Lesson 4 Activity

Case Study

Submitted By:

Vince Arvie I. Cube

4WMAD1

Mrs. Criselda C. Encanto

ITEP 413: Information Assurance and Security 2

November 7. 2023

Case Studies

A. In 2022, a leading e-commerce company, ShopSecure, fell victim to a significant data breach that exposed customer information. The breach had far-reaching consequences, shedding light on various cybersecurity issues and vulnerabilities. ShopSecure was a popular e-commerce platform that catered to millions of customers worldwide. It offered a wide range of products and had a reputation for a seamless and secure shopping experience. However, a breach in their security led to a massive compromise of customer data. On a seemingly ordinary day, ShopSecure's security team noticed unusual activity on their network. It turned out that a cybercriminal had gained unauthorized access to their customer database. The breach exposed sensitive customer information, including names, addresses, payment card details, and purchase history.

Questions:

1. What are the potential consequences of this data breach for ShopSecure and its customers?

I think that the data breach could lead to a severe loss of their customer trust and reputation. It might also cost legal actions since the data of the customers has been taken, and potential compensation to affected customers during the breach. It will also affect on their reputation as a company or organization and might result to multiple losses of revenue. It will also give them a huge amount of confidential data's such as email addresses, images, credit card numbers, and debit card numbers. This data breach will not only affect ShopSecure but also their customers. Their customers might experience identity theft, financial fraud, or other misuse of their personal information and may also result to financial losses and damage to their own privacy.

2. What vulnerabilities or security issues could have allowed the breach to occur?

The most common reason or issues why data breach happen is because of human error or social engineering leading to unauthorized access to the system. Outdate software is also one of the issues in data breach, website that are using outdated software has potential vulnerabilities that can be exploited by hackers. Weak passwords or easily guessable passwords is also a security issues in data breach because it will make it easier for hacker to gain access to the system or websites. Some companies don't have enough security measures in place to protect their system or websites from any type of cyberattacks. There are many vulnerabilities and security issues that allowed the breach to occur like the injection, unvalidated inputs, failure to restrict url access and many more.

3. What immediate actions should ShopSecure take in response to the breach?

They should immediately notify those customers who's been affected of data breach, then conduct a thorough investigation to assess how huge the damage or the breach and the obligations that should be addressed. They can also attempt to isolate all access to the system or websites to prevent the escalation of damage caused by the data breach. Then updating systems or software, improving encryption, and stronger access controls. They can also focus on tracking internal indicators of compromise or tactics, techniques and procedures, and monitor subsequent or related incidents or breaches.

4. How can ShopSecure rebuild customer trust and prevent future breaches?

They can rebuild customer trust by being transparent about the breach, providing support to all of the affected customers and adding or implementing additional security measures. Assessing the

impact and scope of the breach. You need to assess what data has been compromise and what are the potential risk and liabilities of that incidents. By notifying their customers in a transparent and honest way, by explaining them what happen, and what data has been exposed and step that they're doing about the issues. Lastly by restoring and enhancing their relationship to their customers and showing them their commitment and value. By following up them and provide updates on the actions that their doing. By doing all that they can rebuild the trust of their customers and they can improve their systems and services.

5. What regulatory and legal obligations does ShopSecure have following the data breach?

They are obliged to report the data breach to the authorities and regulatory bodies, complying with the data protection laws. They also need to notify their customers who's been affected by the breach and could face legal consequences and fines because of it. ShopSecure might also face to some financial penalties that may dependent on the scope of the breach as well as the data that has been compromise. They are also might face some private lawsuits brought by the customers and shareholders. There still more legal obligations and regulations that I didn't tackle like implementing reasonable data security measures and facing up to five years in jail if they're intentionally and willfully concealing the data breach.

6. How can customers protect themselves in the aftermath of a data breach?

The customers can protect themselves after data breach by immediately changing their passwords on the breach platform and any other platform where the same password was used. They ca also freeze their credit or bank accounts for best protection, freezing customers credit account doesn't affect customers scores. Monitoring financial statements for suspicious activity and considering freezing credit reports are advisable measures. The customers can also place a fraud alert to anyone, fraud alert can last a year and by doing that banks or other people will verify your identity before issuing a new account. Updating all of the passwords that you have on any platforms will also help the customers to protect themselves, including passwords on online banking, and wallet. Lastly, they can also update their information and contact numbers to ensure that your data on another platform is protected.

Reference:

- Team, E. (2020, September 9). 5 Consequences of a data breach in your business. Enstep. https://www.enstep.com/blog/disaster-recovery/5-consequences-of-a-data-breach-in-your-business/
- Savelli, T. (2023, January 19). Vulnerabilities in cyber security: what they are and how to fix them? PSafe Blog. https://www.psafe.com/en/blog/vulnerabilities-in-cyber-security-what-they-are-and-how-to-fix-them/
- Response, S. I. (2023, April 12). *How do you establish and maintain trust and credibility with your customers after a security breach?* www.linkedin.com. https://www.linkedin.com/advice/1/how-do-you-establish-maintain-trust
- Borner, P. (2023, August 8). *The Impact of a Data Breach | Data and Security Breaches | The Data Privacy Group*. The Data Privacy Group. https://thedataprivacygroup.com/blog/2019-9-17-data-breach-the-legal-implications/#
- Jayakumar, A., & O'Shea, B. (2023, September 20). *How to protect yourself after a data breach*. NerdWallet. https://www.nerdwallet.com/article/finance/how-to-protect-yourself-after-data-breach