A Critical Analysis of Information Security -A Case Study of Cognizant Technology Solutions

Anvar Shathik J.[1, 2] & Krishna Prasad K.[3]

[1]Research Scholar, Srinivas University, Mangaluru, Karnataka, India
[2]Assistant Professor, Department of Cloud Technology and Data Science,
College of Engineering & Technology, Srinivas University, Mukka, Mangaluru, India
[3]College of Computer Science and Information Science, Srinivas University, India
Email: anvarshathik@gmail.com

ABSTRACT

Security was not a major concern of the past in Information Technology Organizations. But presently, due to the vast growth in fraud and hacking techniques, the security of organizations is a great concern. Organizations usually spend millions every year just to protect their environment and to maintain security. Yet, no company claims to be a hundred percent secure as fraudulent techniques are more tricky and latest. As the hackers are becoming hard and tricky, the major Information Technology (IT) Organizations are willing to pay a large sum of money for providers offering services of enterprise security schemes. The hackers are always ready to intrude into the company's valuable information sources. As per the recent survey by 'Security Week', nearly seventy percentages of respondents have faced a security threat which ended up in the loss of valuable information or the collapse of functioning last year. An employer of the company can indeed be a major attacker than an outside intruder. An employee of the company is already having all privileges to use resources of the company while various other ways are needed for an outer intruder for accessing the same company's network or data. Cisco, the networking giant has a major focus on Enterprise Security Policies. The company has seen a valuable improvement in the last few decades, which shows the importance of security. Cisco had recently released data that showed a lack of security policies in about 23 percentages of companies worldwide. More than 70% of Information Technology persons say that their organizations lack behind in areas of security policy. Large numbers of IT people fail to practice security policies as they are not easily understandable. For every organization, policies are the building blocks. They function as road maps which each employee of the company uses in various ways. Developing a well-defined policy requires artistic skill. Federal agencies have a Statutory obligation is available for federal agencies for maintaining day-to-day security policies. The primary Information Security Officer (ISO) is usually pledged for implementing these policies and the Chief Executive Officer (CEO) of the Company as well. The best security policies consider the vision and mission of companies, the important assets that need security, and security threats imposed against certain factors. All these come under risk management which needs defect identification by business impact policies. The weakness of a company has to be identified to find the vulnerability ratio of that company. Designing a security policy is not a nightmare once the major scope of policy design is identified. The major challenge lies in identifying the scope and threat areas for security policy. The policy is nothing but a collection of guidelines and procedures on what and how it can be implemented. In this paper, we are analyzing how Cognizant Technology Solutions (CTS) maintaining its standards, policies, technologies, and management policies which are defined for securing data of an organization.

Keywords: Security, Information Security, Cyber security, InfoSec, Security Analysis, Cyber threats, Vulnerability, Security policy, Cloud Security, Cyber Maturity.

How to Cite this Paper:

Anvar Shathik, J. &Krishna Prasad, K. (2020). A Critical Analysis of Information Security -A Case Study of Cognizant Technology Solutions. *International Journal of Case Studies in Business, IT, and Education (IJCSBE), 4*(1), 155-171.

DOI: http://doi.org/10.5281/zenodo.3928673.