We discuss how we evaluate each awareness level as follows:

Level 1: Not being aware of the importance of cyber security to business continuity. Decision-makers at this level are characterized by a lack of basic understanding of cybersecurity matters. They also tend to underestimate possible damages faced by their company. To assess SMB decision-makers' awareness of the importance of cybersecurity to business continuity, we wish to compare key decision-makers' self-assessments of their business's potential damage and the actual potential damage due to cyber-attacks. If the decision-maker anticipates low damage but the business may actually face severe damage, then it is implied that the decision-maker exhibits low awareness of the importance of cybersecurity to business continuity. It should be noted that this actual potential damage is regardless of the precautions taken by the SMB.

However, since our data is based on a self-report survey, we lack objective information about the actual potential damage to SMBs in case of cyber-attacks. Nevertheless, our data does include information from which we can infer about this damage. For instance, the more digital assets an SMB possesses and the more sensitive the functionality of its website, the higher the damage can be as a result of cyber-attacks [13]. This relationship is demonstrated in Figure 1, which shows self-reported perceptions about severe damage as a function of the number of digital assets and website functionalities. We used the SMB population in our study and related SMBs' attributes and decision-makers' perceived potential damage. This created "crowd wisdom", which we used as a benchmark to compare whether the self-assessments of potential damage fit the business' attributes, in comparison to other SMBs with similar attributes. Specifically, we identified SMB decision-makers whose damage assessment was substantially lower than that of comparable SMBs.

To do so, we estimated the following logistic regression model:

$$log\frac{pr(Damage_i=1)}{1-pr(Damage_i=1)} = \beta_0+\beta_1 X_i^{Level\ 1}+\varepsilon_i \quad (1)$$

where, $Damage_i = 1$ if the answer to the question *"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%).

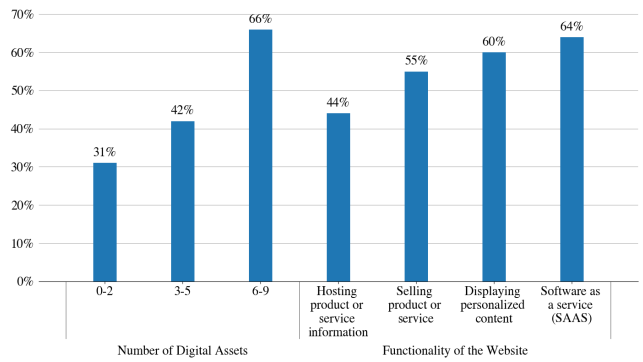


Figure 1: Probability of severe damage to the business due to cyber-attack, grouped by the number of digital assets and website functionality disclosed by interviewees.

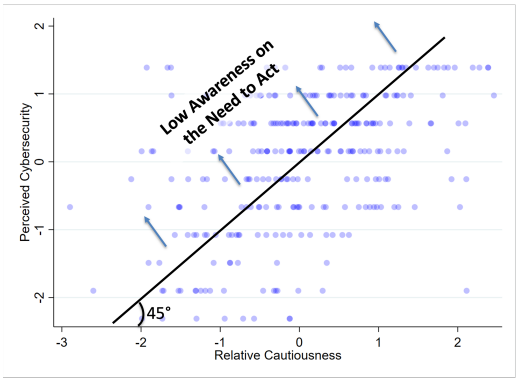


Figure 2: Decision-makers above the 45° line perceive strong cyber protection despite lower relative cautiousness.

The variable $X_i^{Level\ 1}$ includes all the aforementioned dimensions, including the number of digital assets, whether there's a business website and its functionality, number of employees, economic sector, annual revenue, whether the business has cyber insurance, and interaction terms between the economic sector and the number of digital assets, and annual revenue and the number of digital assets. The regression results are included in Appendix G.

The estimated coefficients β_0 and β_1 represent the average relationship between business attributes and the probability of facing severe damage if all digital assets were lost, over our SMB samples, as declared by the decision-makers. 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 other businesses. We standardized ε_i and used it as a level 1 awareness measure. We defined an SMB 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. Decision-makers at this level often have misconceptions about the probability of being attacked. To study SMB decision-makers' awareness of the risk of being exposed to an attack, we asked a self-assessment question, *"On a scale of 0 to 10, what is the likelihood that a business like yours will be attacked in the coming year?"* This variable is standardized and used as a level 2 awareness measure. Those whose self-assessment falls below the 23% threshold (0: 12.8% or 1: 10.6%) were grouped as having low awareness level 2.

Level 3: Not being aware of cyber security precautions and controls. Decision-makers at this level are characterized as lacking knowledge and understanding regarding the actions that need to be taken. To study SMB decision-makers' cyber security precautions and controls, we asked a self-assessment question, *"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 is standardized and used as a level 3 awareness measure. Those whose self-assessment falls below the 27% threshold (1: 13.8%; 2: 13.4%) were grouped as having low awareness level 3.

Level 4: Not being aware of the need to act. Decision-makers 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 figure out which SMB has such a misconception, we first assess to what extent are SMB precautions adequate to its needs. To this end, we estimated the following linear regression model:

$$Precautions_i = \gamma_0 + \gamma_1 X_i^{Level\ 4} + u_i \qquad (2)$$

where $Precautions_i$ is the number of protective measures of the SMB. The variable $X_i^{Level\ 4}$ includes the following SMB attributes: type of digital assets, website functionalities, whether the business has cyber insurance, whether it uses ERP or CRM, whether its workers work remotely, and whether business applications are installed on the cloud. The regression results are included in Appendix G. The residual term u_i represents business i's deviation from the average number of precautions over our population sample, given its attributes included in $X_i^{Level\ 4}$. A large u_i stands for over-cautiousness, and a low u_i stands for under-cautiousness relative to other SMBs. We hereafter refer to the standardized u_i as *relative-cautiousness*.

We next associate the relative-cautiousness with the subjective perception of risk. This allows us to address SMBs decision-makers whose risk perception does not fit its cautiousness. Specifically, we wish to identify under-cautious decision-makers who believe their business is safe. To do so, we stress a 45° line between participants' answers to the question, *"On a scale of 1 to 10, what is the level of cyber*

[2] Those who assessed no damage at all in case of losing all digital assets were also included as having low awareness level 1, 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 awareness level 1, even if they were defined as such by the described mechanism.

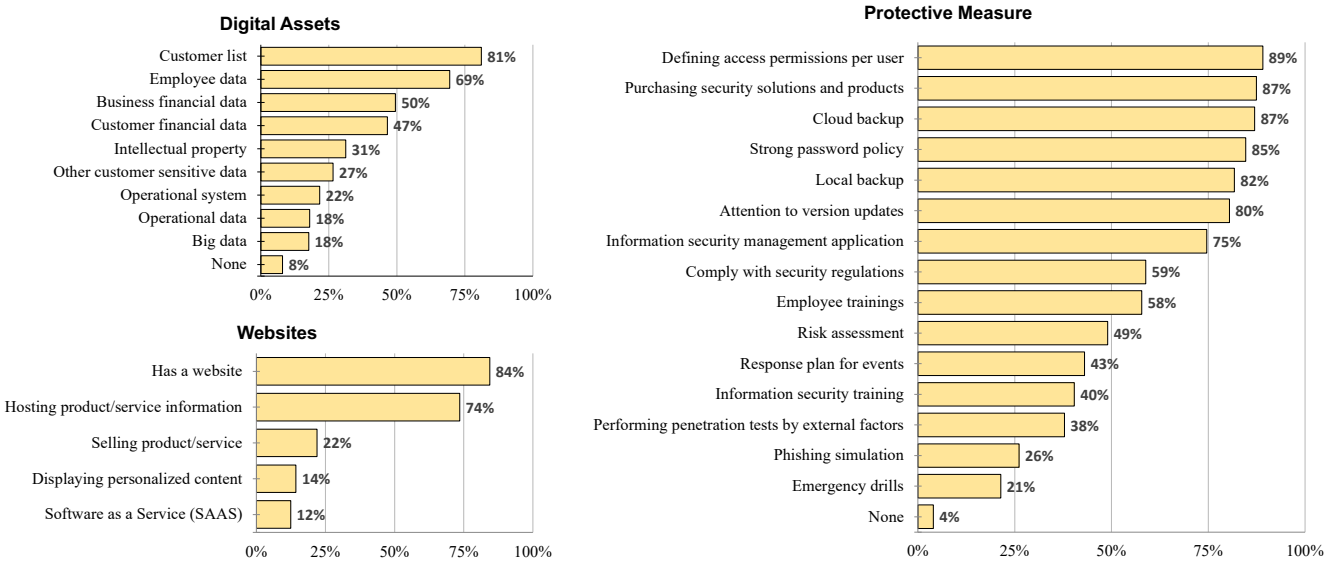


Figure 3: Percentage of SMBs owning digital assets, websites, and protective measures deployed (N = 322).

protection in your business?", with the relative-cautiousness, both being standardized measures, as shown in Figure 2. Accordingly, level 4 awareness equals the distance from the 45° line, where SMBs above the line show low awareness and those below refer to high awareness. We define those at the lowest 20% as having low level 4 awareness.

Level 5: Lack of resources. Decision-makers at this level often face challenges related to a lack of resources for cybersecurity, even though they understand what needs to be done. To study SMB decision-makers' lack of resources, 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 when engaging in cybersecurity. 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 awareness level 5, which took up 25% of the sample (lacking 1 item: 16%; lacking 2 items: 7%; lacking 3 items: 2%).

6 Quantitative Analysis Results

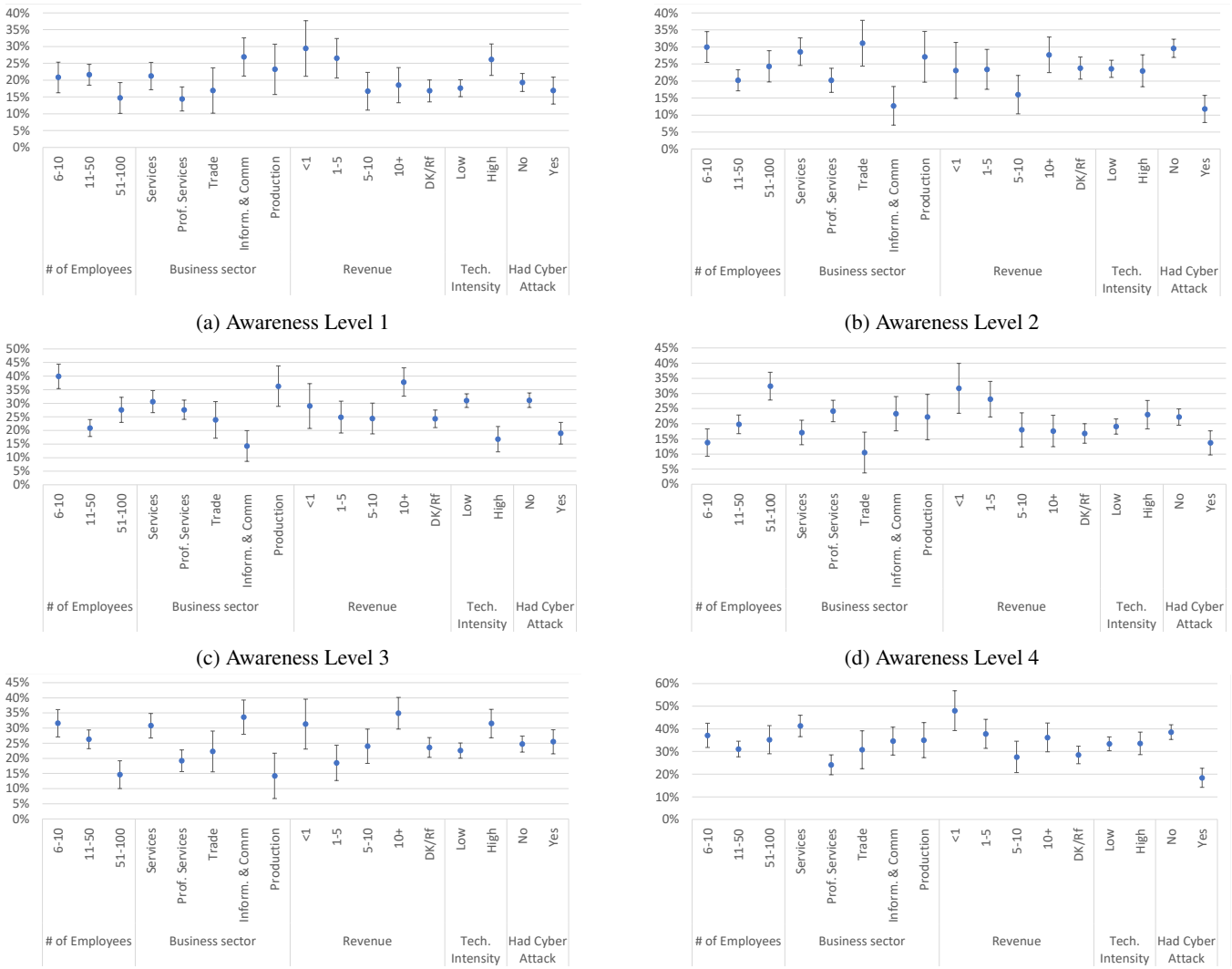
Digital Assets and Protective Measures. Our survey results regarding digital assets and protective measures are presented in Figure 3. Based on our survey, the type of data that most SMBs own regardless of business attributes are personal data of the customers and employees. In addition, a majority of 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 deployed in the business, 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 agrees with findings from [15] in Germany. It is also worth noting that around 4% and 8% of the SMBs shared they do not own any digital assets or implement any protective measures, respectively.

6.1 Situational Awareness vs. Business Characteristics

Figure 4 shows the marginal probabilities for low awareness in each of the levels, grouped by different business attributes. The corresponding coefficients and standard errors are included in Appendix F. We describe our findings below:

Level 1. We found that SMBs with less than 1 million annual revenues are most likely to ignore the importance of cyber security. SMBs that are in the Professional Service sector or have more employees can be aware of the importance more easily. Interestingly, those SMBs that have high technological intensity are more likely to be at low awareness level 1 than others who have relatively lower technological intensity.

Level 2. The average assessment given by all interviewees is 3.4, which indicates that a majority of decision-makers do not believe that they are easily exposed to cyberattacks. Meanwhile, decision-makers in the Trade and Production sector perceived a lower risk of cyberattacks than the ones in the Information and Communication sector, making them more vulnerable in case of an attack. Furthermore, decision-makers



(a) Awareness Level 1

(b) Awareness Level 2

(c) Awareness Level 3

(d) Awareness Level 4

(e) Awareness Level 5

(f) Low Awareness in Multiple Levels

Figure 4: Margins from logistic regressions predicting the probabilities of decision-makers having low awareness, grouped by business attributes.

whose businesses have experienced cyberattacks before generally perceive a higher risk of cyberattacks than those who didn't, indicating that decision-makers may learn from past experiences to raise awareness. In addition, businesses of small sizes are also more likely to overlook the risk of cyber-attacks.

Level 3. Based on our survey, more than half (54%) of the respondents claimed 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 of smaller size, 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 4c, where businesses of small size are the most likely to be at low awareness level 3. Meanwhile, decision-makers from the Production sector and high-revenue businesses express a lower confidence in cybersecurity knowledge. Greater confidence in cybersecurity knowledge sufficiency is seen in those from the Information and Communication sector, and those from technology-intensive businesses. Past experience with cyber-attacks may also prompt decision-makers to understand security precautions more.

Level 4. We observed that businesses having revenues of less than one million NIS may become more likely to overlook the need to act. Referring to Figure 4d, we can see that SMBs from the Trade sector are the least likely to be ignorant about level 4 awareness. We also found that most decision-makers who are not aware of the high risk come from businesses of large size or have a relatively high technology intensity. Businesses that have never experienced cyber-attacks before

Table 4: Clustering of 5 major business types in terms of awareness status

	Cluster 1 (N=105; 34%)	Cluster 2 (N=12; 4%)	Cluster 3 (N=90; 30%)	Cluster 4 (N=30; 10%)	Cluster 5 (N=67; 22%)
Situational Awareness 1	-0.03	3.02	-0.15	0.08	-0.37
Situational Awareness 2	0.87	-0.02	-0.59	0.1	-0.55
Situational Awareness 3	0.73	0.03	-0.57	-0.21	-0.25
Situational Awareness 4	-0.15	0.11	0.82	0.37	-1.07
Situational Awareness 5	0.18	0.16	0.17	-2.53	0.48
Relative Cautiousness	0.21	-0.1	0.24	-0.21	-0.57
Description	Doing the right things and aware	Highly aware of cybersecurity importance	Feels ignorant though are actually relatively cautious	Average awareness but lacks resources	Low awareness of nearly all levels

also tend to overlook the need to act.

Level 5. Our survey indicated that around 1 in 5 decision-makers reported that their available budgets and human resources prevent them from implementing better cyber precautions, while 1 in 10 decision-makers indicated the lack of time as a barrier. It is also worth noting that all three resources seem to be in great shortage among smaller businesses. Interestingly, technology-intensive SMBs reported a higher shortage of resources for cybersecurity than those with lower technological intensity. In addition, both businesses with less than one million and more than ten million in revenue indicated the lack of resources as a major barrier to effective cyber defenses. As for the difference between economic sectors, the Service sector and the Information and Communication sector are most likely to be aware of their lack of resources. Small business size also may lead to resource shortage, and past attack experiences do not significantly affect level 5 awareness.

Low Awareness in Multiple Levels. Figure 4f shows which type of business may have low awareness on multiple levels. The number of employees a business has and its technological intensity seems to be minor factors in this regard. In terms of economic sectors, the Professional Service sector is more aware, while the Service sector is less aware. Businesses that make less than one million NIS annually are also more likely to be indifferent toward cybersecurity. In addition, businesses that have no prior attack experiences are significantly more likely to have low awareness on multiple levels.

6.2 Cluster Analysis

We further conducted a cluster analysis and identified 5 major types of businesses according to their overall situational awareness. By looking at businesses' relative cautiousness of individual clusters, we can understand the actual cybersecurity situation of the businesses and devise customized solutions for companies facing different awareness issues. Table 4 presents the result of the cluster analysis.

Cluster 1 to Cluster 3 show high and average relative cautiousness. This implies that the cybersecurity status of the businesses is generally sound and can be considered role models for other companies. For instance, Cluster 1 shows relatively higher level 2 and level 3 awareness, while possessing average awareness in other levels. This cluster involves many businesses that have suffered cyberattacks before (42% vs. 28% in the entire sample, as shown in Appendix I), consisting majorly of the Information and Communication sector and a low representation of the Production sector. The reason for Cluster 1's high relative cautiousness lies in having more cyber protections, rather than having fewer digital assets that reduce the chance of attacks. Cluster 2 is a very small group whose members are highly aware of the importance of cybersecurity and show other situational awareness that is close to the average. Since their relative cautiousness is also close to average, they have the most balanced security defense against potential threats. Cluster 3 is another group of businesses that require minimal intervention. Members of this cluster feel that they don't understand the risks and precautions, even though they are relatively cautious compared to their peers. This group is characterized by having fewer cyberattack experiences (20% vs. 28%) and possessing fewer digital assets (3 vs. 3.4). Their perceptual insecurity eventually leads to over-cautiousness which is beneficial for the security of the business.

Meanwhile, Cluster 4 and Cluster 5 show low relative cautiousness. Businesses in Cluster 4 have an average level of awareness at each level, but severely lack the resources to sufficiently address the problems. Meanwhile, even though Cluster 5 businesses have sufficient resources, they lack awareness at every level. Note that although both groups have low relative cautiousness, Cluster 5 has the lowest relative cautiousness among the five groups, indicating that it is worse to be capable but unaware than aware but incapable. Interventions targeting these two groups specifically are discussed in § 7.4.

6.3 Holistic Structural Equation Model

Using our sample of businesses and online survey, we constructed a holistic Structural Equation Model (SEM) that draws relations between root causes, attack experience, situational awareness, and relative cautiousness among all kinds of businesses, as shown in Figure 5.

Correlation among Awareness 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 the greater perceived knowledge of the precautions and controls can lead to false beliefs that there's no further need to act. In addition, Level 4 is also 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 awareness levels illustrate the fact that the situational awareness model is a maturity model [19], as it is implied that level 1 influences level

2, which influences level 3, and so on. Our findings imply that each level influences the next level, and thereby indirectly influences the relative cautiousness. The findings also suggest that levels 2, 3, and 4 directly influence the relative cautiousness.

Correlation with Other Factors. Except for awareness level 1, all situational awarenesses are positively correlated with relative cautiousness. Meaning that relative cautiousness can be improved by increasing situational awareness. Moreover, experience with cyberattacks influences awareness and hence indirectly improves readiness for cyber attacks. Nevertheless, it influences only the perceived risk of cyberattack exposure, which in turn motivates SMB decision-makers to also improve their knowledge. It is also shown that root causes are strongly related to situational awareness; therefore, they are critical when considering interventions for both Cluster 4 and Cluster 5, as these two are affected most by a lack of awareness. We discuss the role of root causes in our model and the respective interventions in detail in § 7.4.

Besides the root causes' influence on awareness, they are also found to be directly correlated with relative cautiousness. This implies that there are other factors, rather than situational awareness, which are not included in the model, that link between these root causes and cyber security readiness. Such factors could include the demography of the key decision-makers or due to cultural tendencies, and they should be further explored in future research.

7 Discussion

With both qualitative and quantitative analysis, we have a glimpse of the security mindsets of SMB key decision-makers. Modeling situational awareness into different levels and accounting for the root causes of low awareness shed light on the way awareness could be improved. This enables us to devise solutions to focus on increasing the awareness that could help SMBs the most. We finally answer our research questions below.

7.1 RQ1: What are key decision-makers' perceived cyber threats and risks for SMBs?

We conducted an in-depth analysis of 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 hosted company websites to advertise themselves. However, these are often outdated and can become a point of vulnerability. In addition, many companies offer the option for employees to work from home, which may potentially increase an adversary's attack surface. We also collected the types of digital assets and the specific protective measures SMBs deploy. Comparing SMB's number of digital assets and the number of protective measures shows how individual business evaluate their risks, as well as how they fare against cyber-attacks compared with others.

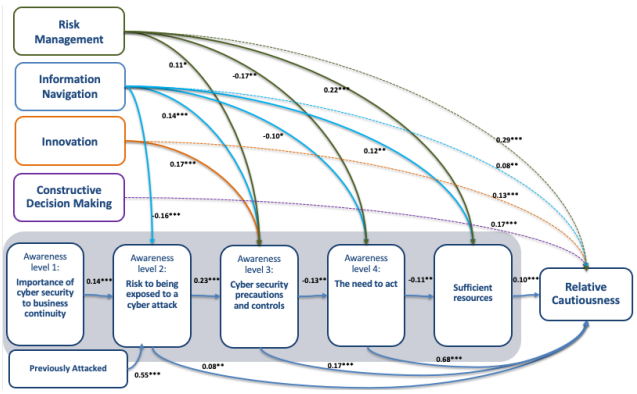


Figure 5: Structural Equation Model of situational awareness, root causes, and relative cautiousness.

7.2 RQ2: How do SMB key decision-makers weigh the cost and effectiveness of the defenses, as well as their impact on company operation?

We observed a tendency for executives to mention more technical measures than employee training, which coincides with the findings of [15]. Interestingly, almost all participants unanimously agreed that backup to cloud storage is important for company operation; however, they have divided opinions regarding the effectiveness of employee training. In addition, SMBs tend to spend minimal effort on implementing firewalls or antivirus software to save budgets, while following guidelines/regulations only if they have to. We also collected SMBs' efforts on security investments to understand how decision-makers allocate their resources. Comparing security investments with key decision-makers' awareness levels shows that the more time decision-makers spend on security efforts, the more likely they are to avoid low awareness of security precautions and the need to act.

7.3 RQ3: What factors influence SMB key decision-makers' security perception?

We uncover the external factors impacting key-decision makers' decisions and their perceived challenges. For example, decision-makers attributed third-party consultants, journals, and news as some of their sources of information. They would also draw from past experiences in cybersecurity, either as an expert in the field or a victim of an incident. Some decision-makers expressed the need for clearer guidelines/regulations to follow. Interestingly, we observed divided views on the impact of security events, with some decision-makers being

motivated to deploy securer defenses, while some are more negligent and only seek to recover as soon as possible to get the business going.

As part of our quantitative study, we also investigated several factors that could have influenced key decision-maker's situational awareness. For awareness level 1 to level 4, whether the company has experienced cyberattacks before actually played a crucial role in deciding whether they have low awareness regarding the importance of cybersecurity, the risks, and the precautions. In addition, being in the Information and Communication sector seems to allow the decision-makers to acknowledge awareness levels 2 and 3. On the other hand, being in a business of a smaller size may prevent decision-makers from reaching awareness levels 2 and 3. As for awareness level 4, both having a smaller business size and being in the Trade sector seem to positively affect decision-maker's awareness. For awareness level 5, business size and annual revenue seem to greatly impact decision-maker's awareness. Interestingly, businesses that have experienced cyberattacks before and companies having annual revenues of 5 to 10 million NIS are more likely to be free of any awareness issues. Those who have low awareness at multiple levels are most likely to be from companies with low annual revenue or have not experienced cyberattacks before.

7.4 RQ4: What are the perceived roadblocks and interventions toward better security?

Inadequate Risk Management. Our holistic model suggested that risk management is highly correlated with situational awareness and also directly correlated with relative cautiousness. Inadequate risk management affects decision-maker's awareness of precautions and the need to act, making them aware of the level of urgency but failing to correctly allocate available resources (e.g., Cluster 4 businesses showing the lowest rating of risk management). For these businesses, how to effectively allocate resources is the key to better security.

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 may not only help build personal connections between SMB executives and government officials, but they may also be the perfect place for educational lectures on how best to manage company resources. Since most SMBs facing this obstacle are from the Trade and Service sector (Appendix H), policies regarding trade incentives, as well as guidance from financial institutions, may also help SMBs adjust their budget allocation.

Difficulty in Information Navigation. The ability to navigate through abundant information can also impact situational awareness and relative cautiousness greatly. In addition to awareness of precautions and the need to act, information navigation is essential for key decision-makers to identify potential cyber threats.

SMB-friendly Information Source. From the policy point of view, more actionable standards and guidelines can be offered to inform SMB's legal obligation in matters of cybersecurity. In addition, 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 recognize and verify the various information sources. Subsidies on counseling services may offer extra aid in offloading some of the decision-making to dedicated experts.

Lack of Technological Orientation and Innovation. Lacking technological innovation is another root cause for insecure SMBs. According to the holistic model, this directly affects level 3 awareness, which decides whether key decision-makers are familiar with cyber security precautions and controls. Understandably, the sector of Information and Communication rates the highest in their technological knowledge.

Identify Security Solutions through Technical Exchange. One way to tackle this issue is to host a venue where merchants of security solutions can showcase their products. This will facilitate the technical exchange between software companies, which can foster new tools that combat cyber criminals more effectively. 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 the various characteristics of their business.

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 situational awareness. According to Appendix H, this is where SMBs perform best and have the least issues.

Preventive Assessment and Detection. To facilitate constructive decision-making, it is recommended that owners and managers assess their business resiliency and find out potential vulnerabilities in advance. There is also the need to encourage organizational measures such as employee training, emergency drills, or attack simulations.

These can help company officials familiarize themselves with incidental situations and prepare them to make more informed decisions under urgency and pressure.

Interventions Targeting Cluster 4 and Cluster 5. According to the cluster analysis, inadequate cybersecurity is associated with either insufficient resources with average cybersecurity awareness (Cluster 4) or insufficient awareness with sufficient resources (Cluster 5). These two types of businesses appear to belong to different populations, with the first more common in the Services and Information and Communication sector, while the second is more common in the Manufacturing and Professional Services sectors. Moreover, the former has more experience with cyberattacks than the latter.

As the reasons for inadequate cybersecurity differ between these different types of SMBs, the solutions will also vary. Interventions that improve cyber defenses while overcoming resource limitations are more suitable for Cluster 4 businesses, such as subsidizing protection tools or promoting free tools. On the other hand, solutions that improve cybersecurity awareness would be helpful for Cluster 5 businesses. Through targeted campaigns or integration into training programs for decision-makers in SMBs, focused engagement on these issues could increase awareness of cybersecurity's importance to business continuity (level 1), cybersecurity risk (level 2), and precautions (level 3).

Moreover, given that both awareness and sufficiency of resources perceived by SMB decision-makers are strongly associated with the root causes, improvements in SMB risk management, information navigation, and technology innovation may indirectly increase Cluster 5 businesses' cybersecurity awareness. As for Cluster 4, improvements in SMB risk management and information navigation may boost SMB decision-makers' perception of the sufficiency of their resources. Either way, addressing the root causes may eventually lead to improvements in cybersecurity for both Clusters 4 and 5. This could be achieved also through targeted training programs for SMB owners and decision-makers.

8 Conclusion

We conducted an initial interview to understand what key decision-makers 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 executive's decision-making process, as well as find out the current status of cybersecurity among Israeli SMBs. Based on our findings, we grouped the SMBs into 5 major clusters, and developed a holistic Structural Equation Model considering potential root causes and the relative cautiousness of a company. We found that the SMBs that are most susceptible to cyberattacks lack awareness, while those who lack resources are also susceptible on a smaller scale. We characterized SMBs who perform well vs. SMBs of these two types, such that we gain a better knowledge of the SMB populations that need a boost in their cybersecurity. Moreover, our findings distinguish which businesses lack awareness and which lack resources. In light of our results, we suggested recommendations and intervention methods to minimize the gap in security misperception and barriers faced by SMB key decision-makers.

References

[1] Israeli Naional Cyber Directorate. *Cybersecurity survey*, 2021.

[2] World bank sme finance: Development news, research, data. *World Bank*, 2022.

[3] 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.

[4] 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.

[5] Yves Barlette, Katherine Gundolf, and Annabelle Jaouen. Ceos' information security behavior in smes: Does ownership matter? *Systemes d'information management*, 22(3):7–45, 2017.

[6] Yves Barlette and Annabelle Jaouen. Information security in smes: determinants of ceos' protective and supportive behaviors. *Systèmes d'information et Management*, 24(3):7–40, 2019.

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

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

[9] 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.

[10] 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.

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

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

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

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] 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.

[21] Celia Paulsen. Cybersecuring small businesses. *Computer*, 49(8):92–97, 2016.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

A Interview Guide

1. Please start by telling me about yourself, including your education and familiarity with computer information in general.
2. Please tell me about your company, what it does, how long it has been operating, and what the annual turnover is.
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 cyber attacks 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 Interview Qualitative Analysis Codebook

- Source: External, human
- Source: External, non-human
- Source: Personal

- Assets: Employee data
- Assets: Customer data
- Assets: Operational data
- Assets: IP data
- Defense: Backup
- Defense: Training
- Defense: Firewall, antivirus, guidelines
- Awareness impact: risk covered
- Awareness impact: level of inconvenience
- Awareness impact: shutdown operation
- Awareness impact: attack on others
- Awareness impact: clear guidelines

C Survey Instrument

Screening

Q1. Which of the following best describes your business ownership?
- ◯ Privately Owned
- ◯ Cooperative Owned
- ◯ Publicly Owned
- ◯ Government 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
- ◯ Unit/Department/Division Manager
- ◯ CEO
- ◯ Vice President
- ◯ Non-management Role

Q4. What type of business do you own?

Q5. What is the economic sector of the business?
- ◯ Activities in real estate
- ◯ Management and support services
- ◯ Wholesale and retail trade and repair of motor vehicles
- ◯ Industry, mining and quarrying
- ◯ Electricity and water supply, sewage services and waste treatment
- ◯ Professional, scientific and technical services
- ◯ Information and communication
- ◯ Hospitality and food services
- ◯ Transportation, storage, mail and courier services
- ◯ Financial services and insurance services
- ◯ Other, please specify
- ◯ Don't know
- ◯ Refuse to answer

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
- ◯ More than 50 million
- ◯ Don't know
- ◯ Refuse to answer

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
- ◯ Don't know
- ◯ No
- ◯ Refuse to answer

Q10. Does the business operate outside of Israel?
- ◯ Yes
- ◯ No

Q11. Where is your business located?
- ◯ The company is located at one site
- ◯ The company is located at several sites

Q12. Are you a member of a business association?
- ◯ Yes, please specify
- ◯ Don't know
- ◯ No
- ◯ Refuse to answer

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

Risk Exposure

Q14. Does your business have an employees(s) who is in charge of computing?
- ◯ Yes
- ◯ No
- ◯ No, an external party/person provides my business with computing services
- ◯ Don't know
- ◯ Refuse to answer

Q15. [If Q14 == Yes] Who is in charge of overseeing all aspects of computing matters for your business, including information security?
- ◯ CIO
- ◯ Other, please specify
- ◯ ICT
- ◯ CISO
- ◯ Refuse to answer

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 him/them to buy products regarding cybersecurity.
- ◯ Other, please specify
- ◯ Refuse to answer

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
- ◯ Refuse to answer

Q18. Is software installed on local servers in the business or are they on the cloud?
- ◯ All our software is on the cloud

- ◯ Some of the software is located on the cloud and some on local servers
- ◯ All our software is located locally
- ◯ Don't know
- ◯ Refuse to answer

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

- ◯ Yes, locally
- ◯ Yes, on the cloud
- ◯ No
- ◯ Don't know
- ◯ Refuse to answer

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

- ◯ Yes, locally
- ◯ Yes, on the cloud
- ◯ No
- ◯ Don't know
- ◯ Refuse to answer

Q21. Does your business have a website?

- ◯ Yes
- ◯ No
- ◯ Refuse to answer

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, please specify
- ◯ Don't know
- ◯ Refuse to answer

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

- ◯ For business information: viewing the products or 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 and view his/her content (personal account)
- ◯ The service provided by the business is located on the website (SAAS)
- ◯ Other
- ◯ Refuse to answer

Q24. How are the payments completed?

- ◯ The customer is charged directly on our website
- ◯ The customer is charged on an external website
- ◯ Payment applications (Bit, Paybox, etc.)
- ◯ Bank transfer
- ◯ Check/Cash
- ◯ Other
- ◯ Don't know
- ◯ Refuse to answer

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
- ◯ Other
- ◯ Refuse to answer

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 the list of digital assets the interviewee 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
- ◯ Fines
- ◯ Other, please specify
- ◯ There will be no damage/harm
- ◯ Refuse to answer

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

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

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

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 cyber-attacks? (Select all that apply)

- ◯ Purchasing security products (antivirus, firewall, and more)
- ◯ Everyone has a username and their security settings are adjusted accordingly
- ◯ Requiring a password
- ◯ Implementing information security procedures
- ◯ Incident response plan
- ◯ Information security training
- ◯ Routine risk assessment
- ◯ Emergency drills
- ◯ Phishing simulation
- ◯ Compliance with information security standards and authorization as a regulatory requirement
- ◯ Conducting penetration tests by external parties

- ◯ Employee training
- ◯ Keeping all software up to date
- ◯ Local backup
- ◯ Cloud backup
- ◯ Other
- ◯ 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 cyber security protection and 10 indicating a very high level of cyber security 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 maximum cybersecurity measures?

- ◯ No need to invest at all
- ◯ up to 5,000
- ◯ 5,000-10,000
- ◯ 10,000-20,000
- ◯ 20,000-50,000
- ◯ 50,000-100,000
- ◯ 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
- ◯ up to 5,000
- ◯ 5,000-10,000
- ◯ 10,000-20,000
- ◯ 20,000-50,000
- ◯ 50,000-100,000
- ◯ Over 100,000

Q37. In your opinion, does the business invest enough budget for cyber security?

- ◯ Invests much more than necessary
- ◯ Invests a little more than necessary
- ◯ Invests approximately the amount needed
- ◯ Invests a little less than necessary
- ◯ The business invests much less than it should
- ◯ Don't know
- ◯ Refuse to answer

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
- ◯ up to 5 hours
- ◯ 5-10
- ◯ 10-20
- ◯ 20-30
- ◯ 30-50
- ◯ More than 50
- ◯ Don't know
- ◯ Refuse to answer

Q39. Are you devoting enough time to cybersecurity?

- ◯ I spend much more time than necessary
- ◯ I spend a little more time than necessary
- ◯ I spend about the same amount of time as needed
- ◯ I spend a little less time than I should
- ◯ I spend much less time than I should
- ◯ Don't know
- ◯ Refuse to answer

Q40. 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 cyber-attacks.
- ◯ I believe that cybersecurity measures are too expensive and are not worth the investment.

Q41. 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 to protect my data.
- ◯ The businesses I interact with believe we need to adopt cybersecurity measures.

Q42. Has your business experienced a cyber-attack?

- ◯ No
- ◯ Yes, once in the last year
- ◯ Yes, several times in the last year
- ◯ Yes, more than a year ago
- ◯ Don't know

Q43. 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)

Q44. [For each selection in Q43] What was the extent of the damage? (Select all that apply)

- ◯ No damage at all
- ◯ Ransom payment
- ◯ Hiring additional computing services
- ◯ Damage to hardware
- ◯ Damage to reputation
- ◯ Damage to the motivation of the employees
- ◯ It took a lot of man-hours to fix
- ◯ Other, please specify
- ◯ Don't know
- ◯ Refuse to answer

Q45. 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 about a business in the same business sector of mine that experienced a cyber attack
- ◯ Yes, there are businesses that I do not know personally that have been attacked.
- ◯ I never heard of cyber-attacks occurring to others.
- ◯ Refuse to answer

Q46. 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
- ◯ There are no clear instructions from a reliable source 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 a 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

Q47. Does your business hold executive/management 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

Q48. 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
- ◯ Very much
- ◯ Slightly
- ◯ Not at all
- ◯ Refuse to answer

Root Causes

Q49. 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

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 a good amount of resources
- ◯ Invested a large amount of resources
- ◯ Don't know
- ◯ Refuse to answer

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 at all to this information
- ◯ Exposed to little information
- ◯ Moderately exposed to information
- ◯ Exposed to this information to a great extent
- ◯ Extremely exposed to information
- ◯ Refuse to answer

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 mainly 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
- ◯ Don't know
- ◯ Refuse to answer

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, please specify
- ◯ Don't know
- ◯ Refuse to answer

Q56. In your opinion, does the business invest enough budget for cyber security?
- ◯ Invests much more than necessary
- ◯ Invests a little more than necessary
- ◯ Invests approximately the amount needed
- ◯ Invests a little less than necessary
- ◯ The business invests much less than it should
- ◯ Don't know
- ◯ Refuse to answer

Q57. Are you devoting enough time to cybersecurity?
- ◯ I spend much more time than necessary
- ◯ I spend a little more time than necessary
- ◯ I spend about the same amount of time as needed
- ◯ I spend a little less time than I should
- ◯ I spend much less time than I should
- ◯ Don't know
- ◯ Refuse to answer

Q58. The following statements refer to your attitudes regarding cyber security. There are no right or wrong answers. Please rate the following from 1 (strongly disagree) to 5 (strongly agree).
- ◯ Cyber-attacks are a growing threat to businesses.
- ◯ My business is too small for hackers to bother attacking it.
- ◯ There is too much information circulating around cyber-attacks 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

Q59. How old are you? (in years)

Q60. What is your gender?

- ◯ Male
- ◯ Female
- ◯ Other
- ◯ Refuse to answer

Q61. With which of the following population groups do you most identify?

- ◯ Jewish
- ◯ Muslim
- ◯ Christian
- ◯ Druze
- ◯ Other, please specify
- ◯ Refuse to answer

Q62. What is your religious level?

- ◯ Secular
- ◯ Traditional
- ◯ Conservative
- ◯ Orthodox
- ◯ Other, please specify
- ◯ Refuse to answer

Q63. 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, please specify
- ◯ Refuse to answer

Q64. How long have you held your *current position* in the business?

Q65. How long have you been in this profession?

Q66. 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 I can solve problems if necessary on my computer.
- ◯ Advanced: I have the advanced ability to install programs and solve related problems.
- ◯ Professional: I have a professional background and the ability to program / professional knowledge of advanced technologies / relevant formal education
- ◯ Refuse to answer

Q67. 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, please specify
- ◯ Refuse to answer

D Detail Information on Interviewed Businesses

#	Economic Sector	Area	Employees (> 50)	Digital Assets	Operational Aspect				Technological Aspect			
					Activity Abroad	Regulation Requirements	In-House IT Person	Work from Home	Ecommerce	Cloud	CRM	Website (content)
P1	Accommodation and food services	South	✓	Employee Data						✓	✓	Informational
P2	Manufacturing	Center		Operational Data							✓	Informational
P3	Administrative and support service activities	Center		Customer Data / Operational Data						✓		N/A
P4	Financial and insurance activities	Center		Customer Data / Operational Data				✓		✓	✓	N/A
P5	Financial and insurance activities	Center		Customer Data						✓	✓	N/A
P6	Construction	South	✓	Intellectual Property / Operational Data						✓		N/A
P7	Information and communication	Center		Intellectual Property / Customer Data	✓		✓	✓		✓	✓	Informational / Online Service
P8	Manufacturing	Center		Operational Data	✓				✓			informational / Online Service
P9	Information and communication	Center		Intellectual Property	✓		✓	✓		✓		Informational
P10	Wholesale and retail trade	Center		Operational Data				✓	✓	✓		Online Services
P11	Information and communication	Center		Customer Data	✓	✓	✓	✓		✓		Online Services
P12	Professional, scientific and technical	Center		Operational Data	✓			✓		✓		Online Services
P13	Accommodation and food services	North		Customer Data		✓			✓	✓		Online Reservations
P14	Professional, scientific and technical	Center	✓	Employee Data / Operational Data			✓	✓		✓		Informational
P15	Accommodation and food services	North		Customers data				✓	✓	✓		Online Reservations
P16	Professional, scientific and technical	Center		Customer Data			✓	✓		✓	✓	N/A
P17	Information and communication	Center		Customer Data		✓	✓	✓		✓	✓	Informational
P18	Manufacturing	South	✓	Operational Data	✓		✓	✓		✓	✓	Informational
P19	Professional, scientific and technical	Center		Intellectual Property / Operational Data	✓	✓		✓		✓	✓	Informational
P20	Information and communication	Center	✓	Intellectual Property / Operational Data		✓		✓		✓	✓	Online Services
P21	Manufacturing	Center	✓	Operational Data					✓		✓	Commercial

E Detail Information on Interviewees

#	Religion	Yrs. Exp	Gender	Age	IT Background	Challenges to Overcome in the Event of a Cyber-Attack						
						Data Recovery Cost	*Operational Damage	*Financial Fines	IP Leakage	Reputational Damage	Bankruptcy	Damage Severity
P1	Jews	6	M	< 36		✓	✓					⦿
P2	Jews	22	F	36-50		✓						○
P3	Jews	6	M	36-50		✓						○
P4	Jews	-	F	36-50		✓	✓	✓		✓	✓	●
P5	Jews	9	M	36-50		✓	✓	✓		✓	✓	●
P6	Jews	-	F	> 50		✓		✓	✓			◉
P7	Jews	-	M	36-50			✓	✓	✓	✓	✓	●
P8	Jews	29	M	> 50		✓						○
P9	Jews	-	M	< 36	✓				✓			◉
P10	Jews	20	F	> 50		✓	✓	✓				◉
P11	Jews	-	F	36-50				✓	✓	✓	✓	●
P12	Jews	16	M	> 50			✓	✓		✓		◉
P13	Arabs	10	M	> 50		✓	✓	✓		✓		◉
P14	Jews	5	F	> 50	✓	✓						○
P15	Arabs	25	F	> 50		✓	✓	✓		✓		◉
P16	Jews	20	M	36-50	✓	✓	✓	✓	✓	✓	✓	●
P17	Orthodox	18	M	36-50	✓	✓	✓	✓		✓	✓	●
P18	Jews	15	M	36-50	✓	✓	✓				✓	◉
P19	Jews	4	M	36-50	✓	✓	✓	✓	✓	✓	✓	●
P20	Jews	2	M	36-50	✓	✓	✓	✓	✓	✓	✓	●
P21	Jews	23	M	36-50		✓	✓		✓			◉

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

Damage Severity: ● - Very Highly, ◉ - Highly, ⦿ - Medium, ⊙ - Low, ○ - Very Low

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	No low awareness	2+ low awareness
Size: 6-10	-0.0522	**0.576***	**1.023*****	0.449	0.272	0.481	0.491
	(0.356)	(0.343)	(0.330)	(0.395)	(0.323)	(0.327)	(0.317)
Size: 51-100	-0.491	0.256	0.402	**1.150****	**-0.775***	**0.729***	-0.0893
	(0.429)	(0.385)	(0.374)	(0.481)	(0.408)	(0.422)	(0.364)
Sector: Professional Services	-0.488	-0.492	-0.159	0.457	**-0.651***	0.428	**-0.857****
	(0.394)	(0.356)	(0.335)	(0.385)	(0.352)	(0.339)	(0.346)
Sector: Trade	-0.289	0.131	-0.369	-0.587	-0.457	0.606	-0.479
	(0.565)	(0.479)	(0.508)	(0.682)	(0.498)	(0.463)	(0.485)
Sector: Info. & Comm.	0.332	**-1.075****	**-1.045****	0.401	0.135	0.315	-0.403
	(0.402)	(0.477)	(0.473)	(0.425)	(0.369)	(0.382)	(0.385)
Sector: Production	0.123	-0.0811	0.285	0.339	**-1.026***	0.0508	0.111
	(0.513)	(0.446)	(0.419)	(0.509)	(0.545)	(0.447)	(0.416)
Revenue: 1-5	-0.155	0.0228	-0.231	-0.183	-0.731	0.153	-0.765
	(0.516)	(0.537)	(0.527)	(0.543)	(0.512)	(0.535)	(0.486)
Revenue: 5-10	-0.766	-0.484	-0.261	-0.792	-0.384	0.747	**-1.103****
	(0.598)	(0.643)	(0.599)	(0.625)	(0.549)	(0.560)	(0.561)
Revenue: 10+	-0.637	0.268	0.454	-0.822	0.176	-0.313	-0.318
	(0.567)	(0.563)	(0.558)	(0.583)	(0.518)	(0.579)	(0.505)
Revenue: undisclosed	-0.765	0.0436	-0.269	**-0.885***	-0.411	0.287	**-0.903****
	(0.488)	(0.493)	(0.487)	(0.521)	(0.450)	(0.492)	(0.442)
Tech. Intensity: High	0.532	-0.0366	**-0.868****	0.250	0.481	**-0.524***	-0.495
	(0.324)	(0.330)	(0.348)	(0.331)	(0.296)	(0.309)	(0.316)
Experienced Cyber Attack	-0.166	**-1.190*****	**-0.720****	**-0.618***	0.0456	**0.617****	**-0.967*****
	(0.348)	(0.382)	(0.343)	(0.374)	(0.312)	(0.287)	(0.343)
Total Percentage	21%	23%	27%	20%	25%	29%	34%
Observations	319	320	320	311	320	320	320

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

G Awareness Level 1 and Level 4 Regression Coefficients

Level 1 Variables	Depndent variable: High Damage		Level 4 Variables	Depndent Variable: Number of Cyber Precautions	
Has Cyber Insurance	-0.847*	(0.450)	Has Cyber Insurance	25.68***	(15.75)
Revenue: 1-5	-1.632	(1.027)	Digital Assets: Customer list	2.177	(1.171)
Revenue: 5-10	-2.058*	(1.190)	Digital Assets: Customer financial data	1.438	(0.597)
Revenue: 10+	-2.439**	(1.211)	Digital Assets: Other customer sensitive data	4.264***	(2.048)
Revenue: undisclosed	-2.395***	(0.925)	Digital Assets: Employee data	-0.577	(0.282)
Sector: Professional Services	-0.645	(0.772)	Digital Assets: Operational system	1.135	(0.609)
Sector: Trade	1.575*	(0.950)	Digital Assets: Operational data	1.754	(1.036)
Sector: Info. and Comm.	0.0443	(0.817)	Digital Assets: Intellectual property	2.724**	(1.291)
Sector: Production	0.546	(0.939)	Digital Assets: Business financial data	0.571	(0.255)
# of Digital Assets	-0.129	(0.280)	Digital Assets: Big data	0.764	(0.439)
Website: Hosting product or service information	0.0662	(0.305)	Website: Hosting product or service information	1.675	(1.078)
Website: Selling product or service	0.842**	(0.335)	Website: Selling product or service	0.800	(0.398)
Website: Displaying personalized content	0.166	(0.419)	Website: Displaying personalized content	2.405	(1.443)
Website: Software as a service (SAAS)	0.901**	(0.432)	Website: Software as a service (SAAS)	2.337	(1.463)
Uses CRM or ERP	0.821**	(0.364)	Uses CRM or ERP	5.443***	(2.816)
Uses CRM or ERP: undisclosed	0.937**	(0.417)	Uses CRM or ERP: undisclosed	4.701***	(2.669)
Revenue (< 1) X # of Digital Assets	0	(0)	Remote Work: Yes	0.832	(0.414)
Revenue (1-5) X # of Digital Assets	0.311	(0.313)	Remote Work: No	0.384*	(0.221)
Revenue (5-10) X # of Digital Assets	0.630*	(0.358)	Program Installation: Cloud	0.607	(0.456)
Revenue (10+) X # of Digital Assets	0.418	(0.323)	Program Installation: Cloud & Local	1.832*	(0.837)
Revenue (undisclosed) X # of Digital Assets	0.511*	(0.282)	Program Installation: Local	0.310*	(0.201)
Sector (Services) X # of Digital Assets	0	(0)	Program Installation: undisclosed	0.117***	(0.0772)
Sector (Prof. Service) X # of Digital Assets	0.246	(0.204)			
Sector (Trade) X # of Digital Assets	-0.712**	(0.298)			
Sector (Info. & Comm.) X # of Digital Assets	0.145	(0.210)			
Sector (Production) X # of Digital Assets	-0.262	(0.215)			
Observations	313		Observations	320	

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

H Root Causes vs. Business Characteristics (Rating ranges from 1 to 5)

		Constructive Decision Making	Information Navigation	Technology Innovation	Risk Management
Total		3.6	2.6	2.6	3.0
Business Size (# of Employees)					
	6-10	3.7	2.4	2.6	3.1
	11-50	3.5	2.6	2.5	2.9
	51-100	3.8	2.9	2.8	3.3
Business Sector					
	Services	3.4	2.8	2.4	2.8
	Prof. Services	3.8	2.4	2.6	3.1
	Trade	3.6	2.3	2.7	2.7
	Info. & Comm.	3.7	2.8	3.1	3.4
	Production	3.6	2.9	2.3	3.1
Revenue					
	<1	3.7	2.6	2.6	2.9
	1-5	3.5	2.7	2.5	3.1
	5-10	3.2	2.8	2.7	2.8
	10+	3.6	2.4	2.6	3.8
	Refuse to answer	3.8	2.6	2.6	3.1
Technology Intensity					
	Low	3.6	2.6	2.5	3.0
	High	3.6	2.6	2.8	3.1
Experienced Cyber Attack					
	No	3.6	2.6	2.6	3.0
	Yes	3.5	2.6	2.7	3.2
	Don't know	3.4	2.3	2.5	2.5
N		311	315	320	320

I Clusters Profile According to Research Variables

	Cluster 1	Cluster 2	Cluster 3	Cluster 4	Cluster 5	Total
Sector-Services	29%	33%	41%	40%	22%	32%
Sector-Professional services	28%	8%	19%	20%	43%	28%
Sector-Trade	11%	25%	9%	10%	6%	9%
Sector-Information and communication	27%	17%	16%	27%	9%	19%
Sector-Production	6%	17%	16%	3%	19%	12%
Had cyber attack	42%	27%	20%	33%	19%	28%
Decision making constructive(1-5)	3.6	3.3	3.4	3.5	3.9	3.6
Decision navigation(1-5)	2.6	2.9	2.5	2.4	2.9	2.62
Innovation(1-5)	2.8	2.3	2.5	2.4	2.6	2.61
Risk management(1-5)	3.2	3.3	2.7	2.6	3.3	3.02
Digital assets sum(0-9)	3.6	2.9	3	3.8	3.7	3.36
Cyber protections sum(0-15)	9.3	7.2	7.6	7.2	6.6	7.9
Relative precautions	0.21	-0.1	0.24	-0.21	-0.57	0