Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 7, Issue 1, 2019

The invisible hole of information on SMB's cybersecurity

Ruti Gafni, The Academic College of Tel Aviv Yaffo, Israel, rutigafn@mta.ac.il

Tal Pavel, The Academic College of Tel Aviv–Yaffo, Israel, talpv@mta.ac.il

Abstract

Small and Medium Businesses (SMB) use Internet and computer-based tools in their daily processes, sometimes without being aware to the cyber threats, or without knowing how to be prepared in case of a cyber-attack, although they are a major target for cyber-attacks. Specific information about cybersecurity needed by SMBs, in order to cope with cyber threats, is not always available or easily accessible. In this study, a vast search of different types of information about SMBs' cybersecurity was performed, in order to find whether a hole of accessible information exists in this area. This exploratory research covered general mass communication media channels, technological and professional cybersecurity websites, and academic journals, and found that indeed very few studies, articles and news items were published in this matter. Leveraging knowledge and awareness, diminishing the shame for reporting cyber-attacks, and increasing mass communication media interest and public attention, may be activities to cover this "invisible hole".

Keywords: Small Medium Business (SMB), Small and Medium Enterprises (SME), cybersecurity, cyber information, cyber-attack.

Introduction

Small and Medium Businesses (SMBs) can get advantages from using the Internet to reach new and larger markets, reach out to their partners and employees from around the world. Furthermore, computer-based tools can provide opportunities to work more efficiently. SMBs, relating to information systems, differ from large companies, as most of them use basic information systems, and do not need to cope with the complexity of information systems as in large firms, thus, they do not have an Information Technology (IT) department, or even no IT specialist (Lopez-Nicolas, & Soto-Acosta, 2010). Therefore, it is likely to assume that SMBs are even not aware and maybe not prepared to deal with cyber-attacks. However, the proliferation of online activity has attracted the attention of existing criminal organizations and a new breed of cyber criminals (Bhattacharya, 2013). Maintaining a website, adopting cloud computing, performing e-commerce, or just using emails, are all vulnerabilities, which should be carefully treated in order to cope with possible cyber-attacks. Cyber-attacks occur in all kinds of firms. However, according to Verizon Enterprise (2018), 58% of the attacked firms in 2017 were SMBs. In the United States (U.S.), the level of risk for being a target of cyber-crime is high, according to the National Small Business Association (NSBA) survey of SMBs in 2017. About 42% of the surveyed SMBs reported being a victim of a cyber-attack, with cost an average

$32,021 for companies whose business banking accounts were hacked, and $7,115 on average for small businesses overall in the U.S. (NSBA, 2017). Every business that uses the Internet is responsible for creating a culture of security that will enhance business and consumer confidence (FCC, 2018). However, the information and knowledge about cybersecurity needed by the owners, managers and decision-makers of SMBs, in order to cope with cyber threats, is not always available or easily accessible. Most of the public information available, report about large business cybersecurity attacks, or specific references to complex systems. In this exploratory study, a vast search of different types of information about SMB's cybersecurity was performed, in order to find whether a hole of accessible information exists in this area.

The definition of Small and Medium Business (SMB) as it is called in the U.S., or Small and Medium Enterprises (SME) as called in the European Union (E.U.), may vary according to countries. For example, E.U. SMEs are firms with fewer than 250 persons (European Commission, 2019), SMBs in the U.S. are firms with fewer than 500 employees (SBA, 2019), and in Israel less than 100 employees (SBA – Small Business Agency, 2018). These small firms are compound from Independent Business who have only one person, which is the owner of the business, micro or Small Office Home Office (SOHO), small firms, and medium-size firms. The subdivisions are according to the number of employees, and normally also the annual turnover of the firm or and/or an annual balance sheet (Kushnir, 2010). In some countries, there are also differences according to industries (SBA, 2019). Table 1 presents the definition of SMBs in E.U., U.S. and Israel (Kushnir, 2010), and the percentage of firms of each size, in E.U. (Muller et al., 2017), U.S. (U.S. Small Business Administration, 2018) and Israel (Asakim Be-Misparim, 2018). As can be seen, the largest amounts of firms are independent and micro (E.U.: 93%; U.S.: 97.85%; Israel: 85.82%).

Table 1: Definition of SMBs and Percentage According to Size

		Independent	Micro	Small	Medium	Total SMBs	Large
E.U.	No. of Employees	1	<10	<50	<250		>=250
	% of Enterprises	93		5.8	0.9	99.7	0.3
U.S.	No. of Employees	1	<19	<100	<500		>=500
	% of Enterprises	80.45	17.4	2.03		99.88	0.12
Israel	No. of Employees	1	<5	<20	<100		>=100
	% of Enterprises	53.55	32.27	11.09	2.72	99.63	0.37

Information about cybersecurity, cyber-attacks, risks, and ways to act in order to be prepared, can be obtained in different ways. Large firms, government entities and critical infrastructure companies, are subject to cybersecurity regulations, which get them involved with the up to date threats, vulnerabilities and ways to cope with those possibilities. However, most SMBs are not subject to cybersecurity regulations. There are guidelines (not regulations) to SMB cybersecurity preparedness, different from those to large firms and critical infrastructure firms, published by relevant country's cybersecurity governmental agencies (US-Cert-SMB, 2018; National Cyber Security Authority, 2017). Unfortunately, these guidelines do not reach all of the SMBs, especially not the smallest ones. Moreover, for an SMB manager or decision maker, the tasks

described in those guidelines can seem overwhelming (Bell, 2017). Another popular way to receive information is through mass communication media channels. The SMB's owners, managers and decision-makers can get information and news reported in newspapers, news websites, radio and television. Reporters to the mass media can get information from professional sources, such as specific websites, and from published research (academic studies & professional white papers). However, most of the breaches and cyber-attacks published in this kind of media are about attacks to large firms. SMBs' owners, managers, and decision-makers do not seem themselves as a target to these kinds of attacks, because they think they are too small to be a relevant target to hackers. Moreover, small businesses owners, managers and decision-makers are preoccupied with everyday business concerns, thus, neglecting cybersecurity issues, resulting in an increase of vulnerability to cybercrime (Bhattacharya, 2013). The challenge is that cybersecurity requires an element of specialist knowledge to be operational, often thought to be a technical person, and it also requires a budget (Bell, 2017). Thus, the vulnerabilities of an SMB are wide, because of various reasons:

(1) The SMB's owners, managers, and decision-makers are not aware of cybersecurity threats;

(2) Part of the insufficiency of awareness derives from the lack of regulation;

(3) Even if the SMB's owners, managers, and decision-makers might be aware to cybersecurity potential feasibility, they may not understand the specifics risks of an attack on their business;

(4) Even if the SMB's owners, managers, and decision-makers understand the risks, and are capable to perform a relevant risks analysis, they might not have enough knowledge on how to prepare the firm in order to mitigate the risk;

(5) The SMB's owners, managers, and decision-makers might not have enough budget in order to cope with cybersecurity threats. Generally, SMBs have less technological, financial and human resources to respond to cyber-attacks, less sophisticated security infrastructure, less organized processes in order to manage threats, and thus, they are found by hackers as more vulnerable.

Information of greater explicitness and broader scope allows for more rational decision-making (Child & Hsieh, 2014). The decision-makers capability for identifying, avoiding, and manage cyber-attacks is essential for more effective decisions. Therefore, information and knowledge are crucial to recognize cybersecurity threats, to reduce the risks and uncertainty and to stimulate awareness manage of. The goal of this study is to find whether the information for SMBs, about threats, risks, vulnerabilities, and suggestions on how to protect the business from a cyber-attack is published and available to the SMB's owners, managers and decision-makers.

Methodology

In order to find the extent of the media coverage of cybersecurity incidents in the SMBs sector, information that may be rolled over to the owners, managers and decision-makers of SMBs, a vast search for publicly available written information was conducted. All cybersecurity articles, news and papers found were read, in order to decide whether they are relevant to SMBs. There

was no necessity to find words like SMB, SME, or the specific size of the firm reported in the article. If those terms were found, the articles were obviously counted. Moreover, other articles, according to their essence, which fit both large and small businesses, were counted as well. The search included three kinds of publications:

1. **General media channels websites** – Nine major general worldwide mass communication media channels websites were covered for cybersecurity news items published between the dates January 1st - December 31st 2018, in order to find the reports about cyber-attacks and breaches of SMBs published during the year 2018. This research used several known lists in order to map the major worldwide general news channels website:
   (a) "Top 10 Most Popular News Channels In The World" (Richi, 2017);
   (b) "International news channels" (International news channels, n.d.);
   (c) "United States cable news" (United States cable news, n.d.);
   (d) "Top 10 famous news channels of the world" (Digvijaya, 2017);
   (e) "MSNBC Ranks as No. 1 Cable Network in Total Viewers for First Time Ever" (Otterson, 2017).

   The websites chosen were those who appear in several of the above lists and represent different countries or different characteristics. Therefore, the following sources were chosen: Reuters (Worldwide, U.K.), BBC (U.K.), CNN (U.S.), CBS (U.S.), Al Jazeera (Qatar), Deutsche Welle (Germany), Russia Today (Russia), CNBC (U.S.), Haaretz (Israel). For each source, the sections, which covered cybersecurity issues, were manually browsed, and in addition, all the articles with the tag "cyber" were read.
2. **Technological and professional cybersecurity websites –** Nine major technological and professional cybersecurity and information security websites were covered in cybersecurity articles published between the dates January 1st - December 31st 2018, in order to find the reports about cyber-attacks and breaches of SMBs published during the year 2018. In order to find the relevant websites, several lists of major technological and professional cybersecurity websites were examined:
   (a) "Top Cyber Security News Websites Newsletter" (FeedSpot, 2018);
   (b) "The Top Cyber Security Blogs and Websites of 2018" (University of San Diego, 2018);
   (c) "Best Cyber Security News Blogs 2018" (CyberDB, 2018);
   (d) "Top Cybersecurity News Sites" (Morgan, 2018);
   (e) "Top 10 Cybersecurity Blogs You Should Add to Your Feed" (GlobalSign, 2018).

   The websites chosen were those who appear in several of the above lists and represent different countries and characteristics. Accordingly, these sources were chosen: HackRead ("Cyber Attacks", "Phishing Scam", "Leaks", "Malware" sections), The Hacker News, Tripwire, Wired, Naked Security, Cnet, Krebs on Security, Dark reading, TelecomNews (Israel).
3. **Academic journals** – 35 peer-reviewed academic journals were browsed, for the last five years (2014-2018), looking for articles published about SMB and cybersecurity. This search included articles referencing to SMB or to individuals, because independent small businesses employ only one person and micro businesses employ one to four persons. The selection of journals was performed in a few stages:

a) Google Scholar, Academic Search Premier (EBSCO) and ABI/INFORM Global (ProQuest) were used in order to find relevant published papers about cybersecurity and small businesses.
b) The journal names of the collected papers were entered in the journal's list.
c) The bibliography of the collected papers was browsed in order to find relevant cited papers. The names of the journals where these relevant papers were published were added to the journal list. This step was performed for several cycles and stopped when papers were older than 10 years.
d) For each found relevant paper, a search was done, in order to find newer papers citing them. The names of the journals where these relevant papers were published were added to the journal list.
e) For each journal in the list, the tables of content of the last five years were manually browsed.

Findings

The findings of the search performed were summarized in the following tables, according to the nature of the information retrieved. Each table consists of the list of browsed sources, and the number of items found, for each month when the search was conducted over one year, of for each year, when the search was conducted for a period of five years.

General Media Channels Websites Findings

The results of the search in the cyber sections in general media channel are displayed in Table 2. The research examined the chosen nine main news channels and covered a total of 1,966 cybersecurity news items during the year 2018 (three sources were available only partly, when not available N/A is written in the specific cells). Each cell in the table contains the number of articles about cybersecurity regarding SMBs that were published in a specific source (row) and month (column) and the total of articles about cybersecurity published in the same source and month. There were found only 5 SMB's related news items.

Table 2: Published Cybersecurity News Articles on General Media Channels Websites

Source	Section	Jan-18	Feb-18	Mar-18	Apr-18	May-18	Jun-18	Jul-18	Aug-18	Sep-18	Oct-18	Nov-18	Dec-18	Total 2018
Reuters	Cybersecurity	0/44	0/42	0/31	1/36	0/32	0/28	0/18	0/26	0/19	0/30	0/20	0/27	**1/343**
BBC	Tag - Cyber	0/5	0/10	0/8	0/8	1/7	0/5	0/2	0/6	0/5	0/23	0/28	2/47	**3/154**
CNN	Tag - Cyber	N/A	N/A	0/1	0/1	N/A	N/A	0/1	N/A	0/21	0/14	0/50	0/26	**0/114**
CBS	Cybersecurity	0/5	0/3	N/A	0/4	N/A	N/A	0/1	0/8	0/7	0/7	0/3	0/11	**0/49**
Al Jazeera	Tag - Cyber	0/3	0/3	0/4	0/8	0/3	0/3	0/6	0/1	0/1	0/8	0/7	0/12	**0/59**
Deutsche Welle	Tag - Cyber	0/6	0/14	0/9	0/14	0/21	0/6	0/10	0/8	0/6	0/10	0/8	0/7	**0/119**
Russia Today	Tag - Cyber	0/24	0/23	0/38	0/18	0/21	0/22	0/25	0/25	0/19	0/29	0/13	0/25	**0/282**

CNBC	Cybersecurity	0/63	0/52	0/62	1/96	0/46	0/47	0/37	0/34	0/38	0/62	0/47	0/65	**1/649**
Haaretz	Captain Internet	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0/57	0/68	0/72	**0/197**
Total		**0/ 150**	**0/ 147**	**0/ 153**	**2/ 185**	**1/ 130**	**0/ 111**	**0/ 100**	**0/ 108**	**0/ 116**	**0/ 230**	**0/ 244**	**2/ 292**	**5/ 1,966**

General media channels are the most accessible source for SMB's managers and decision makers. Most laymen receive information about cybersecurity issues, like threats, attacks, and how to be prepared, from general media channels. However, as can be seen, those channels do not publish such kinds of reports.

Technological and Professional Cybersecurity Websites Findings

The results of the search after professional cybersecurity and information-security media channels are displayed in Table 3. The research examined the chosen nine main news channels and covered 6,138 cybersecurity news items during the year 2018 (two sources were available only partly, N/A is written in the specific cells). Each cell in the table contains the number of articles about cybersecurity regarding SMBs that were published in a specific source (row) and month (column) and the total of articles published in the same source and month. Only 30 SMB's related news items were found.

Table 3: Reports in Technological and Professional Cybersecurity Websites

Source	Section	Jan - 18	Feb-18	Mar -18	Apr-18	May-18	Jun-18	Jul - 18	Aug-18	Sep-18	Oct-18	Nov-18	Dec-18	Total 2018	Total for Source
HackRead	Cyber Attacks	0/ 0	0/ 2	0/ 8	0/ 1	0/ 3	0/ 2	0/ 1	0/ 1	0/ 2	N/A	N/A	N/A	**0/ 21**	**9/ 252**
HackRead	Phishing Scam	0/ 2	0/ 5	0/ 5	0/ 2	0/ 4	N/A	N/A	N/A	N/A	N/A	0/ 1	0/ 2	**0/ 21**	
HackRead	Leaks	0/ 2	0/ 4	2/ 7	0/ 4	2/ 6	0/ 3	0/ 1	0/ 4	1/ 6	0/ 1	0/ 2	0/ 5	**5/ 45**	
HackRead	Malware	1/ 27	0/ 21	0/ 19	3/ 15	0/ 17	0/ 13	0/ 6	0/ 13	0/ 13	0/ 12	0/ 5	0/ 5	**4/ 166**	
The Hacker News		1/ 43	0/ 30	0/ 36	0/ 49	0/ 45	0/ 56	0/ 54	1/ 45	0/ 49	0/ 44	0/ 37	0/ 24	**2/ 512**	**2/ 512**
Tripwire	The State of Security	1/ 96	0/ 66	1/ 71	1/ 68	0/ 67	0/ 61	0/ 67	2/ 65	0/ 59	1/ 69	1/ 60	0/ 47	**6/ 796**	**6/ 796**
Wired	Security	0/ 44	0/ 42	0/ 53	0/ 44	0/ 38	0/ 42	0/ 39	0/ 51	0/ 40	0/ 46	0/ 40	0/ 42	**0/ 481**	**0/ 481**
Naked Security		1/ 99	1/ 89	0/ 97	0/ 86	0/ 87	1/ 94	1/ 104	1/ 98	0/ 95	0/ 102	0/ 96	0/ 72	**5/ 1,119**	**5/ 1,119**
CNET	Security	0/ 66	0/ 52	0/ 98	0/ 85	1/ 96	0/ 87	0/ 91	1/ 102	0/ 75	0/ 90	0/ 81	1/ 55	**3/ 978**	**3/ 978**
Krebs on Security		0/ 14	0/ 13	0/ 14	0/ 10	0/ 13	0/ 12	0/ 10	0/ 13	0/ 13	0/ 9	0/ 13	0/ 13	**0/ 137**	**0/ 147**

Dark reading	News & Commentary	0/ 143	0/ 131	0/ 154	0/ 164	0/ 155	1/ 143	1/ 141	1/ 168	0/ 123	1/ 140	0/ 129	1/ 119	**0/ 1,710**	**5/ 1,710**
Telecom News	Security and Cyber world news	0/ 16	0/ 9	0/ 18	0/ 5	0/ 10	0/ 13	0/ 4	0/ 7	0/ 2	0/ 5	0/ 4	0/ 10	**0/ 103**	**0/ 103**
Total		**4/ 552**	**1/ 464**	**3/ 580**	**4/ 533**	**3/ 541**	**2/ 526**	**2/ 518**	**6/ 567**	**1/ 477**	**1/ 518**	**1/ 468**	**2/ 394**	**30/ 6,138**	

The nature of news items found is varied. Part of the news items includes reports and opinion editorials (op-eds) about cybersecurity, information security relating SMBs. Others relate to small scale cybersecurity incidents, usually, those which happened in SMBs, and only a very few items truly covered cybersecurity incidents related specifically to SMBs. Technological and professional cybersecurity websites are normally not read by laymen, and it is likely to assume that SMB owners, managers, and decision makers do not read them. These websites are relevant mostly to IT and cybersecurity professionals. Therefore, IT personnel, cybersecurity professionals or consultants who may be hired by the managers of an SMB are the focus of these websites. Still, the majority of items are not relevant to SMBs.

Summarizing Tables 2 and 3, it can be seen that a total of 35 SMBs cybersecurity-related news items were found, out of 8,104 cybersecurity and information security news items during 2018. It can be calculated that SMBs related items are only 0.43% out of the total of cybersecurity news reports. Since the covered media channels represent different origin, states, types, and audience, it can be assumed the given results portrayed a quite accurate picture of cyber incidences. Another major finding is that media channels (general & professional) covering cybersecurity incidents if one or more conditions are fulfilled:

(1) large volume of data breached (hundreds of thousands of records & above);

(2) large files of breached data (volume of dozens of description Giga-Bytes & above);

(3) massive damage caused by the cyber-attack;

(4) the importance of the target and the victim of the cyber-attack.

Academic Journals Findings

Table 4 displays studies published during 2014-2018 in peer-reviewed academic journals. These studies include those who are specific for cybersecurity in small business, and tangent studies, which are related to this subject, but not exactly, and can be part of the knowledge needed by SMB's decision-makers in order to raise their awareness and preparedness towards a cyber-attack.

Table 4: Cybersecurity Specific and Tangent Studies Relevant for SMBs Published in Peer-Reviewed Academic Journals

Journal	Publisher	2014	2015	2016	2017	2018	Total
Business and Management Studies	Redfame Publishing	N/A	1	0	0	0	**1**

Journal	Publisher	2014	2015	2016	2017	2018	Total
Business Horizons	Elsevier	0	0	1	0	0	**1**
Communications of the AIS	AIS	0	1	0	0	0	**1**
Computer	IEEE	0	0	1	1	2	**4**
Computer Fraud & Security	Elsevier	0	0	1	1	0	**2**
Computers & security	Elsevier	0	0	0	1	0	**1**
Computers in Human Behavior	Elsevier	0	0	0	2	0	**2**
Cyber Security	Henry Stewart Publications	N/A	N/A	N/A	0	1	**1**
Future Internet	MDPI	0	0	1	0	0	**1**
Industrial Management & Data Systems	Emerald	1	0	1	0	0	**2**
Information & Computer Security/Information Management & Computer Security*	Emerald	1	1	1	0	1	**4**
Information & Management	Elsevier	2	0	0	1	1	**4**
Information Systems Management	Taylor & Francis	0	0	1	2	0	**3**
International Journal of Business Continuity and Risk Management	Inderscience Publishers	0	0	0	0	1	**1**
International Journal of Computers & Technology	Council for Innovative Research, Punjab, India	0	1	1	0	1	**3**
International Journal of Critical Infrastructure Protection	Elsevier	0	1	3	0	0	**4**
International Journal of Information Management	Elsevier	0	0	0	0	0	**0**
International Journal of Information Security and Privacy	IGI Global	0	0	0	0	0	**0**
International Journal of Information Systems for Crisis Response and Management	IGI Global	0	1	0	0	1	**2**
IT Professional	IEEE	0	0	0	0	0	**0**
Journal of Accounting and Public Policy	Elsevier	0	0	0	0	1	**1**
Journal of Business Continuity & Emergency Planning	Henry Stewart Publications	0	0	0	1	0	**1**
Journal of Cyber Policy	Taylor & Francis	N/A	N/A	0	1	0	**1**
Journal of Cybersecurity	Oxford Academy	0	1	2	0	0	**3**
Journal of Cyber Security and Mobility	River Publishers	0	0	0	0	0	**0**
Journal of Hospitality and Tourism Technology	Emerald	0	0	0	0	1	**1**

Journal	Publisher	2014	2015	2016	2017	2018	Total
Journal of Information Security	SCIRP	0	0	0	0	1	**1**
Journal of Small Business and Enterprise Development	Emerald	0	0	0	0	0	**0**
MIS Quarterly	University of Minnesota	0	0	1	0	0	**1**
Privacy and Security (TOPS)	ACM	0	0	0	0	0	**0**
Risk Management	Springer	1	0	0	0	0	**1**
Security & Privacy	IEEE	1	0	0	1	1	**3**
The Journal of Cyber Security and Information Systems	IAC Publisher	0	0	0	0	0	**0**
The Journal of Information Assurance & Cybersecurity	Clute Institute	0	0	0	0	0	**0**
The Online Journal of Applied Knowledge Management (OJAKM)	International Institute for Applied Knowledge Management (IIAKM)	0	1	2	2	3	8
Total		**6**	**8**	**16**	**13**	**15**	**58**

** Journal name was changed over that period*

As can be seen, less than 60 papers were published during the last five years. Each journal published between 0-8 papers on cybersecurity relevant to SMBs. Journals with no relevant publications during these years were counted, because they had a relevant publication during the last 10 years, according to the methodology of searching. The number of total publications is rising very slowly. In 2016, the number of publications was doubled, but not changed much afterwards.

Discussion

The SMBs are the big majority (> 99%) of businesses in Western countries, and, according to reports (Verizon Enterprise, 2018), 58% of data breach victims in 2017 were small businesses. However, surprisingly, the number of news articles, studies, and research published, about SMBs cybersecurity threats, vulnerabilities, attacks, breaches, cybersecurity risk management and preparedness are drastically few. We suspect that the following are some reasons for this "invisible hole" of information:

1. **Lack of knowledge/awareness** – The lack of knowledge can be categorized by two options:
    a. The SMBs not always know they were attacked or breached. In such cases, the information, obviously, does not reach other parties in order to be published.
    b. The SMB owners, managers, and decision-makers may not be aware that data leaked outside the firm, how much data leaked, and what kind of data leaked. Because most of these businesses do not employ experienced cybersecurity professionals, even not as consultants, they may not be aware to what really happened.

2. **Lack of reporting** – When a small business experience a cyber-attack, no matter which kind of attack, most of the owners, managers, and decision-makers do not report on the case to law enforcement agencies or any other relevant institutions. The reasons for this can be one or a combination of the following:
    a. SMBs are not under the regulation to do so. Firms that undergo cybersecurity regulations are obliged to report any cyber-attack they perceived. However, those firms, which are exempted of regulation, may not report.
    b. SMB owners, managers, and decision-makers do not want to expose the existing vulnerabilities or the fact they have been breached in front of customers, suppliers, partners, competitors, regulators, and law enforcement agencies, because they may think this kind of exposure may hinder their business.
3. **Lack of media interest** – Even if the attack was reported (to any law enforcement, media channel, general public, or other institutions), the cyber-attack is treated by the media and law enforcements as an "insignificant" event, which suffers of lack of interest of all the relevant players, and, therefore, lack of general media coverage.
4. **Lack of public attention and information overload** – cyber-attacks are faced on a daily base, and targets all types of victims, more than is known to public, and more than the public can absorb. According to the attention economy perspective (Davenport & Beck, 2001) the scarcest resource in modern organizations is attention. Therefore, the media consumer cannot contain this high volume and frequency of cyber incidents, so they are not reported and/or published.

In terms of knowledge management, it seems that the cybersecurity knowledge needed by SMB owners, managers, and decision-makers is understatedness only partially available. The relevant knowledge must be offered and submitted to SMB owners, managers, and decision-makers in order to leverage their awareness and possibilities of preparedness to cyber-attacks.

Conclusion

According to this exploratory research, it seems that information needed by SMB owners, managers, and decision makers, in order to cope with cybersecurity and being prepared to cyber-attacks, is scarce and not easily available. In order to cover this "invisible hole", some activities and change of culture have to be referenced. For example, cyber-attacks, even the smaller ones, must be reported in order to leverage the awareness of relevant people. Moreover, a campaign like #WeTooWereHacked can raise the awareness of the authorities, the mass communication media, and other SMB owners, managers, and decision-makers. Leveraging the awareness can help bring a better preparedness of these businesses, in order to cope with the threats. Further, the importance of this issue will increase, so academic research will expand, and more researches will find the vulnerability of SMBs as a relevant topic for future studies.

Future research

According to Pérez-González, Trigueros-Preciado, and Popa (2017), SMBs use social media technologies in order to acquire information. Therefore, a comprehensive search of cybersecurity for SMBs information shared on the social networks has to be performed, in order to find if this information may help in "closing the hole".

References

Asakim Be-Misparim (2018). *SBA*. Retrieved from: https://www.sba.org.il/hb/PolicyAndInformation/Researches/Documents/asakim%20be%20misparim%202018.pdf

Bell, S. (2017). Cybersecurity is not just a 'big business' issue. *Governance Directions, 69*(9), 536-539.

Bhattacharya, D. (2013). Evolution of information security issues in small businesses. *The Colloquium for Information System Security Education, 1*(1), 1-10.

Child, J., & Hsieh, L. (2014). Decision mode, information and network attachment in the internationalization of SMEs: A configurational and contingency analysis. *Journal of World Business, 49*(4), 598–610. http://www.doi.org/10.1016/j.jwb.2013.12.012

CyberDB (2018). *Best cyber security news blogs 2018*. Retrieved from: https://www.cyberdb.co/best-cyber-security-news-blogs-2018

Davenport, T. H., & Beck, J. C. (2001). *The attention economy: Understanding the new currency of business*. Boston, MA: Harvard Business School Press.

Digvijaya, S. (2017). *Top 10 famous news channels of the world.* Retrieved from: https://topyaps.com/top-10-famous-news-channels-of-the-world

European Commission (2019). *What is an SME?* Retrieved from: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

Federal Communications Commission (FCC) (2018). *Cybersecurity for small business.* Retrieved from: https://www.fcc.gov/general/cybersecurity-small-business

FeedSpot (2018, June). *Top cyber security news websites newsletter [blog post]*. Retrieved from: https://blog.feedspot.com/cyber_security_news_websites

GlobalSign (2018). *Top 10 cybersecurity blogs you should add to your feed.* Retrieved from https://www.globalsign.com/en/blog/top-10-cybersecurity-blogs

International News Channels. (n.d.). *In wikipedia.* Retrieved from: https://en.wikipedia.org/wiki/International_news_channels

Kushnir, K. (2010). How do economies define micro, small and medium enterprises (MSMEs). *Companion Note for the MSME Country Indicators, 66*. Retrieved from: https://www.ifc.org/wps/wcm/connect/624b8f804a17abc5b4acfddd29332b51/msme-ci-note.pdf?mod=ajperes

Lopez-Nicolas, C., & Soto-Acosta, P. (2010). Analyzing ICT adoption and use effects on knowledge creation: An empirical investigation in SMEs. *International Journal of Information Management*, *30*(6), 521-528.

Morgan, S. (2018). Top cybersecurity news sites. *Cybercrime Magazine*, Cybersecurity Ventures. Retrieved from: https://cybersecurityventures.com/industry-news

Muller, P., Julius, J., Herr, D., Koch, L., Peycheva, V., & McKiernan, S. (2017). Annual report on European SMEs 2016/2017. *EU Publications.*

National Cyber Security Authority (2017). Cyber defense methodology for an organization, Ver. 1.0. Retrieved from: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf

National Small Business Association (NSBA) (2017). *NSBA testifies on cybersecurity.* Retrieved from: https://nsba.biz/nsba-testifies-on-cybersecurity-2

Otterson, J. (2017). *MSNBC ranks as no. 1 cable network in total viewers for first time ever.* Retrieved from: https://variety.com/2017/tv/news/msnbc-cable-news-ratings-charlottesville-1202531567

Pérez-González, D., Trigueros-Preciado, S., & Popa, S. (2017). Social media technologies' use for the competitive information and knowledge sharing, and its effects on industrial SMEs' innovation. *Information Systems Management, 34*(3)*,* 291-301.

Richi, C. (2017). *Top 10 most popular news channels in the world.* Retrieved from: http://www.allrefer.com/top-10-popular-news-channels-world

Small Business Agency (SBA) (2018). Retrieved from: https://www.sba.org.il/, and https://www.gov.il/he/departments/units/small_medium_business_agency_about

Small Business Agency (SBA) (2019). *Size standards.* Retrieved from: https://www.sba.gov/federal-contracting/contracting-guide/size-standards

United States cable news (n.d.). *In Wikipedia.* Retrieved from: https://en.wikipedia.org/wiki/United_States_cable_news

University of San Diego (2018). *The top cyber security blogs and websites of 2018.* Retrieved from: https://onlinedegrees.sandiego.edu/top-cyber-security-blogs-websites

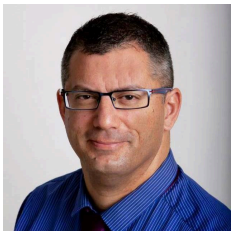
US-Cert-SMB (2018). *Resources for small and midsize businesses.* Retrieved from: https://www.us-cert.gov/ccubedvp/smb

U.S. Small Business Administration (2018). *2018 small business profile.* Retrieved from: https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf

Verizon Enterprise (2018). Verizon 2018 data breach investigations report (DBIR). Retrieved from: http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

Authors' Biographies

Ruti Gafni, Ph.D. is the Head of the Information Systems BSc program at The Academic College of Tel Aviv Yaffo. She holds a PhD from Bar-Ilan University, Israel (in the Business Administration School), focusing on Information Systems, an M.Sc. from Tel Aviv University and a BA (Cum Laude) in Economics and Computer Science from Bar-Ilan University. She has more than 40 years of practical experience as Project Manager and Analyst of information systems.



Tal Pavel, Ph.D. is the Head of Cybersecurity Studies in the Information Systems Program, at The Academic College of Tel Aviv Yaffo. He specializes in cyber threats, ICT and Internet in the Middle East. He holds a Ph.D. in Middle Eastern Studies from Bar-Ilan University, Israel (Dissertation: "Changes in Governmental Restrictions over the Use of Internet in Syria, Egypt, Saudi Arabia and the United Arab Emirates between the Years 2002 – 2005"). He has served as a keynote speaker at international conferences and has been interviewed as an expert cyber commentator on all major Israeli media outlets.