International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
https://ijemr.vandanapublications.com

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.12

The Impact of the Information Security Policies on Organizational Performance

Kamal Aldin Yousif Yaseen
Department of Information System, CEMIS College, University of Nizwa, Nizwa, Oman

Corresponding Author: k.yousif@unizwa.edu.om

Received: 01-10-2023 Revised: 15-10-2023 Accepted: 29-10-2023

ABSTRACT

This study aims to explore the importance of enforcing a solid information security policy on the different institutions, giving a conceptual overview on the relationship between information security practices and organizational performance, presenting global indicators in peer-reviewed journals and records of information security firms and platforms, comparing best practices to productivity and improved performance, Analysing various risks and proposing the best solutions and appropriate protection techniques by following the best various strategies and techniques, propose the mitigation strategic prevention and hybrid techniques to protect the information due to their less expensive and simplicity.

***Keywords*--** Security Policy, Threats, Risk, Performance, Mitigation Strategic, Prevention Tools

I. INTRODUCTION

The cognitive and digital explosion that we are experiencing today has led to a number of challenges facing today's world in terms of the massive spread of digital attacks, viruses, computer worms, spyware files, In addition to negligence and unintended mistakes and other risks that threaten our presence on the Internet, which has become very vital infrastructure for creating important platforms and applications for conducting business for various sectors from Governmental companies and units, including health, education, and other government services, The total dependence of institutions on the Internet to conduct business has brought many problems and challenges that must be studied by specialists to provide the best solutions and practices that must be followed to provide the necessary protection to ensure protection for business continuity and ensure its quality and availability[1].

Cyber security threats are defined as any digital activity that could threaten the integrity of content or endanger access to data and the privacy of users. Here is a list of common threats. A. Cyber Terrorism This threat is a politically based attack on computers and information technology to cause harm and create widespread social disruption.

MalwareIt's Software that enters a computer system without the owner's knowledge or consent, malware is any software intentionally designed to cause damage to a computer, server, client, or computer network, the three primary objectives of malware are to infect a computer system Conceal the malware's malicious actions bring profit from the actions that it performs. **Trojans** These threats also aim to create a backdoor on your computer that gives malicious users access to the system, possibly allowing confidential or personal information to be compromised. Unlike viruses and worms, trojans do not reproduce by infecting other files nor do they self-replicate.

BotnetsIt's hundreds or thousands of zombie computers are under the control of an attacker Zombie An infected computer with a program that will allow the attacker to remotely control it.

Adware this threat delivers advertising content, often as pop-up windows that can slow or crash a computer can monitor or track the user's activities. **SQL Injection** Attackers insert SQL malicious code inside the website in order to request or change the database contents. **Phishing** is described as a fraudulent activity that is done to steal confidential user information such as credit card numbers, login credentials, and passwords. It is usually done by using email or other forms of electronic communication by pretending to be from a reliable business entity.

Man in the Middle Attack (MITM) This status occurs when the attacker is located among the communication channels and monitoring the contents which are sent or received across the channels it may interrupt or change the data nature or destinations.

Denial of Service (DoS) It is a service availability attack by flooding the network with a large number of messages until the server stops responding to user requests.

Viruses It's malicious code Programs that secretly attach to a file and execute when that file is opened, once a virus infects a computer, it performs two separate tasks. Hence the attackers and other threats can

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.12

exploit these fatal gaps and enter the system due to the lack of control and protection4. Internal Threats According to many studies, internal attacks are more common than external ones because most organizations focus on ways to protect against external attacks and neglect internal ones, which enable the use of e-mail or portal contents to attack enterprise resources, in addition to unintended human errors that can cause a data breach[2].

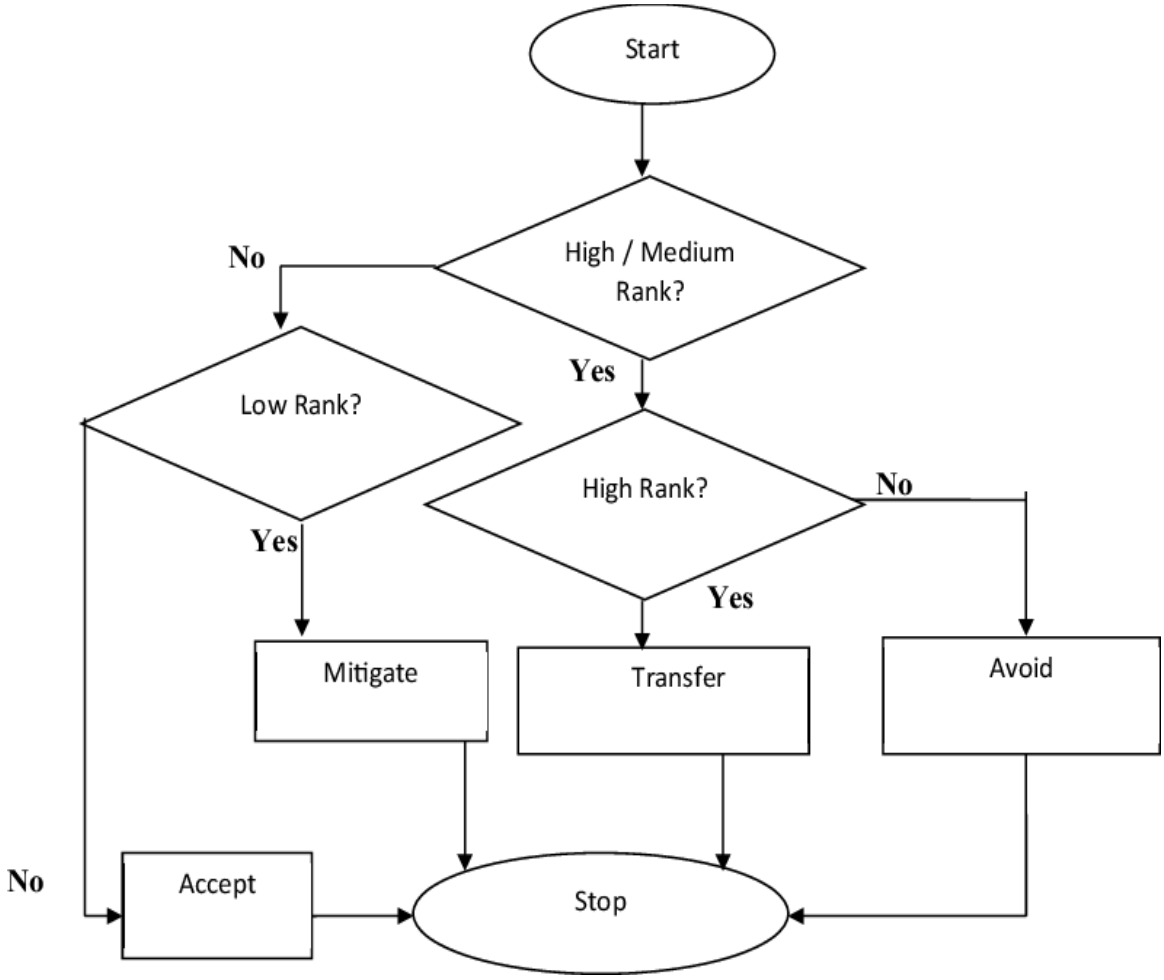

Figure 1: Mitigation strategic planning

II. SECURITY POLICY

A security policy is holistic document which include how the institution plants to protect its physical and information technology (IT)assets and other valuable resources, hence the security policy has to achieve the security triad which are Information Security Fundamental Principles [15]:

- **Confidentiality:** Prevent/detect/deter improper disclosure of information by ensures that only authorized parties can view the information.
- **Integrity:** Prevent/detect/deter improper modification of information ensures that the information is correct and no unauthorized person or malicious software has altered that data.
- **Availability:** Prevent/detect/deter improper denial of access to services provided by the system ensures that data is accessible to authorized users.

The security policy resources composed of the Religions, culture, government regulation, values, mission, vision and the science.

Figure 2: Cyber security mitigation steps

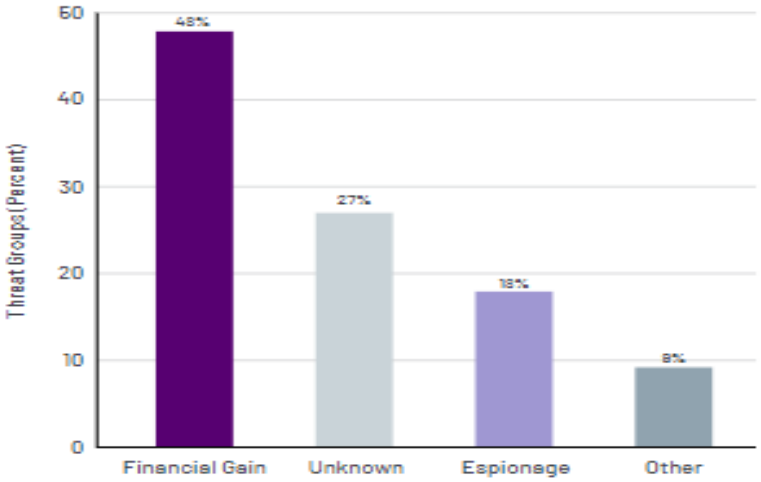

Figure 3: Threats grouped by goal, 2022

2.1 Types of Security Policies

Security policy types can be divided into three types based on the scope and purpose of the policy:

Organizational: These policies are a master blueprint of the entire organization's security program.

System-specific: A system-specific policy covers security procedures for an information system or network.

Issue-specific: These policies target certain aspects of the larger organizational policy. Examples of issue-related security policies include the following:

Acceptable use policies define the rules and regulations for employee use of company assets.

Access control policies say which employees can access which resources.

Change management policies provide procedures for changing IT assets so that adverse effects are minimized.

Disaster recovery policies ensure business continuity after a service disruption. These policies typically are enacted after the damage from an incident has occurred.

Incident response policies define procedures for responding to a security breach or incident as it is happening [13][14].

2.2 Features of the Security Policy

By following the security policies and standards the companies, institution and organization could increase the reliability and decrease the risks and costs associated with the data breaches, cyberattacks and legal liabilities, also the security policies help to identify and mitigate the vulnerabilities and threats that could compromise the information, networks and systems [11][12].

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.12

III. PROPOSED FRAMEWORK

Here I introduce our proposed framework to mitigate the risks characterized in Section V-D. We aggregate and correlate information from NVD, OLB and OSVDB, EDB and SymDB. EDB[8] is an open repository for proof-of-concept exploits while SymDB[9] is an open database of vulnerabilities exploited in the wild. EDB and SymDB have been used for quantitative security assessments [10] but I apply these to create a knowledge base for generating vulnerability signatures/plugins. The first three databases were already introduced in Section IV-A. I leverage on OpenVAS [11] scanning engine for the actual vulnerability scanning. OpenVAS is a popular open-source vulnerability scanning framework consisting of several tools used for security assessment. At the lower level, identification of software flaws is done by the NVTs or plugins. Open Vulnerability Assessment System (OpenVAS) currently employs about 40,627 plugins. These plugins are developed using Nessus Attack Scripting Language (NASL), a scripting language originally developed for Nessus vulnerability scanner, in addition to presenting and analyzing data and reports of companies and institutions specialized in information security and citing published studies.

IV. RESULTS

The contribution of this study is to encourage the institutions to adopt the solid security policies in order to protect them self against the cyber security attacks and other information technology threats, following the rules and standards increase the productivity and reducing the risk, the continuing in training and awareness led to decreasing the risks.

V. DISCUSSION

This study proof that the mitigation techniques very vital to reduce the risk and increase the performance and that is for many institution wasting aloft of time and resources in order to overcome the attacks or information threats, delay in detecting attacks or vulnerabilities may lead to systems failure, which makes it difficult for information security specialists to solve the problem and restore the system completely, as the responsibility of classifying risks and determining the priority in dealing with them.

Based on (MANDIANT) annual report issued in2023 the attacks being detect faster than before from January 1 to December 31 2022 due to following the cyber security policies and adopting the mitigation strategies, organizations were notified of breaches by external entities in 63% compared to 47% with the same period of 2022 which bring the global detection rate best and enhanced gradually, Previous studies showed that large companies are more committed to security policies by 73% than small and medium companies, which amounted to only 12%, which explains that most violations, breaches and compromises occur in these companies, this study shows that there is a very long barge between companies that adopt and implement security policies and those that neglect them, There is also a large gap in the results of implementing and enforcing security policies, Therefore security policies increase productivity by 7% in small and medium enterprises and by 12.3% in large and international institutions[7].

Figure 4 shows that the government sector still have a highest ration of targeting globally 25% and in the second and third the business and financial with 14%, 12% respectively, Likewise, the health sector has a frightening percentage, which is 9%. This explains the cessation of medical services in some institutions and the rely on the Internet and specific applications. This percentage is also due to targeting databases, research and scientific experiments [6][7][8].

We also found that vulnerabilities patching is very important as part of mitigation strategies, as it eliminates about 21% of threats, especially those found in applications, databases, and operating systems, it is inexpensive and the information technology department in any institution can help to activate them. As for operating systems and applications, must purchase the original systems and applications from their origins and be careful to continue activating them and avoid using free products, also to install firewalls and protection devices such as (IDS, NIDS, NPS) from intruders, as they are very effective in filtering inbound and outbound data packets, also the antiviruses still have capabilities to secure our systems and applications and keep them treats free [4][5][9].

Finally, I observe that many institutions have left the market due to their failure to implement strict security policies, especially during the period of economic recession and the Corona pandemic, which has steadily affected the total global production [10].

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.12

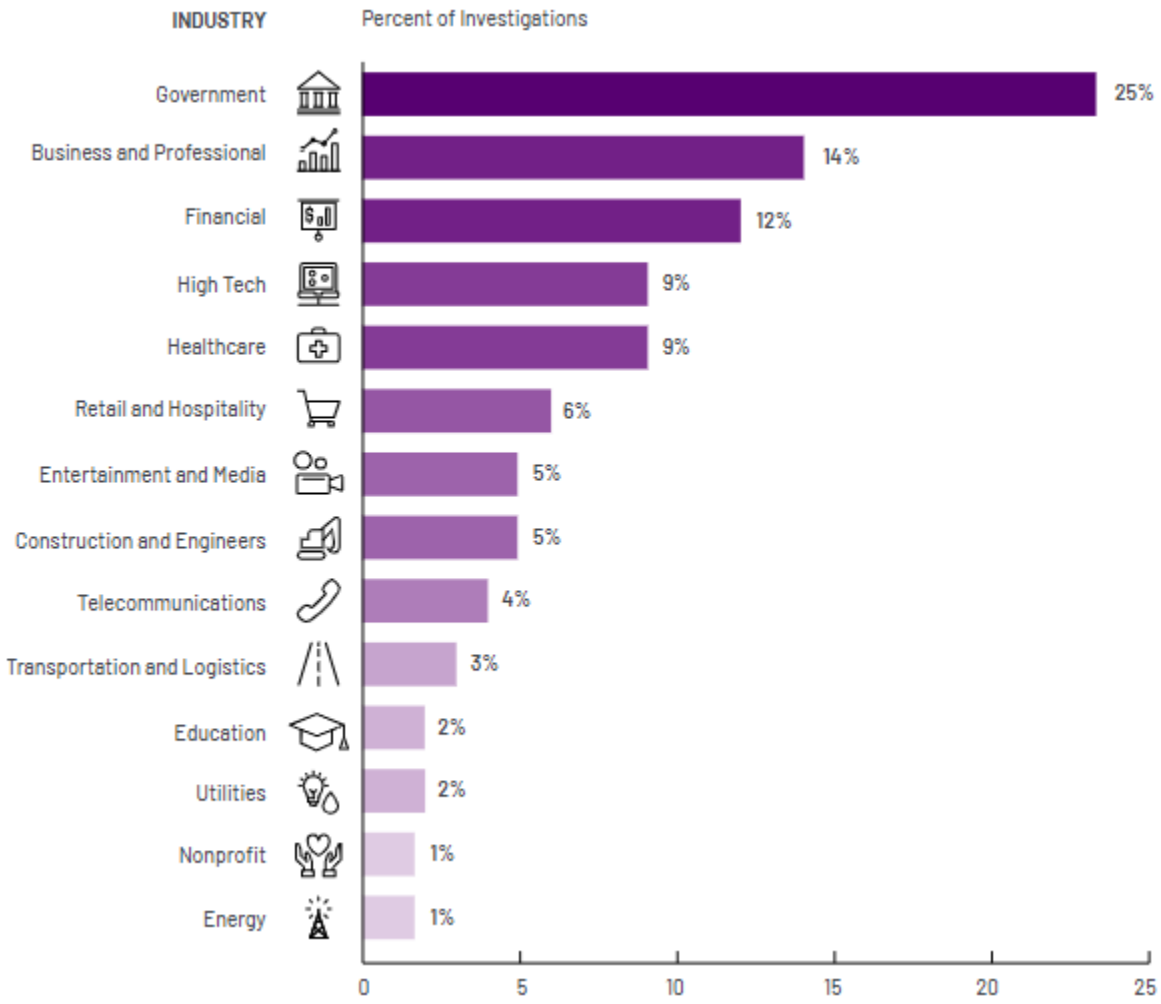

Figure 4: Global industry targeted in 2022

VI. CONCLUSION

Institutions of all sizes not only suffer from cyber-attacks, but poor management and training are among the factors that complicate the risks of these attacks and increase their complexity. Therefore, it is the duty of institutions to develop the necessary security policies to manage risks, mitigate damage, and set clear models that must be adhered to in order to avoid the occurrence of disasters that disrupt work and cause loss. Institutions lose their vitality, credibility, and reputation, and negatively affect their productivity.

Different protection strategies can also mitigate the risks and their impact by a large percentage of up to 86.4%. These hybrid strategies have proven effective with internal and external attacks if the vulnerabilities are discovered in the first three minutes of the attack or infiltration attempt, and their effectiveness gradually decreases the longer the discovery of the attack or threats is delayed.

REFERENCES

[1] Yousif Yaseen, K. A. (2022). Digital education: The cybersecurity challenges in the online classroom (2019-2020). *Asian Journal of Computer Science and Technology*, *11*(2), 33–38.

[2] Yousif Yaseen, K. A. (2023). Enhance moodle platform security against denial-of-service attack (DoS). *Journal of Critical Reviews*, *10*(02).

[3] Park, H.-Ho. (2020) A study on cyber crime deterrence recognition: The influence of recognition of punishment for cyber crime on intention to report crime. *Korean Criminal Psychology Research*, *16*, 85-98.

[4] Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P.C. & Glenn, T. (2021). Increasing

Peer Reviewed & Refereed Journal
Volume-13, Issue-5 (October 2023)
https://doi.org/10.31033/ijemr.13.5.12

cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports, 23*, Article No. 18.

[5] Pawar, S.C., Mente, R.S. & Chendage, B.D. (2021). Cyber crime, cyber space and effects of cyber crime. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7*, 210-214.

[6] Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P.C. & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. *Current Psychiatry Reports, 23*, Article No. 18.

[7] https://mandiant.widen.net/s/ztzxqs9qmh/m-trends-2023-report. 25/09/2023.

[8] OpenStack. *Openstack security*. Available at: https://wiki.openstack.org/wiki/Security.

[9] S. Frei, B. Tellenbach & B. Plattner. (2008). 0-day patch-exposing vendors (in) security performance. BlackHat Europe.

[10] S. Frei, M. May, U. Fiedler & B. Plattner. (2006). Large-scale vulnerability analysis. In: *Proceedings of the 2006 SIGCOMM workshop on Largescale attack defense, ACM*, 2006, 131–138.

[11] J. Bau, E. Bursztein, D. Gupta & J. Mitchell. (2010). State of the art: Automated black-box web application vulnerability testing. In: *Security and Privacy (SP), IEEE Symposium on. IEEE*, pp. 332–345.

[12] S. Breu, R. Premraj, J. Sillito & T. Zimmermann. (2010). Information needs in bug reports: improving cooperation between developers and users. In: *Proceedings of the 2010 ACM Conference on Computer Supported Cooperative Work, ACM*, pp. 301–310.

[13] H. M. Tran & S. T. Le. (2014). Software bug ontology supporting semantic bug search on peer-to-peer networks. *New Generation Computing, 32*(2), 145–162.

[14] W. Jansen. (2010). *Directions in security metrics research*. DIANE Publishing.

[15] S. Neuhaus, T. Zimmermann, C. Holler & A. Zeller. (2007). Predicting vulnerable software components. In: *Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM*, pp. 529–540.

[16] G. Schryen. (2011). Is open source security a myth?. *Communications of the ACM, 54*(5), 130–140, 2011.