Risk Management Project

**Company Products**

VoltronMessenger

The primary source of revenue for the company. This service handles secure electronic medical messages that originate from its customers, such as large hospitals, which are then routed to receiving customers such as clinics.

VoltronPay

Web portal used by many of the company’s VoltronMessenger customers to support the management of secure payments and billings. The VoltronPay web portal, hosted at Health Network production sites, accepts various forms of payments, and interacts with credit card processing organizations.

VoltronConnect

An online directory that list doctors, clinics, and other medicals facilities to allow Health Network customers to find the right type of care at the right locations. It contains doctors’ personal information, world addresses, medical certifications, and types f services that the doctors and clinics offer. Doctors are given credentials and can update the information in their profile.

**Infrastructure**

The company health network has 600 employees and has an annual revenue of $500 million. The company has four product lines namely; VoltronMessenger, VoltronPay, and VoltronConnect.

The three products give an integrated platform to store customer data, Doctors information, clinic details, secure billing, and payments, connect the hospitals and clinics. The integration of the three products is done using HTTPS. Health Network operates in three production data centers that provides high availability across the company’s products. The data centers host about 3,000 production servers, and Health Network maintains 650rate laptops and company – issued mobile devices for its employees.

**Scope and Purpose**

The purpose of the risk management plan is to secure the web servers and browsers of VoltronMessenger, VoltronPay, and VoltronConnect. Also, updating the risk assessment based on: (i) on going determinations of the effectiveness of security controls in organizational information systems or environments of operation; (ii) changes to information systems or environments of operations (e.g., changes to hardware, firmware, software; changes to system-specific, hybrid or common controls; changes to mission/business processes.

* Security of the servers
* Security of the web applications
* Availability of the products
* Integrity of the products

**Compliance Laws and Regulations**

1. The development, distribution, and, implantation of written standards of conduct and written politics and procedures that describes and further the organization’s commitment to meeting and exceeding the legal and ethical standards applicable to the organizations.
2. The designation of a chief compliance officer and other appropriate committees and individuals that are responsible for operating and monitoring the compliance program and who report directly to the organization’s chief executive officer and the governing body.
3. The development and delivery of effective employee education and training programs.
4. The development and maintenance of effective lines of communication that allow individuals to report compliance concermns without retaliation, including the ability to anonymously report concerns and complaints
5. The development and implementation of a process to respond to complaints that includes the imposition of appropriate corrective action including discipline f employees when required.
6. The use of internal monitoring and audits to measure compliance and address known deficiencies.
7. Responding appropriately and quickly to detected offense and implementation corrective actions.

**Schedule**

Effectiveness time frame: Tier 1 and tier2 policy related decisions needs to be relevant for extended period since the governance process for policy changes can be time consuming in many organizations. A reassessment conducted to inform a Tier 3 decision on the use of compensating security control for an information system may be relevant only until the next release of the information technology product providing the required security capability.

For Tier 1 and Tier 2 of VoltronMessenger, VoltronPay, VoltronConnect, do a risk evaluation after 3 years. For tier3, do a risk evaluation every 6 months.

**Information Sources**

Document review, interviewing, SWOT analysis, system logs, video cameras, personal checks, technical process flow of the systems, relationship, and dependencies with external providers, and old risk assessment reports to name a few.

**Risk Assessment**

**Assets**

* Hardware
* Servers, company laptops and mobile devices
* Software
* The service that handles the medical messages.
* Information + Connections
* Online directory that lists doctors, clinics, and other medical facilities
* Doctors’ personal information, work addresses, medical certifications, and types of services that the doctors and clinics offer
* Medical messages
* Billings information

All the data of these systems would be proprietary and private data.

**Threats**

* Loss of company data due to hardware being removed from production systems
* Loss of company information on lost or stolen company owned assets, such as mobile devices and laptops
* Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on
* Internet threat due to company products being accessible on the internet
* Insider threats
* Changes in regulatory landscape that may impact operations

**Vulnerabilities**

VoltronMessenger

* Lack of encryption via plaintext
* Lack of updated firewall
* Lack of patches
* Lack of security training and awareness
* Access controls not implemented properly
* Weak passwords

VoltronPay

* Lack of an updated firewall
* No IDS
* No antivirus software
* Lack of updates for the server
* Lack of security training and awareness
* Lack of patches
* Weak passwords
* Access controls not implemented properly

VoltronConnect

* Directory traversal
* Weak password
* Lack of security training and awareness
* Lack of patches
* Access controls not implemented properly

For all the services a major vulnerability would be weak authentication and authorization online. Also, we basically have the same vulnerabilities for all services because they are all online via HTTPS connections.

**Threat Analysis**

Graphical user interface, application

Description automatically generated

Table

Description automatically generated

Table

Description automatically generated

Risk Rating (likelihood x Impact) from Highest to Lowest

1. Internet threats = 100
2. Loss if customers = 80 and Loss of company information = 80
3. Insider threats = 64
4. Loss of data = 50
5. Changes in regulatory landscape = 10

From the threat analysis, it appears that internet threats pose the highest risk to VoltronMessenger, VoltronPay, and VoltronConnect.

**Risk Mitigation**

**Threat + Proposed Mitigation Plan**

The plan is prioritizing countermeasures based on the risk rating scores from the risk assessment.

* **Loss of company data due to hardware being removed from production systems**

Plan: The organization must have a secure server room where only people with special badges can have access.

Action within 1 month

Physical and Technical control implemented

* **Loss of company information within lost or stolen company owned assets, such as mobile devices and laptops**

Plan: Regularly back up the data and information of all assets. All laptops are to have user passwords and data locking systems which cannot be hacked even if the asset is lost. The use of biometrics to control access to the data will also be used.

Action Immediately

Technical Control implemented

* **Loss of customer due to production outages caused by various events, such as natural disaster, change management, unstable software, and so on**

**Plan: The organization will keep** two places of work at different geographical locations. One locations data will be available to the other location, in case of a crisis the load can be shifted to a second location and minimize the impact of the natural disaster. The backup support will be strengthened. The disaster recovery plan will be reviewed on a regular basis.

**Action within 1 week**

Physical, Technical, and Procedural controls implemented

* **Internet threat due to company products being accessible on the Internet**

Plan: Back up internet and perform patches as needed

Action immediately

Technical control implemented

* **Insider threats**

Plan: The authority for data access must be limited and sanctions are required for accessing critical and vulnerable information. The regular monitoring of data transfers and all traffic from different users will be monitored closely. Alerts will be created to highlighted any violations immediately as they occur.

Action within 1 week

Procedural and Technical controls implemented

* **Changes in regulatory landscaper that may impact operations**

Plan: The necessary plan will be made as per changes are asked for.

Actions within 6 months

Procedural Controls implemented

**Cost Benefit Analysis**

The data in this risk management plan is qualitative, so a quantitative cost benefit analysis will not fit well in this case. Therefore, below is a qualitative cost benefit analysis.

**Plan: the organization must have a secure server room where only people with special badge can have access and/or biometrics.**

This migration plan is beneficial to the organization because an attacker would have a harder time accessing the hardware. With RFID and biometrics, the organization can see who has accessed the room and can keep a log.

**Plan: Regularly back up the data and information of all the assets. All laptops are to have user passwords and data locking system which cannot be hacked even if the asset is lost. The use of biometrics to control access to the data will also be used.**

This mitigation plan is beneficial to the organization because when you have backups of data if the data gets lost you will always have a copy. By having biometrics-controlled access, passwords, and data locking systems on all the laptops, it would be extremely difficulty for an attacker to gain access to the sensitive data.

**Plan: The organization will keep two places of work at different geographic locations. One locations data will be available to the other location, in case of a crisis, the load can be shifted to a second location and minimize the impact of the natural disaster. The backup support will be strengthened. The disaster recovery plan will be reviewed on a regular basis.**

This mitigation plan is beneficial to the organization because if a disaster happens at one geographic location, it will most likely not be occurring at the other geographic location. This is like a location backup. If one physical site gets destroyed, there will be another site to carry the load. It is always good to regularly review and update disaster recovery plans.

**Plan: Back up internet and perform patches as needed**

This mitigation plan is beneficial to the organization because when you have backups of data if the data gets lost you will always have a copy. Installing updated patches is always good because patch management resolves vulnerabilities on software and applications that are susceptible to attacks.

**Plan: The authority for data access must be limited and sanctions are required for accessing critical and vulnerable information. The regular monitoring of data transfers and traffic from different users will be monitored closely. Alerts will be created to highlight any violations immediately as they occur.**

This mitigation plan is beneficial to the organization because we do not want random people accessing the organizations data. It is always good to monitor traffic. For example, the organization could utilize Snort to monitor network traffic. It is beneficial for alerts to go off so that the system or person monitoring the traffic has immediate intrusion detection and can stop the attacker.

**Plan: the necessary plan will be made as per changes are asked for.**

The mitigation plan is beneficial to the organization because the organization needs to remain in compliance with state and federal regulations and laws. As we do know the changes in regularly landscape, all we can do is make the plan when changes are asked for by a supervisor.

**Business Impact Analysis / Business Continuity Plan**

**System Description**

VoltronMessenger, VoltronPay, VoltronConnect all utilize HTTPS. Health Network operates in three production data centers that provide high availability across the company’s products. The data centers host about 1,000 production servers. HTTPS uses port 443 and it operates on the application layer of TCP/IP model. HTTPS encrypts all data, so it is very secure. A production server is a server that hosts and employs websites and web applications. It is a component of the complete software and application development environment. Health Network maintains 650 corporate laptops and company issued mobile devices for its employees. Computers are Windows OS and phones are MAC OS.

|  |  |
| --- | --- |
| **System Resource** | **Description** |
| HTTPS websites and applications | Main product that users interact with |
| Production servers | The main servers for the websites and applications |
| Corporate laptops and mobile devices | Main tools that employees do their daily tasks and work with. May contain sensitive data. |

The most critical systems are:

Production servers = Most critical, numbers one priority

HTTPS website and applications: Critical

Corporate laptops and mobile devices: Least critical

|  |  |  |
| --- | --- | --- |
| **System Resource** | **Impact Category** | **Impact Values** |
| Production servers | Cost | Severe |
| HTTPS websites and applications | Cost | Moderate |
| Corporate laptops and mobile devices | Cost | Minimal |

* ***Severe – temp staffing, overtime, fees are greater than $1 million***
* ***Moderate – fines, penalties, liabilities potential $550k***
* ***Minimal – new contracts, supplies $75k***

**Estimated Downtime**

|  |  |  |  |
| --- | --- | --- | --- |
| **System Resource** | **MTD** | **RTO** | **RPO** |
| Production servers | 15 hours | 24 hours | 12 hours |
| HTTPS websites and applications | 30 hours | 35 hours | 12hours |
| Corporate laptops and mobile devices | 50 hours | 90 hours | 12 hours |

**Recovery Time Objective**

|  |  |
| --- | --- |
| **Priority** | **RTO** |
| Production servers | 24 hours (spare equipment or vendor support contracts to fix outage) |
| HTTPS websites and applications | 35 hours (backups fix outage) |
| Corporate laptops and mobile devices | 90 hours (vendor support contracts or spare equipment fix outage) |

References

Guide for Conducting Risk Assessments - NIST. (n.d.). Retrieved November 24, 2021, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

Contingency planning guide for federal information ... - NIST. (n.d.). Retrieved November 24, 2021, from <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>.

Solved scenario you are an information technology ... - Chegg. (n.d.). Retrieved December 1, 2021, from <https://www.chegg.com/homework-help/questions-and-answers/scenario-information-technology-intern-working-health-network-inc-health-network-fictitiou-q30609167>.