DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN

for

CYBER ATTACKS

www.savorysauce.com

Savory Sauce's Disaster Recovery and Business Continuity Plan

Agbai Obasi, Rajani Shrestha, Sadhana Narasimharaj, Sujitha Govindasamy

Department of Information System Security Management,

Concordia University of Edmonton.

ISSM 551(C): Disaster Recovery and Business Continuity

Instructor: Dr. Shawn Thompson

26th November, 2023

Savory Sauce Contingency Plan Revision History

REVISION	DATE	NAME	DESCRIPTION
1.0	09-09-2023	Agbai Obasi	A draft version of this document, intended for utilization during pre-test planning meeting(s)
2.0	15-09-2023	Rajani Shrestha	The exercise version of this document is intended for use during testing.
3. 0	23-09-2023	Sadhana Narasimharaj	A post-test version of this document, designed for utilization during post-test review meeting(s).
4.0	10-10-2023	Sujitha Govindasamy	The final version of the document now includes the corrective action plan that has been implemented.

Table of Contents

Statement of Intent

This document outlines Savory Sauce restaurant's policies and procedures for disaster recovery and business continuity, detailing process-level plans for restoring critical business functions and infrastructure from the cybersecurity incident. It provides an overview of our recommended procedures. In the case of a real emergency, adjustments may be made to this document to prioritize the physical safety of our personnel, systems, and data. Our mission is to guarantee information system uptime, ensure data integrity and availability, and maintain business continuity.

Policy Statement

The following policy statement has received approval from corporate management:

- Savory Sauce will formulate a comprehensive business resumption plan.
- A formal risk assessment will be conducted to identify critical risks needed for the disaster recovery and business continuity plan.
- The disaster recovery plan is expected to encompass all vital and critical infrastructure components, systems, and networks in alignment with key business activities.
- Regular testing of the plans in a simulated environment will be conducted to ensure its efficacy in emergency situations and to confirm that both management and staff comprehend its execution.
- All staff members are mandated to be familiar with the disaster recovery plan and their respective roles.
- This disaster recovery plan is an integral component of our commitment to maintaining business continuity and safeguarding critical operations.

Objectives

The primary goal of the disaster recovery and business continuity program is to formulate, test, and document a well-organized and easily comprehensible plan. This plan facilitates the company's swift and effective recovery from unforeseen disasters or emergencies that may disrupt information systems and business operations. Additional objectives include:

- Ensuring that all employees thoroughly understand their responsibilities in implementing the plan.
- Guaranteeing adherence to operational policies in all planned activities.
- Assessing the cost-effectiveness of proposed contingency arrangements.
- Considering implications for other company sites.
- Implementing disaster recovery capabilities relevant to critical customers, vendors, and other stakeholders.

These objectives collectively contribute to the robustness of our disaster recovery efforts, enhancing our ability to navigate and overcome challenges posed by unexpected disruptions.

Plan Overview

This business continuity policy upholds Savory Sauce Restaurant's essential operations during emergencies and in the case of a disaster. The report focuses on the business resumption plan of three main cyber incidents: Distributed Denial of Service(DDoS , Ransomware and Phishing.. This document specifies the restaurant recovery facilities, core business functions and authorities to communicate in an emergency, including backups to preserve the files and system state to recover from a disaster. The document should be used to gain insights into the considerations associated with planning for the continuity of Savory Sauce Restaurant's crucial and essential business functions.

Plan Scope

This program applies to vital business functions, people, IT systems and departments of the restaurant at the headquarters in Edmonton, Alberta. It involves activities and necessary resources to ensure the continuity of critical functions during a disruption, and focuses on the restoration of the vital business functions

In Scope:

Critical Business Functions	Critical business functions identified by the company's Business Impact Analysis (BIA).
IT Systems	All IT systems that support the essential function of the Critical Business Functions.
People	Technicians and key knowledge workers that support the identified Critical Business Functions

Out of scope: This program does not include any processes not identified by the BIA as vital.

Assumptions

This disaster recovery and business continuity plan is written under the following assumptions;

- Key personnel must be accessible for participation in continuity activities within the initial 24 hours of a disruption incident, irrespective of circumstances.
- Communication procedures have been established to ensure swift access to other managers, employees, authorities, suppliers, distributors, and customers.
- Savory Sauce Restaurant has trained backup personnel for all skilled positions, the IT technician has a current DRP in place and the restaurant will be able to operate at a reduced capacity in the case of an emergency.

Employee Roles and responsibilities

Chief Information Officer	In charge of integrating and maintaining a variety of technology platforms utilized by the restaurant such as Toast(POS system), mobile apps, website, and contactless payments. To safeguard customer and business data by implementing robust data security measures and enforcing them. Develop and enforce policies to mitigate risks associated with usage of technology
Chief Technology Officers	Formulate and implement a comprehensive technology plan aligned with the objectives and goals of the restaurant Incorporate features and technologies to improve the digital customer experience in all the aspects.
Chief Information Security Officer	Ensure the confidentiality, integrity, and availability of the restaurant's information assets. Conduct regular security awareness programs to educate them and also conduct security audits to identify vulnerability and weaknesses in the information system.
IT Project Managers	Develop detailed project plans including resource allocation, timelines and tasks dependencies. Communicate regularly with key stakeholders such as

	restaurant management to share project updates and ensure alignment with business goals.
IT Zonal Heads	Manage IT operations within the assigned zones and ensure reliable and scalable IT systems Maintain relations with technology vendors offering goods and services in the designated area and ensure service level agreements are met.
IT Zone Manager	Responsible for supervising and controlling all technical within the organization such as managing the POS Systems, Implementing backup solutions and so on.
IT employees	Responsible for Technical assistance, System maintanence, Software development, Online marketing support.
General Managers	Responsible for managing branch employees, supervising operations, guaranteeing outstanding client experiences, and promoting company expansion.
Headwaiters	Responsible for guaranteeing flawless dining operations and outstanding customer support.
Group Chefs	Responsible for managing the kitchen crew and watching over the culinary operations.
Restaurant Managers	Responsible for supervising the workforce, promoting

	company expansion, and guaranteeing top-notch customer service.
Assistant Managers	Responsible for supervising the workforce, promoting company expansion, and guaranteeing top-notch customer service.
Shift running Managers	Responsible for supervising daily operations during designated shifts, making sure that everything runs smoothly, supervising employees, and preserving operational effectiveness.
Floor Managers	Responsible for supervising the service staff, managing the dining area, and overseeing the front-of-house operations to ensure excellent customer service.
Staff Training Crew	In charge of providing both new hires and current employees with training, making sure employees understand rules and guidelines, and supporting the team's overall growth within the restaurant.
Executive Chefs	Responsible for the creation of menus, kitchen operations, and the assurance of food quality and consistency across a variety of cuisines.
Sous chefs	As the Executive Chef's deputy and second-in-command in the kitchen, the Sous Chef plays a crucial role in managing all facets of culinary operations.

Chef de partie	Responsible for supervising a specific station or section and guaranteeing food quality, while working along with the kitchen crew.
Station Headwaiters	In charge of a particular area or section of the dining room, responsible for overseeing a group of servers, and guaranteeing outstanding client experiences in their assigned area.
Waiters	Responsible for Greeting customers, taking and serving their orders efficiently while maintaining a hospitable environment.
busboys	Responsible for keeping the dining area tidy and well-organized.
Marketing and Sales Department	In charge of forming different tactics meant to increase the restaurant's brand, improving exposure, and boost sales
Finance Department	Responsible for overseeing the organization's finances, assuring fiscal responsibility and preserving its stability.
Human Resources	Responsible for maintaining compliance with labor laws and regulations, manages employees, and cultivates a positive work environment.
IT Operations	Responsible for upholding and Overseeing the

	technological infrastructure required for efficient restaurant functioning.
Customer Service	Responsible for providing information to customers, monitoring orders and processing payments.
Supply Chain Department	Responsible for overseeing the relationships with suppliers, logistics, inventory, and procurement that are necessary for the restaurant to run efficiently.
Hygiene Inspection Department	Responsible for ensuring high standards of cleanliness and food safety with the restaurant.

Key Employee contact information

Name	**Title**	**Mobile**	**Alternative Mobile**	**Email address**
Agbai Obasi	Chief Information Officer	+1 (780) 634 4328	+1 (780) 555 0187	agbai.obasi@savorysauce.com
Rajani Shrestha	Chief Technology Officer	+1 (780) 481 9622	+1 (780) 568 2962	rajani.shrestha@savorysauce.com
Sadhana Narasimharaj	Chief Information Security Officer	+1 (403) 202 2577	+1 (403) 291 3801	sadhana.narasimharaj@savorysauce.com

Sujitha Govindasamy	IT Security Specialist or Network Engineer	+1 (403) 207 3498	+1 (403) 214 7632	sujitha.govindasamy@savorysauce.com
Johnny Bucyk	IT Zonal head	+1 (780) 601 7816	+1 (780) 635 9160	johnny.bucyk@savorysauce.com
Nate Burleson	IT Zonal Manager	+1 (780) 852 3995	+1 (780) 852 4061	nate.burleson@savorysauce.com
Michelle Cox	General Manager	+1 (403) 556 1477	+1 (403) 556 7401	michelle.cox@savorysauce.com
Patrick Witherson	IT Auditor	+1 (780) 852 8346	+1 (780) 852 4308	patrick.witherson@savorysauce.com
Carolyn Succini	Operations Manager	+1 (403) 289 9184	+1 (403) 289 4951	carolyn.succini@savorysauce.com
Darren Dreger	Human Resource Manager	+1 (780) 568 5092	+1 (780) 568 9451	darren.dreger@savorysauce.com
Erica Duthi	Supply Chain Manager	+1 (403) 317 0202	+1 (403) 317 3704	erica.duthi@savorysauce.com
Charmin Ruth	Head Customer Service	+1 (780) 710 7692	+1 (780) 710 4051	charmin.ruth@savorysauce.com
Hannah Storm	Fulfillment Manager	+1 (780)	+1 (780)	hannah.storm@sa

		710 5609	710 8023	vorysauce.com
Melinda Gilbert	IT Manager	+1 (780) 852 4710	+1 (780) 852 7094	melinda.gilbert@Savorysauce.com
Lorem Epsum	POS System Administrator	+1 (403) 609 5968	+1 (403) 609 4207	lorem.epsum@savorysauce.com
Robert Patel	Communication Coordinator	+1 (780) 568 7925	+1 (780) 568 6905	robert.patel@Savorysauce.com
Alex Federson	IT Recovery Manager	+1 (403) 245 9641	+1 (403) 245 7942	alex.federson@savorysauce.com
Richard Miloy	Business Continuity Manager	+1 (780) 481 5972	+1 (780) 481 8271	richard.miloy@savorysauce.com
Jenna Fern	Finance Manager	+1 (780) 852 7910	+1 (780) 852 9652	jenna.fern@savorysauce.com

Supplier Contact List

Name	**Company Name**	**Mobile**	**Email Address**
Harold Mackesey	Saputo Food Service, Dairy Supplier	+1 (403) 441 8630	harold.mackesey@saputo.com
Albert Fyn	Gordon Food	+1 (780) 455-3100	edm-info@gfs.ca

	Service, Chicken and Beef Supplier		
Joseph Fernado	NorthSea Fish & Farms, Seafood Supplier	+1 (403) 243-4475	info@northsea.ca
Lily Anderson	Fresh start foods, Vegetables supplier	+1 (604) 277 7740	info@freshstartfoods.com
Vanessa Gilt	Papagino Foods Inc., Flour Supplier	+1 (416) 335 4924	orderdesk@papaginofoods.com
William Smith	Western Rice Mills, Rice Supplier	+1 (604) 321 0338	info@westernricemills.com
Andrew Bhatt	Hudson Traders, Condiments Supplier	+1 (201) 917 3044	support@hudsontraders.com

Key Customer Contact List

Customer Name	**Mobile**	**Email Address**
Emma Reynolds	+1 (780) 350 7092	emma.reynolds@Savorysauce.com
Jonathan Baker	+1 (780) 634 4328	jonathan.baker@Savorysauce.com
Sophia Chen	+1 (780) 801 7791	sophia.chen@Savorysauce.com
Liam Rodriguez	+1 (780) 6 4201	liam.rodriguez@Savorysauce.com

Business impact analysis

A cyberattack can compromise various business functions, negatively impacting the restaurant's operations, customer trust and overall business performance. Conducting a business impact analysis(BIA) entails evaluating the possible outcomes and its impact on various business aspects. It aids the restaurant to gain valuable insights about the potential consequences and create a proactive plan to mitigate risks and enhance resilience against cyberattacks.

Business function	**Potential impact**
POS system	POS systems will be compromised resulting in transaction manipulation, unauthorized access or downtime. This will cause financial loss, compromised customer payment information and reputational damage to the restaurant.
Internet	Toast software will be unable to function properly without the internet. As a result, sales will be affected in various ways because of the inability to respond to customer emails.
Security systems	Customer data including personal and payment information is susceptible to data breach during attack. This may lead to financial penalties, legal consequences and loss of customer trust. It may also lead to malfunctioning of security cameras and access control systems.
Server	Server outages will affect customer service in placing orders which will result in loss of revenue.

Inventory management	Disruption in inventory management can lead to inaccurate stock level reporting, delayed orders and difficulties keeping an efficient supply chain.
Employee management	Systems that handle employee schedules, payroll and HR tasks will be affected. Payroll delays, dissatisfaction among employees and operational disruptions may result from this.
Supply chain and vendor management	Cyberattacks can disrupt vendor relationships in addition to causing delivery delays, increased cost, and communication breakdown with partners and suppliers.
Financial processes	Accounting and budgeting tools which are key components of the financial system will be affected leading to financial losses, breach in private financial data and difficulty in managing the financial stability of the restaurant.
Operational processes	There could be an impact on core operational processes such as kitchen management and order processing. Delays and errors may arise resulting in an overall decline of operational efficiency.
Regulatory compliance	Non-compliance with industry standards and data protection laws can lead to legal repercussions, fines, and reputational damage.

Risk assessment and management

Savory Sauce Restaurant, as a dynamic establishment, gets exposed to a variety of risks which recognizes the need for a thorough assessment to identify potential vulnerabilities and develop effective strategies for business continuity and disaster recovery. This section outlines the key risks associated with three significant threats: ransomware, Distributed Denial of Service (DDoS) attacks, and phishing attacks, since the restaurant heavily relies on an IT platform for the business to operate. Each threat is evaluated based on likelihood level, impact level, risk level, risk factor and mitigation strategy. By systematically addressing these risks, SavorySauce aims to fortify its defenses, ensuring the integrity of its operations, safeguarding customer data, and maintaining uninterrupted service delivery.

Risks	**Likelihood of occurrence**	**Impact level**	**Risk level**	**Risk Factor**	**Mitigation Strategy**
Ransomware Attack	3(Medium)	5(Very High)	15(Medium to High)	Uses POS software, Toast, prone to ransomware.	● Regular employee training on recognizing phishing attempts. ● Regular data backups and offline storage. ● Implementation of antivirus

					and anti-ransomware software.
DDoS Attack	3(Medium)	5(Very High)	15(Medium to High)	● Provides Online Ordering and mobile ordering. ● Relies on online platforms more.	● Periodically review the security practices of online service providers. ● Train staff to recognize signs of a DDoS attack. ● Implement network monitoring to detect unusual traffic patterns.
Phishing Attack	4(High)	4(High)	16(High)	Using toast allows employee to access restaurant data, most	● Conduct regular training sessions to educate employees related to

				probable insider threat	phishing. ● Use advanced email filtering tools to identify and block the phishing emails. ● Use multi factor authentication for critical systems.

The likelihood and impact factor are calculated on the scale of 5 with “1” as “Very Low” and “5” as “Very High”.

Risk Level = Likelihood level X Impact level

Disaster Recovery Strategy:

The disaster recovery strategy begins as soon as the triggering event has been identified for each possible disaster. The plan mainly focuses on three cyber incidents: DDoS Attack, Ransomware Attack and Phishing Attack.

Plan Triggering Event:

Key triggering phase helps to identify possible events that will most likely cause a disaster which could lead to activation of the Disaster Recovery Plan. Key triggering event for each attack are:

DDoS Attack

- Rapid increase in incoming network traffic of POS software and Online services.
- Performance degradation of Online Services impacting critical business functions.
- Complete or partial unavailability of online services.

Ransomware Attack

- Detection of unauthorized encryption of files in POS systems.
- Reports from customers and employees regarding strange system behavior.
- Notification demanding payment for data encryption.

Phishing Attack

- Employees reporting suspicious email or activities.
- Unusual login attempts or unauthorized access to sensitive information.

DRP Activation Phase:

The Business Continuity Plans are implemented during this phase. This phase lasts until the primary site of Savory Sauce is restored, important business functions are reestablished, and the alternative facility is occupied. Notifying and assembling the recovery teams, putting in place temporary measures, moving to the backup site or secondary facility to continue operations, and resuming data communications are the main tasks of this phase.

Activation Phase During Office hour

During an office hour the IT Operations Team and Security Analysts promptly identify the issue. The Chief Information Officer (CIO) or designated Incident Response Coordinator assesses the severity and decides to activate the Disaster Recovery Plan (DRP). The Emergency Response Team (ERT) is mobilized, and the IT Operations Team executes recovery procedures with clear communication to stakeholders.

Activation Phase after office hour

After office hours, automated monitoring systems or designated on-call personnel identify incidents, and the on-call ERT members execute recovery procedures with remote coordination, maintaining transparent communication about progress and expected resolutions.

DDoS Attack DRP Activation

DRP can be activated:

- If the DDoS attack overwhelms mitigation measures and impacts critical business function
- If the attack persists for an extended period, causing significant service disruption.

Ransomware Attack DRP Activation

DRP can be activated:

- If critical systems or data are compromised by ransomware, impacting normal operations.
- If attempts to contain and eradicate the ransomware are unsuccessful.

Phishing Attack DRP Activation

DRP can be activated:

- If a phishing attack leads to unauthorized access or compromise of critical systems.
- If there's a significant breach of customer or employee data.

Activation of Emergency Response Team

To fortify its resilience against unforeseen incidents, SavorySauce has established an Emergency Response Team (ERT). The ERT is a dedicated group of skilled professionals

equipped to swiftly respond to and mitigate the impact of disasters, ensuring the continuity of critical operations.

Responsibilities of Emergency Response Team during disaster are:

- Quickly assess the situation and initiate the activation of the Emergency Response Plan (ERP).
- Implement established procedures and protocols to respond to the disaster.
- Establish and maintain communication channels to notify employees, stakeholders, and relevant authorities about the situation.
- Coordinate the implementation of alternative work arrangements, such as remote work or relocation to backup facilities, to ensure the continuity of operations.
- Deploy available resources, including personnel and equipment, to address immediate needs.
- Continuously assess the situation to gather information on the impact of the disaster.
- Maintain detailed records of the incident, response activities, and outcomes. Provide timely and accurate reports to leadership, regulatory bodies, and other relevant stakeholders.

Emergency, Escalation and DRP Activation

The purpose of the policy and procedure is to guarantee that each employee will know exactly who to contact in the event of an emergency. It is ensured that communications can be established quickly while disaster recovery is activated by attending to the procedures. The management and staff are the only key players in this disaster recovery plan, as they will be the ones to provide the technical and managerial expertise required to ensure a seamless recovery of the business and technology. This section therefore, serves as a strategic guide, outlining the systematic approach led by the Emergency Response Team (ERT) during

emergencies, delineating escalation procedures for informed decision-making, and detailing the activation steps for the DRP to secure IT systems and data integrity

Emergency Alert

Every staff needs to have a card and information on who to contact in case of an emergency in their ease. In case of disaster, the first person who notified an incident, will notify the emergency response team in an order of below mentioned priority:

Emergency Response Team

Name	**Role**	**Primary Contact Number**	**Emergency Contact Number**	**Email**
Agbai Obasi	Chief Information Officer	+1 (780) 634 4328	+1 (780) 555 0187	agbai.obasi@savorysauce.com
Sadhana Narasimharaj	Chief Information Security Officer	+1 (403) 202 2577	+1 (403) 291 3801	sadhana.narasimharaj@savorysauce.com
Robert Patel	Communication Coordinator	+1 (780) 568 7925	+1 (780) 568 6905	robert.patel@Savorysauce.com
Alex Federson	IT Recovery Manager	+1 (403) 245 9641	+1 (403) 245 7942	alex.federson@savorysauce.com

Secondary Response Team

If Emergency Response team are not available, refer to the secondary contact team:

Name	**Role**	**Primary Contact Number**	**Emergency Contact Number**	**Email**
Rajani Shrestha	Chief Technology Officer	+1 (780) 481 9622	+1 (780) 568 2962	rajani.shrestha@savorysauce.com
Sujitha Govindasamy	IT Security Specialist or Network Engineer	+1 (403) 207 3498	+1 (403) 214 7632	sujitha.govindasamy@savorysauce.com
Melinda Gilbert	IT Manager	+1 (780) 852 4710	+1 (780) 852 7094	melinda.gilbert@savorysauce.com

Disaster Recovery

Before formulating a disaster recovery team, an emergency response team will continuously assess the evolving situation and determine whether or not to declare a disaster based on predefined criteria.

- If the team does NOT declare a disaster, the standard procedure for Service restoration is followed which will complete the disaster recovery process.
- If the team does declare a disaster, proceed with implementing the Disaster Recovery Plan's instructions

Contact with Employee

In the event of a disaster or disruptive incident at SavorySauce, effective communication with employees is paramount. The primary point of contact for employees

will be their respective departmental managers, especially restaurant managers, who will serve as key conduits for disseminating crucial updates, safety instructions, and details regarding the progress of recovery efforts. If the employee cannot get information from the department head, contact the other employee to remain up-to-date. Additionally, a designated spokesperson, often a member of the Emergency Response Team or a communications specialist, will collaborate closely with the HR department to ensure organization-wide communication is consistent, accurate, and aligns with the overall strategy.

Name	**Role**	**Primary Contact Number**	**Emergency Contact Number**	**Email**
Robert Patel	Communication Coordinator	+1 (780) 568 7925	+1 (780) 568 6905	robert.patel@Savorysauce.com
Darren Dreger	Human Resource Manager	+1 (780) 568 5092	+1 (780) 568 9451	darren.dreger@savorysauce.com

Backup staff

In instances where departmental managers are unavailable, team leads or supervisors within each department will assume the responsibility of formulating and communicating essential information to their teams. Clear communication protocols and a predefined chain of command will guide this process.

Disaster Recovery Team and Responsibility

The Emergency Response Team in case of disaster will formulate a disaster recovery team.

Name	Roles	Responsibilities	Contact
Agbai Obasi	Chief Information Officer	● Initiates the assessment of a disaster and activates the recovery and associated processes. ● Presents to the management team the extent of the disaster, data loss, and necessary decisions. ● The CIO also acts as the central point of contact, overseeing all backup and recovery operations. ● Coordinates supervises, and manages all aspects of disaster recovery plans, backup, and recovery plans, authoring all updates. ● Organizes, supervises, and	agbai.obasi@savory sauce.com

		manages all disaster recovery plans and backup operations.	
Sadhana Narasimharaj	Chief Information Security Officer	● Identify the time of data loss and communicate it to the CIO, System, and backup team. ● Verify compliance with Backup and restoration plans and policies. ● Ensure that backups receive the same level of security as the backed-up system and isolate any threat actors. ● Apply adequate security measures to backup media to uphold stored data's confidentiality, integrity, and	sadhana.narasimharaj@savorysauce.com

		availability. ● Label backup media following the security requirements of the data it holds. ● Ensure proper sanitization of backup media before recycling and their destruction when they reach the end of their life cycle.	
Rajani Shrestha	Chief Technology Officer	● Formulating strategies to enhance partnerships, technology platforms, and external relationships. ● Performing technical assessments of products and solutions to assess their suitability. ● Efficiently managing	rajani.shresth@savorysauce.com

		infrastructure assets to align with internal financial targets. ● Monitoring, analyzing, and tracking technological performance metrics.	
Sujitha Govindasamy	IT Security Specialist or Network Engineer	● Monitor and analyze cybersecurity threats specific to the restaurant industry. ● Develop and update IT security policies tailored to restaurant operations. ● Implement redundancy and failover mechanisms for critical restaurant systems. ● Ensure availability of communication channels during	sujitha.govindasamy@savorysauce.com

		recovery efforts, especially for order processing.	
Lorem Epsum	POS System Administrator	● Security and recovery of the Point of Sale (POS) system, including payment processing security ● Collaboration with IT Security on POS-related cybersecurity strategies.	lorem.epsum@savorysauce.com
Robert Patel	Communication Coordinator	● Development of clear and consistent communication strategies for internal and external stakeholders/ ● Regular updates to staff, customers, and media during the incident.	robert.patel@savorysauce.com

DRP Activation Procedure:

Here are some types of cyberattacks that can affect Savory Sauce restaurant business and the steps that the disaster recovery team can follow to recover from them:

DDoS Attack

A DDoS attack attempts to make a website or network unavailable to users by overwhelming it with traffic over a large area of the network. In the case of a DDoS attack, the disaster recovery team should follow these steps:

1. Identify the source of the attack and block it.
2. Notify all employees to avoid accessing the affected website or network.
3. Implement additional security measures such as firewalls and intrusion detection systems to prevent future attacks.
4. Monitor the network for any unusual activity.

Ransomware

Ransomware is malware that encrypts the victim's files and demands payment in exchange for the decryption key. In the case of a ransomware attack, the disaster recovery team should follow these steps:

1. Isolate the infected system(s) from the network to prevent further spread of the malware.
2. Identify the type of ransomware and determine if a known decryption tool is available.
3. Restore the encrypted files from a backup that was taken before the attack.

If no backup is available, consider paying the ransom as a last resort.

Phishing

Phishing is a social engineering attack that uses fraudulent emails or websites to trick users into revealing sensitive information. In the case of a phishing attack, the disaster recovery team should follow these steps:

1. Identify the source of the phishing email or website and block it.
2. Notify all employees to avoid clicking on suspicious links or downloading attachments from unknown sources.
3. Change all passwords that may have been compromised.
4. Conduct a thorough scan of all systems to ensure no malware was installed.

Business Continuity Strategy

The Business Continuity Plan aims to ensure the resilience of SavorySauce's operations in the face of potential disaster related to cybersecurity.

Critical functions and technology dependencies

1. Pos system: Utilized for processing orders, handling online safe online transactions and payment information

   Dependencies: Technologically relies on the Toast (POS software) and internet connection.
2. Reservation system: To accept and manage reserved bookings with corresponding seating arrangements and maintain the guest list

   Dependencies: Depends on the internet connectivity and the reservation software to manage bookings.
3. Inventory management: To track supply level placing supply order and controlling food costs.

   Dependencies: Depends on the dedicated software for inventory and the internet. Any disruption of services will impact the supply chain management.
4. Employee management: Manages employee data, work schedules and their payroll.

Relies on scheduling and payroll software to assign shifts to employees and process payrolls seamlessly.

5. Communication systems: Provide internal communication between the staff and the customers.

   Dependencies: Relies on customer service desk, mobile app, website and emails. Disruption of these communication channels will affect the coordination among the staff and possible customer service.

6. Automated kitchen appliances: Utilizing automated kitchen appliances for food preparation.

   Dependencies: Connected or automated smart appliances are vulnerable to cyber attacks leading to disruption of kitchen operation and food preparation.

7. Data backup and recovery: Regular backup is necessary to ensure critical restaurant like customer information, financial records and menu items are stored security.

   Dependencies: Relies on cloud-based backup solution, secure storage with server, recovery tools and the efficiency of backup systems for accurate and timely restoration.

Impact based on RTO and MTD

Critical functions	**RTO**	**MTD**	**Impact**
POS system	12 hours	24 hours	High
Reservation system	10 hours	24 hours	Medium
Inventory management	48 hours	1 week	Medium
Employee management	48 hours	1 week	Low
Communication system	5 days	1 week	Medium
Automated kitchen appliances	1 hour	3 hours	High

Data backup and recovery	48 hours	1 week	High

Insurance coverage

Savorysauce has implemented an insurance policy to take care of the business during a disaster. It covers general and director's liability, business interruption insurance, error coverage.

The staff contact given below should be approached for any insurance-related assistance.

Policy	**Policy detail**	**Staff to contact**	**Coverage amount**	**Coverage period**
Cyber safety insurance	In the event of ransomware, ransom employing a special communication company, restoration costs, and loss of revenue incurred for the business	Jenna Fern(Finance Manager) Contact:+1 (788) 633 4564 Email: jenna.fern@savorysauce.com	$1500/ yr	15 years

Employee training

Cyber security training for all the staff of the restaurant is crucial as the business heavily relies on the various technologies for day-to-day operations. This aids in data

protection, financial security, awareness of regulations and policies, safeguarding the business from cyber attacks and maintaining customer trust and reputation.
Training programs are offered on a regular basis and all the employees are kept up-to-date about the disaster recovery and business continuity plans.

Data backup and recovery

The restaurant data is backed up once a week using the cloud storage to ensure smooth transition and access during a disaster. Shadow copies and complete system state backup are created to ensure business continuity incase of any cyber attack.

Public relationship management

In times of disaster, effective Public Relations (PR) management is essential to safeguard SavorySauce's reputation, maintain transparent communication, and assure stakeholders. This plan outlines key strategies and responsibilities for the PR team during such critical events.

PR Team

Name	**Role**	**Contact**	**Responsibility**
Emily Thompson	Media Manager	Email: emily.thompson@Savorysauce.com Phone: +1 (780) 710 4651	● Develops and executes media engagement strategies. ● Coordinates with spokespersons and other team members. ● Ensures consistency

			in messaging across all media channels.
David Reynolds	Spokesperson	Email: david.reynolds@Savorysauce.com Phone: +1 (780) 710 6703	● Deliver official statements and responses to media inquiries. ● Attend press conferences and interviews.

Public Relation Strategy

A well-crafted public relations (PR) strategy is crucial in managing the public perception and communication during and after an incident.

- Provide immediate responses to media inquiries and public concerns regarding the incident.
- Collaborate closely with designated spokespersons to ensure consistent and accurate messaging.
- Engage with the media through press releases, statements, and interviews.
- Monitor and manage social media channels for real-time updates and responses.
- Develop and disseminate communication to customers regarding the impact, expected resolution times, and alternative services.
- Coordinate with internal communication teams to ensure consistent messaging within the organization
- Communicate the resolution of the incident and the steps taken to prevent future occurrences after an incident

Public Relation Rule

Only a person who is in the PR team are responsible for talking to the media. The set of rules to be followed include.

- Only the PR team is authorized to speak to media inquiries.
- Circulate approved key messages for all media interactions.
- Respond to media inquiries within 1 hour of receipt during office hours and within 4 hours after working hours.
- Be transparent about the incident's impact, acknowledging challenges, and communicating ongoing efforts to resolve the issue.

Testing and exercises

As a very crucial aspect of the disaster recovery plan development process, exercises will be conducted regularly to make sure every participant gain insight into what needs improvement and how these enhancements can be implemented. The purpose of plan exercises is to ensure that emergency teams understand their assignments and gain confidence in their capabilities.

Testing Strategy:

- Tabletop exercise to evaluate the effectiveness of DRP through discussion and analysis without actual system downtime.
- Structure walkthrough of DRP to identify the gap or areas of improvement in the plan’s execution.
- Validating the practicality of recovery procedures and identify any issues through simulation.
- Full-Scale testing so as to assess the plan’s effectiveness and the organization’s ability to fully recover operation.

References

APA. (n.d.). *APA Headings and Seriation - Purdue OWL® - Purdue University*. Purdue OWL. Retrieved November 25, 2023, from https://owl.purdue.edu/owl/research_and_citation/apa_style/apa_formatting_and_style_guide/apa_headings_and_seriation.html

Micro Focus. (n.d.). *IT Disaster Recovery Planning: A Template*. Micro Focus. Retrieved November 10, 2023, from https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf

Appendix

External Contacts

Name, Title	**Contact Option**	**Contact Number**
Landlord/Property Manager		
Account number: 028920371	**Work**	+1(780) 429 5956
	Mobile	+1(780) 429 5937
	Email Address	info@bradenequitiesinc.com
Xoom Energy		
Power Company	**Work**	+1 (866) 999 8483
Account number: 2345437687	**Mobile**	+1 (346) 321 2166
	Email Address	info@xoomenergy.com
Telus		
Telecom Carrier 1	**Work**	+1 (900) 324 3345
Account number: 567398789	**Mobile**	+1 (277) 321 2164
	Email Address	Telusinfo@telus.com

Bell Technologies		
Telecom Carrier 2	**Work**	+1 (900) 087 3346
Account number: 666745874	**Mobile**	+1 (277) 367 2164
	Email Address	Bellinfo@bell.com
Pool Servers		
Server Supplier 1	**Work**	+1 (344) 234 5211
Account number: 22334476	**Mobile**	+1 (780) 546 8743
	Email Address	Poolnfo@poolservers.com
DRT		
Workstation Supplier 1	**Work**	+1 (788) 633 4564
Account number: 370219863	**Mobile**	+1 (346) 999 9834
	Email Address	drtinfo@drt.com
First Canadian Insurance		
Insurance	**Work**	+1 (780) 467 9575
Account number: 231421344	**Mobile**	+1 (800) 561 3242

	Email Address	insclaims@firstcanadian.ca
Austin Security		
Site security	**Work**	+1 (587) 977 3634
Account number: 876322222	**Mobile**	+1 (780) 546 2166
	Email Address	service@austinsecurity.ca
Off-Site Storage 1		
Account number: 098987344	**Work**	+1 (098) 871 8972
	Mobile	+1 (243) 926 5672
	Email Address	savorysauceoffsite@savorysauce.com
HVAC Solutions Ltd		
HVAC		
Account number: 722134987	**Work**	+1 (780) 792 0800
	Home	+1 (277) 367 3211
	Email Address	dispatch@hvac-solution.ca
Prima Power systems		

Power Generator	**Work**	+1 (604) 746 0606
	Mobile	+1 (778) 809 1111
	Email Address	info@primapowersys.com