**Harry and Mae’s Assets Recommended Security Controls.**

The process of managing risks includes the creation of context or the assessment base, identifying potential risks, assessing the risks and treating the identified risks by providing countermeasures. Security factors are one of those that can never be taken disparaged. It covers two areas which incorporate physical security of equipment and security of accessing data on the equipment. Based on identified vulnerabilities and risk exposure, the following control are recommended to address Harry and Mae`s security issues.

Harry and Mae’s have applied a smart card controlled physical access in the office. This is to control access to certain areas containing the organization’s communication equipment and network facilities. Smart cards alone are a risk in when they fall into wrong users. In addition to smartcards, Harry and Mae`s ought to consider actualizing facial recognition along smartcards for places that requires more security than others. This will make it hard for anyone to gain access to a highly restricted area such as surveillance rooms. Access is strictly to authorized personnel. Security smartcards, depending on how well they are implemented, are prone to hacking. In this case, Harrys organization have signified low security standards that make it easier to break through in case of an attack.

In designing of a local and wide area network for an organization, there are a lot of considerations to be made. They include; topology and placement of hosts in the network, choice of software and hardware with the right configurations. For a secure and easier network configuration, devices with similar functions and security profile should be grouped together. This requires the use of a boarder router and a firewall between distinct device groups. As a result, network administrators will have an easy time managing grouped connections. Separation of devices at layer level in a network alone is not enough. Harry’s and Mae’s network devices are separated based on layers, yet the use of firewall between devices with similar functionality and network access properties provides more security. Besides, securing of routers and switches requires segmenting the network into subnets based on functionality and location. Routing at the core of the network ensures that segments are isolated into independent broadcast domains. So, this improves security by preventing sniffers and Address Resolution Protocol (ARP) based attacks. Network performance is also enhanced

When it comes to the organizations network, traffic is allowed in both directions unfiltered. The wireless network interface is directly linked to wire corporate network posing more security risks. Such a scenario increases chances of an attack. It is also easier for an intruder to gain access to the organizations network through the internet. The mobility controller should also be configured to control traffic entering and leaving the network. These include malicious websites, pornographic websites that can be accessed by network users risking the network as a whole. Filtering of traffic enables the organization to control the parts of the internet accessible from the organizations network. The fact that the president of the organization requires open access capabilities calls for other automated levels of authentication. For instance, devices used by employees within the organization’s network should be registered maybe using the employee’s name and identity number. In addition, noting of mac addresses will make it easy to manage devices on the network and also make it easier to logon to a network. A single new MAC address or a flood of MAC addresses will indicate an intrusion. Members with domain access privileges should be trained on safe passwords as a domain is among risky areas for an organization to be attacked. Regular update of passwords must be recommended and enforced. Training of employees on the importance of secure passwords will also be helpful for safety and assurance.

The servers also require more security. Updating of drivers and firmware is something to be done on regular basis. Failure to update puts the organization at a risk of data breach or hardware failure as updates contain patches to security bugs in systems. Improving performance and compatibility of servers with current software should be regular updated. Besides, for better security the internal network of the organization should not be accessible from outside the company’s corporate network. It is easy for an intruder to attack such a network since it is no longer private. Publicly accessed part of the server must also be filtered with an intrusion detection and prevention system which will monitor the traffics into and out of the network. Campus workstations still face a security risk as employees still write down passwords. Someone with evil intentions can easily access the workstations and cause damage or interfere with others privacy. Employees should always be warned without limits about the effects of writing down passwords. There should also be events where they are required to memorize or update passwords, loosening of security standards does more harm than good.

Point of sale computers which are connected to the corporate network already pose as security risk. For instance, the case study states that some of the point of sale computers have been infected with malware yet, they can be linked to corporate network. The point of sale software should run on full-time basis. Payment transactions are also vulnerable as the point of sale computers can be easily attacked by malware. Use of anti-malware applications can help reduce the risk of malware attacks. The anti-malware application must be updated at every point in time and must be running always.

**References**

Canon, T. (2015). *How to Prevent Security Breaches*. Retrieved from, https://www.wired.com/insights/2015/02/the-root-of-the-security-problem/

Harry & Mae’s Case Study. Retrieved: https://cyberactive.bellevue.edu/bbcswebdav/pid-9057691-dt-content-rid-16337187\_2/courses/CYBR610-T201\_2181\_1/Harry%20and%20Mae%20Combined%20Script%281%29.pdf

Harris, K.D. (n.d). Data Breach Report 2012. Retrieved from, https://oag.ca.gov/system/files/attachments/press\_releases/BREACH%20REPORT%202012.pdf#page=23

University of California Santa Cruz (n.d). *Information Technology Services*. Retrieved from, https://its.ucsc.edu/security/breaches.html