Title of the assignment

Name of the student

Professor’s name

Title of the course

Date

Introduction

As technology is increasing day by day due to this, there are a lot of security issues that are raised on the databases. Due to such action, it is extremely difficult to save the system from hacking. There are many companies in the world that are affected by this deadly hacking. Due to this unethical action, many companies are losing their precious data. Moreover, many companies are affected by such attacks. Some of the companies are suffering from high-quality losses that are in the result of their financial losses. Now different huge companies like Google, Amazon, and YouTube are involved in applying significant investment for the protection of their data from such hacking and also wanted to secure their system in a proper way. In this report, there is comprehensive information related to a company that is struggling with such harmful action of hacking. There are some questions related to these issues that will be answered in the section given below.

Evaluation of the level of responsibility required for the company

In the modern world, there are huge security issues related to databases of the companies. This risk has been increased on a daily basis. From the information from different newspapers, it can be seen that every week, there is a case mentioned related to data loss of various companies. In this world of technology, hackers are increasing the risk of hacking that will in result, affect the accounting management of the system. There are many companies that are suffered from this issue. From these companies, one of the companies that are recently affected by hacking is Aadhar. This company has faced a financial loss of more than 1.1 billion dollars. Due to this action, this company was extremely close to bankruptcy. This company had lost the huge data of its customers by the hand of different powerful hackers. This shows that the Aadhar Company was extremely weak in maintaining the main database of its customers. From the report, it can be noted that it was the main responsibility of the software developers. This condition has created a huge argument for the company because they have no proper information about those businessmen. The level of responsibility of the company was extremely high because it was handling important data of the clients like bank accounts and other personal information. This shows that this company has a huge responsibility rate (Genge, Haller, & Kiss, 2015).

It can be seen that Aadhar was one of the huge company in India that is handling the information of the residents that are living in this country. such information includes their names, their phone numbers and their bank account information. The database of this company is hacked in March 2018. This company is an Indian government ID database. The data of the citizen has been leaked on the other systems. The main reason was that the Indane was unable to make comprehensive security on their API. This was the reason why their database was easily accessed to the hacker. At the start, this company was extremely unable to detect the problem of their data loss because their system was extremely weak. After this, when this company was able to detect what was going on with their website. Then this company started to suffer a lot. This company had lost huge data of their customers and their bank accounts. As a result, this company had faced more than 1 million dollars due to this database. The response of this company was too late because they were not able to detect it. In the last week of March, this company successfully detected this problem in their system. Then after this, they are making efforts to enhance their security measures in a proper way. This hacking attack was not a normal one for minimizing it. The Indian government had to apply maximum efforts to control this problem. Then after this, the company was able to make its own investigation for providing a secure plan for its system. The company was involved in making different security enhancement plans like they wanted to encrypt the bank account data of the customers all over India. Another unique enhancement was related to the voltage security that will help the company to lock down the important files of the users. This technology will able to take raw information about bank accounts. This website was involved in making many changes for their security enhancement for making their system stronger (Greitzer, et al., 2008).

From the past few years, technology is increasing, and many companies are moving towards installing the EMV chips and pin technologies in their system. From the last decade, Europe is started to use this technology for payment through its credit cards. This technology is using a lot of information from the user and converts it into anonymous one after the use that makes it completely useless for the hacker (Liebert, 2016).

Additional regulations for saving the business against hacking

When companies are being hacked or faced with any databases lost problems there, the main objective is that they always took serious actions. Their main step is to stop that action from the hacker. The main aim of this action is to protect the main documents of the system for hackers. For that case, many companies are using different types of means for the sake of protection. This may include password protection, mask the information and divert the codes. The companies are changing their password every 30 days. Moreover, many companies are moving towards decentralized networks for personal computers, so their systems are protected perfectly. This will help the company to protect its frameworks, and it will make the system weaker to be hacked.

There is another method the company is using for protecting its system from hacking is to hire a different organization that is able to give strength to their system. This type of organization is involved in making different types of tests for the system. They are making the system and then again hacked it and analyze how much powerful the system is for the company. Then according to that analysis, they tried to make a safer system for the required organization. This strategy is helping the company to determine the weakness of the system. In that case, Aadhar Company is involved in implementing the voltage securities for their system. Then after this, the system is tested by the two independent companies before implementing it. The risk of hacking is increased in such companies that are not focusing on the internal control through this they are able to overcome risk (Maughan, Balenson, Lindqvist, & Tudor, 2013).

For that case, many companies are using different applications that will provide protection over the personal data of their customers. This information must be accurately documented in the form of another document. This makes the document easy to use for the authority and also able to refrain from hacking. On the other hand, the internal control of the system is providing proper information to control the system by creating a sequence of the discrepancy. It will help the company to provide a prediction. This company is working on enhancing the system by implementing voltage security. Also, it can be noted that technology is increasing on a daily basis and many companies are moving towards EMV chip and pin technology in their system. This will help the company to gain more security in their data. Furthermore, it can be seen that every chip card contains a lot of pieces of information that come by installing the card into the system. After the implementation of this technology in the company, it can be noted that there is some variable that is involved in protecting the databases of their customers. For resolving such an issue, the government of India had taken a huge budget for solving it. In the early stage, the database issue was extremely difficult to detect. But now this due to many technologies these issues are quite easy to solve by the companies (Genge, Haller, & Kiss, 2015).

A company using third party accounting system now what is their level of responsibility

One of the main reasons for the data leak of this company was as a result of the third party. This party was involved in assessing the main perimeters of the company. Moreover, if any hacker wanted to access the main files of the company, then it can be extremely pondered. Furthermore, if there is any kind of intentional unapproved access that took place, then there are many reasons behind it. From them, one of the main reasons is that this data may be accessed by the other person and spreading its private information with other systems. There is one of the huge reasons for the entrance of the third party, and that is about the risk of security is increased. Through this action, the level of responsibility is also increased. The reason is that the company has to trust the actions of the third party. As a member of the IT team for the whole company, it is the main duty of the supplier that he has to build such a system that will minimize the risk of hacking. The main aim of the third-party software is to provide complete protection on the accounting of the company and their main records. Moreover, they also have to inform the main department about the problem (Liebert, 2016).

An argument for additional regulation

Whenever there is a problem in the organization related to hacking, then their first main step is to take serious action against it. Their starting step is to block unwanted software from their system. This will help the company to minimize the risk of being hacked. The main of this step is to protect important data from the hackers. This may include password protection, mask the information and divert the codes. The companies are changing their password every 30 days. Moreover, many companies are moving towards decentralized networks for personal computers, so their systems are protected perfectly. This will help the company to protect its frameworks, and it will make the system weaker to be hacked.

There are many companies that are involved in hiring different other organizations to protect their systems. They are involved in making the system more powerful by enhancing the power of firewalls. Moreover, if any hacker wanted to access the main files of the company, then it can be extremely pondered (Walker, 2019).

Three recommendations

There are a lot of recommendations the business through which the businesses are able to make a secure system for protecting it against the hackers. These recommendations may help them by making a perfect system for businesses.

The first recommendation is that the company must have to make a perfect system that will regulate the password on a daily basis. This system will change the password and make a new one again, so it will be quite difficult for the hacker to access it.

The next recommendation is that the business companies have to choose the right ISPs for their system; it will help the company to protect their true assets from hackers. There is only one responsible for the business company that they must have to choose such a system according to their security requirement.

Moreover, another main recommendation is that the company must have to keep a proper eye on their spyware. This will help the company to stay updated and checked the main information about the company properly. This will make huge difficulty for the hackers to hack that system because the system is kept on checking about the threats (Maughan, Balenson, Lindqvist, & Tudor, 2013).

References

Genge, B., Haller, P., & Kiss, I. (2015). Cyber-security-aware network design of industrial control systems. IEEE systems Journal, 11(3), 1373-1384.

Greitzer, F. L., Moore, A. P., Cappelli, D. M., Andrews, D. H., Carroll, L. A., & Hull, T. D. (2008). Combating the insider cyber threat. IEEE Security & Privacy , 6(1), 61-64.

Liebert, A. (2016). Industry 4.0–the intended impact of Cyber Physical Systems in a Smart Factory on the daily business processes: A Study on BMW (UK) Manufacturing Limited.

Maughan, D., Balenson, D., Lindqvist, U., & Tudor, Z. (2013). Crossing the" Valley of Death": Transitioning Cybersecurity Research into Practice. IEEE Security & Privacy , 11(2), 14-23.

Walker, M. (2019). CEH Certified Ethical Hacker Bundle, Fourth Edition. McGraw Hill Professional,.