Journal of Advanced Zoology

ISSN: 0253-7214

Volume ***44*** *Special Issue-****2 Year 2023*** *Page* ***5269:5278***

CYBER SECURITY AND RISK MANAGEMENT: SAFEGUARDING ORGANIZATIONS IN THE DIGITAL AGE

S. SHABANA BEGUM

Designation:Assistant Professor Department: Computer Science and Engineering (Data Science) Institute: G. PULLA REDDY ENGINEERING COLLEGE (Autonomous) District: Kurnool City: Kurnool State: Andhra Pradesh

Email id: shabana.ecs@gprec.ac.in

Dr,Revathi,R

Assistant Professor Computer Science Karpagam Academy Of Higher Education Coimbatore Tamilnadu

revathilakshay@gmail.com

Maulik chandnani

Assistant professor Faculty of commerce and management RNB Global University Bikaner

csmaulikchandnani@gmail.com

Badria Sulaiman Alfurhood

Department of Computer Sciences, College of Computer and Information Sciences, Princess Nourah bint

Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia;

bsalfurhood@pnu.edu.sa

Ms.Samisha. B

Designation: Assistant Professor Department: Commerce

Institute: St.Claret College District: Bangalore Urban City: Bangalore

State: Karnataka

Article History

Received: 06 September 2023

Revised: 05 November 2023

Accepted:08 December 2023

Abstract

Cyber security helps the organization to protect the organizational data from external users. The development of an effective cyber security system is important as this helps the organization to enhance the data safety system. The secondary data collection process has been used for analyzing the most affected factors that affect the security system of an organization. On the other hand, qualitative analysis helps to know the all interrelated factors related to the data safety and risk management system. System theory helps to analyze the ways to develop a better protective system for enhancing the protection of organizational data. The use of centralized servers, double-protected passwords and network security and access control is important for developing a

Introduction

The development of cyber security is important for increasing data security. The development of data security increases the safety of the organization from being affected by external and internal bad actors. This study has analyzed the importance of cyber security in an organization and the most important ways to increase data safety. The implementation of cyber security enhances the data safety management system of the organization and helps the organization protect its data from external cyber-attacks. The development of cyber security is possible through the implication of security risk assessment. Thus, the development of a security framework is important for an organization to save the company from external attacks.

Research background

This research has analysed the interrelated things related to the development of cyber security in an organisation and the way the company can develop better security servers. According to the views of Kumar et al. (2021), a developed cyber security system helps the organsiation to reduce the number of loopholes and increases the security system of the organsiation. The implementation of the risk management system assists the organsiation in protecting the server data from any external accessors. Based on the views of Ertan et al. (2020), the development of cyber security is a must for protecting data from outsiders. This means the adaptation of a modernised security system of servers is important for making the organisational server safer.

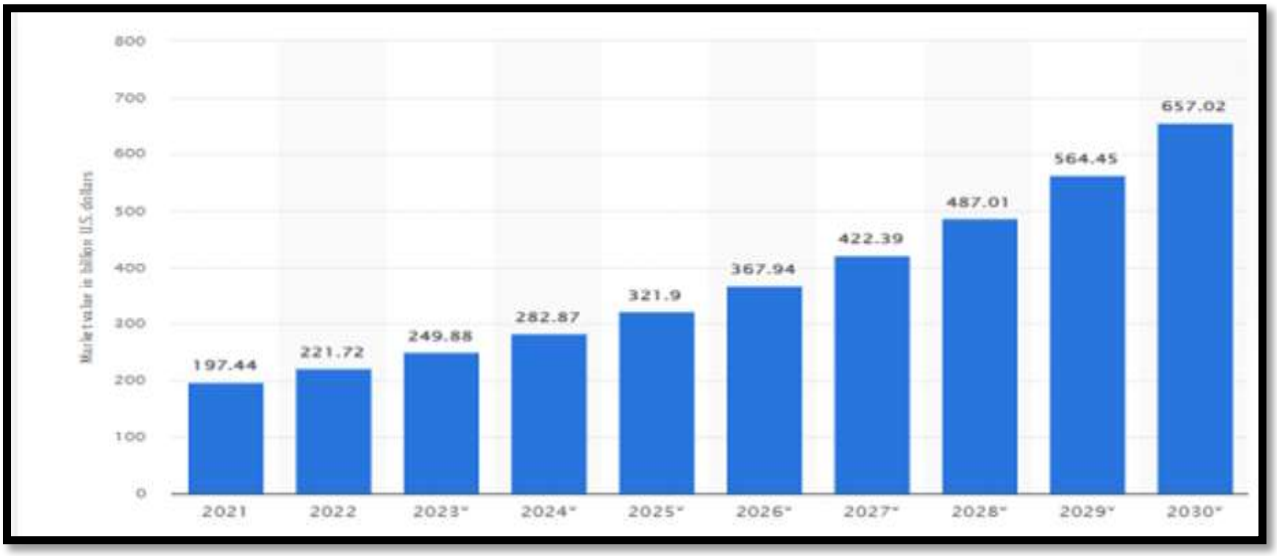

Figure 1: market size of cyber security systems from 2021 to 2030

(Source: Statista, 2023)

The above figure represents the development of the cyber security market size from 2021 to 20230. The market size of the cyber security system was 197.44 billion US dollars in 2021 and that increased to 249.88 US dollars in 2023 (Statista, 2023). This denotes that the demand for the cyber security system is high and increasing positively. This figure has been used in this study as this represents the need of the people which increases the market size of cyber security continuously. According to the views of Filipczuk, Mason, & Snow (2019), the main objective behind the use of cyber security is to increase the data safety of the organsiation and server. Thus, the use of cyber security systems is continuously increasing among organisations to protect their data from external effects.

Problem statement

The main problem is the probability of cybercrime is increasing with the development of software technology. Data safety is the most risk task in modern times and several organisations have started to use modern strong cyber security systems to protect data. The development of a risk management system is mandatory for increasing the data safety of organisations.

Research aim and objectives

Research aim

This research aims to analyse the effectiveness of using cyber security in organisations and the way it protects the organsiation from the attack of external users.

Research objectives

- To know details about cyber security and the way it helps the organisations to protect their data
- To analyse the importance of a risk management system to increase the organisational performance
- To know the challenges faced by the organsiation for protecting their server through cyber security systems
- To suggest better ways to develop a strong cyber security system to enhance the data protection system

Research questions

- What is a cyber-security system and through which way it helps to protect organizational data?
- What is the importance of risk management systems in organizations?
- How the organizations face challenges in developing a strong cybersecurity system?
- What are the best possible ways to increase the data safety of the organizations?

Research significance

This study is important for all business holders and people as this helps to know the importance of data safety and cyber security. According to the views of Tagarev (2020), the incidents of cybercrime have increased and it caused several monetary losses. Thus, this research provides ample knowledge about cyber security which increases data safety. Thus, this study is important for all to learn about the effectiveness of cyber security.

Research structure

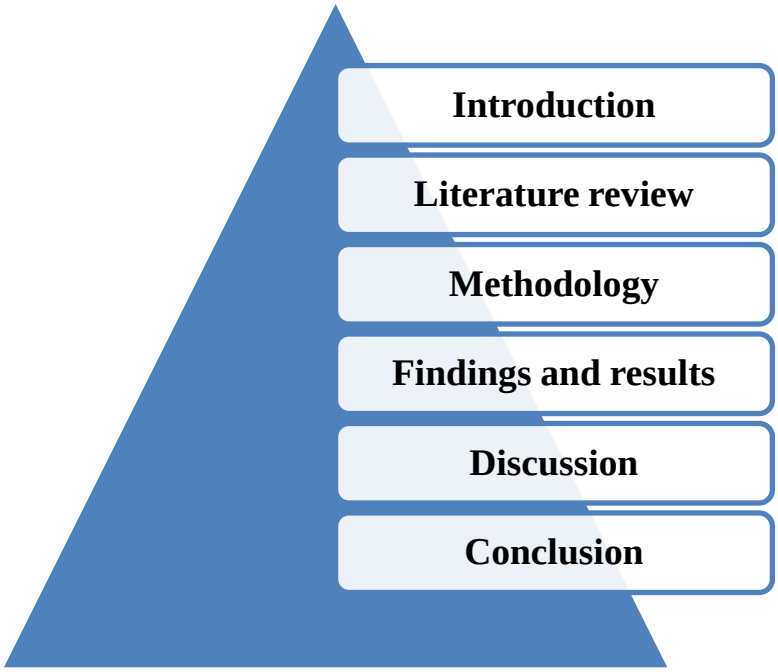

Figure 2: Research structure

Literature review

Concept of cyber security and risk management strategies for developing organization's security

Cyber security has included advanced technologies to protect the system from cyber-attack. It has a focus on unauthorized access to the systems and protects the systems from criminal activities. According to the views of Nifakos et al. (2021), cyber security protects those systems which are connected to the internet and protects the computer systems from cyber threats.

Figure 3: Big investment in cybersecurity development

(Source: Statista, 2023)

The above has shown the big investment in developing cybersecurity. This investment has increased gradually and the highest investment has found 2397 million dollars in the year 2021. It has a significant contribution to the development process of organization security. On the other hand, Demirkan, Demirkan, & McKee (2020), argued that cyber security has provided safeguards to organizations for protecting against cyber-attack-related issues. This safeguard helps the organization to protect the sensitive as well as the confidential information. Organizations can recognise the security risks and can implement plans to identify the problems. It helps the organization to monitor the systems regularly.

Effect of safeguarding organizations from any type of cybercrime

Cyber security safeguards help the organization to protect the systems from unauthorized access. Organizations can prevent confidential data from cybercrimes

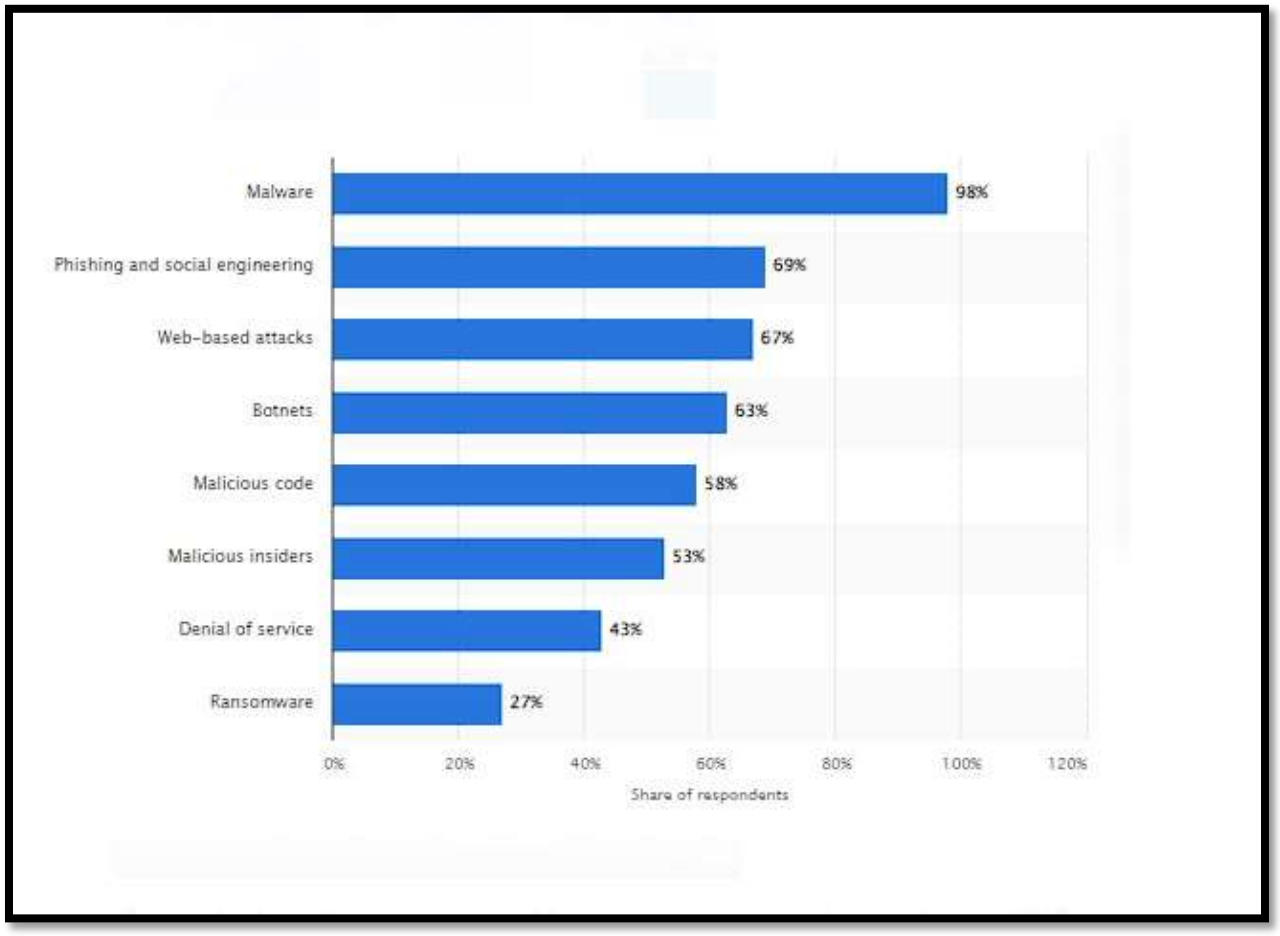

Figure 4: Companies faced various types of cyber-attacks in 2017 throughout the world

(Source: Statista, 2023)

The above figure represents that companies have experienced various cyber-attacks worldwide. This figure shows that 98% of respondents have faced malware-related issues and 67 % of respondents shared their experiences based on web-based attacks. It helps to create strong passwords securing the internet connection of the organization. Safeguards help to

monitor the computer systems and also help to update the systems. According to the views of Karpiuk (2021), cyber security can mitigate the risk of unauthorized access to the systems through the use of safeguards. It helps to improve the data management process and cyber posture.

Challenges faced by the organizations to develop cyber security and online safeguards

Different organizations or companies lead different IT technologies and solutions for cyber risk. As per the views of Tagarev (2020), the actors of cyber threats are continuously working to evolve and build decisions to overcome the advanced cyber security determination. As per the judgment, the landscape of cyber intimidation is constantly changing and new types of offensive facts are built all the time. The organization is faced with major problems due to a deficiency of efficient cybersecurity professionals.

Theoretical framework

System Theory of Cyber Security

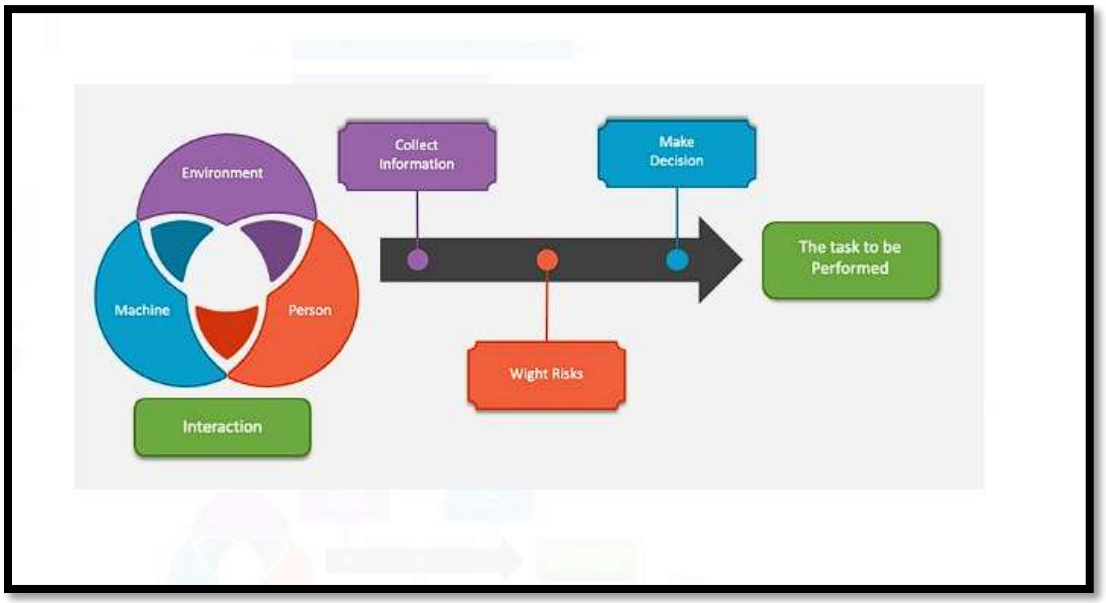

Figure 5: System theory

(Source: Yohanandhan et al. 2020)

This study has used system theory which was provided by Ludwig Von Bertalanffy for understanding the individual components part of the system. According to the views of Yohanandhan et al. (2020), system theory has provided opportunities for the organization to understand the components of the systems properly. It helps to understand the relationship among the components of the system.

Methodology

The methodology section of the study included all the methods which have been used for the development of the research. This study has been developed by using secondary qualitative methods. Secondary qualitative methods include secondary data collection and qualitative analysis processes. According to the views of Nayak & Narayan (2019), secondary data are those data which have been collected from different sources and these data are also called ready-made

data. This means secondary data are already to meet other demands. On the other hand, the secondary data include journals, official reports, news sources and articles. Qualitative analysis helps to analyse all the secondary data by comparing the information from different sources. Based on the views of Taherdoost (2022), qualitative analysis helps to gather more information about the topic. This means this method is dependent on the observation process which helps to increase the depth of knowledge on the study topic.

Finding and results

Resources	**Code**	**Themes**
Kumar et al. (2021), Ertan et al. (2020),	Cyber security, organization, computing system	Theme 1: Cybersecurity reduces the risk of organizations being affected by cybercrime
Filipczuk, Mason, & Snow (2019), Tagarev (2020),	Cyber security, organization, cyber security network	Theme 2: Cybersecurity strategies enhance the data security and networking system of organizations
Karpiuk (2021), Rodgers, Attah-Boakye, & Adams (2020)	Cyber security, national system, algorithmic cognitive decision trust modelling	Theme 3: The algorithm-based model of cyber security helps to protect the organizational system of work from external effects

Table 1: Theme Analysis

(Source: Self-created)

"Theme 1: Cyber security reduces the risk of the organizations from being affected by cybercrime"

Cyber security safeguards organizations from cybercrime-related activities. It protects the systems from loss of confidential information. According to the views of Kumar et al. (2021), cyber security helps to monitor the system to protect the personal data of the organization. It has provided an advantage to the organization in protecting data from online assaults.

"Theme 2: Cyber security strategies enhance the data security and networking system of organizations"

Cyber security has made strategies to increase the data security as well as the networking systems of organizations. It has taken the initiative to update the software to get better results. Based on the views of Ertan et al. (2020), better cybersecurity strategies can secure devices from cybercrimes. Strong passwords can help to reduce the risk of cyber threats.

"Theme 3: The algorithm-based model of cyber security helps to protect the organizational system of work from external effects"

Triple DES has been used to protect the data safety of the organizations. According to the views of Tagarev (2020), algorithms of cyber security are used for the process of encryption. This algorithm is mostly used by organizations to protect the systems from hackers.

Discussion

The development of a central security system is important for an organization to reduce the chances of cybercrime incidents. According to the views of Karpiuk (2021), the development of the organisational opportunity increases with the enhancement of data safety. This helps the organsiation to protect the important data in a more safe condition and it helps to develop organisational potential to achieve success in the future. Based on the views of Rodgers, Attah-Boakye & Adams (2020), the development of the cyber security system becomes stronger with the use multifactor authentication system to enter the organisational server. This denotes that increasing server security decreases the probability of data leakage problems. On the other hand, organisations need to inform the organisation password to the employees only as this helps to know the server access history and helps to detect the criminals. Enhanced data safety increases the risk management system of the organisations and helps to keep the most important data in a safe zone. The probability of data losses has increased with increasing the number of internet users. The Internet accessing facilities increase the loopholes of the systems and help cyber criminals access the data of other people.

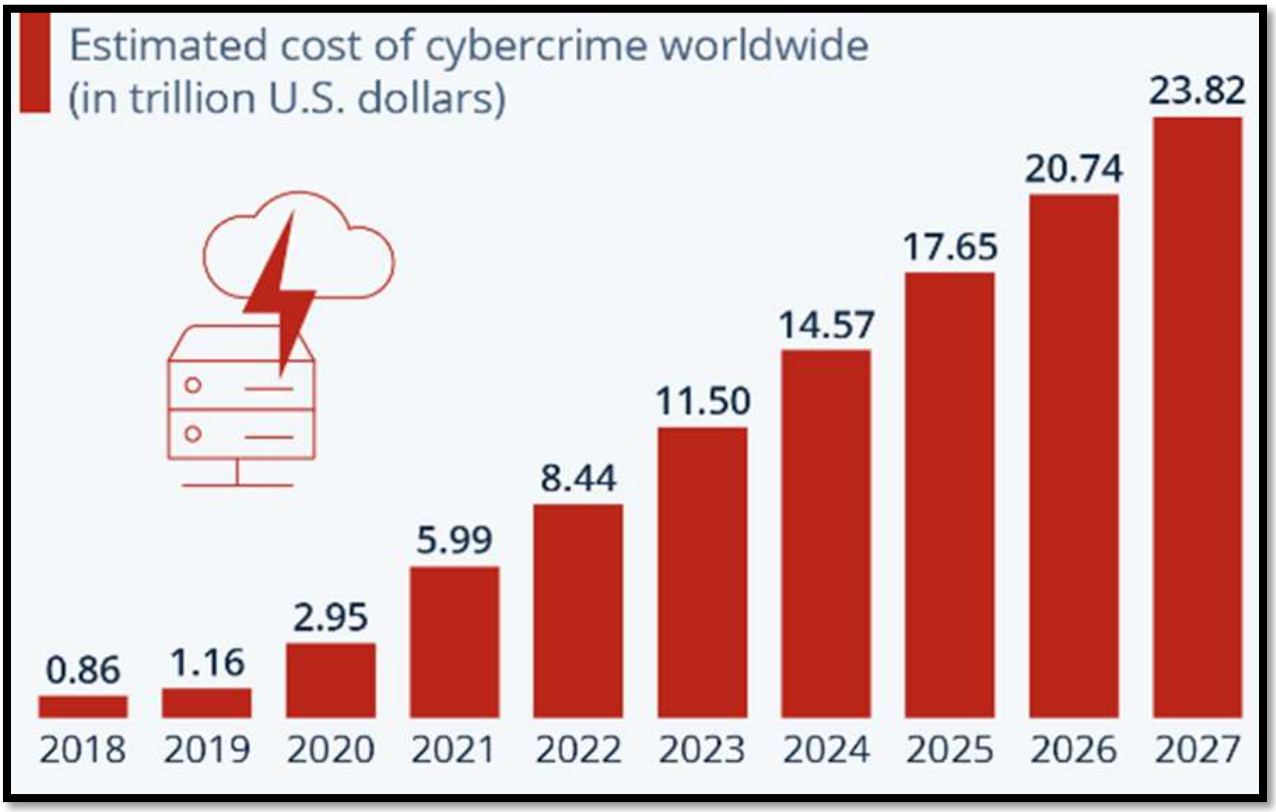

Figure 6: The cost of cybercrime in the whole world from 2018 to 2027

(Source: Statista, 2023)

The above figure represents the cost of cybercrime and that increases with time. The cost of cybercrime was 0.86 trillion US dollars in 2018 and that increased to 11.50 trillion US dollars in 2023 (Statista, 2023). This means the incidents of cybercrime have drastically increased in the whole world. This has been increased with the development of internet networks and software

technology. Thus, the development of a strong security system for organizational servers is important for increasing its strength.

Conclusion

The security system of the server needs to be strong to increase the data management system of the organsiation. The data safety of the employees and other important stakeholders is important for an organsiation and this organisation has developed a better server. The development of enhanced server protection decreases the chances of cybercrime incidents. Implementation of a security awareness system, enhanced data management, and strong network security helps the organsiation to save the organisational data from external people. Thus, the development of strong server and network systems has become compulsory to manage the risk of data losses and data leakage.

References

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. *Journal of Management Analytics*, *7*(2), 189-208. Retrieved on: 11th December 2023 from: https://www.researchgate.net/profile/Irem-Demirkan-2/publication/339509334_Blockchain_technology_in_the_future_of_business_cyber_security/links/5f28388992851cd302d6c5da/Blockchain-technology-in-the-future-of-business-cyber-security.pdf

Ertan, A., Crossland, G., Heath, C., Denny, D., & Jensen, R. (2020). Cyber security behaviour in organisations. *arXiv preprint arXiv:2004.11768*. Retrieved on: 11th December 2023 from: https://arxiv.org/pdf/2004.11768

Filipczuk, D., Mason, C., & Snow, S. (2019, May). Using a game to explore notions of responsibility for cyber security in organisations. In *Extended abstracts of the 2019 CHI conference on human factors in computing systems* (pp. 1-6). Retrieved on: 11th December 2023 from: http://library.usc.edu.ph/ACM/CHI2019/2exabs/LBW0267.pdf

Karpiuk, M. (2021). Organisation of the National System of Cybersecurity: Selected Issues. *Studia Iuridica Lublinensia*, *30*(2), 233-244. Retrieved on: 11th December 2023 from: https://pdfs.semanticscholar.org/a5cd/d37e40835e86081d13be516e104e3353fca3.pdf

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597-1629. Retrieved on: 11th December 2023 from: https://bura.brunel.ac.uk/bitstream/2438/21548/2/FullText.pdf

Nayak, M. S. D. P., & Narayan, K. A. (2019). Strengths and weaknesses of online surveys. *technology*, *6*(7), 0837-2405053138. Retrieved on: 11th December 2023 from: https://www.researchgate.net/profile/Mudavath-Nayak/publication/333207786_Strengths_and_Weakness_of_Online_Surveys/links/61176e5a0c2bfa282a42253b/Strengths-and-Weakness-of-Online-Surveys.pdf

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119. Retrieved on: 11th December 2023 from: https://www.mdpi.com/1424-8220/21/15/5119/pdf

Rodgers, W., Attah-Boakye, R., & Adams, K. (2020). Application of algorithmic cognitive decision trust modelling for cyber security within organisations. *IEEE Transactions on Engineering Management*, *69*(6), 3792-3801. Retrieved on: 11th December 2023 from: https://pure.hud.ac.uk/ws/files/21880764/FINAL_VERSION_WORD.pdf

Statista, 2022.

Big Tech Invests Big in Cybersecurity. Retrieved on: 11th December 2023 from: https://www.statista.com/chart/27088/gafam-spending-on-cybersecurity-deals-and-funding-per-year/

Statista, 2023. *Cybercrime Expected To Skyrocket in Coming Years*. Retrieved on: 11th December 2023 from: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Statista, 2023. *Size of cyber security market worldwide from 2021 to 2030*. Retrieved on: 11th December 2023 from: https://www.statista.com/statistics/1256346/worldwide-cyber-security-market-revenues/

Statista, 2023. *Types of cyber-attacks experienced by companies worldwide as of August 2017*. Retrieved on: 11th December 2023 from: https://www.statista.com/statistics/474937/cyber-crime-attacks-experienced-by-global-companies/

Tagarev, T. (2020). Towards the design of a collaborative cybersecurity networked organisation: Identification and prioritisation of governance needs and objectives. *Future Internet*, *12*(4), 62. Retrieved on: 11th December 2023 from: https://www.mdpi.com/1999-5903/12/4/62/pdf

Taherdoost, H. (2022). What are different research approaches? Comprehensive Review of Qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, *5*(1), 53-63. Retrieved on: 11th December 2023 from: https://hal.science/hal-03741840/document

Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., & Mihet-Popa, L. (2020). Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications. *IEEE Access*, *8*, 151019-151064. Retrieved on: 11th December 2023 from: https://ieeexplore.ieee.org/iel7/6287639/6514899/09167203.pdf