Security awareness

Technology, Information Technology

Security awareness campaign Dell is an American private Company with headquarters in Texas. The company manufactures and sells technology, hardware and equipment. Threats from inside the company continue to be the main source of information security breaches, and therefore effective security awareness campaign targeting the employees of the company can help identify and prevent threats like social engineering and phishing. Threats have continued to emerge from within the company due to inadequate awareness on issues targeting security among the workers in the company. Organizing a security awareness campaign will ensure the employees are informed and updated on various security issues that are vital in protection of the company's resources. Security awareness campaign will aim at creating an environment that is secure in order to protect the organization and clients from breaches (McGovern, 52).

The campaign will target creation of awareness and will incorporate the use of topical posters, online general awareness courses, newsletter, videos, email campaigns and forums. The goal of the campaign is to ensure reinforcement of security best practices. The campaign will target all the departments in the organization. The topics to be covered during the training entails email safety, mobile security, physical security, passwords and access control, importance of individual responsibility, definition of key cyber security terms, phishing, social engineering, data protection and destruction, threats and virus protection, internet safety, federal information and security management act together with demonstration of practical examples of vulnerability and security threats. The campaign and training will target one department at a time with an intention of ensuring all the departments are

covered. At the end of the training the employees should be able to avoid breaches, pass audit requirement for compliance, create a secure environment for the organization, practice and learn secure habits and gain awareness of vulnerabilities and information security threats. The employees will be observed after the training period to assess the impact of the program (McGovern, 54).

Work cited

McGovern, M. Opening Eyes: Building Company-Wide IT Security Awareness. IT Prof. 4. 3 (2009): 52-54. Web.