Hikes R Us

Business Continuity Plan

Table of Contents

1.0 Introduction ……3

2.0 Business Impact Analysis ……..4

2.1 Important Functions & Downtime ……4

2.2 Assets and Resources ……4

3.0 Strategy Development ……...6

3.1 Continuity Plans ……6

4.0 Implementation Plan ……..10

5.0 Training and Awareness ……18

6.0 Testing and Maintenance ……22

7.0 Conclusion ……...30

Sources ……...31

1.0 Introduction:

Hikes R Us is a small hiking business located in Glassboro, New Jersey. With a team of 7 employees, Hikes R Us conducts the sale of outdoor equipment in-store and online via our website. Additionally, we provide guided hikes and workshops around the New Jersey and Pennsylvania areas.

Employees as of 11/2/2024:

Business Owner (acts as HR as well)

IT Support and Web Developer

Marketing Specialist & Workshop Coordinator

Inventory and Sales Manager (also does scheduling)

Part-Time Sales Associates (3 in total)

Tour Guide (paid per trip)

2.0 Business Impact Analysis:

2.1 Important Functions & Downtime

Functions and Processes	Maximum Downtime
Customer Payment Processing	1 Hour
Data Retrieval	1 Day
Data Entry	1 Day
Employee hours logging	1 Week
Employee payment process	1 Day
Marketing/Advertising	1 Month
Tour Guidance	1 Day
Inventory ordering/delivery	1 Weeks
Updates/patches for hardware/software	1 Month
Employee Training	1 Week

2.2 Assets and Resources

Assets and Resources	How to Protect/Replace
Employee/Customer data	Keep backups and/or use third-party cloud storage.
Internet Access	Use nearby wireless networks. Have an alternate facility.
Electricity	Have a generator on standby for if power is lost.
Telephone System	● Use cell phones. ● Have backup landline telephones on standby.
Copier	● Have multiple or a secondary copier. ● Arrange for the use of another business's copier.

Financial Records	● Store hard copies and virtual copies. ● Use third-party cloud services. ● Have a schedule of when to back up these records.
Computers	● Have multiple or secondary computers within the facility. ● Have an agreement with another business for the use of their hardware. ● Install anti-virus software. ● Keep updated.
Inventory	● Backstock should be held in a separate facility/warehouse. ● Order more inventory.
Web Server	● Outsource this function to a third-party provider so they can host our website while we still own it. ● Have a redundant web server that takes over if the first one fails. ● Keep updated.
The Building	● Cameras monitor the building 24/7. ● Locks on doors.

3.0 Strategy Development:

3.1 Continuity Plans:

Phone/Internet Failure

How will we keep up with business operations?	● Cell phones will be used for all calls ● Hot spots can be used in the meantime for internet access. ● Use of other Wi-Fi-providing devices
Who must be told and how?	All employees and customers must be informed of the outage and the slow business production during that time.
What is needed for this to work?	● Allowed use of employee's cell phones. ● Wi-Fi dongles ● List of important numbers needed for business operations.

Malware/Ransomware Attack

How will we keep up with business operations?	● Isolate the infected device from the network. ● Scan the rest of the network to locate the spread of malware. ● Acquire other hardware for use until the malware is terminated. ● Use software to detect malware and ransomware.
Who must be told and how?	● All employees must be told by upper management of the situation. ● This should be handled solely by management and business executives since this is a serious situation.
What is needed for this to work?	● Arrange an agreement with another business to use their hardware. ● Employee training to be able to identify and react to signs of malware.

Computer Systems

How will we keep up with business operations?	● Employee-led hikes will still be conducted as regularly scheduled. ● Arrange the use of another business's equipment.
Who must be told and how?	All employees and the partnered business must be notified.
What is needed for this to work?	● Cooperation from the arranged business. ● Surplus of computing devices. ● Storage for old devices.

Data Loss

How will we keep up with business operations?	● There should be data backups including financial records, employee data, and customer data. ● Using the cloud allows for our data to be readily available the majority of the time. ● We will also store data ourselves via our own servers and storage system.
Who must be told and how?	Upper management and the manager on duty should be notified immediately before anyone else to avoid panic.
What is needed for this to work?	● We must have our own storage server and storage drives to be capable of handling all the data. ● We must purchase

Supplies/Inventory Loss

How will we keep up with business operations?	● The business will continue operations of scheduling hikes through the in-person facility or from home if needed. ● Employee lead hikes will continue. ● The sale of the product will be re-established once the product is received.
Who must be told and how?	All employees on duty must be informed right away and the manager in charge should go to the back to start the generator so the business can continue running.
What is needed for this to work?	● We must have a new working generator that is tested regularly. ● Diesel needs to be stored at all times to provide fuel for the generator to operate. ● The manager in charge must make sure there is enough fuel to keep operations running until power is restored.

Power Outage

How will we keep up with business operations?	The business will be back up and running within the hour provided by a diesel generator stored in the back of the building.
Who must be told and how?	All employees on duty must be informed right away and the manager in charge should go to the back to start the generator so the business can continue running.
What is needed for this to work?	● We must have a new working generator that is tested regularly. ● Diesel needs to be stored at all times to provide fuel for the generator to operate. ● The manager in charge must make sure there is enough fuel to keep

	operations running until power is restored.

Natural Disaster

How will we keep up with business operations?	Business operations will continue besides the selling of equipment. Using our online website customers will still be able to book hikes and communicate with our staff to keep business alive until new in-person facilities are acquired.
How will our systems and data be accessed?	Having our data backed up and stored onto the cloud allows us easy access to all information to keep business running. Employees will be given access to use personal computers to continue with booking of hikes.
Who must be told and how?	● All employees must be told right away about what happened and how business will continue from there on. ● Customers will be notified through social media and the website that the facility will be closed until further notice and that the regular business of scheduling hikes will continue.
What is needed for this to work?	● All data must be stored and backed up to the cloud regularly. ● All employees must be up to date and acknowledge they have read and understand the business continuity plan.

4.0 Implementation Plan:

Phone/Internet Failure

In case of a phone or internet failure, the following steps need to be taken:

Who	All employees are present, led by the Inventory and Sales Manager and IT Support team.
What	1. Assess the extent of the outage. 2. Communicate with service providers to determine the cause and estimated time for restoration. 3. Implement alternative communication methods, such as mobile phones 4. Notify customers of any disruptions to service.
When	As soon as the failure is detected.
How	**IT Support Team** 1. Monitor the status of internet service and troubleshoot any issues. 2. Identify and communicate potential workarounds for employees, such as using personal hotspots. **Inventory and Sales Manager** 1. Inform staff about alternative communication methods and ensure they have access to necessary tools. 2. Coordinate with employees to manage customer inquiries and sales processes during the outage.
Where	The initial assessment will be conducted in the office if accessible; otherwise, the team may communicate remotely through personal devices or via Microsoft Teams to ensure everyone is informed.

Malware/Ransomware Attack

In case of a malware or ransomware attack, the following steps need to be taken:

Who	All employees present, led by the IT Support team and Web Developer.
What	1. Assess the extent of the attack. 2. Isolate the affected systems to prevent further spread. 3. Initiate recovery procedures to secure data and restore operations.
When	As soon as the attack is detected.
How	**IT Support Team** 1. Investigate the attack vector and determine the scope of the compromise. 2. Disconnect infected devices from the network. 3. Use anti-virus and malware detection software to assess the attack. 4. Restore affected data from secure backups. 5. Notify employees about the incident and required actions. **Web Developer** 1. Assess the impact on the website and online services. 2. Collaborate with the IT Support team to restore website functionality. 3. Implement security enhancements to prevent future attacks. 4. Communicate with the Business Owner and Marketing Specialist regarding the status of the website and any necessary updates for customers.
Where	Actions will be taken primarily in the office; however, coordination may also occur via Microsoft Teams if employees are remote.

Computer Systems

In case of a computer systems failure, the following steps will be taken:

Who?	All employees present, led by the IT Support team and Web Developer.
What?	1. Assess the effect of the failure on all operational areas, including sales, inventory management, and online services. 2. Identify critical systems affected (ex. POS systems, inventory management software) and prioritize recovery efforts. 3. Establish a clear recovery plan, detailing which systems need immediate attention and the sequence of restoration.
When?	As soon as the failure is detected.
How?	**IT Support Team** 1. Investigate the cause of the computer system failure to determine the effect on critical business functions. 2. Disconnect any impacted devices if necessary to prevent further issues. 3. Restore affected systems from secure backups, verifying the integrity and completeness of recovered data. 4. Notify all employees about the system's status, including any temporary workaround or adjustments during recovery. **Web Developer** 1. Assess any impact on the website and online store, verifying that customer-focused services are functioning properly. 2. Coordinate with IT Support to fully restore website functionality if impacted. 3. Apply updates or security patches to strengthen systems and minimize the risk of future failures.

Where?	Actions will be conducted in the office; with further communications via Microsoft Teams.

Data Loss

In case of data loss, the following steps will be taken:

Who?	All employees present, led by the IT Support team.
What?	1. Identify the scope of data loss, including which systems and files are affected. 2. Determine whether the loss was due to accidental deletion, system failure, or a cyber incident. 3. Assess the integrity of existing data and identify any potential security risks. 4. Initiate data recovery procedures using secure backups and recovery tools. 5. Communicate with affected employees regarding the status of the data and any necessary action they need to take.
When?	As soon as the data loss is detected.
How?	**IT Support Team** 1. Investigate the data loss incident to determine its cause and effect. 2. Initiate data recovery protocols utilizing backup systems and recovery software. 3. Ensure that systems are secure and free from any threats before restoring data. 4. Communicate with all employees to inform them about the incident and provide guidance on any necessary changes in their workflow. **Web Developer** 1. Collaborate with the IT Support team to assess the impact on web-based services and data. 2. Ensure that website functionalities

	reliant on recovered data are restored quickly. 3. Implement additional security measures to protect against future data loss incidents.
Where?	Actions will be conducted in the office; with further communications via Microsoft Teams.

Supplies/Inventory Loss

In case of a supplies & inventory loss, the following steps will be taken:

Who	Led by the Inventory and Sales Manager, with help from the Business Owner and Sales Associates.
What	1. Evaluate the impact of the inventory loss and identify any critical items that need immediate restocking. 2. Investigate the cause of the loss, such as theft, damage, or supply chain delay. 3. Arrange for replacement orders for essential items. 4. Inform customers of any delays or unavailability of affected products.
When	As soon as the shortage or inventory loss is detected.
How	**Inventory and Sales Manager** 1. Conduct an initial inventory check to assess the affected items and determine the extent of the loss. 2. Contact suppliers to expedite restocking of critical products if necessary. 3. Update the inventory system to maintain accurate stock levels. 4. Communicate inventory issues to the Business Owner and coordinate any necessary customer notifications. **Business Owner** 1. Approve emergency funds or budget

	adjustments if needed to prioritize essential stock replenishment. 2. Determine customer price adjustments if the inventory issues impact sales for an extended period. **Sales Associate (if needed)** 1. Assist with physical counts and provide support during the assessment of missing or damaged items. 2. Report and unusual findings that may help clarify the cause of the inventory loss.
Where	The inventory assessment and response are conducted in the office, with communication with supplies and customers via phone.

Power Outage

In case of data loss, the following steps will be taken:

Who	All employees present, led by on-duty Manager and IT Support Team, with oversight from the Business Owner
What	1. Assess the situation and determine the expected duration of the outage. 2. Activate backup power and ensure all essential operations can continue. 3. Communicate with employees about the status of the power outage and any necessary changes to operations. 4. Decide whether to close the business or adjust staffing based on the severity of the outage.
When	As soon as the power outage is detected.
How	**Inventory and Sales Manager** 1. Activate backup power (generator). 2. Ensure alternative arrangements for sales. 3. Monitor inventory levels and supply access during the outage. **IT Support Team**

	1. Ensure that critical systems remain operational with backup power. 2. Monitor any IT systems for issues related to power loss. **Business Owner** 1. Communicate with staff about the situation and any operational changes. 2. Make decisions regarding customer notification and business closing until power is restored.
Where	Communication will occur on-site. Communication may also occur over mobile devices if office systems are impacted.

Natural Disaster

In case of a natural disaster, the following steps will be taken:

Who?	All employees present, led by the Business Owner and Inventory & Sales Manager, with additional help from IT Support & Web Developer if systems are impacted.
What?	1. Secure the physical premises if safe to do so. 2. Confirm the safety and well-being of all employees. 3. Assess damage to physical assets. 4. Determine any immediate actions required for business continuity such as relocating to a safer location.
When?	As soon as it is safe and practical to address the situation following the disaster.
How?	**Business Owner** 1. Communicate with all employees to confirm their safety 2. Oversee evacuation procedures if necessary 3. Decide on temporary closure or relocation **Inventory and Sales Manager** 1. Assess the status of store inventory

	and supplies. 2. Organize any necessary moves of valuable assets. 3. Assist with securing the office if possible. **IT Support Team** 1. Evaluate the status of electronic systems and backups 2. Ensure critical data and systems are protected and operational 3. If necessary, prepare the website to communicate temporary closure or service delays.
Where?	The initial response will take place at the office if it is safe to remain. If the office is inaccessible communication will take place on Microsoft Teams and mobile devices, depending on available communication options.

5.0 Training and Awareness:

Hikes R US, is focused on establishing clear communication to ensure all employees are well prepared to respond effectively during an emergency. The following section outlines the training and communication procedures to support consistent and confident interactions with key external contacts in times of crisis.

Employee Training

What training programs will be implemented to prepare employees for emergencies?	● Business Continuity Awareness Training: All employees will undergo annual training to understand the Business Continuity Plan (BCP) and their specific roles during a disruption. This training will cover emergency procedures, communication protocols, and resource access. ● Crisis Response Simulation Drills: Regular simulation exercises will be conducted at least bi-annually to practice the BCP. These drills will prepare employees for various scenarios, such as cyber-attacks and natural disasters. ● Department-Specific Training: Tailored training sessions will address the unique responsibilities of each department during a disruption, ensuring that every team understands their critical roles in the recovery process.

Media Communication

Who?	The Business Owner is the primary spokesperson for media interaction, with the Marketing Specialist available to assist with message preparation and distribution if necessary.
What?	1. Prepare and distribute written statements 2. Respond to media inquiries
When?	Media communication should occur after gathering initial facts and formulating a response strategy.
How?	1. Communications should be prepared to ensure messaging is clear and consistent with the company's image. 2. All communications must be approved by the Marketing specialist before distribution.
Where?	1. Statements can be emailed to media outlets. 2. Inquiries can be handled via phone or email.

Law Enforcement Communication

Who?	The Business Owner is the primary spokesperson for law enforcement, with support from IT as needed.
What?	1. Report incidents that may require law enforcement involvement. 2. Provide any necessary documentation 3. Cooperate fully during investigations
When?	Communication with law enforcement should occur immediately following any incident that requires their involvement.
How?	**Business Owner** 1. Responsible for contacting law

	enforcement 2. Relay critical information about the incident 3. Ensure all relevant details are communicated. **IT Support Team** 1. Provide technical support and any relevant information regarding systems or data breaches if applicable.
Where?	Initial communication can be conducted via phone or in person at the office depending on the nature of the incident.

Public Communication

Who?	The Business Owner is the primary spokesperson for all public communications.
What?	Communicate essential information regarding the incident, including safety measures, operational changes, and updates to customers.
When?	Public communication should occur as soon as accurate information is available and a response strategy is created.
How?	**Business Owner** 1. Drafts and distributes public statements or updates through the company's website and social media pages. **Marketing Specialist** 1. Assists with crafting messages to ensure clarity and relevance for public audiences.
Where?	Public updates can be posted on the Hikes R Us website and shared via social media platforms to reach customers.

Client Communication

Who?	The Business Owner and Marketing Specialist will manage communication with clients.
What?	Provide clients with timely updates regarding disruptions, including changes to services, safety protocols, and next steps.
When?	Communication should occur as soon as possible after the incident has been assessed and appropriate information is available.
How?	**Business Owner** 1. Personally reaches out to customers as needed and oversees communication strategies. **Marketing Specialist** 2. Sends emails or messages through the company's online booking system to notify all customers about changes in services or operations.
Where?	Client communications can be conducted via email, phone calls, or through the company's booking system to ensure clients receive direct updates.

6.0 Testing and Maintenance:

Hikes R Us is committed to ensuring the availability of our systems and the integrity of our continuity plans. **Hikes R Us has deemed that across all continuity plans, there will be testing held on an annual basis, at the beginning of the second quarter each year. This testing will last approximately half of the second quarter to compensate for all business continuity plans.** The justification for this decision is based on collected sales data, which has demonstrated to the company that the business sees an increase in revenue during the middle of the second quarter on a yearly basis. To ensure the company can continue business in the event of an incident, conducting testing for all parts of the business continuity plan is crucial.

The company has considered the complexity of the system environment and physical retail stores and has opted to look at each continuity plan on a case-by-case basis throughout the year, for both testing and maintenance.

Testing and maintenance will be overseen by the President of Hikes R Us, and testing will be conducted by the IT professionals within the company. Employees from other departments will be notified if needed.

Changes to the testing documentation should be made whenever there are any shortcomings discovered through testing and/or maintenance. When these changes are made, they should be recorded within the version control of the continuity plan, and should be denoted as a minor change (using a 0.1 scale), and denoted as a major change (using a 1.0 scale). For instance, versions 1.0, 1.1, 1.2, 2.0, etc.

For any changes that are identified as urgent and must be fixed immediately, the IT employees are allowed to submit a change request. Change requests are reviewed by the IT team and President, and can be rejected if the group has objections.

The individual testing timelines and maintenance timelines have been detailed below:

Phone/Internet Failure

Testing Timeline	Testing will be conducted during the first week of November each year. In preparation for the holiday season, as well as a reduction in booked hiking trips, the company has deemed that the business must have access to the Internet and phones, as the company will be conducting business primarily indoors. **- AND -** Testing will be conducted after the acquisition and implementation of newly acquired phone/Internet systems, but before the systems go live into production. This is meant to ensure the systems are available in the event of an emergency before being introduced to the company's production system environment.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of inadequate resources in retail locations (phones, routers, employees), limited network bandwidth, and changes to the local environment (e.g. expected downtime due to phone company maintenance). There is no limit to this maintenance, as it will be evaluated on a case-by-case basis. The choice of conducting simulations or drills is evaluated on a case-by-case basis.

Malware/Ransomware Attack

Testing Timeline	Testing will be conducted during the second week of November each year. In preparation for the holiday shopping season, the company has evaluated this time as the most critical. Testing at this time allows the business to get an accurate read of the efficacy of the plan as close to the shopping season as possible. This ensures the business can manage an attack, even during peak business months.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of outdated systems, limited IT staff, a change to the company's cyber-insurance plan (if acquired), and significant changes to the company's system environment. Due to the exhaustiveness of testing this continuity plan, the company has allowed 3 maintenance windows throughout the calendar year as acceptable for ensuring the plan is adequate. Maintenance windows can be used on a case-by-case basis. A simulation will be conducted at each maintenance window.

Computer Systems

Testing Timeline	Testing will be conducted during the first week of October each year. As the peak hiking season begins to draw to a close, the company must ensure its computer systems are adequate for the hiking off-season, as business operations prepare for primarily indoor business.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of outdated systems, limited IT staff, and newly acquired systems deployed on a massive scale (e.g. new workstations in each retail store). Due to the exhaustiveness of this maintenance, the company has allowed 2 maintenance windows throughout the calendar year. One practice drill and one simulation can be used, as each poses a different set of operations the company must conduct. Maintenance windows can be used on a case-by-case basis, but are encouraged to be used during non-peak business time (e.g. middle of winter).

Data Loss

Testing Timeline	Testing will be conducted during the last week of October each year. Performing testing at this time is critical, as the company must ensure that any data loss that has occurred (e.g. ransomware attack) can be restored if an attack occurs. This testing occurs only a few weeks after the computer system testing, meaning that the continuity plan should be validated and good to go.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of outdated systems, limited IT staff, new types of data being collected, new data classifications, and federal/state regulations. There is no limit to this maintenance, as data is one of the most critical assets for the company. The continuity plan must be prepared to adjust at a moment's notice. The choice of conducting a simulation or drill is evaluated on a case-by-case basis, however, the company is encouraged to use a mixture of both.

Supplies/Inventory Outage

Testing Timeline	Testing will be conducted during the first week of July each year. While this is not far from the annual testing period, the continuity plan must be validated before the holiday shopping season well in advance. Performing at this time allows the business to identify any issues, and address them before inventory is ordered.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of supply chain issues, unforeseen increases in business, fashion industry shifts, world events, limited staff, and inadequate inventory management. Due to the exhaustiveness of this maintenance, the company has allowed 2 maintenance windows each calendar year. The maintenance windows are specifically designated for each of the testing sessions throughout the year, with the intent of making improvements to the plan after testing has concluded. A simulation should be used to conduct this testing, as the company has not allotted any inventory/money to ensure this plan is effective.

Power Outage

Testing Timeline	Testing will be conducted during the first week of September each year. In preparation for peak hurricane season (typically occurring during the autumn season), it is crucial that the company is prepared for any potential power outages. Conducting testing at this time allows the company to be fully prepared for this extreme weather.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of fluctuations in energy costs, changed weather patterns, local environmental events, power company maintenance, and building renovations. Due to the exhaustiveness of this maintenance, the company has allowed 2 maintenance windows each calendar year. The maintenance windows are specifically designated for each of the testing sessions throughout the year, with the intent of making improvements to the plan after testing has concluded. A simulation should be used to conduct this testing, as the company has not allotted any inventory/money to ensure this plan is effective.

Natural Disaster

Testing Timeline	Testing will be conducted during the first and second weeks of September. The timing is intended to align with power outage testing, as both are connected to one another (most natural disasters, if extreme enough, will lead to a loss of power. Testing is conducted for two weeks to compensate for the length of testing.
Maintenance Timeline	Ensuring the efficacy of this continuity plan, the business is prepared to make adjustments to this plan as shortcomings/adjustments are identified from the business' continuous expansion in scale and scope. Shortcomings/adjustments consist of world events, natural disaster seasons, and local events. Due to the exhaustiveness of this maintenance, the company has allowed 1 maintenance window each calendar year. The maintenance window is specifically designated for the annual testing session. A practice drill will be used to validate this maintenance, as conducting a simulation would be too expensive.

7.0 Conclusion:

Hikes R Us considers its business continuity plan as one of the most critical components of the business. The plan is thorough and encompasses all components of the business, everything from how to continue business operations following a natural disaster, to handling a ransomware incident.

The most critical components of the business continuity plan are the “Phone/Internet Failure”, “Data Loss”, and “Supplies/Inventory Outage” continuity plans. While each of the continuity plans are essential to ensuring the business can continue to be successful, these continuity plans are critical to conducting business, even in its most basic form. With these business functionalities being unavailable (and their plans being unavailable as well), the company cannot conduct business at all, as there would be nothing to sell!

Having a business continuity plan allows the company to be prepared in the event of any of the emergencies above occurring. It demonstrates to other vendors that the company values their availability (good for profits), as well as the company itself (keeps employees employed as well as customers happy). Including a business continuity plan in a company’s culture mitigates risks and prepares the business for the eventuality of any of these events occurring. Most importantly, customers feel more inclined to shop at Hikes R Us, as it establishes their promise to make the customer satisfied.

Nonetheless, having this plan will ensure long-term success for Hikes R Us. By being prepared for any relevant unfortunate events, Hikes R Us stands against the many factors that prevent a business from being able to operate. Without having a plan, the company would likely fail, far beyond the point of recovery. In the cybersecurity world, it is always a matter of when, not if, which enforces the importance of preparedness. With this plan, Hikes R Us builds and sustains long-term resiliency.

Sources

https://canvas.rowan.edu/courses/4122928/files/297444256?wrap=1