INFORMATION TECHNOLOGY SECURITY POLICY

Name

Course

Tutor

Date

Information Technology Security Policy

**About RollinOn Inc**

RollinOn Inc is an American company that designs pre-made and custom designed skateboards. Over the last few years, the company has experienced massive growth in the aspects of the customer base, revenues, infrastructure, and personnel. In the course of conducting its operations, RollinOn relies heavily on various forms of computer technology to design the products. As a matter of policy, the company has allowed employees to carry their computers to work. The fact that these workers take their tablets and laptops and use them in the enterprise has exposed the company's information technology infrastructure to serious threats. The company is in need of advanced security policies that would protect the technological appliances in its possession. The following is a discussion of the information technology policies that the company can use to improve the security of the computer systems.

**The current state of Web application technology at RollinOn**

In the recent past, the information technology sector introduced and embraced a new web application known as web 2.0. One of the primary benefits of this application is that it allows for direct sharing of information through social networking (O’Riley, 2009). With this new development, most business organizations resorted to the adoption of the application to promote their commercial practices. RollinOn was not left behind. The availability of this application enabled it to venture into the field of e-commerce to promote its business interests. However, there is a problem with this application. In the modern cyber crimes, hackers have come up with technology that allows them to hack into the websites and compromise the information contained on the websites. The hackers are capable of pulling down the entire website or injecting a bug that may alter the information provided on the websites. Besides, the persons can hijack and take control of the site so that they do whatever they want with the information.

The problem with the management of RollinOn is that it has also allowed the employees to bring their laptops and tablets and link them to the organization's website. In these instances, provided that the group lacks strong policies, it is possible that the individuals may inadvertently make mistakes that may put the organization at significant risk. Instructively, in most of the cyber attacks, the hackers use the end-users when they drive them to drive-by downloading. As a result, very dangerous bugs could be introduced into the system. This situation compels RollinOn to evaluate its information Technology security to seal all the security loopholes that are evident in the current state.

**Potential security risks**

There are a number of security risks that the information technology infrastructure of RollinOn is exposed to in their desire to maintain its web presence while at the same time improving its e-commerce activities. The following are some of the potential risks that the technology faces:

* Cross-site scripting (XSS) is one of the most common computer vulnerabilities that many organizations face. The threat is mostly found in web applications like the one that is being used by RollinOn. The most significant risk of this security concern is that it allows the hackers to have mechanisms of bypassing certain aspects of access controls including the same-origin policy (Wassermann & Su, 2008). The threat of this vulnerability is measured with regards to the relevance of data being targeted. In some instances, it may affect data that is at the core of the operations of the company.
* Data breach is another vulnerability that the organization faces with its use of the web application. Data breach entails the release of confidential information to an environment or third party where they will cause maximum damage to the company. In organized crime, there are persons who are consistently aiming at accessing confidential information from organizations so that they may use such information to stage major attacks to the targeted institutions (Baker et al, 2011). In this happens to RollinOn, a lot of information will reach its competitor, and that may affect its position in the market.
* The last attack that can be used against the company is the denial of service attack. In this vulnerability, a bug is placed on the website such that it makes the services temporarily unavailable to the users. When doing this, the hackers disrupt the services of the host which have been linked to the server. In this regard, the services become crippled. When that happens, the organization is prevented from providing services to its clients.

**Techniques and technologies to use in mitigating these risks**

In the face of these challenges, it is possible to develop techniques and technologies to reduce the effects of the risks. Firstly, RollinOn has to constantly keep an eye on all the activities taking the place of the website. In most instances, the activities of hackers are noticeable. In these cases, the system administrators would note some irregular activities are going on in the systems. Ordinarily, system administrators know the manner in which the websites are set up and the various ways in which they work. In the event of any irregular activity on the web, the officials need to initiate the necessary security procedures to protect the integrity of the system.

Another approach that the company can take is to make sure that it adopts only the technologies that have been certified by the relevant authorities. In the modern technological era, there are a lot of fake products in the market. It is important for the company to go for those technologies that are certified and have valid certificates for their operations. While a product may appear genuine, it takes an expert to distinguish whether it is dubious or not. Products that are not genuine are always prone to attacks since they lack the relevant security features that would protect the systems in the event of an assault.

**IT security policies for RollinOn**

*Internet usage*; from research, when individuals come with their computers to the establishment and down load items from the web, they increase the security threat to the technology of the company. In that regard, the first security policy that the company must put in place is to forbid individuals from carrying their laptops and tablets to work. The system would be effective in dealing with the risks that relate to cross site scripting (Peltier, 2016). Since the organization's computers would be fixed with special security features such as anti malware, it would be difficult to cause damage using the approach of cross-site scripting.

*Key control method*; in the web application that is being employed by the company, there are mechanical keys that are being used to manage the system. The problem of the mechanical keys is that it is easy to duplicate them and use them without leaving a trail. The key control policy of the organization should include features that enable the administrator to trace the holder of the mechanical keys and those who are capable of duplicating them. In that regard, it would be possible to prevent the denial of service attacks that the information technology system can face.

*Visitor management*; since some threats can be executed by persons who present themselves physically to the premises of RollinOn, it would be necessary to have effective visitor management policies, especially those that seek to have access to the information techno logy system. They need to be escorted by experts and all their actions monitored closely.

**Resistance to the implementation of the policies**

Ordinarily, people are resistant to change. During implementing the policies, there are a lot of resistances that may be faced by the members of staff. Firstly, employees who have been used to carrying their laptops and tablets to work will find it difficult leaving their gadgets at home. The most famous people who may resist this policy are some of the senior most personnel in the IT department.

Since the new approach would include keeping track of the activities of the individuals, there would be problems with compliance. Some people may feel that the introduction of such policies would infringe on their rights to privacy. To overcome the resistance, it would be necessary to appeal to the reasoning of the personnel of the staff and win their trust and confidence.

References

Baker, W., Hylender, A., Pamula, C. D., Porter, J., & Spitler, C. (2011). 2011 data breach investigations report. Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp\_databreach-investigationsreport-2011\_en\_xg. pdf, 1-72.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.

Wassermann, G., & Su, Z. (2008, May). Static detection of cross-site scripting vulnerabilities. In Proceedings of the 30th international conference on Software engineering (pp. 171-180). ACM.

o'Reilly, T. (2009). What is web 2.0. " O'Reilly Media, Inc.".