Security Measures for Protecting of Information Technology Assets

Masese Nelson

Kabarak University
Corresponding Author Email: *nmasese[at]kabarak.ac.ke*

Abstract: ***Information systems security is very important to help protect against this type of theft. Organizations are especially vulnerable hence there is need to have appropriate measures to protect the information technology assets. The objectives of this paper include. To review risk mitigation measures and To identify techniques used to safeguard information assets Methods/Statistical analysis: Primary data was used drawn from mobile social users in Nairobi and Mombasa Counties in Kenya.481 respondents, both descriptive and inferential statistics was used to analyze the data. Findings: From the study it was found out that user education is important to safeguard information technology assets the study indicated that 65.6% of the respondents agreed user education can mitigate threats and risks. Further 62.3% who emphasized that authentication of various users is also important to safeguard the information technology assets. The study findings indicated that 73.8% of the respondents acknowledged encryption protects data from unauthorized access recommendations there is need to explore digital forensics security so that to enhance the security of information technology assets***

Keywords: Security, Mitigation, Measures, Information Technology, Techniques

1. Introduction

Information today is one of the most important assets within an organization. The evolution of its importance comes riddled with issues pertaining its management. Organizations are grappling with issues to identify who really “owns” the data? Who is the “custodian”? Who is responsible for what? [1]. An information asset is a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilized effectively. Information assets have recognizable and manageable value, risk, content and lifecycles [2].

As information asset is any valuable information that the organization has. Valuable here means that the organization either acquired it at some cost, is actively using it now in some process or could use it for some purpose in the future. The definition of an asset is deliberately wide: it is important to recognize all kinds and types of assets. An information assets can have many different forms: it can be a paper document, a digital document, a database, a password or encryption key or any other digital file [3]

This paper presents user education, authentication, roles and permissions, network protocols, encryption, logging and audit and legislations and standards as measures to be used to safeguard information assets.

1.1 Objective

1) To review risk mitigation measures
2) To identify techniques used to safeguard information assets

2. Literature Survey

Information assets have economic and business value, among other significance. The loss of data can lead to decline in financial standing or even reputation which is an important factor in different fields of life. To prevent destruction or unauthorized use of data assets and consequently expose an entity to damages, various measures can be employed to protect and secure information and supporting systems [4]. These counter-measures aimed at securing information assets can be broadly categorized into three categories as outlined below:

i. User education
ii. Technological implementations:
iii. Legal protection:

2.1 User Education

Users are the human resource or other persons interacting with the information asset. These are the people authorized to use the information asset by accessing it via nodes of the system [5] Users ought to follow certain rules and obey necessary guidelines in order to ensure their interactions with the system do not expose the information assets in question to risks and threats. They ought to use secure passwords and protect their credentials from access by unauthorized persons [6].

Organizations have policies and standards that dictate how users interact with information systems so as to maintain the confidentiality, integrity and availability of the services and information being offered by the facility [6].

User education is greatly dependent on the skills and capabilities of an individual. The technical understanding of an individual can limit the ability of the said user to follow some specification due to a steep learning curve [7] Human behavior is also a complex issue that cannot be accurately be crated to fit a standard way of behavior when interacting with an information system. That is why most data breaches are facilitated by social engineering with the perpetrators relying heavily on users as a weak link to gaining access into an ICT installation [8].

2.2 Technological implementations

i. Authentication*:*
Each user needs to log in to the system with credentials and only allowed to use the information system ones valid credentials are provided. This prevents malicious external parties from getting open access into a system [9]. A shortcoming of authentication is that it is dependent on the user's ability to select a secure password and keeping it secret. Even with a secure authentication mechanism, users can set weak passwords with obvious hints like their names and date of birth. Such information can be used in guesses when malicious persons attempt to crack a password [10]

ii. Roles and permissions:
Roles specify specific actions allowed to a set of users within a system. A super user can carry out a range of operations on a system while some end-user roles restrict specific persons to lower level tasks. An example is a parent who can only view their child's score on a school management system. A principal, on the other hand can view any of his student's scores and even edit them [11], [12].

Roles and permissions are a design issue that must be well thought out. A poor implementation of roles can create complexities in the authentication mechanism and create loopholes. Such weaknesses can be exploited and are counter-productive to infrastructure security Tabrizchi & Rafsanjani, (2020). [13]

iii. Data encryption:
Data encryption is the conversion of information into an 'unreadable' format to prevent snooping entities from understanding the contained communication when they get access to the raw bytes. Data is jumbled up using a given key and only the receiver with the said key can reconstruct the information 14].

Though encryption offer a secure means of sending and storing data, they can be cracked. Older encryption standards like Data Encryption Standard (DES) have been proven to be breakable and are not so reliable in protecting data without coupling with additional measures [15].

iv. Encapsulation and separation:
Encapsulation is the development of elements within a larger system in a manner that ensures individual modules are self-reliant and separated from other elements. The respective modules communicate using a set of protocols with authentication and secure communication between the parties. Therefore, an attack to a system only poses a threat to a single element at a specific time and successful attacks to not compromise the whole system but a single sub-system [16].

Compartmentalization is good for security but increases the system complexity with increasing number of subsystems. This complexity is what created the need for cluster management tools like Kubernetes and Docker that may also present new challenges to security within an ICT facility [17].

v. Logging and audit measures:
Logs are crucial records of all operations and actions performed on a system. They enable auditors to carry out reviews after possible threats and see how the processes interacted to cause risks to the information assets within a system [18].

Logs and audits are dependent on human skills to be well interpreted. A poor audit process or defective handling of audit materials would lead to inadequate findings that do not serve to improve the system's security. Logging may also add overheads to the system resulting in slower processing time and need for more processing power 19].

vi. Network protocols:
Network protocols govern how the elements within a network communicate. They ensure the transmission of data is between the intended parties and following certain rules that include security controls [20].

Network protocols interact closely with firewalls among other network features which can be quite technical. Protocols come in different flavors that require technical know-how for proper implementation [21].

2.3 Legislations and Standards

Laws and legislations like the Data Protection Act of 2018 and the Computer Misuse and Cybercrime Act of 2018 are Kenyan laws that seek to legally protect ICT assets from malicious people. They can be called upon in the protection of crucial Information assets against criminal actions. The Courts are important in giving legitimacy to the undertaking of protecting information assets.

Standards such as ISO/IEC 27001 offer a guideline to protect information from unnecessary disclosures and misappropriations.

Even with the above tools of information asset protection, conformity is still low especially in developing countries like Kenya. This is partly due to deficient enforcement of the regulations contained within the laws and standards.

2.4 Risk Control Techniques

Risk Avoidance: This technique aims at avoiding the risk at all costs, thus the organization will have a 0% chance of risk hence no loss can be suffered [22].

Risk Transfer: This is a technique whereby the organization shifts the responsibility and accountability of a risk to a stakeholder who majors on that type of risk. For instance, the organization may opt to outsource some responsibilities which may be expensive for them to control should a risk materialize. A good example is taking an Insurance policy against fire on the organization's asset [23].

Risk Acceptance: This technique is implemented on risks which cannot be avoided at all cost. Instead of avoiding the risk, you accept the risk but try to minimize the chances of the risk materializing. For example, the organization can be susceptible to theft, therefore the organization will be forced to install surveillance systems, hire security guards and install various biometric security tools to protect against physical theft [12].

Risk Control: It is accepting the risk as well as the threat it poses on the organization. This means that the organizations will be aiming at minimizing the loss in an event that the risk materializes. For instance, a company that handles flammable products, will ensure that oxygen suppressants, smoke detectors and water sprinklers are installed to mitigate the loss of items should a fire start [22].

Risk Monitoring: This technique aims at constantly observing new ICT threats that may emerge as a result of the nature of business that the organization is involved with [15].

Separation: This a risk management technique where the organization distributes the various key assets on different locations so that in an instant where a risk materializes on one location, only few assets are affected and the others are safe [23].

Avoidance: The avoidance of risk is a conventional precaution taken by many business institutions when they're aware of the possibility of an imminent or unpredictable event unfolding. The key to avoiding risk is through making the right projections and comprehensive planning. If you can gain access to information that identifies risk in a timely manner, you can often avoid the situation altogether. This basically means you plan ahead and conduct extensive research to ensure you have access to all the relevant information that could inform you of impending risk. When it comes to avoiding risk, knowledge really is power. By identifying risk early, you can alter your plans and pursue a course of action that steers well clear of unnecessary exposure to volatile situations [21].

Acceptance: The acceptance of risk is also built on a base of knowledge and information. If your research suggests the risk involved in a given scenario is relatively minuscule when compared to the possible benefits, then accepting the risk may be the best course of action. Accepting risk should only be advised when you've conducting sufficient research and identified the relative potential of problems occurring. Commit resources to calculate the pros and cons of accepting risk in every individual scenario and make a decision based on objective data. Once you've ascertained the potential negative effects of a decision, don't proceed unless your business can definitively handle the situation if it goes wrong [22].

Transferal: Risk transfer involves shifting the risk to an entity that you perceive to be more resilient or better equipped to handle the situation. If you identify an impending risk, delegating the task of dealing with it can help to transfer the risk to a department or staff member that is better qualified or more experienced [23].

Transferring financial risk among several separate entities reduces the chance of a company being irrevocably damaged by unforeseen losses. The key to effective risk transferral is knowing which entity would be the best equipped to deal with the situation [17].

3. Methodology

Primary data was used in the study was drawn from a survey carried at Nairobi and Nakuru counties in Kenya, targeting medium and large organizations. The study was conducted on 315 respondents. The questionnaires were issued to respondents. The study achieved 95.3% response of the target. This response rate was considered appropriate for analysis and reporting as supported by indicating that a response rate of 70% and above is excellent. Descriptive data analysis was used to analyze the collected data.

4. Results and Discussion

Table 1: Techniques used to safeguard information technology assets

Statement	SD	D	U	A	SA	Mean	SD
User education is important so that to safeguard technological assess	(8.2%)	(19.7%)	(6.6%)	(45.9%)	(19.7%)	3.49	1.24
Authentication prevents malicious external parties from getting open access into a system	(13.1%)	(8.2%)	(16.4%)	(44.3%)	(18.0%)	3.45	1.25
Roles and permissions helps to specify specific actions allowed to a set of users within a system	(3.3%)	(13.1%)	(13.1%)	(41.0%)	(29.5%)	3.80	1.10
Network protocols can be used to enhance security of information assets	(6.6%)	(14.8%)	(6.6%)	(31.1%)	(41.0%)	3.85	1.28
Encryption offer a secure means of sending and storing data, to avoid being cracked		(11.5%)	(11.5%)	(50.8%)	(23.0%)	3.78	1.03
Logging and audit measures helps to identify weak/ vulnerable areas of a system.	(4.9%)	(13.1%)	(3.3%)	(47.5%)	(31.1%)	3.86	1.14
Legislations and Standards helps to protect information technology assets.	(4.9%)	(14.8%)	(8.2%)	(49.2%)	(23.0%)	3.70	1.13

Source: Survey Data (2021)

From the study it was found out that user education is important to safeguard information technology assets the study indicated that 65.6% of the respondents agreed user education can mitigate threats and risks caused due to lack of sufficient knowledge on the utilization of the assets. This view was supported by 62.3% who emphasized that authentication of various users is also important to safeguard the information technology assets.

Additionally, the study found that 70.5% of the respondents assert that roles and permissions provide various that guide the rights that different users have on the system. Where by some can have more privileges compared to others. The study further indicated that data encryption is crucial in protecting the information assets the study findings indicated that 73.8% of the respondents acknowledged encryption protects data from unauthorized access.

This finding was reiterated by 78.6% encapsulation & separation is effective in protecting information assets from unwanted access. Further the study indicate that 87.8% of the respondents affirmed that logging and auditing helps to secure information assets by taking necessary measures to prevent information breaches Finally, 71.0% of the respondents were of the opinion that network protocols helps in ensuring that information is delivered to the right owner/ system hence securing the channel while transferring the information.

5. Conclusion

From the results it indicates user education authentication, roles and permissions, network protocols, encryption, logging and audit measures are effective measures that can effectively implementation of security measures that organizations can take to secure their information technology assets.

6. Future Scope

There is need to explore digital forensics security so that to enhance the security of information technology assets

References

[1] Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, *59*, 102168.

[2] Shabou, B. M. (2019). An Information Governance Policy Is Required for My Institution, What to Do?: Practical Method and Tool Enabling Efficient Management for Corporate Information Assets. In *Diverse applications and transferability of maturity models* (pp.61-91). IGI Global.

[3] [Abdeldayem, M. M., & Aldulaimi, S. H. (2020). Trends and opportunities of artificial intelligence in human resource management: Aspirations for public sector in Bahrain. *International Journal of Scientific and Technology Research*, *9* (1), 3867-3871.

[4] Sukharev, O. S. (2020). Economic crisis as a consequence COVID-19 virus attack: risk and damage assessment. *Quantitative Finance and Economics*, *4* (2), 274-293.

[5] Khan, P. W., Byun, Y. C., & Park, N. (2020). IoT-blockchain enabled optimized provenance system for food industry 4.0 using advanced deep learning. *Sensors*, *20* (10), 2990.

[6] Sahid, A., Maleh, Y., & Belaissaoui, M. (2020). Information system evolution. In *Strategic information system agility: From theory to practices*. Emerald Publishing Limited.

[7] Aguboshim, F. C., & Udobi, J. I. (2019). Security Issues with Mobile IT: A Narrative Review of Bring Your Own Device (BYOD). *Information Technology (IT)*, *8* (1).

[8] Jaber, M. Y. (Ed.). (2019). *Learning curves: Theory, models, and applications*. CRC Press.

[9] Shin, D., & Park, Y. J. (2019). Role of fairness, accountability, and transparency in algorithmic affordance. *Computers in Human Behavior*, *98*, 277-284.

[10] Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58* (2), 102468.

[11] Kaur, A. A., & Mustafa, K. K. (2019). A Critical appraisal on Password based Authentication. *International Journal of Computer Network & Information Security*, *11* (1).

[12] Alsalemi, A., Sardianos, C., Bensaali, F., Varlamis, I., Amira, A., & Dimitrakopoulos, G. (2019). The role of micro-moments: A survey of habitual behavior change and recommender systems for energy saving. *IEEE Systems Journal*, *13* (3), 3376-3387.

[13] Tabrizchi, H., & Rafsanjani, M. K. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. *The journal of supercomputing*, *76* (12), 9493-9532.

[14] Sihag, V., Vardhan, M., & Singh, P. (2021). A survey of android application and malware hardening. *Computer Science Review*, *39*, 100365.

[15] Cheng, J. K., Lim, E. M., Krikorian, Y. Y., Sklar, D. J., & Kong, V. J. (2021, March). A Survey of Encryption Standard and Potential Impact Due to Quantum Computing. In *2021 IEEE Aerospace Conference (50100)* (pp.1-10). IEEE.

[16] Sharma, S., & Kaushik, B. (2019). A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications*, *20*, 100182.

[17] Boudi, A., Farris, I., Bagaa, M., & Taleb, T. (2019). Assessing lightweight virtualization for security-as-a-service at the network edge. *IEICE Transactions on Communications*, *102* (5), 970-977

[18] Chen, Y., Lu, Y., Yang, F., Wang, Q., Wang, Y., & Shu, J. (2020, March). FlatStore: An efficient log-structured key-value storage engine for persistent memory. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems* (pp.1077-1091).

[19] Chen, Y., Lu, Y., Yang, F., Wang, Q., Wang, Y., & Shu, J. (2020, March). FlatStore: An efficient log-structured key-value storage engine for persistent memory. In *Proceedings of the Twenty-Fifth International Conference on Architectural Support for Programming Languages and Operating Systems* (pp.1077-1091).

[20] Naoui, S., Elhdhili, M. E., & Saidane, L. A. (2020). Novel enhanced LoRaWAN framework for smart home remote control security. *Wireless Personal Communications*, *110* (4), 2109-2130.

[21] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2021). A survey on

internet of things security: Requirements, challenges, and solutions. *Internet of Things*, *14*, 100129.

[22] Trnka, M., Feng, S., Semenov, M. A., Olesen, J. E., Kersebaum, K. C., Rötter, R. P.,. . . & Büntgen, U. (2019). Mitigation efforts will not fully alleviate the increase in water scarcity occurrence probability in wheat-producing areas. *Science Advances*, *5* (9),

[23] Sng, K., Au, T. Y., & Pang, A. (2019). Social media influencers as a crisis risk in strategic communication: Impact of indiscretions on professional endorsements. *International journal of strategic communication*, *13* (4), 301-320.

Author Profile

Masese Nelson holds Phd Information Technology from Kibabii university, Masters of Computer Applications Degree from Periyar university India, currently a He is currently a lecturer at Kabarak university Kenya. His research interest are mobile applications, Digital & cyber forensics and cloud computing security.