**Report on security breaches of Amazon Company**

October 29/10/2022

Rasolosoa Jimmy

**Summary:**

This report will assess the results and causes of the security breaches within the Amazon company.

**Introduction:**

This report will address the following question: How are the breaches within our cyber security compromises our image? Are there any financial repercussions because of these breaches? What are the options to prevent and limit those attacks?

**Finding:**

1. Through the different research that I have done for this study. I have found that in the year 2019 there was a capital breach within our cyber security system. The capital one breach happened when 140,000 social security numbers were accessed by the hackers, as well as 80,000 bank account numbers. Our company was part of the company that has been hacked. In fact, there was one of our employees was used by hackers. It appears that a hacker used her knowledge to hack over 30 companies and illegally access the personal data of more than 100 million people.

There were also recent breaches in our security system that happened on October 6, 2021. On this date, an unknown hacker leaked data pertaining to one of our services: Twitch. Due to the leak, there were numerous Twitch source codes, and streaming earnings numbers have been disclosed.

1. It also looks that within our own company the security and privacy of data aren’t totally in control. Reports have shown that some low-level employees were using this private data that we must check out on the purchases of celebrities. In addition, there was a program was created which allow Amazon’s sellers to extract their own metrics. This program is a sort of backdoor for third-party developers to help them steal Amazon customer data. In fact, we have discovered that in one of our Chinese data firms, the data had been harvested by millions of customers’ information.
2. We have then looked at the consequences that these breaches within our cyber security and within our employees can have. We have noticed an evident loss of customers and stakeholders. We have found that the overwhelming majority of people would not do business with a company that had been breached. This is even more flagrant when the company is holding and must protect customers’ data. By losing this trust to other companies or individuals, the business is losing tremendously.
3. There is also a financial impact that breaches have on big companies. The money lost by these attacks can be counted as millions of dollars. IBM and Ponemon Institute have said that the average cost of a data breach in 2021 is $4.24M, a 10% rise from its average cost of $3.86M in 2019. When a breach is discovered sooner, the cost is less than when it remains for months undiscovered. An example of these would be that for breaches that took less than 200 days to identify, the cost would be around 3.61 million. However, if the breaches took more than 200 days to be discovered, the price there would be 4.87 million. This is almost a 1.23 million dollar of difference.
4. Some solutions have been already put into practice. Starting in October, Amazon is offering Security Awareness training. This training is free of charge and is for both individuals and organizations. There is also an opportunity for them to build their own solution in addition to the amazon training that works for them. There is also a Multi-Factor Authentication that has been created. This can help customers to authenticate themselves by typing in their password securing more security device. For example, there is an MFA security token that will be plugged into their computer’s USB port allowing it to be more secure. These will add a layer of security against session hijacking, man-in-the-middle, and malware attacks.

**Conclusion:**

In a conclusion, we have noticed that there are breaches within our company. These breaches can be through our cyber security but il also can be within our employees. These breaches have a negative impact on the image of our company since some organizations and customers would not trust us anymore. In addition, the price to repair these damages is very high and expensive. Some solutions have already been put into practice that is helping the brand remain as good as it is.

*References:*

*Amazon announces two new cybersecurity initiatives aimed to protect organizations and individuals*. Amazon.com, Inc. - Press Room. (n.d.). Retrieved October 29, 2022, from <https://press.aboutamazon.com/news-releases/news-release-details/amazon-announces-two-new-cybersecurity-initiatives-aimed-protect>

AS, S. (n.d.). *The consequences of a cyber security breach*. Sungard AS United States. Retrieved October 29, 2022, from <https://www.sungardas.com/en-us/blog/the-consequences-of-a-cyber-security-breach/>

Evans, W. (2021, November 18). *Amazon's dark secret: It has failed to protect your data*. Wired. Retrieved October 29, 2022, from https://www.wired.com/story/amazon-failed-to-protect-your-data-investigation/

Heiligenstein, M. X., Ambjer, Vanzanella, T., Kramer, C., Biobot, & F., S. (2022, June 22). *Amazon data breaches: Full timeline through 2022*. Firewall Times. Retrieved October 29, 2022, from https://firewalltimes.com/amazon-data-breach-timeline/

Whalen, T. (n.d.). *Customers affected by Capital One data breach have limited days to file a claim*. https://www.wibw.com. Retrieved October 29, 2022, from https://www.wibw.com/2022/09/08/customers-affected-by-capital-one-data-breach-have-limited-days-file-claim/