Semester Case Part #3 – Summary, Cost-Benefit Analysis, & Recommendations

Melvin Moreno

Table of Contents

Executive Summary

After running risk assessments and other analyses on TMXBank and its assets, I would like to highlight three critical assets crucial to your business and the vulnerabilities and threats that can exploit them. To start off, the multi-core transaction processing server which runs the banking app suite is of high importance to your business. Its vulnerabilities include a non-TLS connection, loss of connectivity, no intrusion detection system, and no anti-virus software. Such vulnerabilities leave it open to threats like data capture, malicious hackers, DoS/DDoS attacks, and system loss. The next asset I want to cover is the banking app suite which is the application used to support all core banking account transactions by customers. It also faces vulnerabilities from no intrusion detection system and needing operating system updates. As a result, its threats include malicious attackers, DoS/DDoS attacks, and disruptions in system processes. Lastly, I want to go over the customer management software. This software manages all aspects of customer information. As such, it has vulnerabilities like needing operating system updates and having unneeded protocols running. In turn, it faces threats like malicious attackers, Dos/DDoS attacks, malware, and disruptions in system processes. After making note of the most important assets and their vulnerabilities and threats, we can now focus on the biggest risks facing your company. In our risk assessments, we determined that employees clicking on phishing emails, SQL injections, and malicious hackers were the biggest risks. We deduced this by performing both a quantitative and qualitative assessment. In our quantitative assessment, all three of these risks fell under the high likelihood and high consequence category, meaning they were the most dangerous and likely risks to occur. Then in our qualitative assessment, we deduced that phishing emails account for an estimated $4.91 million annual loss, SQL injections account for an estimated $4.82 million annual loss, and malicious hackers account for an estimated $4.10 million annual loss. Evidently, these risks should be taken care of immediately. Any loss to your critical business functions and assets as a result of these risks would cost your company millions of dollars. It would also lower customer-trust in your business. Therefore, in our cost-benefit analysis and business impact analysis, we have determined the best courses of action to take to help mitigate these risks. We discussed easily implementable software to help prevent phishing emails, hackers, and SQL injections from happening at a reasonable cost that yields a high cost-benefit. These software programs are proven to work amongst thousands of other companies, and I am fully confident in endorsing them for use in yours. I have shown all calculations below to help navigate where your money is being used and show that it is being well-spent. In conclusion, after performing risk assessments and other analysis, I believe I have given ample options and solutions to the threats and vulnerabilities your company faces.

Cost-Benefit Analysis

- Employees clicking on phishing emails
  - Recommendation – Install an Anti-Phishing Software (Avanan) on the Mail server.
  - Cost of Recommendation - $72 / year
  - Background – Anti-phishing software was not installed on the Mail server in the past. After conducting a risk assessment, we have determined that employees clicking on phishing emails is the greatest risk. The Mail server provides the necessary communication between our business and our customers. The anti-phishing software is expected to prevent 95 percent of phishing emails from getting through.
  - Loss Before Anti-Phishing Software – $4,910,000 annual loss expectancy. $250,000 loss per instance at an annual rate of occurrence = 19.6.
  - Expected Loss with Anti-Phishing Software – $245,500. The Anti-Phishing Software is expected to reduce the losses by 95 percent ($4,910,000 – ($4,910,000 x .95) = $245,500)
  - Benefit of Anti-Phishing Software – $4,664,500 (($4,910,000 * .95) = $4,664,500).
  - Cost-Benefit Analysis – $4,664,928. The cost-benefit analysis is calculated as:
    - Loss Before Anti-Phishing Software – Loss with Anti-Phishing Software – Cost of Anti-Phishing Software
    - $4,910,000 - $245,000 - $72 = $4,664,928
- An SQL Injection on the Customer Database
  - Recommendation – Install a Vulnerability Scanner (Acunetix) on the Database server
  - Cost of Recommendation - $4,495
  - Background – Vulnerability scanners were not put into place on the database server in the past. After conducting a risk assessment, we have determined that SQL injections are one of the greatest risks to your business and customers. The database server hosts all of the sensitive customer data on it, so it is a high risk for customer confidentiality.
  - Loss Before Vulnerability Scanner – $4,820,000 annual loss expectancy. $125,000 loss per instance at an annual rate of occurrence = 38.6
  - Expected Loss with Vulnerability Scanner – $144,600. The Vulnerability Scanner is expected to reduce the losses by 97 percent ($4,820,000 – ($4,820,000 x .97) = $144,600
  - Benefit of Vulnerability Scanner – $4,675,400 (($4,820,000 x .97) = $4,675,400)
  - Cost-Benefit Analysis – $4,670,905. The cost-benefit analysis is calculated as:
    - Loss Before Vulnerability Scanner – Loss with Vulnerability Scanner – Cost of Vulnerability Scanner
    - $4,820,000 - $144,600 - $4,495 = $4,670,905

Cost-Benefit Analysis (cont.)

- Malicious Hackers gaining access to confidential and business critical assets.
    - Recommendation – Install a Vulnerability Scanner (Rapid7 Nexpose) on the Authorization server
    - Cost of Recommendation - $4,495
    - Background – Malicious hackers are amongst the greatest risk your business faces. As a banking institution, you will be faced consistently with hackers trying to gain access to your banking system and customer information. Prior to this risk assessment, there was no vulnerability scanner put in place on your authorization server leading to an increased risk of unauthorized personnel getting in.
    - Loss Before Vulnerability Scanner – $4,100,000 annual loss expectancy. $4,100,000 loss per instance at an annual rate of occurrence = 1.
    - Expected Loss with Vulnerability Scanner – $205,000. The Vulnerability Scanner is expected to reduce the losses by 95 percent. ($4,100,000 – ($4,100,000 x .95) = $205,000)
    - Benefit of Vulnerability Scanner – $3,895,000 (($4,100,000 x .95) = $3,895,000)
    - Cost-Benefit Analysis – $3,890,505. The cost-benefit analysis is calculated as:
        - Loss Before Vulnerability Scanner – Loss with Vulnerability Scanner – Cost of Vulnerability Scanner
        - $4,100,000 - $205,000 - $4,495 = $3,890,505

Business Impact Analysis

- Critical Business Functions – The following are CBFs that are integral to the business, either by generating revenue or being critical to the customer.
    - All Servers on the TMXBank System
        - Web Server
        - Internet Banking Server
        - Authorization Server
        - Customer SQL Database
        - Transaction Processing Server
        - Branch Servers
    - In-Branch Terminals
- Critical Business Systems – The following are, likewise, systems that are integral to the business, either because they generate revenue, or they are critical to the customer.
    - Banking App Suite
    - Firewall appliance
- Maximum Acceptable Outage (MAO) – This is the maximum amount of time each CBF can be down.
    - Web Server – 5 minutes. This is due to bank's systems all running on an online platform which requires the server to be up. If it exceeds 5 minutes then the cost of disruption exceeds the cost to recover easily.
    - Internet Banking Server – 10 minutes. This is a bit longer than the web server MAO due to the fact that you can still bank in-person if this server is down. This server is for those banking online. However, the cost of disruption still exceeds the cost of recovery quickly.
    - Authorization Server – 1 hour. This server can be down for a maximum of one hour before the cost of disruption exceeds the cost of recovery. Most of the bank's systems can still function without this server leading it to have a higher MAO.
    - Customer SQL Database – 1 hour. This database can also be down for an hour before the cost of disruption exceeds the cost of recovery. While inconvenient, most of the bank's services will still function.
    - Transaction Processing Server – 5 minutes. This is the main reason people come to banks – to do a transaction process with their account. If this server is down for more than 5 minutes, the amount of money lost increases exponentially.
    - Branch Servers – 24 hours. Because each server can server as a backup to the other, the MAO is longer for each of them.
    - In-Branch Terminals – 24 hours. Because you can use bank tellers instead of the branch terminals to conduct transactions, the MAO is also long for these functions.

Business Impact Analysis Recommendations

- Server Failure
  - If a server fails or goes down for any reason, I recommend the following:
    - Off-site backup servers that can immediately replace the given server at any moment.
    - A helpline number that customers can call in case of any system failure when conducting an online transaction.
- Branch Terminal Failure
  - If the Branch terminals fail, I recommend the following:
    - Working bank tellers during all normal business hours available to help customers with their queries and transactions while systems are down.
    - A 24-hour helpline capable of assisting customers during system failure.
- Banking App Suite Failure
  - If the banking app is inaccessible or unfunctional, I recommend the following:
    - An online web page that can execute the app's functionality as well.
    - A 24-hour helpline to help customers.
    - A redirect to the nearest TMXBank location to conduct business with in-person.
- Firewall Appliance Failure
  - If the firewall appliances fail to work properly, I would recommend the following:
    - Consistent updates and maintenance from CISO.
    - Consistent pen-testing from CISO.

Works Cited

https://www.avanan.com/anti-phishing-software

https://www.saasworthy.com/product/acunetix/pricing

https://www.esecurityplanet.com/networks/vulnerability-scanning-tools/