Journal of Cardiovascular Disease Research

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

The Effectiveness of Different Cyber Security Measures in Protecting Organization for Cyber Threats

Suruchi Sharma,
Associate Professor, School of Management, Graphic Era Hill University, Dehradun Uttarakhand India

DOI:10.48047/jcdr.2021.12.06.339

Abstract

Data theft is becoming more and more of a danger as data value rises. In today's digital world, the necessity of cyber security has grown because of several cyberattacks on numerous organizations. Cyber assaults are nothing new in the realm of technology. The relevance of cyber security in every area has increased because of the cyberattacks. Due to unexpected cyberattacks, as technology advances daily, the necessity for cyber security measures also grows. Today, every single firm working on a small scale is just as concerned about the significant concerns associated with cyber assaults as the biggest organizations in the world. Numerous organizations deal with sensitive and huge data that must be kept private. Cyber and internet assaults are getting riskier for every firm due to the rising value of data. To shield the data from danger, comprehensive and sophisticated technology is required. Different security measures are required to shield the firm against deadly cyber assaults. The protection of data is the primary goal of cyber security. The numerous cyber security procedures guard against data theft and corruption. Data breaching, or unlawful access to and dissemination of sensitive data, is one of these cyber assault threats. There is a need for good threat management and cyber security technologies to limit cyber assaults since data breaches might negatively affect the person to whom the data is linked.

Keywords: Cyber Security, Cyber Treats, Data Protection, Data Breaching, Cyber Attacks

Introduction

Businesses formerly believed that by installing a few fire walls and antivirus programmes, they could safeguard their firm against cyberattacks. However, as technology advanced, hackers improved their capacity to bypass any firewall or anti-virus programme. The attackers have highly developed technical skills and may design unique malware for a particular target to attack the company. The truth is that every enterprise, no matter how big or little, faces cyber danger,

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

and to protect the organisation from deadly cyberattacks, a new strategy is required. Almost every firm in the world now takes cyber security extremely seriously. Businesses are more worried about data breaches and information theft. Hackers plan their attacks and do background research to identify any loopholes in the firms' defense programmed before targeting any company. Even while businesses deploy a variety of attack-prevention techniques, it's crucial for them to be aware of the strategies hackers use to circumvent the defenses. When compromises occur, enterprises or companies must process and priorities detection techniques. It implies that they must act as soon as possible. In addition, these businesses must comprehend that threat prevention is not an absolute measure of prevention, necessitating the necessity for a robust defensive system to fend off persistent hackers. To protect themselves from cyber dangers, companies and corporations do enable security intelligence systems. They also use specialized security products and technology-based solutions, both of which play essential roles. However, in order to identify threats as soon as possible, businesses today need to concentrate on developing and maturing their detection and response capabilities. Businesses must deploy the most extreme, sophisticated, and real-time system possible to decrease risk. (Brewer, 2015 and Berry, & Berry, 2018).

Data breaching is the act of disclosing highly sensitive information that is meant to remain private. When a third party or an unauthorized person tries to seal or access private data, this is known as a data breach. Data breaches may take many various forms, including phishing, malware, and denial-of-service attacks. The method used for data breaching is unlawful, and it's possible that a person or business participating in the breach may want something in exchange for the data. This is a cyberattack, and there are more and more discussions about it every day. Although data theft prevention techniques have improved, it is still possible and might have negative effects. Data breaching is prevented via cyber security. There is a need to put security measures in place and stop the flow of data breaches as the number of databases used in activities rises daily. There are several procedures one must take to prevent data breaches. The first is to limit data transmission, which entails forbidding data migration from one device to another inside an enterprise. The second option is red file shredding file, folders, and disc inverse deletion, which permanently deletes the chosen data without making a backup copy. Confidential data destruction can stop data breaches. In addition to prohibiting the use of encrypted devices that are vulnerable to data leakage, it is critical to create passwords that are difficult to guess and

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

unexpected in order to stop unauthorized access to data. It is also a good idea to change the passwords frequently. Reduce the danger of a data breach by using an automated system to check the setup of firewalls and password-setting servers. Restricting downloads of sensitive data might lessen the likelihood of data transmission to an external device. The protection of sensitive information is also essential. Setting up a breach response strategy is a crucial step in preventing data breaches because it may deliver important notification to management in the event of a breach, alerting them to the assault and lowering the risk (Veena, Divyalakshmi, Poornima, 2018).

Qualified Audit Academy has given some good cybersecurity measures (Figure 1).

Figure 1 Cybersecurity Measures

Source: Qualified Audit Academy

High integrated and complicated technology is required to safeguard a system from a wide range of adversaries. A good cyber security plan is essential to prevent cyber-attacks on an organization by ensuring that each component and the combination of components have adequate protection to handle the issue. Planning, designing, monitoring, and implementing various cyber

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

security measures at various levels are required for a cyber security strategy. The risk assessment is the initial stage in developing a cyber security plan. The effective considerations of dangers and strategic risk must be included by the professional handling cyber security concerns. In the second phase of this technique, which involves identifying and quantifying system and component interactions, a cyber security expert considers potential risk that might result from interactions between technological components and external systems. The expert assesses the dependencies and inherited risk in the third phase, trusted dependencies, to guarantee the proper degree of confidence. The fourth phase is preparation and attacker response, when a cyber security specialist assures that the system can successfully counteract any potential assaults (Woody, Ellison, 2020 and Tabassum, 2020).

Literature Review

According to research, cyber security attacks are divided into two groups attack passing and active attack. In passive assaults, an attacker listens to and examines communication between two workstations to gain access without altering the substance of messages. In active attacks, the attacker can alter, remove, or copy file contents, reveal himself as an authorized user, stop regular data flow, and other things. Three requirements should be met to safeguard network systems: Confidentiality which means to avoid purposeful or unintentional unauthorized decline, Availability: reliable access to data and resources of data and resources; integrity-ensuring the correctness and integrity of information. A top-notch firewall and monitoring system must be provided. Next come intrusion detection systems and top-notch, cutting-edge antivirus scanners. This entails developing a multilayered defense against infiltration, quickly spotting an infection, and using the defense after infection. There is a need develop an advanced protection procedure that goes beyond the security range to do this, which includes: Advanced detection methods, it includes traffic analysis and the use of tools that can identify the formation of attacks. As a crucial learning strategy, use hazard identification to gradually improve the defence. The elimination of viruses, the recovery of disadvantaged systems, and the ensuing recovery procedures should all be covered by advanced threat mitigation (Vukašinović, 2018 and Eswaran, Vinayagamoorthi, 2019).

A study claims that data mining is the process of sifting through, evaluating, and finally deriving the meaning from vast volumes of data with the use of computers. It also entails the process of

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

compiling data from various analyses and synthesizing it into informative summaries. The accuracy, performance, and speed of forecasting cybercrime may all be improved by using data mining prediction algorithms. Since businesses began utilizing computers in their everyday operations, cybercrime has become more sophisticated and expensive. Cybercriminals have become more skilled and now target both public and private organizations as well as consumers. For the disclosure of upcoming cybercrime patterns, it is essential to develop a high-caliber cybercrime tool that can swiftly and effectively detect criminal prototypes. Intrusion recognition techniques should be planned, carried out, and controlled to protect against cybercrimes. The suggested approach was developed to access many criminal records so that predictions based on the prior behaviour of criminal people could be produced. There is no need to input the information when the records in the system improve. The modern digital era raises a lot of questions about how to safeguard vast amounts of data from a broad culture of cybercriminals (Lekha, & Prakasam, 2017 and Muckin, 2019).

A study found that keeping up with new technologies, security trends, and threat information may be challenging. To protect data and other assets from various cyberattacks, it is necessary to take this action. In a kind of malware known as ransomware, the victim's computer system files are encrypted and locked by the attacker, who then demands something in return to decrypt and release them. Trojan horses, worms, computer viruses, and spyware are examples of applications known as malware that are used to harm computer users. In order to get sensitive information that is generally secured, social engineering attacks employ human contact to persuade people to violate security protocols. Phishing is a sort of fraud where phoney emails that seem to be from trustworthy sources are sent; nonetheless, the goal of these emails is to steal sensitive data, such as login or credit card information. Application security refers to the measures used to protect applications against hazards that may come because of flaws in the design, development, deployment, update, or maintenance of the application throughout the development life cycle. Information security guards against unauthorised access of data and prevents identity theft and safeguard privacy. Risk assessment, setting priorities, and devising recovery plans are all steps in the process of disaster recovery planning. Any company should have a clear plan for recovering after a crisis so that regular activities may continue as soon as feasible. Activities that safeguard the network's usability, dependability, integrity, and safety are included in network security. A

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

range of risks are targeted by efficient network security, which prevents them from propagating or accessing the network (Kosare, Likhar, & Manapure, 2020).

According to a study, the rapid shift to digitalization in the business sector is putting greater strain than ever on security. The use of dated security architectures to handle all of this is the most common cause of failure and security issues. As a result, businesses must implement fifth-generation architecture, which includes cloud infrastructure and the Internet of Things, but they can do so without single points of failure by providing them with the strength and resilience needed to maintain operations and security under all circumstances. This security architecture must offer a consolidated, unified security architecture that manages and interacts with mobile, cloud, and networks to halt and protect against fifth-generation cyber threats. Machine learning has had a significant positive impact on cybersecurity. Filters are primarily used in spam detection to evaluate the communication's content and determine if it is spam or not. The Bayesian classifier, SVM, MapReduce, neural network-based behavior-based spam detection, the text detection method for picture spam filtering, and the Bayesian classifier were among the machine learning techniques that were available (Saravanan, & Bama, 2019).

According to a research, Data leaks represent a serious threat to commercial operations, particularly those of businesses and governmental agencies. Losing sensitive data might have a detrimental effect on a company's long-term viability and result in significant reputational and monetary harm. Information leaks usually involve medical records, intellectual property, employee or customer data, and other types of information. Due to the exponential expansion of data volume in the digital era and the increased frequency of data leaks, one of the top security concerns for organizations is preventing the release of sensitive information to unauthorised parties. It is challenging for organizations to protect data against information breaches in the age of big data. Managing and interpreting enormous amounts of data, one of an enterprise's most crucial components, offers organizations a significant competitive edge through methods like business intelligence or the provision of customized business services. Due to the risk it poses to sensitive and valuable enterprise data, businesses face significant security challenges. Because of the need to collect, process, and analyze larger and larger volumes of data, businesses are using modern communication channels more often, which raises the risk of data leaks. DLPD systems are designed primarily to solve issues caused by data leakage, in contrast to more fundamental

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

security measures like firewalls, antivirus software, intrusion detection, authentication, access control, and encryption. Locating, monitoring, and protecting private information from unauthorised access is the main duty of DLPD. The genuine content or context of the monitored data is frequently used to identify potential leaks. Recent growth in demand for designated DLPD products signals their impending importance as a component of the enterprise's security architecture. (Cheng, Liu, & Yao, 2017).

Conclusion

The risk of data theft is increasing as data value increases. The need for cyber security in the modern digital world has increased because of various cyberattacks on different companies. Cyber attacks are not a recent development in the world of technology. Because of cyberattacks, cyber security is now more important than ever. As technology develops daily and there are more unforeseen intrusions, the need for cyber security measures also increases. Today, even the smallest businesses are just as concerned as the largest organizations in the world about the serious risks posed by cyberattacks. Many organizations work with large amounts of sensitive data that must be kept confidential. Due to the increasing importance of data, cyber and internet attacks are becoming riskier for every business. Comprehensive and cutting-edge technology is needed to protect the data. To protect the company against lethal cyberattacks, many security measures are needed. The main objective of cyber security is the protection of data. The multiple cyber security measures prevent data loss and tampering. One of these cyber attack dangers is data breaching, or unauthorised access to and disclosure of sensitive data. Since data breaches may have a negative impact on the individual to whom the data is related, effective threat management and cyber security solutions are required to reduce cyberattacks. Businesses used to think that adding a few fire walls and antivirus software would protect their company from cyberattacks. Hackers have enhanced their ability to get beyond any firewall or anti-virus system, nevertheless, as technology has grown. The attackers may create special malware for a specific target to attack the firm. They have highly developed technological capabilities. The fact is that every business, regardless of size, confronts cyber risk, and a new approach is needed to safeguard the company against lethal assaults.

ISSN: 0975-3583, 0976-2833 VOL12, ISSUE 06, 2021

References

- Berry, C. T., & Berry, R. (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1.
- Brewer, R. (2015). Cyber threats: reducing the time to detection and response. *Network Security*, *2015*(5), 5–8.
- Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews-Data Mining and Knowledge Discovery*, *7*(5), e1211.
- Eswaran, R., Vinayagamoorthi, G. (2019). Cyber Security and Information Security, *International Journal of Recent Technology and Engineering*, *8*(3S), 372–374.
- Kosare, H. R., Likhar, K., & Manapure, P. (2020). Survey on Cyber Security and Defensive Measures. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 144–151.
- Lekha, K. C., & Prakasam, S. (2017). *Data mining techniques in detecting and predicting cyber crimes in banking sector*.
- Muckin, M. (2019). A Threat Driven Approach to Cyber Security, *Lookhee Martin.*
- Saravanan, A., & Bama, S. S. (2019). A Review on Cyber Security and the Fifth Generation Cyberattacks. *Oriental Journal of Computer Science and Technology*, *12*(2), 50–56.
- Tabassum, L. (2020). Cyber Security and Safety Measures, *International Journal of Modernization in Engineering Technology and Science*, 2(6), 1358-1360.
- Veena, S., Divyalakshmi, M., Poornima, M. (2018). Study of Cyber security in Data Breaching, *International Journal of Advance Engineering and Research Development*, 5(3), 1513-1516.
- Vukašinović, M. (2018). Cyber Security Measures in Companies, *International Journal Of Economics And Statistics,* 6, 125-128.
- Woody, C., Ellison, R. (2020). Building a Cyber Security Strategy, *Systemics, Cybernetics and Informatics,* 18 (1), 206-216.