Technology evaluation and recommendation

Technology, Information Technology

Technology Evaluation and Recommendation Technology Evaluation and Recommendation Security Threats The peer-to-peer (P2P) file sharing application allows users to share video, music, games, and documents and facilitate online telephone conversations. As described in the Bureau of Consumer Protection website, this application enables other computers using similar P2P programs to create a network and thereby to share digital files with other computers through this network. P2P file sharing applications are able to set the drives and folders from which digital files can be shared with others on the network. Sometimes employees who use P2P file sharing software may accidently share files or folders which contain sensitive client information, or they may save a confidential file or folder to a shared drive by mistake. As a result of these issues, confidential customer information will be made available to others (Bureau of Consumer Protection). An organization always needs to securely store a variety of sensitive client information including passwords, system registry, file backups, and other data. Many of the organizations have developed local area networks to improve employee access to information within the organizational environment and thereby to enhance the firm’s operational efficiency. Therefore, if an employee installs an unsecure application in his computer, the security of the overall network would be compromised. In addition, today many employees connect their smarphones to company networks to browse internet. Those unfair employee practices may cause to spread malwares and viruses across the company network and this situation in turn would threaten the security of sensitive client information. Similarly, computer hacking is one of the major information security threats associated with P2P

file sharing because professional hacker can create fictitious file sharing pages that are capable of trapping sensitive client information. The organization also faces many security threats during the process of information collection because of the fraudulent practices like phishing, vishing, and smishing. Technology Based Solutions In order to enhance the security of sensitive client data, it is necessary for organizations to minimize the use of P2P file sharing applications. The organization can strictly monitor and regulate the traffic associated with unapproved P2P file sharing programs using network firewalls. In addition, it is also better to train employees about the security risks and vulnerabilities associated with using P2P file sharing software. URF filtering and patch management are some potential technology based solutions to address malware and virus attacks and Trojan horse programs. Through URL filtering, an organization can effectively categorize the websites and prevent its employees from opening unwanted websites that might become a threat to the confidentiality of the client information. As Ciampa (2013) notes, a patch can be simply defined as a software designed to deal with updating a computer program or to deal with security vulnerabilities. Patch management is an effective tool to improve the performance of information security systems (p. 89). Similarly, effective System Update Administration can play a significant role in fighting security failures associated with P2P file sharing and open source applications. By regularly updating anti-virus and spyware protections, the organization can improve its vulnerability to those security risks. As Scarfone and Mell (2007) describe, intrusion prevention systems (IPS) are network security tools that continuously monitor the company network and system

activities to detect malicious activities; and intrusion prevention systems are classified into four different types such as network-based intrusion prevention systems (NIPS), wireless intrusion prevention systems (WIPS), network behavior analysis (NBA), and host-based intrusion prevention systems (HIPS). Recommendations Among the different technology based solutions discussed, host-based intrusion prevention systems (HIPS) are more recommendable for providing effective protection measures because they greatly minimize the risk of confidential data loss associated with using P2P file sharing applications and other open sources. Many technical experts opine that HIPS can be very effective to monitor systems and to check for anomalous behavior. More precisely, HIPS can play a crucial role in detecting applications that are attempting to be installed, non-standard events, and user escalation. The HIPS is an installed software package that analyzes events occurring in a particular host in order to detect suspicious activities (Scarfone, K & Mell). This system is able to ensure that only authorized IT professionals have access to sensitive client information. What Is the Risk or Vulnerability? What Needs to Be Protected? (e. g., passwords, data, file backups, system registry) Candidate Technology Solution How the Technology Solution Works Effectiveness (High, Medium, Low) P2P file sharing application Passwords and browsing history URL filtering This technique categorizes websites and prevents employees from opening unwanted and insecure websites. Low Employees' personal use of company network Credit card details and other financial data Patch management It uses software to fix security vulnerabilities and to update computer programs. Medium Computer hacking Purchase details and file backups

Host based intrusion prevention systems (HIPS) This tools monitors systems and checks for different anomalous behavior within a specific host. High References Bureau of Consumer Protection Business Center. Peer-to-Peer File Sharing: A Guide for Business. Retrieved from http://business. ftc. gov/documents/bus46-peer-peer-file-sharing-guide-business Ciampa, M. (2013). Security Awareness: Applying Practical Security in Your World. US: Cengage Learning. Scarfone, K & Mell, P. (2007). National Institute of Standards and Security. Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology. Retrieved from http://csrc. nist. gov/publications/nistpubs/800-94/SP800-94. pdf