Risks And Threats Of Data Security

Posted on September 11, 2019

The success of companies in today's environment is mostly dependent on innovation, and appropriate data is its key component. However, companies that are based on data and run businesses based on the quality of data have to uncover the vulnerability and data breach associated with it. For every company, it is important that they tend to focus on data security and privacy (Terzi, Terzi & Sagiroglu, 2015). Staying ahead of the criminal and illegal data activities requires that the company should improve its security controls and data security activities.

Most companies nowadays do not cater to warnings for their cybersecurity or data security and fail to standardize the company's privacy. According to studies, AT&T analyzed that 50% of the companies did not update their data securities in the last three years (Terzi, Terzi & Sagiroglu, 2015). The protection and privacy of confidential information are gaining more interest as each year advances. A survey conducted by World Quality Report 2015-16 found that data security (cyber or any other) is the most important aspect for the companies to be measured. However, there are threats and risks to data security, which are imposed as a direct loss for the company if it is not managed accordingly. These risks and threats to data security as discussed below:

- Non-existence of security architecture: Some organizations do not have any security architecture in the workplace, which leaves the company's data to be exploited and loss of any identifiable information. This is sometimes caused by the lack of resources from the company or unqualified IT staff, which has to ensure data protection (Rao & Selvamani, 2015). As a result, the networks of the employees are directly linked to the internet, without any privacy measures. This can become a threat when the data is transmitted to the internet without any firewall or protection layer. Inappropriate networking of data security can also result in data vulnerability, including hardware and software, which can also include threats of hacking and viruses. The structure of data security is mostly influenced by the IT staff, and having unskilled staff for data protection becomes a threat, which negatively affects the companies' success (Rao & Selvamani, 2015).
- Cybercrime: One of the most important threats to a company is cybercrime. It usually arises as hacking into a company's computer/system through the internet. Due to the lack of data protection on the internet, hackers get leverage to breach a company's system and access private data (Rao & Selvamani, 2015). It also includes Trojan Horse and malware, which are viruses on the internet that cause a PC or the entire system of the company to be corrupted. This threat is increased when a company does not have measures to secure its data online, which gives leverage to cyber criminals.
- Employee breach: Some of the threats to data protection come from within the company. A threat from the employees always exists in the company that they might impose a potential loss for the company. Employees tend to breach the private data of the company, and it makes

it easy for them when the data security measures are not appropriate (Lane, Shrestha, & Ali, 2017). These breaches are made easy when the company shares the secret passwords to confidential files and systems. Physical storage like Flash Drives, external storage and metadata from the internet to access the company's private data are mostly accessible by the employees (Lane, Shrestha, & Ali, 2017). Threats of employees gathering data are mostly important to manage. Ultimately, it becomes a risk whether or not to allow the employees to be flexible in the workplace.

Policies/Procedures To Mitigate These Issues

- First, the company should hire experienced IT staff to ensure data protection. These IT individuals should know about SQL and malware functions (Lane, Shrestha, & Ali, 2017). Hiring quality individuals will make the company more protective in terms of data security and improve the continuity of the business.
- Cybercrime has increased a lot in the technological world. A number of techniques, including proxy servers and firewalls, are the means to create more protective data systems. Cyber crimes, such as hacking the data and feeding viruses to the systems, can be dealt with by installing firewalls, which are renewed every day by the employees (Terzi, Terzi & Sagiroglu, 2015). Using proxy networks disables hackers' ability to intercept the company's data.
- The most important measure to consider is the employee breaching the confidentiality of the company. These issues can be resolved by utilizing security solutions like hidden cameras in the workplace, and for home tasks, appropriate software can be allocated to monitor the PCs or the systems used for completing the tasks (Rao & Selvamani, 2015). If a situation arises where the employee wants to copy the data from the PC to his/her private flash drive, the company can resolve it by setting up passwords for unknown devices whenever they are attached to the PC.

References

Lane, M., Shrestha, A., & Ali, O. (2017). Managing the risks of data security and privacy in the cloud: a shared responsibility between the cloud service provider and the client organisation.

Rao, R. V., & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, *48*, 204-209.

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2015, December). A survey on security and privacy issues in big data. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for* (pp. 202-207). IEEE.