Belmont state bank essay sample

Literature, Russian Literature

Belmont State Bank is a large bank with hundreds of branches that are connected to a central computer system. Some branches are connected over dedicated circuits and others use the dial-up telephone network. Each branch has a variety of client computers and ATMs connected to a server. The server stores the branch's daily transaction data and transmits it several times during the day to the central computer system. Tellers at each branch use a four-digit numeric password, and each teller's computer is transaction-coded to accept only its authorized transactions. Perform a risk assessment.

First, I will begin with building a control spreadsheet for the bank; which looks much like Figure 11. 2: (Fitzgerald, 374).

Then I would identify the assets. In this case, the assets I worry about most are hardware, network software, client software, data and mission critical applications. The hardware that I am concentrated on is the mail servers, web servers, and client computers and ATMs connected to them. As far as network software, I look at the application software (mail server and web server) along with server operating systems and system settings. With client software, it's the overall operating systems and system settings. Organizational data and storage is the focus; the databases with records. The mission critical applications are the company website and financial database with spreadsheets/personal history/ applications and appraisals; along with transaction history.

At the top of the list; is the mission critical applications necessary to conduct business/ for business survival. Next, is the organizational data, client software, hardware, and network software. As far as threats, the biggest threats in order of dollar loss and likelihood of occurrence are intrusion

(internal, external and eavesdropping/hacking), sabotage, fraud, theft of information, denial of service, virus, theft of equipment and finally natural disasters. When it comes to identifying and documenting the controls, I would have preventative controls(security guard in the branch buildings), and software to encrypt the teller passwords. I would also have application layer firewall(to protect information shared with the central computer), virus/malware programs in place, a disaster recovery plan and extensive training regarding both passwords and viruses among others. The controls and their roles would be placed in a numerical list and the controls number placed in the cell. The original spreadsheet would look similar to Figure 11. 5 afterward: (Fitzgerald, 379).

The last step would be to evaluate how adequate the controls are that are in place now, and the degree of risk associated with each threat. The Delphi team will detect, prevent and correct the threats according to priority. Being that a dedicated circuit/dial up telephone network is used to connect branches and servers transmit information daily to the central computer, security is an issue. The intrusion controls work decently, but can be upgraded and should be checked quarterly. The disaster and destruction threat could use further business continuity controls, as there is a high degree of risk here.