ISSN: 1987-6521, E-ISSN: 2346-7541
DECEMBER 2022 VOLUME 59 ISSUE 01
MINI-REVIEW

EFFECTS OF CYBER ATTACKS ON SMALL AND MEDIUM ENTERPRISES (SMEs)

Abdulova Aygun, Quluyeva Sevinc, Farhadova Sadat, Huseynova Efsane, Qafarov Mecid

Department of Economics and Management, Azerbaijan State University of Economics, Baku, Azerbaijan

Email: sabah.aygun2015@gmail.com; quluyevasevinc00@gmail.com; seadetferhadova@gmail.com; huseynovaafsana0@gmail.com; mecid7qafarov@gmail.com

Received: 21-Mar-2022, Manuscript No. BSSJAR-22-57926; **Editor assigned:** 23-Mar-2022, PreQC No. BSSJAR-22-57926(PQ); **Reviewed:** 04-Apr-2022, QC No. BSSJAR-22-57926; **Revised:** 06-Apr-2022, Manuscript No. BSSJAR-22-57926(A); **Published:** 13-Apr-2022, DOI: 10.36962/gbssjar/59.1.002

ABSTRACT

Small businesses are just as vulnerable to cyber security threats as large corporations. A typical assumption for small businesses is that they are safe because of a lack of definition, that their business is too little to be a target, which is regrettably not the case. Assailants are increasingly automating their attacks; it is becoming easier for them to target hundreds, if not thousands, of small firms at once. Little businesses regularly have less rigid mechanical guards, less mindfulness of dangers and less time and asset to put into cyber security. As a result, they are a more straightforward target for programmers than larger enterprises.

Cyber-attacks continue to wreak havoc on corporate computer security. These assaults progress in a predictable pattern, becoming increasingly advanced and powerful. They expand through exploiting security flaws in both public and private organizations and businesses. SMBs (Small and Medium-Sized Businesses), due to their structure and financial characteristics, are especially harmed when a cyber-attack takes put. In spite of the fact that organizations and companies put parts of endeavors in executing security arrangements, they are not continuously compelling. This is often extraordinarily important for SMEs, which don't have sufficient financial assets to present such arrangements.

In this way, there's a require of giving SMEs with affordable, brilliantly security frameworks with the capacity of identifying and recuperating from the foremost hindering assaults. In this paper, we propose a brilliantly cyber security stage, which has been planned with the objective of making a difference SMEs to create their frameworks and organize more secure.

Keywords: Cyber security, SME, Efficiency, Cyber-attacks, Information security management.

INTRODUCTION

The word "cyber security" has been the subject of academic and popular literature, much of which has taken a particular approach to the subject. The phrase is used broadly, and its definitions are very diverse, context-bound, often subjective, and, at times, uninformative, according to the literature review provided in this article. There is a scarcity of research on what the term signifies and how it is used in different circumstances. The lack of a concise, widely accepted definition that captures the multidimensionality of cyber security could stymie technological and scientific progress by reinforcing a primarily technical view of cyber security while separating disciplines that should work together to address complex cyber security challenges. There are a variety of technical solutions that support cyber security, for example. However, these solutions alone do not solve the problem; there are numerous examples and substantial scholarly work that demonstrate the

ISSN: 1987-6521, E-ISSN: 2346-7541
DECEMBER 2022 VOLUME 59 ISSUE 01

challenges related to organizational, economic, social, political, and other human dimensions that are inextricably linked to cyber security efforts. Former Director of Research at the US National Security Agency discusses the interdisciplinary nature of cyber security.

“A Science of Cyber security offers many opportunities for advances based on a multidisciplinary approach, because after all, cyber security if fundamental about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics.”

LITERATURE REVIEW

Cyber security threats and attacks are on the rise, especially in light of recent geopolitical developments. Governments, institutions, and multinational corporations are no longer the targets of cyber-attacks. Cyber-attacks are now affecting smaller firms and even individuals, either directly or as a result of side effects. Simultaneously, political and regulatory pressure to prevent cyber-attacks is increasing, particularly in Europe. Different labels, particular regulations, or practical instructions are being established to protect Small and Medium Enterprises (SMEs). This article does a comparative analysis of similar efforts with the goal of launching one in Belgium that is consistent with other existing approaches while also allowing for longer-term convergence with a possible European plan. Our goal is to reach a sufficient number of SMEs with a minimum level of cyber security and involve them in ongoing improvement in order to maintain a secure level that is both sustainable and efficient. We discuss how to set up the broad organizational structures, fundamental management processes, and some supporting tools on a more practical level.

From 2018 to 2025, the cyber security market is expected to increase at a CAGR of 11.9 percent, from $104.60 billion in 2017 to $258.99 billion in 2025. Cyber security, also known as Information Technology (IT) security, focuses on preventing unauthorized or spontaneous access to computers, applications, networks, and data. As the prominence of cyber threats has grown, so have security solutions. The cyber security market is growing due to factors such as an increase in malware and phishing attacks, as well as an increase in the use of IoT and the BYOD trend among businesses.

One of the primary reasons driving market expansion is the growing demand for cloud-based cyber security solutions. The ongoing requirement to comply with cyber security industry standards, laws, and the complexities of device security, on the other hand, are some of the primary challenges impeding market growth. Furthermore, in order to minimize the damage to IT resources, cyber security efforts are now being prioritized and integrated with important business activities, which presents a significant opportunity for market growth. Furthermore, the market is likely to benefit from an increase in the demand for strong authentication techniques.

The solutions category led the overall cyber security market in 2017 and is likely to continue to do so during the forecast period, owing to the growing demand for large and small businesses to monitor external and internal threats. In addition, the services market is predicted to expand rapidly over the next few years (Figures 1-3).

ISSN: 1987-6521, E-ISSN: 2346-7541
DECEMBER 2022 VOLUME 59 ISSUE 01

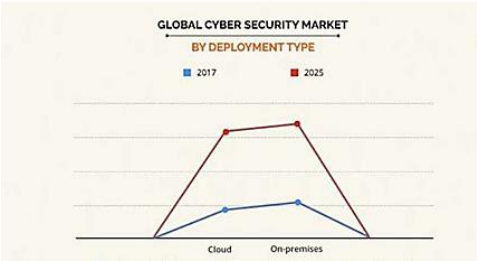

Fig. 1. Cloud is projected as one of the most lucrative segments and it would exhibit the highest CAGR of 13.90% during 2018-2025

During the forecast period, the cloud segment of the cyber security market is predicted to rise at a substantial rate. Low maintenance costs, which are favored by small and medium businesses, are largely responsible for the segment's growth. On the contrary, the on-premises market is likely to expand rapidly over the next several years.

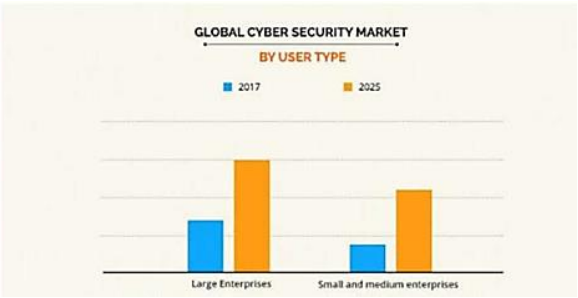

Fig. 2. Small and medium enterprises would exhibit the highest CAGR of 14.50% during 2018-2025

The big businesses category had the greatest revenue cyber security market share in 2017; this sector's growth can be ascribed to large enterprises' increased attention on deploying effective security solutions as a result of their expanding perimeter.

The cyber security market study is the centre of the report, which examines development potential, restraints, and trends. Porter's five forces analysis is used in the study to evaluate the impact of several aspects on cyber security, such as supplier bargaining power, competitor competitive intensity, threat of new entrants, threat of substitutes, and buyer bargaining power market.

© THE BALTIC SCIENTIFIC JOURNALS
BLACK SEA
SCIENTIFIC JOURNAL OF ACADEMIC RESEARCH
ISSN: 1987-6521, E-ISSN: 2346-7541
DECEMBER 2022 VOLUME 59 ISSUE 01

Fig. 3. Health care would exhibit the highest CAGR of 14.90% during 2018-2025

In order to get as a more universally acceptable term that reflects the genuine intrigue nature of cyber security, we looked at relevant material to distinguish between definitions, observe overwhelming subjects, and recognise cyber security views. Several interactions with a heterogeneous group of cyber security experts, academics, and graduate students aided our investigation. Together, these two exercises result in a modern, more comprehensive and binding definition of cyber security that, in theory, will enable an improved and improved centre on intrigue.

Arguments about cyber security have an impact on how academics, industry, government, and non-government organizations address cyber security concerns.

This article illustrates the process used to develop a more all-encompassing description that better situates cyber security as an interest movement, intentionally stepping back from the overpowering specialist view by combining multiple perspectives.

Computer science, design, political ponders, brain research, security ponders, and management, education, and humanism were among the subjects of our writing survey, which covered a wide range of scholarly disciplines. Building, innovation, computer science, and security and resistance are the most common disciplines found in our writing audit. But, to a much lesser degree, there was too prove of the subject of cyber security in diaries related to approach improvement, law, healthcare, open organization, bookkeeping, administration, humanism, brain research, and instruction [1-6].

The purpose of this research is to determine the elements that contribute to the success of information security management in SMEs. Azerbaijan is the focus of the study's geographical scope. The research team narrowed the scope of the study to four main factors based on a literature review of the most important information security management success factors: compliance of information security management with the company's business activities (F1), top management support (F2), security controls (F3), and organizational awareness (F4). The following scientific hypotheses were proposed by the research team.

H1: Four main factors (F1 to F4) of information security management are equally important.

H2: The cause and effect relationship among the factors of information security management (F1, F2, F3 and F4) does not exist.

DISCUSSION

Because employing a dedicated full-time security manager is ineffective in small firms, responsibility for safety management is centralized at the level of the statutory body. Another option is to consolidate functions within an organization or to hire an information security manager on the outside (CISO). The survey research in the sector of SMEs' information security

management is pretty difficult. In a survey of information security management in the United States, Kotulic and Clark discovered that as many as 23% of those who declined to complete the questionnaire's questions stated that they are unwilling to share any information about their computer security rules with outside groups.

This study employs a Qualitative Risk Assessment (QRA) approach, as recommended by the World Economic Forum (WEF). This will allow us to compare the study's findings to the findings of the worldwide risk report. Because of its low cost, ease of use, and speed, qualitative risk assessment is one of the most extensively utilised risk assessment methods. Potential repercussions and likelihoods are rated on a qualitative scale of low, medium, and high in QRA. Qualitative risk assessment relies on subjective likelihood and consequence values gathered from experts and decision-makers, and as a result, they aren't necessarily accurate assessments and are prone to biases and heuristics. The risk matrix is created by plotting the assessed likelihoods and implications for selected risks in a two-dimensional space. Risk assessment reports have mentioned many types and sizes of risk matrix. A risk matrix is a tool for visualising, comparing, and ranking various risks based on their severity locations in the matrix. The majority of the time, colour coding is utilised to indicate the importance of each risk. The risk matrix approach is also used to identify potential risk control measures and to keep track of the inherent, present, and target risk levels.

CONCLUSION

The topic of information security management is becoming increasingly essential, particularly among small and medium-sized businesses. The goal of this article was to determine the elements that contributed to the success of information security management in Slovakia's SMEs. We narrowed the scope of our research based on the previous literature review and focused on four main factors of information security management success, which were defined by most of the authors as the most important, namely compliance of information security management with the company's business activities, top management support, security controls, and organizational awareness. We spoke with top IT security professionals from small and medium-sized businesses in Slovakia to determine the importance and linkages of the mentioned parameters. The importance of four elements was appraised by experts from the perspective of information security management success, and the results of the expert review were processed using the DEMATEL technique. The findings of the study demonstrate that Security Controls, which include technical and procedural information security controls, risk management, and the application of standards, are the most important factors in the success of information security management. The supporting top management is the second most critical aspect. Our findings also suggest that, in the short term, organizational knowledge is the most obvious and crucial aspect for information security management success.

REFERENCES

1. Barabási, A. L., & Albert, R. (1999). Emergence of scaling in random networks. Science, 286(5439), 509-512.
2. Cavelty, M. D. (2008). Cyber-terror-looming threat or phantom menace? The framing of the US cyber-threat debate. Journal of Information Technology and Politics, 4(1), 19-36.
3. Deibert, R., & Rohozinski, R. (2010). Liberation vs. control: The future of cyberspace. Journal of Democracy, 21(4), 43-57.

ISSN: 1987-6521, E-ISSN: 2346-7541
DECEMBER 2022 VOLUME 59 ISSUE 01

4. Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Developing expertise for network intrusion detection. Information Technology and People.
5. Kozlenkova, I. V., Samaha, S. A., & Palmatier, R. W. (2014). Resource-based theory in marketing. Journal of the Academy of Marketing Science, 42(1), 1-21.
6. Kavakiotis, I., Tsave, O., Salifoglou, A., Maglaveras, N., Vlahavas, I., & Chouvarda, I. (2017). Machine learning and data mining methods in diabetes research. Computational and Structural Biotechnology Journal, 15, 104-116.

Citation: Aygun, A., Sevinc, Q., Sadat, F., Efsane, H., & Mecid, Q. (2022). Effects of cyber attacks on Small and Medium Enterprises (SMEs). GBSSJAR. 59(1), 1-5. DOI: 10.36962/gbssjar/59.1.002