IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 3, Ser. I (May. –June. 2022), PP 55-59
www.iosrjournals.org

Organizations in the face of cyber-attacks: The Mitigation Strategies

Friday Ehi Ikuero
[1]*Nigeria Computer Emergency Response Team, Nigeria*

Abstract:
Background*: The use of computer and internet in today's world has brought about certain benefits such as ease of communication to aid business operation of organizations. However, this prompted cyberattack on the rise in recent times. This paper analyzed how to mitigate cyber-attacks in organizations.*
Materials and Methods*: This study used secondary source methodology by reviewing existing scholarly works related to cyber-attacks in organizations.*
Results*: This paper identified some problems that affect the mitigation of cyber-attacks, which include failure to classify assets, Non-compliance on reporting. Accordingly, it provided solutions including assets classification, implementation of strategy, provision of control standards, and compliance on reporting.*
Conclusion: *Implementation strategies to mitigate cyber-attacks against organizations' computer systems will sustain their business growth. This paper discussed the problems of cyberattack. Thereafter, it examined some solutions to the problem and finally makes some recommendations.*
Key Word*: Organization, Cyber-attacks, Cloud Computing, Mitigation, Strategies, Information Security policy*

Date of Submission: 26-05-2022 Date of Acceptance: 07-06-2022

I. Introduction

The use of computers and the internet has become a necessity in conducting business and executing activities. New threats emerge every day when computing devices are connected to the internet; thereby exposing users and their organizations to possible cyber-attacks [1]. The target of attack could be an individual, an organization a country [2]. Cyberattack is now a lucrative business, and as such exposes organizations more to threats [3]. Cyber-attacks occur when there are inadequate cybersecurity measures, which could affect the targeted organization [4]. In a cybersecurity breach survey conducted in 2018, it was revealed that organizations 38% of small organizations in the UK expose themselves to cyber-attacks emanating from impersonation, and emails among others [5, 6]. Another research by Ponemon Institute in 2019 estimated the cost implication of cyber-attacks to be USD 3 million [7].

In another development, a study revealed that over 20% of organizations suffer successful cyberattacks no less than once a week [8]. A cyber-attack can also damage the reputation of organizations. The damage could affect the organization's customers, suppliers, partners and investors. Therefore, organizations are to abide by the provisions of the laws that regulate cybersecurity, information security, data protection and privacy to prevent cyber-attacks [9].

Given the above-mentioned, organizations need to deliberately emplace measures to mitigate cyber-attacks before and after their occurrence. However, organizations face many challenges in mitigating cyber-attacks including lack of technical know-how, and poor funding among others [5, 10]. It is given the foregoing that this paper seeks to appraise cyber-attack in organizations to make recommendations.

The subsequent part of the paper is structured as follows; Section I is the literature review. Section II is the related works and Section III is the terminologies. Section IV consists of the problems of cyberattack mitigation and Section V is the solutions to problems of cyberattack mitigation while Section VI is the conclusion.

II. Literature review

In [1], the writers asserted that cyberspace is now an integral part of organizations as it aids business activities especially and makes living more affordable. However, there is a concern about cyber-attacks on infrastructure and internet components with devastating impacts. Cyberattack leads to damage and loss to organizations [11]. Therefore, cyber-attacks focus more on the impact than the efforts making it a result-oriented target; hence organizations should make cybersecurity a result-oriented effort and as such can be considered a

result-oriented objective. Mitigation against cyber-attacks requires international cooperation as the attack can be trans-border in nature [12].

According to [12], a cyber-attack relates to data collection and compromise while a network attack consists of a network interruption. In [13], a cyber-attack is an intentional act to disrupt or destroy a computer network. However, [14] asserted that this definition did not point out a clear difference between cyberattack, cyber warfare and cybercrime; therefore providing incomplete information to policy makers.

Different types of cyber-attacks were recorded in recent times including the Distribution Denial of Service (DDoS) attack on Amazon Web Service in 2020 [15]. DDoS attack overwhelms a system and prevents it from responding to service requests [12]. A remote code execution attack was launched against Microsoft Exchange in 2021 that affected more than 60,000 private businesses in the United States of America [15].

Appropriate application of strategy will mitigate cyber-attacks [12]. The National Institute of Standards and Technology has developed a cybersecurity framework and outlined five functions for mitigating cyber-attacks as below:

1. Identification
2. Protection
3. Detection
4. Respond
5. Recovery

III. Related Works

In [1], the writers asserted that cyberspace is now an integral part of organizations as it aids business activities especially and makes living more affordable. However, there is a concern about cyber-attacks on infrastructure and ICT components with devastating impacts.

According to [12], cyber-attacks relate to data collection and compromise while network attack consists of a network interruption. In [13], a cyberattack is an intentional act to disrupt or destroy a computer network. However, [14] asserted that this definition did not point out a clear difference between cyberattack, cyber warfare and cybercrime; therefore providing incomplete information to policy makers.

A cyberattack is a digital attack on computer systems through the internet targeted at the data compromise of an individual or organization [3]. Every organization that has an online presence is prone to cyber-attacks.

In [5], it was opined that cloud computing, connotes transmitting and receiving of services over using the internet. Transactions on the internet could be susceptible to attack without adequate security measures. To prevent the consequences of cyber-attacks, organizations must implement mitigation strategies.

IV. Terminologies

An organization refers to the official group that composes of more than one individual functioning together to accomplish a specific goal [16]. Examples of the organization include government agencies, academic institutions, banking offices, retail outlets and construction companies among others. An organization consists of four major components; hierarchy, coordination, division of labour and common goal [16].

Cyber-attack is a deliberate and malicious attempt to breach the computer systems and networks of a target organization [17]. This action is referred to as cybercrime. It leads to altering, compromising and stealing of data [17]. Examples of cyber-attacks consist of; phishing, cross-site scripting attack and DDoS.

Cloud computing delivers services, which include website hosting, data storage, analytics, and database management through the internet [18]. It is remote access enabled technology. Examples include the use of emails, social media and other platforms to send and retrieve data as well as information. In [5], it was opined that cloud computing, connotes transmitting and receiving of services over using the internet. Transactions on the internet could be susceptible to attack without adequate security measures. To prevent the consequences of cyber-attacks, organizations must implement mitigation strategies.

Mitigation is considered the act of reducing the impact and severity of any undesirable incident [17, 19]. Ignorantly, organizations are exposed to diverse risks at different levels; therefore it is vital to mitigate the risks to reduce their impact on the organization and ensures business prosperity [19].

Strategy connotes a carefully outlined plan of action for achieving a particular goal [19]. Every strategy needs constant improvement to achieve desired objectives. The application of appropriate measures will produce the desired result [9].

Information security policy and strategy consists of rules and procedures in a workforce that provides a standard for using technology, network and applications belonging to an organization to ensure integrity, confidentiality, and availability of data [20].

V. Problems of mitigating cyber-attacks

Mitigation of cyber-attacks is necessary for the continuity of organizational business especially if their services have a significant online presence. Hence, the need to implement the appropriate strategies that will enable the mitigation of cyber-attacks in organizations. However, there are problems facing strategies for mitigating cyber-attacks in organizations. Some of them will be discussed subsequently.

Failure to classify assets

Classification of cyber assets and infrastructure is very important in preventing attacks. Consequently, organizations must understand the security risk within their organization's context [21]. Organizations must classify their assets concerning the level of risks and impacts on them. For example, the exploitation of a vulnerability in an organization's database server will have more impact than exploiting the vulnerability in an employee's computer system. Hence, the mitigation strategy for safeguarding must be more resilient than the protection of a computer system.

Inadequate Knowledge

Technology is constantly advancing and there are corresponding changes in the ways things are conducted in the global cyber ecosystem. Cyber-attack increase without a proportional increase in the security awareness by the users in organizations such as cyber hygiene on the internet; posing challenges to mitigation strategies. According to research, cybersecurity must evolve in proportion to evolving cyberattack activities [22]. Lack of adequate and appropriate information on the strategies to use in mitigating cyber-attacks will expose the vulnerability of the organizations to successful attacks [23].

Lack of implementation

Implementing strategies leads to the realisation of any set goals. When strategies are developed, there must be an implementation plan that requires enforcement otherwise; the goal will not be achieved. For example, organizations may include daily data backup in their strategy implementation plan but failure to execute will affect the mitigation process.

Ineffective control

Cyber infrastructure and assets belonging to organizations must be under control. Effective control should provide for security, data segregation, compartmentalization, risk management and standard of operation of hardware and software applications [24]. Therefore, organizations must continue monitoring all processes and mechanisms for ensuring that controls meet the mitigation expectation [25]. Failure to ensure effective control could pave the way for attacks on an organization's critical cyber infrastructure.

Non-compliance with reporting

It is imperative for all users and owners of a computer system to include reporting of cyber attacks on their information security policy and must be treated accordingly [25]. Organizations should inform their employees of the procedures for reporting cyber-attacks. Organizations should endeavour to educate their employees on the legal implications for failure to report attacks on their computers and networks as may be enshrined in national instruments such as the National Cybersecurity Policy and Strategy, Data Privacy Regulation, Cybercrimes and Cybersecurity Acts. There should be proceedings for employees to report cyber-attacks [25].

VI. Solutions to problems of cyberattack mitigation

The solutions to the above stated are discussed below:

Assets classification

Organizations must classify all their cyber and computer-related components following the criticality of their job functions. Consultation from relevant governments and agencies responsible for the coordination of Critical National Information Infrastructure could be necessary.

Cybersecurity education

Constant update on evolving technology and application is necessary to avert attacks on computer systems and networks. Therefore employees who engage in any of the organizations' computer systems require training on current ways of administering and using the systems. The more employees are knowledgeable, the better they will secure the computer systems. Therefore, cybersecurity education is paramount.

Implementation of strategy

The strategy that has an implementation plan is a step ahead. Every initiative of the plan should have a time frame and measure to access progress. The earlier strategies are implemented, the better the chances for reducing attacks.

Provision of control standards

There are international standards on cybersecurity, which conform to ISO27001. Organizations could also leverage the strategy contained therein in their National Cybersecurity Policy and Strategy.

Compliance with cyberattack reporting

Many countries have national acts and legal instruments such as Data Privacy Regulation, Cybercrimes and Cybersecurity Acts. Reporting cyber-attacks and cybersecurity incidents is a statutory responsibility of users and owners of computer systems. Organizations could better mitigate cyber-attacks if they report incidents.

Recommendations

It is recommended that organizations should:

1. Classify their assets as CNII.
2. Develop implementation plan
3. Enforce the provision of the National Cybercrimes and Cybersecurity Acts
4. Develop Information Security Policy and enforce standards.

VII. Conclusion

The computer and the internet are relevant tools in our daily transactions across every sector in the world. For business sustainability, attacks against organizational cyber assets must be mitigated. The paper discussed the problems of cyberattack mitigations including failure to classify assets, non-compliance with cyberattack reporting, inadequate knowledge, ineffective control and Inadequate Knowledge. Thereafter, it discussed some solutions to the problems. The solutions include assets classification, cybersecurity education, implementation of strategy, provision of control standards, and compliance with reporting. Consequently, recommendations were made

References

[1]. Snider KL, Shandler R, Zandani S, Canetti D. Cyber-attacks, cyber threats, and attitudes toward cybersecurity policies. Journal of Cybersecurity. 2021;7(1):tyab019.

[2]. Sumi FH, Dutta L, Sarker F. A review on cyber-attacks and their preventive measures. International Journal of Cyber Research and Education (IJCRE). 2019 Jul 1;1(2):12-29.

[3]. Quigley K, Burns C, Stallard K. 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. Government Information Quarterly. 2015 Apr 1;32(2):108-17.

[4]. Catota FE, Morgan MG, Sicker DC. Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity. 2018;4(1):tyy002.

[5]. Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 2021 Nov 1;7:8176-86.

[6]. Ahmady GA, Mehrpour M, Nikooravesh A. Organizational structure. Procedia-Social and Behavioral Sciences. 2016 Sep 12;230:455-62.

[7]. Bada M, Sasse AM, Nurse JR. Cyber security awareness campaigns: Why do they fail to change behaviour?. arXiv preprint arXiv:1901.02672. 2019 Jan 9.

[8]. Singh J. Comprehensive solution to mitigate the cyber-attacks in cloud computing. International Journal of Cyber-Security and Digital Forensics (IJCSDF). 2014 Apr 1;3(2):84-92.

[9]. Cirnu CE, Rotună CI, Vevera AV, Boncea R. Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. Studies in Informatics and Control. 2018 Sep 1;27(3):359-68.

[10]. Opara EU, Mahfouz AY. Conquering the cyber attacks: analysis and protecting the enterprise resources. International Journal of Business Continuity and Risk Management. 2016;6(4):314-29.

[11]. Bullock JA, Haddow GD, Coppola DP. Cybersecurity and critical infrastructure protection. Introduction to Homeland Security. 2021:425-97.

[12]. Alghamdi MI. Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia. Materials Today: Proceedings. 2021 Apr 29.

[13]. Robinson M, Jones K, Janicke H. Cyber warfare: Issues and challenges. Computers & security. 2015 Mar 1;49:70-94.

[14]. Edgar, Thomas W., and David O. Manz. Research Methods for Cyber Security. 2017.

[15]. Imperva, 2021. *Cyber Attack*. [Online]
Available at: https://www.imperva.com/learn/application-security/cyber-attack/
[Accessed 30 May 2022].

[16]. Gonzales-Miranda DR. Organizational identity: components and construction. Innovar. 2020 Dec;30(78):89-104.

[17]. Bendovschi A. Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance. 2015 Jan 1;28:24-31.

[18]. Gangwar H. Cloud computing usage and its effect on organizational performance. Human systems management. 2017 Jan 1;36(1):13-26.

[19]. Falco G, Noriega A, Susskind L. Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyber-attacks. Journal of Cyber Policy. 2019 Jan 2;4(1):90-116.
[20]. Hina S, Dominic PD. Information security policies' compliance: a perspective for higher education institutions. Journal of Computer Information Systems. 2018 Mar 30.
[21]. Ananth P, Chen YC, Chung KM, Lin H, Lin WK. Delegating RAM computations with adaptive soundness and privacy. InTheory of Cryptography Conference 2016 Nov 1 (pp. 3-30). Springer, Berlin, Heidelberg.
[22]. Erendor ME, Yildirim M. Cybersecurity Awareness in Online Education: A Case Study Analysis. IEEE Access. 2022 May
[23]. Ncubukezit T. Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses. InInternational Conference on Cyber Warfare and Security 2022 Mar 2 (Vol. 17, No. 1, pp. 395-403).
[24]. Schneller L, Porter CN, Wakefield A. Implementing Converged Security Risk Management: Drivers, Barriers, and Facilitators. Security Journal. 2022 May 12:1-7.
[25]. Ali MS, editor. Digitalization and Economic Development: Insights from Developing Countries. Taylor & Francis; 2022

Friday Ehi Ikuero. "Organizations in the face of cyber-attacks: The Mitigation Strategies." *IOSR Journal of Computer Engineering (IOSR-JCE)*, 24(3), 2022, pp. 55-59.