OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Commentary

Cyber Security Hazard to Sensitive Data in Organization

Javier Segovia*

Department of Information Technology, Addis Ababa University, Addis Ababa, Ethiopia

DESCRIPTION

Cyber security is a technique for defending a network, system, or application against cyber-attacks. Cyber security, also known as information security or InfoSec, is the action taken to protect information and information systems from unauthorised access, use, disclosure, interruption, alteration, or destruction. Digital technology has emerged as the most significant tool for boosting innovation, competitiveness, and growth. When it comes to providing services to customers, information is crucial. At the same time, there are threats of intruders or attackers, which we may not be able to avoid, but which we may mitigate through proactive management techniques.

Organizations must be vigilant in securing their data and networks as cyber security threats continue to change and become more sophisticated. Cyber criminals are becoming more sophisticated, and they are devising new methods to gain access to a company's information systems. The biggest hazards to information security in a corporation are insider threats or workers. Former organization personnel, in particular. Keep an eye out for security concerns in the news, and keep ourselves and our organisations up to date. Attitudes and awareness among employees need to shift. Malicious attackers can break corporate security through people interactions using social engineering tactics.

This paper proposes a security awareness programme that may be used to educate key information operators about various social engineering security threats such as ransomware, social engineering, and malware. Information security refers to the process of ensuring the confidentiality, integrity, and availability of data assets, whether they are being stored, processed, or communicated. It is accomplished by the use of technology, as well as strategy, education, training, and consciousness. Information security is a set of procedures and technologies for safeguarding sensitive data. It includes paper and digital records, as well as intellectual property.

Information security is defined by the Committee on National Security Systems (CNSS) as the protection of information and its important elements, such as the systems and hardware that use, store, and transport that information. The broad topics of information security management, computer and data security, and network security are all covered under information security. In today's interconnected world, cyber security has raised to the top of the priority list, affecting every aspect of our lives, particularly sensitive data. Critical information is defined in a variety of ways. If there is no disruption from other parties, living in the digital age today might be so simple and fulfilling.

We may be able to communicate with one another on the internet and through technological equipment. Users are unaware that they are being watched by cyber attackers while exchanging data over the internet. Regardless of the size or nature of the business, Information Technology (IT) is a lifeline for organisations. As a result of this position, information security crime is no longer a national priority, but rather a matter for individuals, businesses, and non-profit organisations.

CONCLUSION

With the world moving at a faster pace, so are hackers, such as social engineering security threats such as ransom ware, social engineering, and malware, among others. We should take responsibility in managing our own sensitive information and information systems, and also take the commitment to protect and secure our data, and help build the capacities of those responsible employees for the security and investments of our organisations. With the world moving at a faster pace, so are hackers, such as social engineering security threats such as ransom ware, social engineering, malware, and there are other cyber criminals that take advantage of employees' lack of knowledge about information security issues. Information security will improve the world for everyone. And make it illegal for anyone in the globe to use a computer or the Internet to offend an innocent people.

Correspondence to: Javier Segovia, Department of Information Technology, Addis Ababa University, Addis Ababa, Ethiopia, E-mail: javiersegovia@fi.upm.org

Received: October 14, 2021; **Accepted**: October 28, 2021; **Published**: November 4, 2021

Citation: Segovia J (2021) Cyber Security Hazard to Sensitive Data in Organization. J Inform Tech Softw Eng. S5:003.