SEP_AIN3130

by Student Help

Submission date: 25-Apr-2023 03:14AM (UTC-0700)
Submission ID: 2074972754
File name: SEP_AIN3130.docx (156.88K)
Word count: 2566
Character count: 15509

Business Systems Security COS7035-B (2023-2024)

How business services firms can implement an effective security strategy, protect their own data and sensitive client information, and continuously monitor third-party risks

Abstract

The research paper has provided information regarding the protection security and privacy of data of businesses and clients. Security strategies necessary for data protection are discussed in the research. It has emphasised the protection of data using information systems and technology. Vulnerabilities associated with the implementation of security strategies such as cyber security is also highlighted. This has provided a clear knowledge about various categories of vulnerabilities prevailing in businesses and their services. The research has also embedded information related to security measures taken to prevent the breaching of data and data privacy of clients and business firms. The benefits of implementing government laws and regulations such as the "General Data Protection Regulation (GDPR)" and the "Data Protection Act 2018" are also discussed in the research paper.

Table of Contents

Introduction

A "***Security strategy***" is known as a series of actions taken by business firms to recognise, remediate and manage various risks in data protection. It is considered a dynamic and comprehensive approach to avoid incidences of data breaches through internet attacks, phishing and hacking. It is thereby essential for organisations to focus on problems related to data security through effective decision-making and strategic planning of security measures. Guidelines provided in the government legislations and standards have helped in protecting the data of businesses and customers. Business services should be improved with the effective implementation of security and data protection measures in business activities.

Implementation of security strategy in business firms

Implementation of an "***information system***" is considered a complicated process in business. Businesses today are more reliant on computers and the electronic environment which has increased the number of rising e-commerce across the world today (Achar, 2022). It requires effective planning of security strategy for developing and maintaining the security of computer systems. It also requires increased security of business services such as e-Mail, accounting, client information and transportation of products. Security strategy primarily focuses on combat vulnerabilities existing in the implementation of businesses technologically. The security strategy has included various electronic data protection methods such as "***cyber security***" and "***cloud computing security***" (Bandari, 2023). It also includes the introduction of "***secure user productivity***" as one of the KPIs of business security. These aid in the development of effective data security for the organisation that includes sensitive information of both businesses and clients. The implementation of ***cyber security*** in business services installation of a specific firewall system in the private network helps in preventing outside access to data.

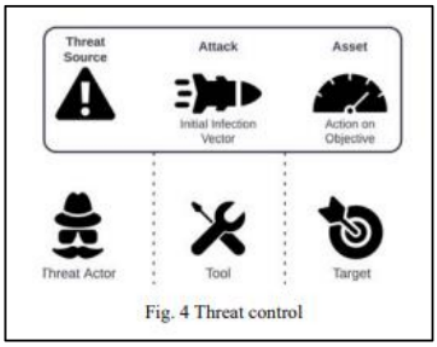

Figure 1: Threat Control

(Source: Achar, 2022)

Protection of network, information and computers is achieved with the installation and time-to-time update of antispyware and antivirus software. The software should be set to check for updates automatically at a certain scheduled time. Any new information that is fed into the computer system requires effective scanning using antivirus software (Stankov and Tsochev, 2020). Unwanted applications and devices need to be either uninstalled or updated regularly. Every employee of the company needs proficient training by cyber experts to prevent any inefficient management of client and business information. Limited accessibility of data requires to be implemented for avoiding any data theft and data leakage from the database system. Effective "***cloud computing security***" needs to be implemented to effectively manage the risk associated with a "***database management system***" (Dhaya *et al*. 2021). DBMS of a business should be focused on to avoid any data risk of data theft and data loss.

Vulnerabilities of implementing security strategy in business Services

Vulnerability in information security is meant as an opportunity or weakness in an information system that is exploited by cybercriminals which leads to unauthorised access to computers. Vulnerability acts as a primary door open for malicious attacks (Stankov and Tsochev, 2020). Various kinds of vulnerabilities are experienced by businesses in implementing the security strategy. These vulnerabilities in "***Operating system (OS) vulnerabilities***", "***Human vulnerabilities***", "***Network vulnerabilities***" and "***Process vulnerabilities***".

Operating system (OS) vulnerabilities: It causes exposure to an operating system allowing cyber attackers to damage all devices installed with the same operating system. The attackers repeatedly send fake requests of a clogged system which make the computer overloaded (Khan and Byun, 2020). An outdated and unlatched is responsible for creating OS vulnerabilities due to the exposure of information of the system on which the application is running.

Human vulnerabilities: It is usually created by errors caused by users that expose information related to hardware and networks. This also results in the exposure of sensitive information to individuals conducting malicious activities (Yang *et al*. 2020). It commonly poses security threats to both software and hardware and the networking system of a computer. It increases the probability rate of phishing attacks.

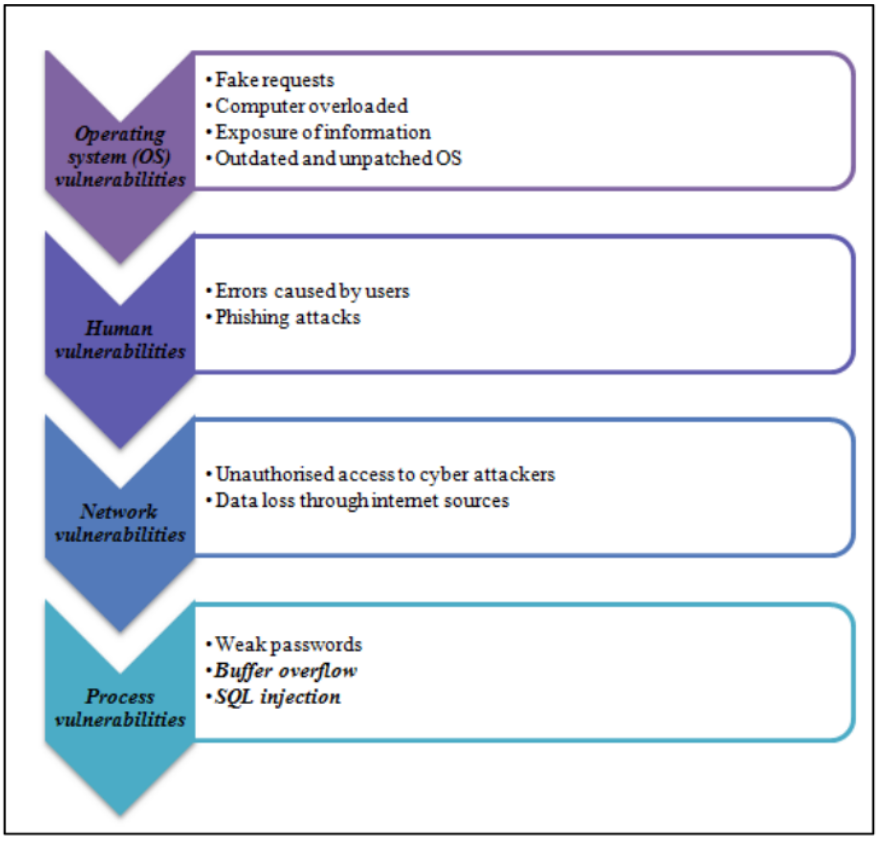

Figure 2: Vulnerabilities of cyber security

(Source: Self-created)

Network vulnerabilities: It is a weakness in the software and hardware infrastructure of a business firm which gives unauthorised access to cyber attackers. It causes a disruption in the network system of the organisation which results in data loss through internet sources.

Process vulnerabilities: It is caused due to prevalence of insufficient security measures. The vulnerability is a result of weak passwords and poor access to users (Arogundade, 2023). Software vulnerabilities such as ***buffer overflow*** and ***SQL injection*** help identify process vulnerabilities.

Therefore, it is important to keep a check on the existing vulnerabilities of implementing cyber security to prevent cyber attacks, Trojan attacks, malicious spyware and phishing of data on computer systems and mobile devices.

Effective protection and security of business information

Business information requires protection and security against different types of cyber-attacks and unauthorised access. Effective information security encounters risks associated with

threats, disruption, modification, destruction and confidentiality. The primary goal is to prevent data theft by cybercriminals using strategies namely "***encryption***", "***access control***", "***firewalls***", and "***data backup***" (Chang *et al*. 2022). Encryption has protected sensitive information from cybercriminals and hackers with the use of specific passwords. It aids business firms to comply with regulations of data protection such as "***General Data Protection Regulation (GDPR)***". It is considered a cost-effective measure of data protection and security. Access control is marked as an effective tool for the prevention of data breaches. Access control focuses on limiting the accessibility of users to business information portals and databases (Chitre *et al*. 2022). Passcoded DBMS is shared with a limited number of employees thereby keeping track of the risk of "***insider threats***".

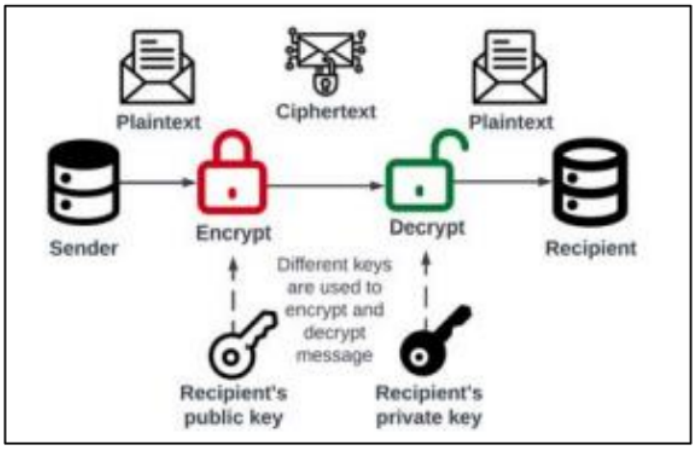

Figure 3: Data encryption

(Source: Achar, 2022)

Firewalls play an important in the protection of network transmission which limits the accessibility and transfer of data packages. It reduces the chances of inbound traffic due to external attacks and unknown resources. These are beneficial for configuring advanced threats to packets of data being transmitted that are blocked based on threat type (Rasner, 2021). Data backup has also played a crucial role in providing efficient security to business information. Online transfer of data packets and transactions is controlled by backing data in a safe storage area. It helps in the easy recovery of lost data at the time of hardware failure and ransomware attacks (Duan *et al*. 2021). These security measures have therefore aided in the easy functioning of cyber security and cloud computing security in computer networks and systems.

Security strategy for sensitive information of clients

Management of the risk of data loss of sensitive information of clients is important for businesses today. Information security is effectively implemented in organisations with the inclusion of "***cloud computing security***" and "***cyber security***". "***Data loss prevention (DLP)***" is one of the strategies applied in security measures of cloud computing that confidentiality of sensitive data. It is known to provide robust control of security by interlinking with "***identity and access management (IAM)***". ***Data encryption*** of the personal information of clients is encouraged with the use of tools such as "***FileVault***" and "***BitLocker***" (Achar, 2022). Advanced encryption includes cryptographic keys and digital signatures for preventing unauthorised access of cybercriminals to customer data. Cloud services provide control of traffic through "***egress or ingress traffic management***" (Arogundade, 2023). It is implemented to protect file transfer in a private network with the use of authorised and specific IP addresses. It configures traffic control through ingress and egress ways for securing data in a "***multi-cloud environment***".

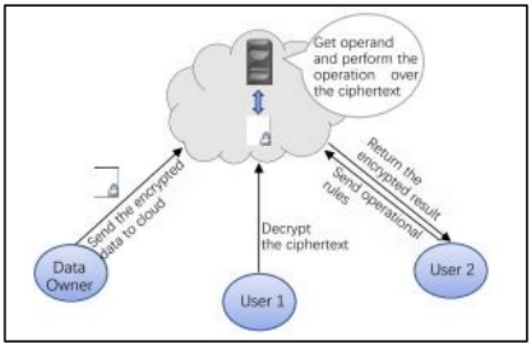

Figure 4: Homographic Data Encryption in Cloud

(Source: Yang *et al*. 2020)

Insider attack on information is managed and prevented with the implementation of cyber security. Information of consumers is protected in password-protected tools and applications such as DBMS. Cyber security ensures "***Data Integrity***" thereby increasing the reliability of data. File storage is technologically managed with the use of "***Network Attached Storage (NAS) technology***". It helps in the effective storing of files that are accessed and shared using internet technology (Yang *et al*. 2020). "***Privacy Protection***" is emphasised with the deployment of firewalls and digital signatures for protecting and encrypting data. Appointment of data privacy experts and cyber experts is necessary to keep track of threats associated with lost, theft and unauthorised access to data. Therefore, the protection of sensitive data of customers is protected using privacy protection methods, data integrity, encryption and digital signatures.

Effective monitoring of possible third-party risks associated with Business

An application of the technologies of Industry 4.0 is important for monitoring the risks linked with third-party in business. One of the I4.0 technologies mostly used is "***Blockchain technology***" for preventing privacy breaches in businesses today (Khan and Byun, 2020). This fourth-generation technology has helped in implementing the security process of "***image encryption***" using devices such as image sensors and smart cameras. Blockchain technology is recognised as a modern solution to issues of trust and minimising or eliminating the role-play of third-party. Images stored in Blockchain make use of "***cryptographic pixel values***" ensuring the security and privacy of image data of both clients and businesses. Automation in the environment of IIoT has revealed a far-reaching impact on cyber attacks (Kobusińska, 2022). This has prevented the disruption in the process of manufacturing and production, SCM and loss of sensitive data.

Cyber security has focused on the management of third-party risks. "***Cyber Third-Party Risk Management (C-TPRM)***" has helped in providing protection against security threats and vulnerability from various partners and vendors. It prevents the penetration of unauthorised vendors into the organisational data related to business and clients (Keskin *et al*. 2021). Non-intrusive methods are applied for conducting C-TPRM by effectively synthesising public information available within an organisation. C-TPRM is thereby considered an effective way to mitigate vulnerabilities thereby avoiding risks linked with dependencies. The application of C-TPRM has helped in enhancing risk management, risk analysis and cyber security of the supply chain. It elevated the network of the supply chain, manufacturing process and production line technologically (Vitunskaite *et al*. 2019). The security of accounts and inventory is also enhanced with the inclusion of C-TPRM in the business process both globally and domestically. Therefore, it is important to apply C-TPRM and Blockchain technology for ensuring the protection and security of information from third-party risk.

Advantages of implementing security standards for data protection in business services

The government has aimed at protecting the personal and sensitive information of businesses, clients and customers. Steps taken by the government for the protection of data and to prevent breaching of data privacy is the formulation of legislative standards. The various data protection legislations include the "***General Data Protection Regulation (GDPR)***" and the "***Data Protection Act 2018***". The "***General Data Protection Regulation (GDPR)***" has focused on effective cyber security measures for the protection of information (Ncsc.gov.uk 2023). It has aimed at managing the risks related to data security and data and privacy breaching. Breaching of data privacy is considered as a punishable offence thereby providing

measures to reduce the impact of cyber attacks. Protection of personal data from cybercriminals and detection of security events are also aimed by the "***General Data Protection Regulation (GDPR)***".

The "***Data Protection Act 2018***" has provided strict rules on making use of personal data which are commonly known as "***data protection principles***". The Act has aimed at transparent, lawful and fair protection of personal information based on accessibility, data portability and data processing (Gov.uk 2023). These principles have enabled the effective protection of information for both clients and business firms. Data protection and privacy are strictly prohibited using the strict guidance and principles of the Act.

Conclusion

The above information has highlighted the various modes of implementation of strategies related to the security of information in business services including "***cloud computing security***" and "***cyber security***". These have enabled data encryption, data integrity, digital signatures and privacy protection for the purpose of preventing data theft and privacy breaching. Businesses have also applied guidance and principles of government legislation such as the "***General Data Protection Regulation (GDPR)***" and the "***Data Protection Act 2018***". Therefore, it can be concluded that vulnerabilities related to the security of data and privacy are prevented with the implementation of government Acts and regulations, I4.0 technology and security services.

References

Achar, S., (2022). Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape. International Journal of Computer and Systems Engineering, 16(9), pp.379-384.

Arogundade, O.R., (2023). Addressing Cloud Computing Security and Visibility Issues.

Bandari, V., (2023). Enterprise Data Security Measures: A Comparative Review of Effectiveness and Risks Across Different Industries and Organization Types. International Journal of Business Intelligence and Big Data Analytics, 6(1), pp.1-11.

Chang, V., Golightly, L., Modesti, P., Xu, Q.A., Doan, L.M.T., Hall, K., Boddu, S. and Kobusińska, A., (2022). A survey on intrusion detection systems for fog and cloud computing. Future Internet, 14(3), p.89.

Chitre, M.D., Dhoke, M.A. and Shriniwar, M.A., (2022). A Review: Insider Attack in New Normal. 06

Dhaya, R., Kanthavel, R. and Venusamy, K., (2021). Dynamic secure and automated infrastructure for private cloud data center. Annals of Operations Research, pp.1-21.

Duan, Y., Hofer, C. and Aloysius, J.A., (2021). Consumers care and firms should too: On the benefits of disclosing supplier monitoring activities. Journal of Operations Management, 67(3), pp.360-381.

Gov.uk, (2023). *The Data Protection Act*, https://www.ncsc.gov.uk/pdfs/information/gdpr.pdf Accessed 25 April 2023

Keskin, O.F., Caramancion, K.M., Tatar, I., Raza, O. and Tatar, U., (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. Electronics, 10(10), p.1168.

Khan, P.W. and Byun, Y., (2020). A blockchain-based secure image encryption scheme for the industrial Internet of Things. Entropy, 22(2), p.175.

Ncsc.gov.uk, (2023). *General Data Protection Regulation (GDPR)*, https://www.ncsc.gov.uk/pdfs/information/gdpr.pdf Accessed 25 April 2023

Rasner, G.C., (2021). Cybersecurity and third-party risk: Third party threat hunting. John Wiley & Sons.

Stankov, I. and Tsochev, G., (2020). Vulnerability and protection of business management systems: threats and challenges. Problems of Engineering Cybernetics and Robotics, 72, pp.29-40.

Vitunskaite, M., He, Y., Brandstetter, T. and Janicke, H., (2019). Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third party risk management and security ownership. Computers & Security, 83, pp.313-331.

Yang, P., Xiong, N. and Ren, J., (2020). Data security and privacy protection for cloud storage: A survey. IEEE Access, 8, pp.131723-131740.

SEP_AIN3130

ORIGINALITY REPORT

2%	1%	0%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Bradford Student Paper	1%
2	research.tensorgate.org Internet Source	<1%
3	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
4	www.ed.ac.uk Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		