Upgrading Organizational Information Security System

Lashuna Bond

Strayer University

BUS 375: Project Management

Professor Shetty

10/28/2019

Upgrading Organizational Information Security System

Brief Summary

Safeguarding information technology is one of the key business requirements that will enable a firm to be able to attain a unique competitive advantage. The current digital era has been characterized by increased incidences of cyber threats that cripple major operations within an organization (William & Anne, 2017). The current project is meant to strengthen information security system by ensuring that it is fully upgraded to the current quality standards. Indeed, successful upgrading of the information security strategy is a noble requirement for business organizations to safeguard their information systems and databases. This is a requirement for them to be able to streamline the manner, in which they engage with customers across the globe, deal with various cyber security threats (instigated and orchestrated attacks on organizational information system, illegal access to sensitive organizational information, espionage and virus attacks among others).

Project Goals

Android mobile devices and desktop computers have become targets for hackers. IT security is a prime concern for small and large businesses (Charles et al., 2016). There is no doubt that cybercriminals are after important information such as financial records, intellectual property and customer data among others. Hackers are aware that small businesses do have defective information security systems, thus they capitalize on this to launch attacks with the intention of meeting their personal goals such as bringing organizational businesses down or for financial gains. Enforcing strong password policies is one of the goals of the current project under implementation. It is considered to create strong user login credentials so that computer criminals will find it hard to have illegal access. In order to accomplish this, coming up with a workable business plan of creating strong password policies is a key requirement that should be accorded due attention.

Another goal to be accomplished is mapping out a disaster preparedness plan. The project is intended to identify critical resources so that there is use of appropriate security and backup solutions to eliminate incidences of cyber threats. The project will also accomplish the goal of implementing top notch encryption technologies on organizational desktops, laptops and other removable media so that there is zero unauthorized access to confidential information. The project will also educate the organizational employees by developing internet security guidelines, informing them about the safety of the internet and informing them what they are supposed to do in the event that they have misplaced organizational information or there is a possibility of a malware on their machine (Cichonski et al., 2012). In case of security breach, employees will be encouraged to come forward immediately as opposed to trying to solve the problem by themselves or hoping that the incident will blow over. There is also need to accomplish the goal of using a reliable security solution. Employees will be informed on the importance of scanning system and user files by use of latest antivirus programs and identify warming signs of cyber-attacks such as espionage and phishing.

Project Objectives

Enhancing confidentiality, integrity and availability are the three major objectives of the current project. The project will create a conducive organizational environment where confidential information will be kept away from people who don’t require it. There will be provision of protection mechanisms for organizational data and also understanding the application programs that are used within the organization. The second objective of upgrading the information security system is integrity. The integrity mechanisms will ensure that information stored in the organizational systems is never contaminated or be changed in a way so as to suit individual interests. Availability is the third and last objective of the current project under implementation. Availability will ensure that organizational data is accessed by all authorized personnel in order to make informed decisions on a number of issues.

Project Structure

The current project will be implemented and managed under agile project management methodology. This is a comprehensive approach under which the requirements and the collaborative efforts of the self organizing and cross functional teams are made possible (Abrahamsson et al., 2017). Under this, there will be adaptive planning, evolutionary development and other forms of continual improvements during the entire phase of project implementation and management. The project will be implemented under various phases. The inception phase is where the costs of the project under implementation will be determined by a project management team. Product design phase will entail determination of the hardware required to run the proposed software of upgrading the security system. At coding phase, the system programmers will create a new information security system and infuse it with required features. Testing the developed software with the intention of establishing its compatibility with different operating systems, hardware, or browsers will be done at the testing phase. At deployment phase, the new information system will be made available to general public within the organization. Finally, fixing problems and updating information security system will be done at the operation and maintenance phase.

Key Customer(S) and Stakeholders

E-commerce firms such as online shops, huge electronic shops and wholesalers are major customers. These are the right clients who are known to upgrade their information security systems on occasional and need basis. Managers, stakeholders and entire technical team are project stakeholders who will gather system requirements during the real process of project implementation and management. System developers will be responsible for coding the new information security software, maintain the workability of the system and increase memory capacity of the information security system to accommodate new users.

References

Abrahamsson, P., Salo, O., Ronkainen, J., &Warsta, J. (2017). Agile software development methods: Review and analysis. *arXiv preprint arXiv: 1709.08439*.

Charles, A.; Sennewald and Balloe, C. (2016). Effective Security Management. 6th edition. <https://doi.org/10.1016/C2014-0-03448-X>

Cichonski, P., Millar, Tim, Grance, T., Scarfone, K. (2012). Computer security Incident handling Guide. Computer security Resource Center.

William, A. & Anne, K. (2017). Cyber Resilience: An Essential new Paradigm for Ensuring National Survival. 2017. Pages 126-131.