student plagarism report

by Xxxx Xxxx

Submission date: 15-May-2021 05:41AM (UTC-0400)
Submission ID: 1586607962
File name: UCCyber.edited.edited.docx (25.51K)
Word count: 1556
Character count: 9170

UCCyber's scenario

Student's Name

Institution of Affiliation

Course Code and Title

Instructor Name

Due Date

Abstract

The rapid advancement of the internet and related technologies has led to several cyber insecurities, such as cyber-attack.[1] For that reason, the development of UCCyber's has contributed to the improvement of cybersecurity offering protection to people and organizations from any cyber-attack. Adobe system software is one of the organizations that experienced a cyber-attack where the system was hacked, and personal details were stolen. Several challenges in the organization contributed to the Adobe software attack scenario, and several strategies were applied to offer a solution for the scenario.

Introduction

In 2013, hackers accessed the adobe system and stole customers' credit cards and their login details, resulting in leakage of the data.[2] The occurrence affected a huge number of adobe users. The company's failure to provide privacy to users' InformationInformation facilitated the incident happen. Unfortunately, the customers' details which were lost not recovered. However, Adobe could have improved its organizational performance to prevent the incident, follow the ethical instructions, and embrace external standards to prevent the scenario. Therefore, Adobe integrating threat management would have facilitated the analyses of susceptibilities and fears for its software, thus prevent the incident. This paper will focus on the significant problems present in the scenario, solutions to the issues, and mitigation strategies on ethical issues that would resolve the problem.

Major problems that contributed to the adobe system attack

The company had several challenges that contributed to the incidents. These challenges include the organization's weak cybersecurity and failure to comply with the legal policies. The organization's personally identifiable data and cybersecurity were weak, thus easy access. [6] The methods used in the software system were ineffective because the hackers acquired the company's details, such as detecting passwords, length, and hints in an easing approach. Hackers targeted adobe company since it had defective codes and outdated technological methods. This is because it was not easy to address the flaws in the software since it was created on top of the coding. Therefore, the hackers acquired a lot of the details since they easily accessed the user's database of the company with less effort. Also, the company's weak cybersecurity failed to keep privacy for its users.

Users' confidential InformationInformation was accessed quickly due to workers' failure to protect the closed source code. The closed source code offered protection to the company's data. For that reason, the hackers could obtain the company's closed source, which leads to the software being weak, thus easy access. Therefore, hackers could identify the operation of adobe security with ease after accessing the closed source code.[6] Unfortunately, after the incident, the company was more exposed to attack, resulting in the PDFs' disclosure using adobe acrobat readers. Lack of privacy exposes the InformationInformation to attackers.

Adobe Company did not comply with the California data protection laws. Adobe failed to apply appropriate procedures that would have prevented hacking. As a result, Adobe's insufficient safety activities exposed the users' documents to misuse and theft of private information. [2] A back scheme that was weakly encrypted could be accessed easily by hackers,

as stated by a data breach lawsuit. The firm defiled California Internet Privacy Protection Act which prohibits any organization from gaining access to private information. Many adobe users shifted from the company since they felt their data was not safe again. Since the organization did not observe legal issues, it made it vulnerable to cybercrime which stimulated hackers to access Information.

In addition, the organization never observed the unfair competition law. The act inhibits unlawful or stolen data technology software which could cause unfair advantages by combating unfair business practices. The stealing of data happened since the organization had a large amount of InformationInformation that made it difficult to accommodate many workers. The organization's activities involved deceitful actions that mislead the users on their data safety. Therefore, lack of compliance motivated hackers to access the company's system and use the data to gain profits.

Proposed solutions to the problems

The adobe company should reset the passwords to inhibit illegal access. Therefore, the users whose accounts were altered to be contacted through email provide guidelines for changing their passwords.[3] Adobe management should urge their customers to create a complex password that would not be easy for hackers to guess. Also, Adobe discards weak passwords that hackers could quickly detect by enacting techniques of phrasing passwords instead of using words.

Adobe Company should have offered training to all their employees. [3]This will aid in staff acquiring knowledge on cybersecurity and data policies, thus preventing leakage of customer information. For that reason, employees would be informed of cyber attacks and the

formation of the policy if frequent training would be done to them. The policies would guide employees on handling, acquiring, disposing, and transferring data, thus protecting the company vulnerable to hackers.

Adobe should apply cyber law to which would assist them in suing the hackers. For example, they can punish the hacker who accessed the users' Information using the universality principle. The universality principle can assist in recovering the incident losseThe use of passive nationality principle may also take the cyber attack criminals by using passive nationality principle. The customers' credit cards and account login details could be protected if they can use the protective principle.

A safety audit should be conducted to prevent further leakage of customer details in the organization. The experts would assess data storage, accessibility and ensures the information privacy was adhered to. Therefore, the organization should employ safety strategies to provide safe control of the customers' data.

Mitigation strategies for the scenario solution

The organization can embrace a risk management plan capable of relating to the point of sale (POS) and other target systems. The best approach to risks within the company would entail examining all susceptibilities and threats of their schemes regularly. The due analysis of all the exposures and threats for the organization's schemes can prevent data leakage. [3] It was also essential that the organization prioritize the threats. The establishment of the best threat models

for all their systems, particularly in the network and information hubs, reveals all attacks those hackers can use to gain access to the POS schemes. Moreover, having in-depth knowledge of data flow through encryption can show InformationInformation that resides unencrypted in the systems, accessible to hackers who use malicious software to steal data. It is also crucial that the firm trains all staff on cybersecurity matters to avoid data loss. [3]Employees' knowledge of all indicators and dangers in looking at phishing dispatches within the company will prevent such scenarios. Creating policies that indicate how workers should be handling, retrieving, disposing, and transmitting InformationInformation can be crucial in preventing future occurrences. Therefore, implementing measures, policies, and techniques to avoid security intimidations can help to tackle the varying threats in the modern world.

Mitigation strategies on ethical issues

Adobe Company could have embraced the practice of whitelisting that permits only recognized software to operate the POS system. [5]A different process from that of software organization and POS scheme could have accomplished whitelisting practice. This practice is achievable either by hardware or software systems. POS schemes and code software packages use up-to-date signatures and a hardware-safeguarded signing key, which guarantees that only a sincere manufacturer’s coding is installed in all the gadgets.

Consistently planned audits on information safety usually prevent data leaks in organizations. The safety audit entails an exhaustive assessment of all security policies compared to penetration tests and susceptibilities valuations. The specialists know the storage, availability, and safety of data when they assess during a scheduled audit. Thus, it is essential to strike an equilibrium between accessibility and information privacy during the adobe company review.

[5]Safety strategies provide the organization with an understanding of safety control. Furthermore, the company can enforce the use of unique passwords to guarantee user's data safety.

Conclusion

Although the UCCybers offers cybersecurity and protection to an organization's Information, it encounters several scenarios such as cyber-attack. For instance, the adobe system was hacked, and customer information was leaked. The user's data leaked and was unable to recover. The organization's access to Information was made accessible due to its ineffectiveness of cybersecurity and personally identifiable information. Also, the hacking was contributed by Adobe's defective codes and outdated technological approaches. The company should have identified the threat and weaknesses of their system, offer training to their employees on cybersecurity, urge their customers to use a unique password on their accounts, and regular safety auditing to prevent the incident.

Reference

[1] Arlitsch, Kenning, and Adam Edelman. "Staying Safe: Cybersecurity for people and organizations." *Journal of Library Administration* 54.1 (2014): 46-56.

[2] Kirsch, Cassandra. "The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law." *N. Ky. L. Rev.* 41 (2014): 383.

[3] Jump, Michelle. "Fighting cyber threats with technology solutions." *Biomedical instrumentation & technology* 53.1 (2019): 38-43.

[4] Miller, Lauren. "Cybersecurity insurance: Incentive alignment solution to weak corporate data protection." *Available at SSRN 3113771* (2018).

[5] Cheng, Long, Fang Liu, and Danfeng Yao. "Enterprise data breach: causes, challenges, prevention, and future directions." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7.5 (2017): e1211.

[6] Nunes, E., Shakarian, P., & Simari, G. I. (2018, May). At-risk system identification via analysis of discussions on the dark web. In *2018 APWG symposium on electronic crime research (eCrime)* (pp. 1-12). IEEE.

student plagarism report

ORIGINALITY REPORT

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

PRIMARY SOURCES

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

student plagarism report

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8