GROUP 4

RISK MANAGEMENT

PLAN

INFX 590

Ipek Kaya

Ceren Engin

Project Part 1: Risk Management Plan Outline and Research

Introduction

To identify risks first, we should know all the events related to our project, irrespective of the impact negatively or positively. It can be tracked by project milestones, financial concepts, and limitations and then the threats arise. Simultaneously, looking at the vulnerabilities is highly valuable, and tool analysis helps to achieve this. Reviewing previous or similar projects is also very significant because historical mistakes frequently occur and shed light on issues. It is crucial to note the big challenges and occurrences in earlier efforts in a plan. Lastly, estimating the likelihood and power of a threat can affect the project by means of vulnerabilities as well as assets. A risk's impact can be measured by different values, ranging from low to high.

After identifying and assessing a risk, it is important to now mitigate the found risk(s). Threats and impacts of the risk along with vulnerabilities of the business should be prioritized, evaluated, and implemented in the way of risk acceptance, reduction, transference, or avoidance. The method and model would be opted based on previous project analysis and managers.

Finally, Risk mitigation should be assessed and reviewed after changes are made and mitigated risks are completed. All changes should be controlled and reported to be confident about the result. Although this is the final step, it does not mean the steps won't continue.

Purpose

The purpose of the risk management plan is to define the risks associated with the discovered current threats for Health Network company products and determine what security implements needed for reducing the risks.

Background

- Health Network company has three main products HNetExchange, HNetPay, HNetConnect.
- HNetExchange handles secure electronic medical messages which is also the primary source of revenue for the company.
- HNetPayis a web portal for secure payments and billing.
- HNetConnect has lists of doctors, clinics and other medical facilities to help customers find best fit for their needs. It includes doctors' personal information.
- Health Network company and customers use HTTPS to connect all three of the company's products.

Plan Scope

The scope of the plan includes 1000 production servers in three data centers, 650 corporate networks and company-issued mobile devices for its employees. It focuses on the IT department, network infrastructure, privacy and security.

Basic Risk Management Outline

First, a list of threats should be found to create an outline. In this project, there are loads of found threats and vulnerabilities from the previous plan listed below:

- The company mentions that there is data loss due to removed hardware; the weakness here is obvious, they didn't have backup data and they lost all the information stored in the hardware
- Production outage is another threat that can cause customer loss and explicit security threats. This will cause the company to lose its profit, reputation, and income and potential data leakage.
- Company's employees: if they are not satisfied with their company circumstances, it can be an indispensable threat.
- Changing decisions over the project will harm the whole or some part of the project. Changing the plan of risk management can be the idea.

The cost associated with risk and mitigation should be the suitable ratio of annual profit and assets. It cannot be a low or high amount of income/ profit. A list of recommendations comes next, and needs to be associated specifically for that. Recommendations are listed with the aim of risk mitigation. Then, a cost-benefit analysis (CBA) should be provided to evaluate decisions made for the projects. After this level, reports need to be prepared periodically to evaluate the project.

Summary of Compliance Laws and Regulations

The Health Network company serves healthcare and medical websites which host critical information about patients. For this reason, the company should follow laws

and regulations for secure hosting and having patient information. The company should ensure HIPAA and PCI DSS compliance which cover the privacy of individual health information and security standards of health information. Based on the vulnerabilities and risks the company should focus on those two standards. The standards that the company needs to focus on are explained below;

1- Data Encryption

Data protection is essential for the health network company because it stores individuals' critical health information and identifying information. Therefore, data should be encrypted so any attackers cannot use the information even if they access it. There are some algorithms that the company can use such as 256-bit AES.

2- High-Level Protection

Encryption can protect the data however it is still not adequate for security and privacy. That information is in contact with administrators and third-party partners, therefore, we cannot ensure where the threats are coming from.

Controlling compliance with policies and processes regarding patient information and their implementation authentication reduce risks. In addition, the websites that customers are connecting to should be protected.

3- Auditing and Backups

Health network companies should have a backup plan for securing patient data for any emergency situation. It will cause a critical impact if the company loses patients'

information. Therefore the company must keep copies and those copies must be accessible in any emergency situation.

4- Access Control

Each person's access must be identified and every person should have limited access based on their responsibilities. Customer information should be protected by limiting its accessibility.

5- Security Personnel

A covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.

6- Workstation and Devices Security

The company must implement security policies and procedures to protect workstations and devices. Each person's access to devices must be identified in the policies and procedures. Devices that have critical information must be in a high-security place.

Personal Roles and responsibilities

The organization assign the following roles and responsibilities for their services;

- Data Expert, ensure data that entered in the portal meets with the national medical standards.

- Network Administrator, manage any network outage situations that company might face and networking infrastructure
- Database Administrator, ensure that data is secured and has a backup plan.
- IT department, responsible data encryption.
- Security administers, controls compliance of the company with the policies and procedures.
- Security manager, control device security and personal access.
- Customer administrator, provide support and manage solutions for customer issues such as payment, outage, or updating.

Planning Schedule for Risk Management

First Scheduling Step: Identifying all Risks

- First, we must identify the risks that are present in our business, and then keep a list of them for future reference as well as pinpointing the work/manage level of each task
- As for scheduling, this is preferably done immediately when a risk management process is created or brought to light.

Second Scheduling Step: Identify important assets; Identify specific risks that attack those assets.

- Next in scheduling as well as importance, we must identify our assets and protect those as they are integral to our business

- Protect assets through identifying the specific risks from our list that affect or attack our assets.
- Keeping our assets safe is a priority when it comes to scheduling and order of the rest of the tasks.

Third Scheduling Step: Develop Management Plan for each risk; assign plan and employees to risks

- Divide risks throughout the team and develop plans for each risk to begin managing.
- Begin managing risks (risks against assets first) by scheduling management processes for each risk for a team.

Fourth Scheduling Step: Review and check over risks that are completed and/or avoided. Review remaining tasks and the impact of mitigation

- Lastly, we should review the risks that have been mitigated, as well as continue to look at future risks i.e the next risk to be managed on the schedule
- Also we must review and ensure that mitigated risks are indeed mitigated correctly and without error or without cause for another risk. We must look at the impact that the mitigated risks have on the business as a whole and how mitigating said risks have helped positively or negatively.
- Check up on the lists of remaining risks after discluding the completely mitigated risks

Project Part 2: Risk Assessment Plan Part 1

Purpose of IT Risk Assessment

Risk assessment ensures security in an Information Technology Infrastructure and it strengthens policies within the organization. This risk assessment supplies rules and guidelines for the Health Network by considering the risk management plan. In addition, risks are analyzed and evaluated along with risk controls and their effectiveness. The negative impact created by the discovered threats and vulnerabilities will be mitigated and reduced. This impact can be individuals, the environment, or assets with risk assessment covering all of these listed aspects. By using this assessment the company will increase its security and protect its assets from any attackers or volatile risks.

Scope and Boundaries

The scope of this risk assessment includes security of 1,000 production servers, and Health Network maintains 650 corporate laptops and company-issued mobile devices for its employees that include the assets company/customer information. Scope focuses on four different areas which include the IT system department, security department, Information Technology Infrastructure, and the customer service department. In these areas, scope covers management and security on user accounts and information, increasing security in the company to protect servers, devices, and laptops. This also includes increasing the security on HNetExchange, HNetPay, and HNetConnect products, and controlling the compliance of HIPAA, PCI DSS, and other

necessary compliances. By doing this we can improve the backup plan for the emergency situation in which our assets are threatened.

Data center assets and activities to be assessed

Data centers are an essential technology building meant to centralize the organization's data, IT operations, equipment, and tools. Simply put, all crucial information and tools that should be maintained are gathered in the data center. This means that having a good illustration of data center assets and activities done there is indispensable. Here are some data center assets listed below:

- At first glance, physical or hardware equipment, including routers, switches, firewalls, cables, modems, etc., are assets. Taking care of the data center's software and technology is also significant. In addition, technologies involving asset protections are also assets for the data center.
- Data center components such as servers, computers and network connectivity, monitoring, and repository infrastructure are considered assets.
- Equipment for cooling, airflow, and activities to prevent damages from intentional and unintentional accidents like fire, electrical and power outages are assets for the organization. All these pieces of equipment assist the data center in maintaining data and information; that is to say, they are assets for the company.
- Different centers' locations and geographical situations are known as assets. For instance, the data centers are located in Minneapolis, Portland, and Arlington (next to the central locations); each one possesses buildings, equipment, and employees that count as assets for the organization.

- The company has three products in which all their information, including payments, lists of doctors, clinics, work addresses, and certifications, is stored in the data center; thus, these three products and services count as vital assets for the organization.

Relevant threats and vulnerabilities

In this project, there are loads of found threats and vulnerabilities listed below:

- Threat: Loss of company data due to hardware being removed from production systems

  Vulnerability: No backup data

- Threat: Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops

  Vulnerability: Lack of user management system, lack of mobile device management/policies

- Threat: Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on

  Vulnerability: Lack of Business Impact Analysis and Business Continuity Plan, Lack of compliances

- Threat: Internet threats due to company products being accessible on the Internet

Vulnerability: Firewall configuration, DMZ Zone

- Threat: Insider threats

  Vulnerability: Lack of user management system

- Threat: Changes in regulatory landscape that may impact operations

  Vulnerability: Delayed security implements

Controls

- Data should be regularly replicated as a backup to the cloud to avoid data loss due to hardware failure, hardware removal, and so on. Recovery point objectives must be set and backups must be done according to that.
- User authentication and authorization measures must be set to protect the data from unauthorized access. Mobile Device Management (MDM) solutions must be implemented to devices to track the malicious activity.
- Production outages root causes must be found and take actions to prevent them. Some actions can be listed as below:
  - Disaster Recovery Plan must be prepared in case of natural disasters.
  - Change management system policies must be reviewed and updated if necessary.
  - Unstable software must be detected and be patched or replaced with an alternative.

- HIPAA, PCI DSS and PII compliances must be up to date.

- Firewalls need to be configured to keep them secure. DMZ zone must be created to stop attacker access to the company network through the web server.
- Change management policies must be updated. POAM's must be created for the IT department and every change in the IT infrastructure must be recorded to keep everyone informed.

Key Roles and Responsibilities

Common Control Provider: Selecting control assessors and ensuring they have access to common control providers.

Chief Information Officer: Guide authorizing official decisions

Senior Agency Official for Privacy: Ensure controls implemented properly and compliance with acceptable privacy requirements and they are consistent.

Authorizing Official: Review and approve the assessment plans and determine which ones require immediate action.

Information Owner: Select control accessors based on technical expertise and ensure they have access to the system. Provide support for privacy and security assessments. Determine previous assessments' relevance if any. Resolve the issues found during the assessment.

System Security Officer: Coordinate assessments activities and reports reviewing the security and privacy assessment plans.

System Security Engineer: Review the assessment reports and design remediation plan according to them. Control Assessor: Develop security and privacy assessment plan(s). Create assessment reports reflecting effectiveness of implemented control. Reassess if the corrected controls are weak.

Proposed Schedule Process

The purpose surrounding the following schedule will be based around protecting assets, separating risks, and assessing them adequately.

- Firstly we should begin by separating risks by level of harshness. We find the risks that are most volatile and attack our assets first and then separate the rest accordingly.
    - Time Gauge: 2-4 weeks
- Then we must assign risks to teams or sections where we can assess and mitigate them accurately and/or quickly if needed. In this case we must mitigate the most volatile risks first
    - Time Gauge: 2 weeks
- After risks are mitigated(one or many) we must study the asset or issue to see if the risk helps us or to see how the system or business reacts to the mitigated risk i.e if another is created as a domino effect and so on
    - Time Gauge: 1-2 months depending on volatility
- We continue this cycle as new risks jump to us and in response to risks being worse or better for our system. We continue to study how certain risks affect our assets and repeat the cycle accordingly

- Time Gauge: 1-3 months

The important aspect of creating and scheduling for risk assessment and mitigation is to study the risks and find how they affect our system. Then we mitigate based on the impact that we find the said risks could have. Protection of our assets is at the forefront of this idea. In this case with the business at hand, it is pinnacle to find the risks that heavily impact the heart of our mission or job that the company has

Project Part 3: Risk Mitigation Plan

In the risk assessment plan we identified and evaluated the risks. In the risk mitigation plan, the project team focuses on reducing the impact of the risks that are identified in risk assessment. The risks can be mitigated in various ways:

- Risk avoidance
- Risk sharing
- Risk reduction
- Risk transfer

In this risk mitigation plan the project team will mitigate the risks that are mentioned below;

- Threat: Loss of company data due to hardware being removed from production systems

  Vulnerability: Data backup restore unsuccessful

- Threat: Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops

  Vulnerability: Lack of user management system, lack of mobile device management, security, and policies

- Threat: Loss of customers due to production outages caused by various events, such as natural disasters, change management, unstable software, and so on

  Vulnerability: Lack of Business Impact Analysis and Business Continuity Plan, Lack of compliances

- Threat: Internet threats due to company products being accessible on the Internet

  Vulnerability: Firewall configuration, DMZ Zone

- Threat: Insider threats

  Vulnerability: Lack of user access management

- Threat: Changes in regulatory landscape that may impact operations

  Vulnerability: Delayed security implements

Scopes

- Providing UPS
- Implement of firewall

- Creating DMZ
- Assigning user account manager
- Training technical personal
- Using locks for doors and increasing security in the building such as cameras, and monitoring security guard
- Determine of employees access control
- Creating new policy that is applied compliances
- Creating backup
- Preventing thief for accessing data or assets

Risk Controls

To mitigate the risk, we must identify controls for the related risk and vulnerability pair. We have already done a risk assessment and we will be using the findings from our risk assessment plan. In this section, the controls identified to mitigate the risks will be explained.

Identifying Countermeasures

Threat	**Vulnerability**	**Countermeasures**
Loss of company information on lost or stolen company-owned assets, such as mobile devices and laptops	There is not adequate security to protect assets such as laptop, devices.	Discourage thief to intrude and stole asset Detecting security breaches and control them , including locking doors, cameras, cables for devices, etc.

		Recording available assets
Loss of customers due to production outages caused by power lost	There is no alternative power system There are no technical personnel for managing UPS.	Provide UPS to supply lost power
Loss of power because of lack of technical personals	Employees are not trained about new systems.	Provide training programs for UPS. Assign 2 technical personals for new system.
Loss of data due to Hardware failure/hardware removal	There is no backup	Data should be regularly replicated as a backup. Recovery point objectives must be set.
Loss of customers, loss of repudiation and fines	Lack of compliance	HIPAA, PCI DSS and PII compliances must be applied
Internet threats	Firewall configurations are not complete. No DMZ zone	Firewalls need to be configured. A DMZ zone must be created.

Insider threats	Lack of user access management	User access controls must be set. User management policies must be created.
Changes Affecting Operational impact	Change of business management, Change of employee measures and operation	Meetings and precise research measurements must be made towards making changes to the working landscape. Acquire input from all affected sides(management, employees,upper bosses)

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

Mentioned removing hardware above can be intentional and unintentional. The deliberate purpose would be related to an internal threat; however, the other causes some problems. At first glance, the prevention method that comes to mind is to have a routine backup plan due to data loss prevention. Next can be a miscalculation in not needing hardware, leading the company to data loss. The other probability can be stolen hardware, especially vital hardware, for the company.

As there is a requirement to prioritize countermeasures and stay within an allocated budget, the method opted here is to create a data backup plan. Furthermore, there is no clear information about the amount of data for the company, so an accurate CBA for the backup plan cannot be estimated. What is obvious for the company is to

have a plan for maintaining data so that it would be a need based on the project and the company's budget.

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

There are several methods for preventing stolen assets, including laptops and mobile devices. As discussed above, four outstanding ways can be implemented for risk mitigation; an effortless one to avoid this risk is to discourage an intrusion, making the stolen steps arduous as well as inaccessible. In addition, the possibility of detecting security breaches make companies vulnerable and prone to loss. Since this approach is sufficient in terms of the company's budget and can be its priority, it will be chosen as a countermeasure method in this part. Next prevention method can be recording the available assets and tracking them frequently to thwart the stolen attempt.

Impact of Landscape Changes

The changing of a work environment can happen numerous ways and directly change multiple work factors of the business. Aspects such as employee morale and satisfaction, managerial and employee workload, Work office availability(wiring,furniture etc) are all aspects of risks here. Ways to mitigate risks may include hearing input from all sides and voting on changes, holding meetings to discuss the risks made from said changes, and research on the changes to see past occurrences and how they were handled. These are all based around being proficient and caring towards the impact of changes and how they may affect everyone included. The keys are communication and research in order to learn and mitigate the risks that work landscape changes can

cause. There exists a lot of relevancy towards all levels of work including upper bosses, investors, employees, and managers. It is important during the risk mitigation of changes to focus on including all phases of work and seeing the general consensus on changes before they are implemented. Test implementations can also help and show what could happen as a risk during said change.

Compliances with Global Policies

Under risk mitigation, certain policies and rule sets must be managed and looked at in regards to how certain things can be changed. These global policy groups include HIPAA and PCI DSS. These groups essentially hold down herbal rules and restrictions for how a business can run related to risk management and mitigation.

HIPAA includes protecting citizens and people within the workforce. This includes not discrimination against things like race or sexuality. We have to ensure, especially in areas like landscape changes, that we protect our employees and mitigate risk without impacting things under the HIPAA guidelines. PCI DSS is something referring to payments, credit card/ bank information, and protecting the information related to our employees and bosses. It is important to mitigate risks without endangering the private financial information of our team. In all it is extremely Important to protect the rights of our employees and to assure the safety of these rights during risk management.

Employees Training

The company uses new systems to reduce risk. Technical employees who are responsible for managing the new systems should be trained. This training program

should be completed before the new system is applied. These technical personnel are responsible for monitoring the systems daily and reporting it.

Emergency Power

The company should provide alternate power to supply the lost power. This alternative system will activate itself in 10 minutes when the company loses its power. Technical personnels will manage this transaction and ensure that alternative power is activated. Also, this alternative power can be activated manually. If the system does not detect the power loss, then the technical person will manage the system manually.

Insider Threats

To mitigate insider threats, combination of physical security, personnel awareness, and user access management is the best working approach. However, in this risk mitigation plan we will be focusing on user access controls and user management since we identified some vulnerabilities on the risk assessment.

Access control means that the information is available only to the authorized personnel. Authentication must be used for users to log in with their credentials and their logins and activities must be monitored and recorded. If there is any malicious activity, these records may be used to identify who attended them and to reduce chances of denial by the user.

Old employees may become an insider threat if they can access their company infrastructure using their account after their employment ends with the company. To avoid this, the user credentials must be changed immediately with the coordination of the HR department and the account must be removed/deleted after 90 days.

Internet Threats

The Health Network company uses HTTPS connections for their services. They have web servers to provide web service and it is accessible on the internet. Thus, they are open to internet threats such as attackers. To secure the system, the firewall needs to be configured depending on the company needs. The unused ports must be closed and filtration must be set to control the traffic. For better protection, DMZ zones must be created to block the access to company network infrastructure from outside.

Cost to Implement

Countermeasures	**Initial cost**	**Facility cost**	**Installation cost**	**Training cost**	**Time to implement**
UPS	$3000	$200	$200	$2400	10 days to 1 months
Backup Plan	$1-$4 per GB of data per month	NA	NA	$1000	48 hours for each 100 GB
Security System		$160 for each camera, cable lock and door lock	$ 250 for each camera, cable lock and door lock	$1200	1 or 2 days for installation and being ready to use.

Firewall	$100-$400 a month depending on firewall brand and strength	Down payment is usually included in the monthly rate.	NA	NA	1 to 2 weeks . dependent on amount of networks
DMZ	Depends on numerous factors, usually included in facility cost.	$1000-3000	NA	NA	2-4 weeks dependent on management and upkeep desired
User Access Controls	NA	NA	NA	NA	1-3 months
Delayed security implements	NA	NA	NA	NA	2-3 weeks dependent on system implement

Threat likelihood Impact Matrix

Threats	Likelihood	Impact	Score
Data loss	High value of 100 %	High value of 100	100
Asset stolen In one year there were 8 stolen laptops.	Medium value of 50 %	High value of 100	50
Production Outage Because of power loss there has been 3 outages in one year	High value of 100 %	High value of 100	100
Employees training Personal training program is created but employees are not in new systems	High value of 100 %	Medium value of 50	50
Insider threats User access controls are not set	Medium value of 50%	High value of 100	50

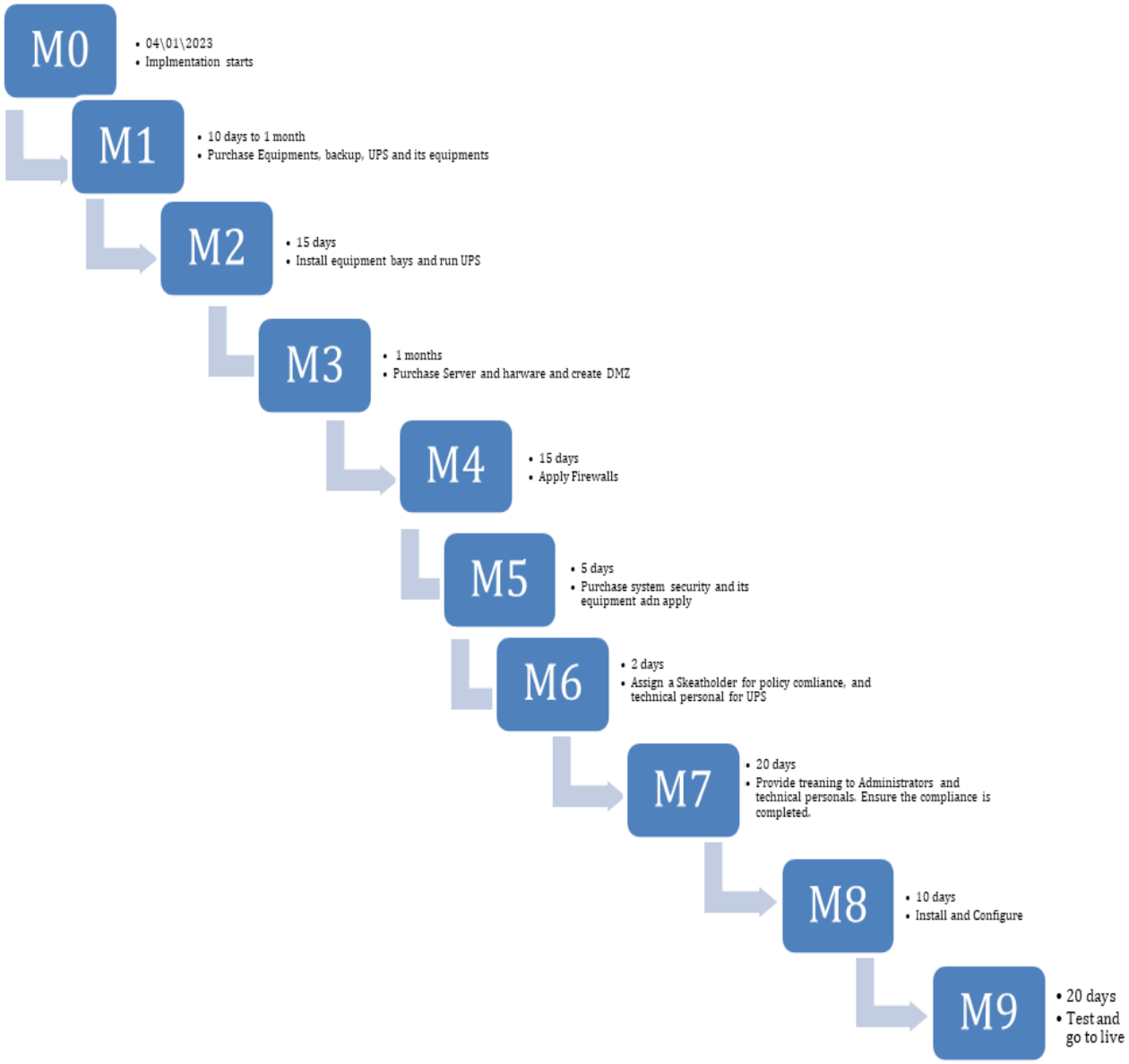
Internet threats The firewall configuration is not complete. There is no DMZ zone.	High value of 100	High value of 100	100
Landscape Changes Business changes affect employee and management mood and workload Morale is also affected	Low value of 25	Medium Value of 50	25
Lack of compliance	Low value of 25%	Medium Value of 50	25

Calculating CBA

	Loss Before Counter measure	**Loss After Counter measure**	**Protected Benefit**	**Cost of Counter measure**	**Counter measure value**	**Result**
Security Breaches	$12,000 if any laptop costs $1500	$2000	$10,000	$410	$9,590	The countermeasure should be implemented.
UPS	$1 million dollars	$200,000	$800,000	$5800	$794,200	The countermeasure should be implemented.
Firewall	**$600,000 dollars**	**$10,000**	**$570,000**	**$300**	**$569,700**	The countermeasure should be

						implemented.
DMZ	**$600,000**	**$10,000**	**$590,000**	**$2000**	**$588,000**	The countermeasure should be implemented.
Backup Plan	**$1 million dollars**	**$20,000**	**$980,000**	**$24,000**	**$956,000**	The countermeasure should be implemented.

Schedule



Mitigation plan is planned to complete between 5 months to 6 months.

Project Part 4: Business Impact Analysis (BIA) and Business Continuity Plan (BCP)

1. Scope

In this part, the first scope of the project is the location of Arlington. Harsh weather conditions prevent the company from working all seasons of the year. Simply put, the possibility of a storm on the East Coast is a threat to the company in winter. Being a primary location for business units can also count as another limitation for the company, as in severe winter having access to the financial, legal, and customer support location would be a challenge. Then, working with virtual private networks possesses its own matters, including losing the connection, significantly affecting the company's mission. Last but not least, regarding the lack of being backed up recently, the new plan should be implemented immediately to store data.

Business Impact Analysis Plan

2. Identifying objectives

Objectives are considered by scopes, thus, as can be seen above:

- The first scope is taking the erratic weather conditions for the Arlington data center into consideration:
    - The direct impact of the loss due to the winter storm includes the loss of customers when the service in the data center stops working, loss of

employees’ access to the server, physical damage, employees' safety, etc. All these should be considered in one business day.

- The indirect impact can be the possibility of being attacked while staff has no access to data, or maybe a bad reputation due to service loss, exchanging using provided services by customers. Regarding the indirect impacts, one business day can be sufficient.

- Accumulating all direct and indirect impacts and losses for three days

- The last step would be the repeating former step for five business days.

- The second one is related to having a single location for some indispensable rules and tasks like supporting customers:

    - The direct impact of having limited access to some services, if storms of fire etc. make damages, progressing would be effortless.

    - The indirect impact for a single location can be the traffic workload in some aspects, leading to delays in customer service and increasing dissatisfaction.

- The third scope would be VPN services:

    - Limited or lack of access is the obvious direct impact of the loss of VPN connections. Another one might be the importance of firewalls for a company's online system. This leads to many different issues called

indirect ones including customer loss, hacker attacks and data breaches or manipulations, benefit loss et.

- Datacenter backup and the significance of applying a new plan is the final objective that should be perused:

    - When a data center does not possess a backed-up plan, the main problem would be the loss of data. This will lead the company to a bad reputation, loss of benefits, and even bankruptcy.

3. Identifying mission-critical business functions and processes

Earlier the four objectives were discussed, and the first one, which is related to harsh weather conditions, should be considered. The main functions in this part can be counted as mission-critical functions since storms can cease some parts of companies' daily activities. Simply put, employees' safety while working in specific locations, the service while not working properly, and access loss while the staff is working or monitoring can seriously matter, leading the company to critical circumstances. Thus, the following list details the steps when a storm happens:

1. Storms happen during winter
2. Roads are closed and pretty hard to commute
3. Employees' safeties are in danger
4. Physical damage can happen
5. Outages can occur

6. Works needed to be done on the site cannot happen

In addition, a virtual private network plays a significant role for data centers during storms. It will meet the needs of caring for employees' safety and supporting customers remotely. However, critical functions causing the VPN service not to work cannot be neglected. Possessing a firewall, 24/7 access to server and data, etc. might be critical functions while VPN services have opted as a superseded procedure. Here, are some steps to follow :

1. Employees can visit the website and use the network to connect
2. Sign in with the account and make sure the account is still private
3. Employees can access the data in the data center
4. Firewalls are working
5. Data should be encrypted in a suitable way
6. Data and activity should be protected
7. Employees start their monitoring and their job.

The last objective's processes can be crucial and critical as well. Lack of data backup can be a game changer, and face the company with various threats and risks. The steps below should be followed:

1. The company uses a third-party company for having a backup.
2. Required data for backup should be recognized (what data should be backed up)

3. Data is stored in every periodic interval (how often data should be backed up)

4. Data should be stored in an appropriate and suitable method.

5. Results and reports will send to the company

6. Employees should test and monitor recovery plans for data and a third-party company

4. BIA Critical Resources

Critical resources in a BIA are essential resources that need to be protected, critical resources can also include helpful things to be used within the BIA. Critical resources that refer to resources needing protection and/or at risk include:

- Sales and income in relation to the company
- Customer info
- Accounting applications
- Customer satisfaction
- Expenses related to company as well as associated risks.

Now, critical resources related to helpful and/or useful resources towards risk mitigation within the plan:

- Employee Satisfaction/turnover
- The strong areas of the IT system in place i.e the senior employees and tech
- Managerial/Business aspects such as high up managers and business team

- The most important critical resources within the company in question is most definitely private customer information and income. We want to prioritize the protection of information among other sensitive aspects of our customers and business as a whole. We focus the BIA on protecting these resources by first gathering them together and then ensuring ways of protection and mitigation against opposing risks.

5. Mapping business functions and processes to IT systems

Company Critical Business Function 1		
Critical Business Function for a winter storm: Employees' safety and their commuting		
Business Process to Complete: Human resources can be at risk while they are commuting toward the company. Also, employees' safety can be in danger by building damage or any physical damage.		
Supporting Elements		
Supporting Activities	**Vital Records**	**Critically**

Storms happen in winter	Insurance, necessary keys	High
Transportation ways are closed	Safe transportation	High
Visit the site	Access to hardware, software and data.	High
Employee's safety are at risk	Insurance	High

Company Critical Business Function 2
Critical Business Function for VPN: Accessing the website and database server
Business Process to Complete: A virtual private network is used while remote access to the server is necessary. However, loads of risks can be faced while working remotely.
Supporting Elements

Supporting Activities	Vital Records	Critically
Visit the website	Software and hardware work	High
Sign into the website	Safe network, password and system	High
Have access to the server	Firewall works	High

Company Critical Business Function 3
Critical Business Function for data backup: Having a data backup
Business Process to Complete: Data should be backed up by the internal section or third-party company, otherwise, data should be at high risk of loss or manipulation.

Supporting Elements		
Supporting Activities	**Vital Records**	**Critically**
Having a third-party company maintain data	Contract, policies and procedures, payment policies	High
Data should be backed up	Continuity of the company	High
How often should be backed up	Policies and procedure, contract	High
Method of backup	Contract, policy	High

6. Maximum acceptable outage (MAO) and impact

Critical Business Resources	**MAO**	**Impact**
Employees	30 minutes	Loss of employees will slow down the company.

		30 minutes of downtime result in a loss of about $20,000
Web server	5 minutes	Loss of direct and indirect sales revenue. Company won't be able to serve their three main products. Five minutes of downtime result in a loss of about $15,000
Database server	5 minutes	Loss of direct and indirect sales revenue. Five minutes of downtime result in a loss of about $10,000
Backup	10 minutes	Loss of data. Ten minutes of downtime result in a loss of about $8,000

7. Recovery point objective (RPO) and recovery time objective (RTO)

Critical and Resources	RTO	RPO
Employees	30 minutes or less	Not applicable
Web Server	5 minutes or less	Not applicable
Database Server	5 minutes or less	Not applicable
Backup	Not applicable	10 minutes or less

Business Continuity Plan

Purpose

The Business Continuity Plan helps the company to decrease the damage from the Winter storm. This plan will be applied when the disaster starts until the disaster is over. The plan will be a guide for the company during the disaster and identify responsibilities, recovery steps, and critical action that company should take during the disaster, etc.

Scope

In this part, the first scope of the project is the location of Arlington. Harsh weather conditions prevent the company from working all seasons of the year. Simply put, the possibility of a storm on the East Coast is a threat to the company in winter. Being a primary location for business units can also count as another limitation for the company, as in severe winter having access to the financial, legal, and customer support location would be a challenge. Then, working with virtual private networks

possesses its own matters, including losing the connection, significantly affecting the company's mission. Last but not least, regarding the lack of being backed up recently, the new plan should be implemented immediately to store data.

Planning Principles

The company will provide a safety area for the personnel. The operation will continue when the disaster starts until 5 days after the disaster is over. Foods, extra clothes, supplies and water will be provided by the company until the operation is over. Transmission for the personal will be provided by the company. 10 different transmissions will be taking the personal 2 times in a day.

Priorities

There are three priorities for the company.

- First of all, life safety is the most important priority for the company.
- Web and database servers are the second priority for the company. The employees and teams will make an effort to keep the function of it.
- Backup is the third priority for the company.

System description and architecture

The primary location for Health Network is located in Arlington and contains business units such as Finance, Legal, and Customer Support. Some of the corporate systems, such as the payroll and accounting applications, are located only in the corporate

offices. VPN is available for each corporation location to access other two corporate offices and the production data center.

Employees are crucial for the Health Network because for the system functioning since its functions are people based. Database center is necessary for the business function such as patient information or payroll information etc. It is very important for employees to access the corporate locations and production data center remotely in case of Winter storms hitting through VPNs. Thus, web servers also have a crucial role during the Winter storm to keep business running. Also, they must keep running backups because data is very important for the company and data loss would be a big disaster.

BCP Teams

Teams	**Responsibilities**
EMT	This team includes 3 senior managers. They are responsible for leading the recovery of the system.
DAT	This team includes 3 IT personnel and 2 facility personnel. Team is responsible to collect the data of damage from the winter storm and report it to team EMT.
TRT	This team includes 4 IT personnel to

	recover the database and WEB server. If there are other IT critical resources during the disaster, they have responsibility to recover the IT resources. They are allowed to assign extra personnel who have necessary technical knowledge.

Notification and Activation Phase

Winter storms are expected disasters and companies and individuals receive warnings when it is likely to occur. Thus, the notification and activation phase must start according to forecasts received.

TIME FRAME	**ACTIONS**
96 hours winter storm stage 4	Inform personnel that a winter storm can hit within 96 hours. Begin general cleanup outside to ensure that pipes and other systems are protected from freezing. Review steps and responsibilities for other stages
72 hours winter storm stage 3	Review the supply list and make sure all needed supplies are available. Make sure the precautions taken for power outages and server room temperature changes.
48 hours winter storm stage 2	Notify the storm crew that they are on call. Release nonessential personnel. Test backup generators.

24 hours winter storm stage 1	Bring the storm crew on site and release other personnel.

BCP coordinator must be notified first. BCP coordinator must notify EMT, DAT and TRT team leaders and team leaders must notify the teams. The DAT team must complete Damage Assessment Procedure and report it to the BCP coordinator. Then, data passes through the EMT leader and they determine the extent of the damage working together with the BCP coordinator. After, the EMT lead determines what to do and the TRT team begins the recovery process.

BCP coordinator must activate the plan if there are valid reasons such as:

- Safety of personnel.
- Loss of operations affecting one or more CBFs.
- Damage of buildings affected CBFs result of Winter storm.
- Winter Storm hits.

Recovery and Reconstitution Phases of the BCP

The purpose of these BCP phases include recovering critical resources and identifying steps to recover themselves as a whole. Through this phase, the business re-evaluates its critical resources and implements processes to get back to where it needs to be. The main general resources needed to go about this phase includes having adequate employees, high end equipment, the data of critical resources, and surveys of customers.

The main goals are ensuring adequate employee availability to make sure tasks can be completed, making sure the business has strong equipment that can assist where needed, making sure we have the correct data and that we protect said data. Another good idea for recovery in a BCP is surveying customers about their experience and about what they may have lost or gained. All of these things are essential aspects of recovery and reconstitution in a BCP. Naturally,we're using our critical resources, to protect and recover *other* critical resources. Through doing this we can adequately make an attempt of recovery from risks and issues tackled within a business continuity plan.

BCP Training and Testing

The company ought to provide different workplace training programs in order to maintain the company's assets, profits, reputation, and resources like employees, human resources, properties, etc. This leads company's to survive in a competitive market. The more company succeeds in training employees, the better they can behave in critical circumstances. To do that, the company must initially recognize its business requirements and needs, hazards, limitations, and strengths. Then, consider employees and their skills, knowledge, or weaknesses, whether they are aware of the dangers and problems ahead or not. Next would be considering the suitable plan or program for training and courageous staff to participate in the training. After that, controlling and

monitoring the consequence of training is needed, leading the company to start the Testing phase.

Testing phase always comes after the Training part in order to check and see the result of the training. This phase requires different methods and procedures based on the company's prerequisites. Outcomes lead the company to start another step or back to the training phase. The more employees are prepared for an emergency situation, the better the company can continue its goals. Testing can be quizzes, surprise inspections, training other novices, etc. While testing, the weaknesses of training programs will be notified and corrected by the monitoring team.

Furthermore, testing assists managers and leaders in finding drawbacks of different sections of the company and consider a backed-up plan for that parts and aspects. In addition, training should be easy to understand for all employees, and testing can prove how convenient they are and familiar with critical concepts. Testing determines that if the training does not meet staff meets, there is an indispensable shortage in the training phase.

Safety of employees:

Safety training requirements mainly vary by frequency and content. As hurricane and storm occur every winter, providing different training, including classes and other tools based on the company's budget, play a significant role in maintaining human resources. Tools can also vary, like simulations, using gamification to staff have been faced with the situation. The best method for testing employee safety might be using the simulation method, facing the team with similar circumstances before, during, and after

storms and asking them for some tasks to evaluate their performance and reactions. Testing how they can assist themselves, and other colleagues can keep tools and assets like data under storm hazard pressure.

Web and Data server:

Training and testing in this section can be in two parts:

1. Training and testing employees

2. Training and testing systems

Employees first should be trained in all physical aspects of the databases, and what should be done to maintain and utilize cables, tools, devices, etc. Maybe new devices need new instructions, so adequate knowledge of utility usage should be implemented in training and testing.

Systems should be tested in terms of consistency, isolation, durability, transactions, and so on. Testing related to the system and database should contain a specific interval and repeats frequently. Staff working with databases need to be trained on how to test systems, the web, and databases. Testing can occur randomly from a small part of the database or contain many aspects.

What should not be neglected is to provide a testing environment and implement all training and testing phases there since there is a possibility of damage or loss while employees have been trained or testing what they have been taught. Preparing a suitable environment, running the test, and checking and validating the results will help

leaders understand their database and employees' skills, knowledge, and weaknesses. Skipping testing of databases will cause massive losses, leading the company to failure.

Backup Plan:

This part can be similar to the server and database in terms of training and testing plans for the company. The problem in this part is there is no backup plan. So for the company, the first training and testing plan should consider the data is not backed up; what can they do? What should be the pros and cons of not having a backed-up plan? Creating an environment and implementing various methods can be substituted for not having a backup plan might work in some parts.

The second step is to point out the steps that there is a backed-up plan; what kind of skills should be taught, and what should be their testing phase? Data backup will be tested, and results illustrate the insight into application performance under defined scenarios. The software of the company, methods of data repository, data integration, confidentiality, etc. should be tested. Also, employees working with data servers and backup must possess sufficient knowledge of their tasks. Their knowledge should be tested; if there is a lack of knowledge in some part, they must have been taught and trained.

BIA and BCP Conclusion

In its entirety, the BCP plan is essentially useful for ensuring the continuation and liveliness of a company after a large risk mitigation or instance. The plan ensures quality of business, recovery and protection of critical resources, and employee/customer

satisfaction in the future. In terms of a BCP's role in a risk management plan, it's extremely important and wraps up how the business will continue forward. Without a proper BCP, a company might be in the dark about how to move on and 'save' their business and/or resources. All of these factors go to show how essential a BCP is.

As for a BIA, this part of a risk management plan is also quite essential in its own right. It is used mainly for analyzing the changes and impacts that risk actions have on the business. The BIA examines the general impacts and how the business can react correctly in a direction that will help the business and protect it. In accordance with each other, a BCP and BIA are extremely crucial to the analysis and continuation of a business in regard to the handling of risks and affected resources.

Work Cited

HHS, The *Standards for Privacy of Individually Identifiable Health Information* (“Privacy Rule”)

https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

HHS, The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule)

https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

The Risk Management Process

https://www.migso-pcubed.com/blog/pmo-project-delivery/four-step-risk-management-process/

Admin. “5 Types of Equipment Your Data Center Must Have.” *RackSolutions*, RackSolutions, 30 Oct. 2020, https://www.racksolutions.com/news/blog/most-important-data-center-equipment/.

Difference Between Quantitative and Qualitative Risk Analysis:

https://www.youtube.com/watch?v=CPZ_JVsa3nQ

.“Data Center Design Best Practices & Components.” *CDW*, https://www.cdw.com/content/cdw/en/articles/datacenter/strategies-and-best-practices-to-data-center-buildouts.html.

"How to Prevent Data Loss from Hardware Failure." *Invenio IT*, https://invenioit.com/continuity/prevent-data-loss-from-hardware-failure/

NIST Risk Management Framework Quick Start Guide, ROLES AND RESPONSIBILITIES CROSSWALK (October 1, 2021) https://csrc.nist.gov/CSRC/media/Projects/risk-management/documents/Additional%20Resources/NIST%20RMF%20Roles%20and%20Responsibilities%20Crosswalk.pdf

"What Is Mobile Device Management?" IBM, 1 Oct. 2015, https://www.ibm.com/topics/mobile-device-management.

7 Ways to Protect Fixed Assets against Theft - Tool Tracking Software. https://gocodes.com/7-ways-to-protect-fixed-assets-against-theft/.

Bader, Sarah. "Balancing Investment in Data Backup with the Cost of Data Loss: Rewind." *Rewind Backups*, 15 June 2022, https://rewind.com/blog/data-backup-cost/#:~:text=A%20business%20may%20pay%20as,the%20cost%20of%20data%20loss.

NIST SP 800-53

https://www.nist.gov/privacy-framework/nist-sp-800-53

Matthew McGill & Trevor Meers. “Matthew McGill & Trevor Meers.” Pratum, https://pratum.com/blog/443-risk-assessment-likelihood-impact.

How to Mitigate Insider Threats: Strategies That Work: IEEE Computer Society. https://www.computer.org/publications/tech-news/trends/how-to-mitigate-insider-threats-strategies-that-work.

“Authentication vs. Access Controls vs. Authorization.” Technology Concepts Group International, 4 Apr. 2020, https://technologyconcepts.com/authentication-vs-access-controls-vs-authorization/.

CISCO GPL 2022 https://itprice.com/cisco-gpl/dmz

Goldstein, Murray, and Murray GoldsteinVice President. “Murray Goldstein.” Cox BLUE, https://www.coxblue.com/9-critical-functions-of-a-strong-business-continuity-plan/.

Business Continuity Plan (BCP) Template Checklist https://public-library.safetyculture.io/products/business-continuity-plan-bcp-template?amp_dev=a9c3f36b-885a-445e-ab65-f7b132156e56&sid=1669489110798

ISMS Business Continuity Plan

https://iso-docs.com/products/business-continuity-plan-isms-27001

Business Continuity Planning Template

https://cloudaccountingkingston.co.uk/business-continuity-planning-template/

Regan, Rea. “What Is Workplace Safety Training and Why Do You Need It?” Connecteam, 29 Aug. 2022, https://connecteam.com/workplace-safety-training-need/#:~:text=Workplace%20safety%20training%20is%20a,them%2C%20and%20deal%20with%20incidents.

“Testing Employee Safety.” SimplifyTraining, https://simplifytraining.com/category/testing-employee-safety/.

Sachin, et al. “Database Testing Complete Guide (Why, What, and How to Test Data).” Software Testing Help, 5 Dec. 2022, https://www.softwaretestinghelp.com/database-testing-process/.

Hamilton, Thomas. “Database (Data) Testing Tutorial with Sample Test Cases.” Guru99, 29 Oct. 2022, https://www.guru99.com/data-testing.html.