**Name:** CENSORED

**Due Date:** 9/30/19

**Class:** ISMN-5740

**CASE 1**

1. **Executive Summary of my Findings:**

* **Single Point of Failures:**
  + **Main Branch:** If data is compromised/destroyed, are there backups? If there is server downtime, are the remote branches affected? If any of the servers are compromised/destroyed, can the system continue working?
  + **Remote Branches (3):** If one of the branch servers/terminals was accessed physically, would the branch know? Would the servers be able to mitigate/stop the attack? If one of the branches are compromised, would the other remote branches or the main branch (or both) be compromised?
* **Risk Priorities:** Based on the findings within the table at the bottom of this document, the main risks to address first (with the first item being the most important) are:
  1. Social Engineering Attacks: This should be addressed within the branches themselves; educate employees on dealing with these attacks and familiarize them with the attacks through regular drills. If someone tricks an employee into giving up a login, they could have access to the *entire* customer database, which would be a total loss.
  2. Web Server Attacks: This should be addressed within the Main Branch by strengthening the security of the public facing web server. If this is not done and an attack is performed, it could result in a denial of service attack being performed on the web server. This could result in many people losing access to their bank accounts and disrupt communications with the database; this would be an unprecedented loss depending on the amount of downtime experienced by the web server.
  3. Data Loss: This should be addressed directly with the Customer SQL Database; regular backups should be performed in case of system malfunction/corruption/destruction. This needs to be performed within the Main Branch and may require some system downtime. Firewalls should also be configured properly so that data is transmitted properly and no service interruption occurs.
  4. Firewall Penetration: If the firewalls are misconfigured and an attack is performed on a server that affects the whole network, the other servers/systems may be at risk. This is a problem that affects both the Main Branch and the 3 Remote Branches, and in some cases both at the same time.
  5. Physical Server Attacks: If the physical security of any of the four branches is obsolete, then physical attacks are possible. If an employee has important access to systems and no controls are put in place, then they can unleash any number of attacks on the system. Total loss is a probable outcome of any physical attack but can be slightly mitigated by data backups.

1. **Asset Register & Discussion:**

* **Register:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **#** | **Asset** | **Location** | **# of Instances** | **Source** | **Sharing** | **Description** | **Importance to Business** | **Value** |
| 1 | Web Server | Main Branch | 1 | External and Internal | No | Public facing web server; connected to the Internet | High | High |
| 2 | Internet Banking Server | Main Branch | 1 | Internal | No | Internet banking server | High | High |
| 3 | Authorization Server | Main Branch | 1 | Internal | No | Authorizes users interacting with the Customer SQL Database | High | High |
| 4 | Transaction Processing Server | Main Branch | 1 | Internal | No | Processes transaction and saves records to Customer SQL Database | High | High |
| 5 | Customer SQL Database | Main Branch | 1 | Internal | Yes | Holds records of all customers with an account | High | High |
| 6 | Dedicated Leased Lines | Between Main Branch and Remote Branches | 3 | External | No | Connects the Remote Branches to the Main Branch | High | Medium |
| 7 | Firewalls | All Branches | 4 in Main Branch, 1 in each Remote Branch | Internal | Yes | Filter data going through ports on the networks | High | High |
| 8 | Branch Servers | All Remote Branches | 1 in each Remote Branch | Internal | No | Sends and receives data to/from the Main Branch | High | High |
| 9 | In-Branch Terminals | All Remote Branches | 1 in each Remote Branch | Internal | No | Interface for the remote branches for tellers | High | Medium |
| 10 | SQL Database Communications Software | All Branches | 2 for Main Branch Servers (Authorization and Transaction Processing Servers), 1 for each Remote Branch | External | No | Software that communicates with the database for retrieving/storing information | High | Low |
| 11 | Operating Systems | All Branches | 5 for Main Branch Servers, 1 for each Remote Branch | External | Yes | Operating systems for the servers/terminals | Medium | Low |
| 12 | Management | All Branches | 1 for Main Branch, 1 for each Remote Branch | Internal | Yes | Management for local branches and main branch | High | Medium |
| 13 | Staff | All Branches | Varying amount for each branch | Internal | Yes | Staff for Main Branch (IT/general staff) and local staff for Remote Branches (IT/general staff) | High | High |

* **Discussion:** Above is every company asset listed out for both the Main Branch and the Remote Branches. I have listed some guesses as to what a Single Point of Failure for each branch may be; these listed areas should be under constant surveillance for any problems. How much data is inputted into the systems manually, and how much are inputted via automated processes? What is the location, manufacturer, model number, components, peripherals, and BIOS versions of all the hardware in each branch? What is the OS/application specifics that are necessary for the systems? How is the data stored/maintained and are backups in place? The answers to these questions are imperative for determining which assets are the most important within the branches, but my guess would be that it is the servers; therefore, I am going to proceed in this Risk Assessment as if the servers in all the branches are the most important assets to protect.

1. **Threat Register & Discussion:**

* **Register:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Threat** | **Description** | **Source (External/Internal)** | **Type (Physical/Technical)** | **Asset at Risk** |
| 1 | Disgruntled Ex-Employees | Ex-Employees who still posses login credentials can exploit it | Internal | Can be Physical or Technical (Although it’s more than likely Technical in this situation) | Any system that ex-employees can access remotely (Ex: web server) |
| 2 | Malicious Current Employees | Current employees that will try to exploit the system for personal gain | Internal | Can be Physical or Technical (Although it’s more than likely Physical in this situation) | Any system that a malicious current employee has access to |
| 3 | Equipment Failure | Equipment fails and renders certain services unusable | Internal | Physical | Any system if not properly maintained |
| 4 | Data Loss | The database can become corrupted and result in customer data being lost (or it could be stolen and deleted from the servers) | External/Internal | Can be Physical or Technical (Although it’s more than likely Physical in this situation, i.e., an employee accidentally destroys company equipment, etc.) | Any system containing customer or employee data |
| 5 | Physical Attacks | Company assets can be physically attacked (either by malware being physically uploaded or a literal attack) | Internal | Physical | Any system that can be accessed physically by an employee or a customer |
| 6 | Phishing Attempts | Employee credentials are given to attackers through social engineering resulting in data breaches | Internal | Technical | Any employee is at risk; any system with remote logins enabled is at risk as well |
| 7 | The Art of Shoulder Surfing | Employee credentials are read and stolen over their shoulders through various means | Internal | Physical | Any system with physical or remote login capabilities |
| 8 | The Art of Dumpster Diving | Valuable company information or credentials can be recovered by sifting through the company dumpsters | Internal | Physical | Targeted company employees and systems with remote login capabilities |
| 9 | The Art of Piggybacking | Access to areas without authority are gained by following another person in (usually with some form of social engineering) | Internal | Physical | Systems in off limits areas that should not be accessed by people with the incorrect permissions |
| 10 | Natural Disasters | Natural disasters (such as earthquakes, hurricanes, tornadoes, floods, etc.) | External | Physical | Entire company if the disaster is big enough |

* **Discussion:** Piggybacking on the discussion from 2.), I will be assuming that the servers in all branches are the most important assets to protect; therefore, I will focus my viewpoint on what threats can compromise/destroy one or all the servers. The first set of threats are the external threats; most of these are out of your control, like natural disasters and weather conditions, but protection/countermeasures can still be put in place to assure that an external threat does not result in a total loss. The main external threat that is highly more likely to occur is attacks through the public facing web server in the Main Branch; the Internet is an entry point into the main servers, so any exploit that takes advantage of this can result in a total loss. Internal threats are also important to think about, so physical security is a highly important aspect. Only a select group of employees should be able to access any servers in either branch; if an attacker gained physical access to a server, they could compromise it through a multitude of ways. Appropriate countermeasures should be in place so that separation of duties and job rotation (and other important countermeasures) is maintained, making it harder for employees to access data without permissions. If physical attacks can be mitigated in all branches, then this will take out most internal threats from even being possibilities.

1. **Vulnerabilities Register & Discussion:**

* **Register:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Vulnerability** | **Description** | **Source (External/Internal)** | **Type (Physical/Technical)** | **Threats that can Exploit It** |
| 1 | Server OS | If the server OS’s are not updated, they are open to attacks | Internal | Technical | Physical Attacks (Malware uploading), Equipment Failure, Natural Disasters |
| 2 | Web Server | If it is not updated regularly, external attacks from the Internet can affect user access | External | Technical | Equipment Failure, Data Loss, Disgruntled Ex-Employees, Malicious Current Employees, Natural Disasters |
| 3 | Local Network | If the firewalls are out of date are unproperly configured, the entire Local Network can be attacked | Can be either External (via the Web Server) or Internal (Physical Firewall Changes) | Technical in the first case, Physical in the second case | Malicious Current Employees, Disgruntled Ex-Employees, The Art of Piggybacking, Equipment Failure, Physical Attacks |
| 4 | Personnel | If an attacker targets a specific employee, they can use them to gain access to company assets or gain information illegally; employees can also attack the company for their own reasons | Internal | Technical in the first case, Physical in the second case | Malicious Current Employees, Disgruntled Ex-Employees, Physical Attacks, Natural Disasters, Phishing Attempts, The Art of Shoulder Surfing, The Art of Piggybacking |

* **Discussion:** I have included a list of relevant questions above to help determine where vulnerabilities may lie within the business. If vulnerabilities go undetected, they may later be exploited for an attack; this is of course in the case of a high or medium risk, as vulnerabilities with a low risk of occurring will be mostly negligible. I believe server vulnerabilities may exist in one (or possibly even all) of the branches, and vulnerability scans should be used to help determine if this is true or not. Alongside this, the local network could be at risk in any (or all) of the branches from external attacks through the public-facing web server; if the Main Branch is compromised through an external attack, the Remote Branches could be compromised as well. If the firewalls are not properly configured (and therefore certain ports are left open and vulnerable to attacks) then the entire network will be at stake, but if they are configured properly then external attacks should only compromise the web server.

1. **Risk Assessment & Discussion:**

* **Risks:**
  + **Main Branch:**
    - Firewall Penetration
    - Unauthorized Customer SQL Database Interaction
    - Web Server Attacks
    - Physical Server Attacks
      * Uploading Malware
      * Physically Destroying a Server
    - Natural Disasters
    - Equipment Failure
    - Data Loss
    - Phishing Attacks / Theft of Employee Credentials
    - Social Engineering
  + **Remote Branches (3):**
    - Firewall Penetration
    - Unauthorized Customer SQL Database Interaction
    - Physical Server Attacks
      * Uploading Malware
      * Physically Destroying a Server
    - Natural Disasters
    - Equipment Failure
    - Phishing Attacks / Theft of Employee Credentials
    - Unauthorized Terminal Interaction
      * Extracting Customer Data
      * Authorizing Fraudulent Transactions
    - Social Engineering
* **Discussion:** I believe extensive background checks, audits, and personal interviews should be performed on the employees at regular intervals for internal vulnerabilities/threats to be minimal. I believe system testing should be rigorously and regularly performed alongside regular risk assessments to help manage this. External factors will also be a problem but should be negligible if the public-facing web server and firewalls and secure. I will provide a table of all the risks and their appropriate categorization below. As a side note: the risks I have found are very generalized, as no specific information was given about the servers or general layout of the branches; the risks should be investigated individually by appropriate professionals. The high likelihood/impact risks should be investigated/managed initially before any other risks, as they are the most damaging and would almost certainly result in a total loss. Every other risk should be managed appropriately afterwards, with the remaining low likelihood/impact risks being addressed last.

1. **Prioritization of Risks:**

* **Schema:**
  + **Impact Categories:**
    - High: Risks that are an immediate danger to the entire company and will absolutely result in bankruptcy are categorized as this. If the risk can compromise everything and cause extremely large financial damages, this will be what it is categorized as.
    - Medium: These are risks that are a danger to the company and should be addressed immediately. They will not cause a total loss if they are exploited, but the financial loss will still be large so they should be fixed/managed appropriately.
    - Low: These are risks that will not cause much damage if exploited and can usually be ignored for some time. These are problems that usually bug users or could cause small local damage, so they should be addressed last.
  + **Likelihood Categories:**
    - High: There is an almost guaranteed chance of this risk being exploited; fixing/mitigating the issue is very time sensitive.
    - Medium: There is a moderate chance of this risk being exploited.
    - Low: There is a minimal chance of this risk being exploited.
  + **Branches:**
    - M: Signifies that the risk is targeting the Main Branch.
    - R: Signifies that the risk is targeting every Remote Branch.
    - B: Signifies that the risk is targeting both the Main Branch and every Remote Branch.
  + **Risk Scores:** The risk with the lowest number (#1) is the most significant risk and it should be paid the most attention. The risk with the highest number (#10) is the most insignificant risk and can be safely ignored while other risks are attended to.
  + **Schema Justification:** I will be using this schema because three categories are the most appropriate way to divide up risks; if more categories were introduced, it would be harder to determine which ones fit and which risks should be addressed first. In this schema, the high risks should be addressed first, the medium risks should be addressed next, and the low risks should be addressed last, as is customary and intended.
* **Risk Register:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **#** | **Risk** | **Branch** | **Impact** | **Likelihood** | **Risk Score** |
| 1 | Social Engineering | B | Medium | High | 1 |
| 2 | Firewall Penetration | B | High | Low | 4 |
| 3 | Web Server Attacks | M | Medium | High | 2 |
| 4 | Physical Server Attacks | B | High | Low | 5 |
| 5 | Natural Disasters | B | Low - Medium | Low | 10 |
| 6 | Equipment Failure | B | Medium | Low | 8 |
| 7 | Phishing Attacks | B | Medium | Low | 9 |
| 8 | Data Loss | B | High | Medium | 3 |
| 9 | Unauthorized Database Interaction | B | High | Low | 6 |
| 10 | Unauthorized Terminal Interaction | R | Medium | Medium | 7 |

**Table of Contents:**

1. **Executive Summary:** Page 1
2. **Asset Register & Discussion:** Pages 2 – 3
3. **Threat Register & Discussion:** Pages 4 – 5
4. **Vulnerability Register & Discussion:** Pages 6 – 7
5. **Risk Assessment & Discussion:** Page 8
6. **Prioritization of Risks:** Pages 9 – 10