CYBERSECURITY PACKAGE.

FOR MISS JEAN'S FLOWERS AND FLOWERPOWER HQ.

Security assessment and tools developed by BRONSON CORP.

PUBLISHED BY SAM BRONSON.

December 6, 2024.

CONTENTS

OVERVIEW.

COMPANY PROFILE.

Miss Jean's Flowers, founded in 1972, started as a roadside flower stand with the simple mission of making the world smell better. Over five decades, Miss Jean has grown her passion project into a thriving business with three locations: two retail stores and the FlowerPower Headquarters, which houses the main office and a centralized flower distribution center. With a team of 20 employees across the retail stores and a reliable IT manager, Vern, the organization strives to provide exceptional service and beautiful floral arrangements.

CURRENT IT INFRASTRUCTURE

- A centralized Point-of-Sale system at FlowerPower HQ, accessed via VPN by terminals at retail locations. The system supports sales, billing, manufacturing, and accounting.
- Email services are managed via Office 365.
- Employee workstations are connected to a Windows domain.
- Weekly backups are performed on an external hard drive, with old backups overwritten when the disk gets full.

PRIMARY CYBERSECURITY CONCERNS AND FOCUS OF SOLUTION DELIVERY

1. Ransomware disrupts operations by targeting the POS system and HQ servers.
2. Phishing attacks compromise employee accounts and serve as an entry point for attackers.

CYBERSECURITY TOOLS AND FRAMEWORKS.

These headers are hyperlinked for ease of navigation.

1. NIST SELF-ASSESSMENT

A structured self-assessment using the NIST Cybersecurity Framework provides a clear roadmap to improving security posture. The assessment will highlight gaps and provide actionable recommendations to align with industry best practices.

2. TABLETOP EXERCISE

Conducting a ransomware-focused tabletop exercise engages key stakeholders, tests incident preparedness, and validates response strategies.

3. INCIDENT RESPONSE PLAYBOOK

A customized playbook that ensures a swift and coordinated response to cybersecurity incidents.

FLOWERPOWER HQ

NIST SELF-ASSESSMENT TOOL

VERSION 1.0

PUBLISHED BY SAM BRONSON.

December 6, 2024.

INTRODUCTION

This assessment tool provides an independent and objective evaluation of your organization's cybersecurity posture. It's designed to identify vulnerabilities and areas for improvement, offering a clear and prioritized view of your security risks. This tool is an external, supplemental assessment and is not integrated with this existing cybersecurity package. Please review the tool that is supplemented with this package.

IMMEDIATE FOCUS AREAS FOR MISS JEAN'S FLOWERS INCLUDES THE FOLLOWING.

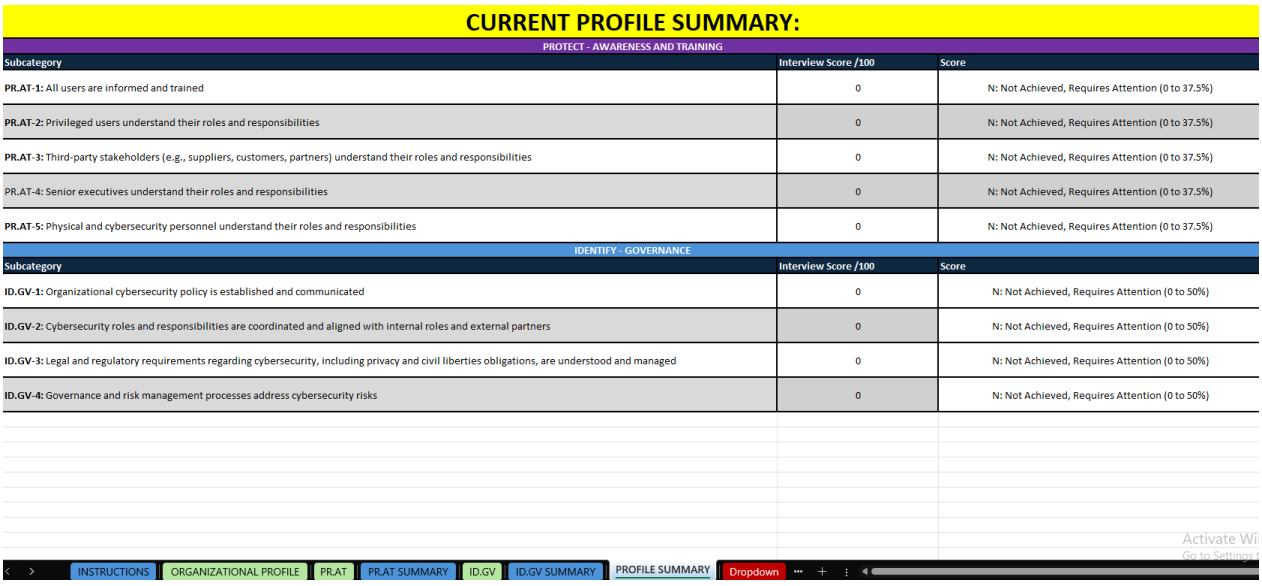
PR.AT (PROTECT - AWARENESS AND TRAINING):

- Educate employees about phishing attacks and cybersecurity hygiene.
- Train staff to recognize malicious emails, suspicious links, and attachments.
- Implement regular phishing simulations to test awareness.

ID.GV (IDENTIFY - GOVERNANCE):

- Define clear roles and responsibilities for cybersecurity.
- Develop and communicate policies on data access, backup, and acceptable use.

TOOL PREVIEW



CURRENT PROFILE SUMMARY:

PROTECT - AWARENESS AND TRAINING		
Subcategory	**Interview Score /100**	**Score**
PR.AT-1: All users are informed and trained	0	N: Not Achieved, Requires Attention (0 to 37.5%)
PR.AT-2: Privileged users understand their roles and responsibilities	0	N: Not Achieved, Requires Attention (0 to 37.5%)
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	0	N: Not Achieved, Requires Attention (0 to 37.5%)
PR.AT-4: Senior executives understand their roles and responsibilities	0	N: Not Achieved, Requires Attention (0 to 37.5%)
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	0	N: Not Achieved, Requires Attention (0 to 37.5%)
IDENTIFY - GOVERNANCE		
Subcategory	**Interview Score /100**	**Score**
ID.GV-1: Organizational cybersecurity policy is established and communicated	0	N: Not Achieved, Requires Attention (0 to 50%)
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	0	N: Not Achieved, Requires Attention (0 to 50%)
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	0	N: Not Achieved, Requires Attention (0 to 50%)
ID.GV-4: Governance and risk management processes address cybersecurity risks	0	N: Not Achieved, Requires Attention (0 to 50%)

FLOWERPOWER HQ

FLOWER HQ INCIDENT

TABLETOP EXERCISE

VERSION 1.0

EDITED BY SAM BRONSON.

December 5, 2024.

PUBLISHED BY SAM BRONSON.

December 6, 2024.

OBJECTIVES.

The primary goal of this tabletop exercise is to prepare the executives of Miss Jean's Flowers for a potential ransomware attack on their POS system and phishing attacks targeting employee accounts. The exercise aims to increase security awareness, validate the disaster recovery plan, and ensure that the organization can effectively respond to and recover from such incidents.

- Test the incident response plan for ransomware attacks.
- Evaluate the effectiveness of current phishing prevention measures.
- Enhance communication and decision-making among executives during a crisis.

FACILITATOR'S GUIDE.

Print this page separately for the facilitator.

TIMELINE OF INPUTS

TABLETOP SETUP (0-5 MINUTES)

ROOM SETUP

- Arrange seating to facilitate discussion, ideally to encourage interaction.
- Ensure all necessary equipment is set up, including a projector or screen for visual aids, if used.

MATERIALS DISTRIBUTION

- Hand out the Participant's Guide to each participant.
- Provide any additional materials, such as notepads and pens for notetaking.

INTRODUCTION

- Welcome participants as they arrive and introduce yourself as the facilitator.
- Briefly explain the purpose of the exercise and what participants can expect.

GROUND RULES

- Set expectations for participation, emphasizing open communication and respect for all contributions.
- Remind participants that the exercise is a safe space for learning and that there are no wrong answers

TIME MANAGEMENT

- Inform participants of the exercise timeline and key phases.

- Encourage them to manage their time effectively during discussions.

INITIAL INCIDENT (5-30 MINUTES)

FACILITATOR INPUT

Announce that the POS system is locked by ransomware and show the ransom note.

DISCUSSION POINTS

- What immediate actions should be taken?
- Who needs to be informed?
- How will communication be managed internally and externally?

ESCALATION (30-60 MINUTES)

FACILITATOR INPUT

Inform participants that backups may be compromised.

DISCUSSION POINTS

- Evaluate the pros and cons of paying the ransom.
- Discuss alternative recovery strategies.

PHISHING ATTACK (60-90 MINUTES)

FACILITATOR INPUT

Distribute examples of phishing emails received by employees. (These can be found in the printables section)

DISCUSSION POINTS

- How should employees be trained to recognize phishing attempts?
- What steps should be taken to secure potentially compromised accounts?

FORENSIC DISCOVERY (90-120 MINUTES)

FACILITATOR INPUT

Announce the discovery of data exfiltration.

DISCUSSION POINTS

- What are the legal and regulatory implications?
- How should the organization communicate with affected customers?

RESOLUTION AND DEBRIEF (120-150 MINUTES)

FACILITATOR INPUT

Lead a discussion on lessons learned and improvements to the incident response plan.

DISCUSSION POINTS

- What worked well?
- What could be improved?
- How can the organization better prepare for future incidents?

FACILITATOR'S PRINTABLES.

RANSOM NOTE.

Hello,

All your important files have been encrypted. To regain access to your data, you must pay a ransom. Failure to do so will result in the permanent loss of your files.

To decrypt your files, follow these instructions:

1. Purchase Bitcoin equivalent to $5,000.
2. Send the Bitcoin to the following address: [Bitcoin Address]
3. Once the payment is confirmed, you will receive a decryption key.

You have 72 hours to complete the payment. After this period, the decryption key will be destroyed, and your files will be lost forever.

Do not attempt to decrypt the files yourself or use third-party software, as this may result in permanent data loss.

We are monitoring your actions, so do not try anything foolish.

- The Encryptor

PHISHING EMAILS.

Dear Customer,

We have detected unusual activity on your bank account and need you to verify your identity to ensure your account's security. Please click the link below to verify your account information:

Yurbanking.com/verificate

Failure to verify your account within 24 hours may result in temporary suspension.

Thank you for your prompt attntion to this matter.

Sincerely,
Your Bank's Security Team

Hello Trisha,

Our records indicate that your email password will expire in 24 hours. To avod any disruption in service, please update your password immediately by clicking the link below:

flowersIt.support.com/resetpassword

If you have any questions, please contact the IT support team.

Best regards,
IT Support Team

Dear Miss Jean,

We attempted to deliver your flowers today, but no one was available to receive it. Please click the link below to reschedule your delivery:

Ups.shipit.com/reschedule/sxa3wraf23/

If you do not reschedule within 48 hours, your packag will be returned to the sender.

Thank you for choosing our delivery service.

Best,
UPS Customer Service Team

PARTICIPANTS GUIDE.

Print this page separately for each participant.

KEY PARTICIPANT ROLES

Participants will assume roles within the incident response team.

- Executive Leadership
- IT and Security Management
- Legal and Compliance
- Communications

EXERCISE STRUCTURE

The exercise will progress through several scenarios, each requiring participants to discuss and decide on appropriate actions..

SCENARIO PHASES

PHASE 1: INITIAL INCIDENT

- Discuss immediate actions and communication strategies.

PHASE 2: ESCALATION

- Consider response options and recovery strategies.

PHASE 3: PHISHING ATTACK

- Explore training and account security measures.

PHASE 4: FORENSIC DISCOVERY

- Discuss implications and communication with stakeholders.

PHASE 5: RESOLUTION AND DEBRIEF

- Reflect on lessons learned and potential improvements.

DIRECTORS NOTES AND RESPONSE PLAN.			
ASPECT	RESPONSE	INFORMATION	NOTES
IMMEDIATE SITUATION CONTROL	Isolate the centralized Point-of-Sale (POS) system and HQ servers to prevent further ransomware spread.	Isolation will disrupt sales, billing, manufacturing, and accounting operations.	Notify retail locations and department heads about the temporary shutdown. Review offline sales processes.
RANSOMWARE IDENTIFICATION	IT to identify the ransomware variant affecting the POS system and HQ servers.	Alert executives, legal counsel, and insurance providers. Assess the risk of data exposure.	Decision to negotiate or not should involve executive team, legal counsel, and law enforcement.
PHISHING ATTACK RESPONSE	Conduct an immediate review of compromised employee accounts and reset passwords.	Phishing attacks may have provided attackers with VPN access to the POS system.	Implement multi-factor authentication (MFA) for all accounts to prevent future breaches.
CYBER INSURANCE	Notify the cyber insurance provider of the ransomware and phishing incidents.	Insurance may offer external forensic services and crisis management guidance.	Verify incident response plans provided by cyber insurance, including legal guidance and forensics.
LEGAL RESPONSE	Legal counsel to ensure compliance with breach notification laws and coordinate with IT and PR.	Legal will advise on contacting law enforcement and managing communications.	Consider privacy laws (GDPR, CCPA) for notifying stakeholders and customers.
FORENSIC INVESTIGATION	Initiate a forensic investigation to determine the extent of the breach and entry points.	The forensic process can take time and may reveal additional vulnerabilities.	Preserve evidence for forensics while working to restore critical operations.
BACKUP SYSTEMS	Evaluate the integrity of weekly backups stored on external hard drives.	Risk of data loss due to overwritten backups and uncertainty of ransomware infiltration timing.	Consider implementing a more robust backup strategy with offsite and cloud-based solutions.
PRIVACY BREACH IMPLICATIONS	Assume a data breach has occurred due to compromised employee accounts.	Privacy officer to enact data breach protocols if personal data is involved.	Breach reporting to regulators and customers may be required within specific timeframes (GDPR, CCPA).
SHORT-TERM COMMUNICATIONS PLAN	Communicate internally with staff and affected clients about the incident. Prepare holding statements for press inquiries.	Transparency is key; however, the extent of details disclosed needs to be strategic.	Share information on a need-to-know basis, balancing business operations and public trust.
OPERATIONAL CONTINUITY	Develop offline operational plans for retail locations and HQ departments.	Impacted departments should outline alternate methods for sales and accounting.	Include contingency plans for prolonged system downtime, such as manual transaction processing.

SECURITY RESPONSE	Enforce a password reset for all employees and review user privileges across the Windows domain.	IT to guide the password change process securely. Review VPN access controls.	Ensure secure communication of password change instructions and monitor for residual vulnerabilities.
LAW ENFORCEMENT RESPONSE	Consult with law enforcement regarding the ransomware and phishing incidents.	Law enforcement may advise against negotiations to avoid compromising investigations.	Collaborate with law enforcement while safeguarding business continuity.
MEDIUM-TERM COMMUNICATIONS PLAN	Develop a plan to communicate with external media and the public, focusing on reputation management.	PR should prepare a press release and FAQ for potential questions from media outlets.	Simulate a media inquiry to practice response timing and message control.
RECOVERY STRATEGY	IT to confirm the feasibility of restoring systems from backups and address any data gaps.	Operations must plan for extended downtime. Communicate recovery progress internally.	Balance between recovering operations quickly and ensuring a comprehensive forensic investigation.
DECISION ON RANSOM PAYMENT	Executive team to decide on halting operations, paying the ransom, or proceeding with partial recovery.	Consider time-to-recovery estimates, costs, and long-term business impact.	Final decision should reflect business priorities, legal advice, and cybersecurity risk management.
LONG-TERM COMMUNICATIONS PLAN	Communicate the long-term impact to stakeholders, including data breach remedies for affected individuals.	Provide resources such as identity theft protection, a 24/7 call center, and updated FAQs.	Focus on rebuilding trust with customers and the public through transparent updates and assistance.
POST-INCIDENT REFLECTION	Summarize key lessons learned and update incident response and recovery plans accordingly.	Conduct a post-mortem analysis to assess response effectiveness and identify improvement areas.	Use findings to enhance future incident response plans, backup strategies, and employee training.

FLOWERPOWER HQ

PHISHING AND RANSOMWARE

INCIDENT RESPONSE PLAYBOOK

VERSION 1.0

EDITED BY SAM BRONSON.

December 5, 2024.

PUBLISHED BY SAM BRONSON.

December 6, 2024.

TABLE OF CONTENTS

INTRODUCTION.

DESCRIPTION.

This playbook outlines a comprehensive response plan to mitigate and recover from a ransomware attack targeting FlowerPower's centralized POS system. Highlighted as a key area of risk, a ransomware attack against this centralized POS system could severely disrupt sales, halt operations, disrupt customer service, and compromise sensitive financial data. With phishing as a likely entry vector, this playbook outlines procedures to detect, analyze, mitigate and recover from ransomware incidents.

Note: Update this playbook as needed to support relevant systems.

HOW PHISHING CAN OCCUR.

Phishing is a common entry point for ransomware and often manifests itself as:

1. Malicious emails. Employees may be a target for emails that contain links or attachments with malware.
2. Credential Harvesting. Fake login portals can trick employees into divulging domain credentials, granting attackers access to systems.
3. Exploitation Office 365. Attackers may leverage compromised email accounts to propagate phishing emails internally.

Given the heavy reliance on Office 365, educating employees about phishing emails and implementing email security protocols is critical.

HOW IT CAN BE IDENTIFIED

Phishing takes advantage of social engineering techniques.

Phishing is a cyberattack where criminals impersonate trustworthy sources via email, text, or websites to trick victims into revealing sensitive information like passwords or credit card details. These deceptive communications often contain very strong emotional language, urgent requests or threats to pressure quick action. Identifying phishing attempts involves operating with a level of skepticism and suspicion, scrutinizing sender addresses and URLs for inconsistencies, noting generic greetings, suspicious attachments, grammatical errors, and requests for personal information. If suspicious, avoid clicking links or opening attachments, don't reply, report the attempt to the impersonated organization, and change your passwords immediately if you suspect compromise.

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software designed to encrypt a victim's files, rendering them inaccessible until a ransom is paid to the attacker. It typically spreads through phishing emails, malicious attachments, or vulnerabilities in a system, and once executed, it locks critical data and systems, disrupting operations. The attackers demand payment, often in cryptocurrency, and threaten to delete or expose the data if the ransom is not met. In many cases, ransomware also targets backups, leaving organizations without a recovery option. Its primary impact includes financial loss, operational downtime, and potential reputational damage.

PREPARATION.

PRIMARY RISKS.

- Ransomware Infection. This can disrupt the POS system and critical servers.
- Phishing Emails. Likely an entry point for attackers.

PREPAREDNESS STEPS.

- Training. Conduct phishing awareness training for employees.
- Backup Strategy. Implement a 3-2-1 backup policy (three copies of data on two different storage media, with one offsite).
- Patch Management. Ensure timely updates to all software and operating systems.
- Access Controls. Limit VPN and administrative access to only necessary personnel.
- Email Filtering. Deploy threat protection for Office 365.

The following table outlines the activities involved in preparing for such a cyber incident.

PREPARATION.	
PHASE OBJECTIVES.	• Prepare the organization to respond in a timely and effective manner to a cyber incident. • Inform employees of their role in remediating such cyber incidents.
KEY STAKEHOLDERS.	• IT Manager • Executives overseeing business continuity • Managed Security Service Provider (if applicable)
SYSTEMS OVERVIEW.	• Centralized POS System. Accessible over VPN from retail terminals; supports billing, manufacturing, and accounting. • Email Services. Managed through Office 365. • Windows Domain Workstations. Used by employees for daily operations. • Backup Process. Weekly backups on an external hard drive with old backups overwritten when full.
ACTIVITY.	DESCRIPTION.
	ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO:

Prepare to respond.	• Conduct a thorough review and rehearsal of cyber incident response procedures. • Ensure clarity of both technical and business roles and responsibilities.
Inform employees	• Conduct regular training and awareness to remain in compliance with the NIST Framework highlighting information security risks faced by employees: - Phishing - Ransomware - Reporting suspected cyber incidents • For employees that manage confidential or high-risk data, and or systems, ensure regular training is mandated.

DETECTION AND ANALYSIS.

Proper detection and analysis are critical for understanding the scope of a ransomware incident and determining an effective response.

Assess the following table that outlines the detection phase process.

DETECT.	
PHASE OBJECTIVES.	• Complete initial investigation. • Report the incident formally and to the correct team.
KEY STAKEHOLDERS.	• IT Manager • Incident Response Team • Managed Security Service Provider (if applicable)
ACTIVITY.	DESCRIPTION.
DETECTION AND REPORTING.	ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO: • Monitor detection channels and common attack methods. - Spoofed emails. - Web browser vulnerabilities. - Emails with external or unknown links. - Notifications in internal communications of suspicious emails. • Report on the incident. Raise a ticket if one does not exist. • Follow the communication and escalation process defined in the playbook.

	• Consider whether data loss or breach has occurred.
INITIAL SIGNS AND INVESTIGATION.	• Identify initial signs. - POS terminal fails to sync with HQ systems. - Employees report being locked out of accounts. - Ransom notes appear on screens. - Employees may notice suspicious emails, system slowdowns or file inaccessibility with strange file extensions. • System behaviour monitoring. - Unusual file activity with a spike in file writes, deletion or renames. This would be especially concerning in shared drives. - High outbound traffic, especially with unfamiliar IP addresses. - Significant number of login attempts. • Log analysis: - Check for unusual authentication attempts. - Look for unknown connections. - Office 365 audit logs, suspicious email forwarding rules, or mass emails sent to employees or customers. • Identify spoofed emails. • Thoroughly document the initial incident. - Incident type. - How many users received phishing emails? - Incident cause. - Current actions. - System and location of detection. - Indicators of Compromise (e.g .locked .crypt, unauthorized access logs to VPN or POS, or suspicious changes in Office 365 accounts or email forwarding rules) - Number of affected systems. • Secure artifacts for further hardware and memory forensics and analysis steps.

INCIDENT ANALYSIS.

This section is more thorough to help identify and proceed with incident response and reporting.

ASSESSMENT.

In the assessment phase, focus on understanding the full scope and impact of the ransomware incident. This involves identifying which systems, such as servers, workstations, and services like the POS system and Office 365, have been affected. Key questions include whether the POS terminals remain operational if their connection to headquarters has been disrupted and whether Office 365 accounts have been compromised or used to further the attack. The assessment also examines the extent of the compromise, determining if only encrypted files are affected or if the malware has accessed sensitive data and spread to other systems. Additionally, identifying the time of infection is crucial, which involves tracing the initial infection point using timestamps from ransomware-related file modifications or login attempts to pinpoint the patient zero system.

The following chart outlines an effective assessment and response process.

Source - CyberAlberta

DAMAGE ESTIMATION.

Damage estimation involves evaluating both the business and data impacts of the incident. From a business perspective, this includes estimating revenue loss due to downtime of the POS systems, which affects the ability to process sales, and assessing the disruption to customer order fulfillment. On the data side, it is important to identify which critical files have been encrypted or deleted, such as financial records and inventory data. Additionally, verifying the status of backups to determine whether they have compromised or remain intact, is crucial for recovery efforts.

- Downtime for POS systems: Estimate revenue loss from the inability to process sales.
- Assess disruption to order fulfillment.
- Identify critical files encrypted or deleted (e.g., financial records, inventory).
- Verify whether any backups have been compromised or are still intact.

ROOT CAUSE ANALYSIS.

Root cause analysis aims to uncover how the ransomware incident occurred and to prevent future occurrences. This involves analyzing any suspected phishing emails to determine their effectiveness, who received them, and the nature of the malicious payload, such as an attachment or link. It also examines whether the email was forwarded internally, potentially spreading the threat. Investigating compromised accounts is another step that is critical, specifically focusing on whether Office 365 credentials were used to access the VPN or other systems. Additionally, malware behaviour analysis is conducted using sandboxing tools to safely execute the ransomware in a controlled environment. This helps to observe its behaviour, such as the types of files it encrypts and whether it attempts to exfiltrate datas. This comprehensive analysis helps in understanding the attack vector and implementing measures to mitigate future risks.

- Was the email convincing, and who received it?
- What malicious payload did the email contain (e.g., an attachment, a link)?
- Was the email forwarded internally?

KEY QUESTIONS TO ANSWER

- What systems and data are affected?
- How did the ransomware gain entry?
- Are backups intact and secure?
- What is the estimated time for recovery?
- Has any customer or financial data been exfiltrated?

INCIDENT CLASSIFICATION.

LEVEL 1. MINOR INCIDENT. MINIMAL DISRUPTION THAT CAN BE QUICKLY RESOLVED	• A single workstation is infected. • No sensitive data is compromised. • Ransomware is contained with minimal disruption.
LEVEL 2. MODERATE INCIDENT. SOME OPERATIONAL IMPACT THAT REQUIRES ATTENTION.	• POS terminals or multiple workstations are impacted. • Partial service disruption occurs. • Recovery can be managed internally with existing backups,
LEVEL 3. MAJOR INCIDENT. SIGNIFICANT DISRUPTION WITH HIGH RISK TO DATA AND OPERATIONS.	• Centralized POS system or Office 365 services are compromised. • Operations are at a standstill. • Financial or customer data is at risk of exfiltration. • External cybersecurity assistance is required.

ESCALATION DECISIONS.

Level 1: Managed by Vern and the internal IT team.

Level 2: Notify leadership and involve external cybersecurity consultants.

Level 3: Declare a major incident, involve legal counsel, and contact law enforcement if data exfiltration is suspected.

ESCALATION.	
ACTIVITY.	DESCRIPTION.
MINOR INCIDENT	ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO: Affects a single workstation, no sensitive data compromised, minimal disruption. • Assign the incident to Vern and the internal IT team for immediate resolution. • Document the incident details, actions taken, and resolution in the incident management system. • Monitor the situation to ensure containment and resolution. Inform relevant internal stakeholders of the incident and resolution.
MODERATE INCIDENT	Impacts multiple workstations or POS terminals, partial service disruption, manageable internally.

	• Notify IT leadership and convene an internal incident response team. • Engage external cybersecurity consultants for additional support and expertise. • Conduct a detailed investigation to understand the scope and impact. • Implement recovery procedures using existing backups. • Inform leadership and affected departments of the incident and response actions. - Prepare external communication if customer-facing services are impacted, ensuring transparency and reassurance.
MAJOR INCIDENT	Centralized systems compromised, operations at a standstill, high risk of data exfiltration. • Declare a major incident and activate the full incident response plan. • Assemble a cross-functional incident response team, including IT, legal, communications, and executive leadership. • Engage external cybersecurity experts for comprehensive incident management. • Conduct a thorough investigation to assess the extent of the compromise and potential data exfiltration. • Coordinate with legal counsel to understand regulatory and legal obligations. • Contact law enforcement if data exfiltration or criminal activity is suspected. Provide regular updates to executive leadership and the board of directors. - Develop and execute a communication plan for internal and external stakeholders, including customers, partners, and regulators. - Ensure all communications are clear, accurate, and consistent with legal and regulatory requirements.
CONTAINMENT, MITIGATION, REMEDIATION.	
ACTIVITY.	DESCRIPTION.
CONTAINMENT	ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO: • Identify systems being impacted or at risk of impact • Reduce any further malicious activity by:

	- Preventing the phishing activity. - Quarantining affected systems and removing them from the network. - Applying access controls to isolate from production networks. • Block access to any identified remote access tools. - Prevent communication with command-and-control servers, websites, and exploited applications.
MITIGATION	• Use network monitoring tools to detect unusual activity and identify systems showing signs of compromise. • Segment the network to isolate compromised segments from the rest of the network. • Disable any unnecessary services or ports on affected systems to reduce the attack surface.
ERADICATION	• Identify removal methods from the results of the attack. • Conduct a restoration of affected networked systems from a trusted backup. • Reinstall any standalone systems from a clean OS backup before updating with trusted data backups. • Change any compromised account details. • Confirm policy compliance.
RECOVER TO BAU	• Recover systems based on business impact analysis and business criticality. • Complete vulnerability scanning of all systems, across the estate. • Reset credentials and user account details of all involved systems. • Reintegrate previously compromised systems. • Restore any corrupted or destroyed data. • Restore any suspended services. • Establish monitoring to detect further suspicious activity. • Coordinate the implementation of any necessary patches or vulnerability remediation activities.

COMMUNICATION.

The following table outlines an appropriate communication process.

Timing	From	To	General Message
After initial assessment is completed and initial communication occurred	Cybersecurity	Forensics Team IT Support Teams Leadership	Notify Forensics team to preserve any evidence as required for root cause analysis. IT support teams (namely, server, storage and/or back-up teams) to resolve encrypted files. Leadership should be provided a high-level resolution plan.
Routinely according to the impact and urgency to restore the data	Cybersecurity	Leadership	Leadership should retrieve routine status updates.
After the initial impact has been assessed	Cybersecurity	Communications Team	If your organization has a communications team, they may be able to support stakeholder, internal, and public communications. Ensure communications is aware of high-level updates, as they may impact messaging. Public communications materials and approach should be approved by appropriate members of cybersecurity and leadership.
After privacy impacts have been discovered	Cybersecurity	Privacy Team	The Privacy team will need to be notified to initiate their own processes for response to privacy beaches.
After the initial impact has been assessed and there are any suspected acts, regulation, or policy violations	Cybersecurity	Legal Team	The legal team should be notified of the nature of the impact, including the type of data, and whom the stakeholders are for this data. They may need to look at the legal implications the loss could present.

Timing	From	Tactic	General Message
Upon notification	Communications	Communications plan Key messages	Outline the overall communications approach for stakeholders, staff, and the public. Develop key messages that share the most important pieces of information with the audience to help keep messaging consistent. Consider timing and messaging. Be transparent without sharing sensitive information. The plan and messaging should be approved by appropriate members of cybersecurity and leadership.
In response to public inquiries	Communications	Social media	Provide high-level updates to keep clients informed on the situation. Responding to public comments can help control the narrative and reduce speculation. Individuals will often go to social media when experiencing a technical issue. Avoid sharing sensitive or undetermined information, including restoration timelines. Depending on the level of public impact, consider whether a reactive or proactive approach is most appropriate. Reactive may be more suitable when public impacts are minimal, whereas proactive may be more suitable for larger incidents.
In response to media inquiries	Communications	Media statement or response Web content Direct stakeholder communications	Provide information about the incident. If a breach results in significant public impacts, inform stakeholders of the incident and steps being taken to resolve the situation. Use existing channels and, if required, provide multiple updates. This will help reduce speculation and assure clients they are being considered during response. Be transparent without sharing sensitive information. Avoid undetermined information, including restoration timelines. It should be approved by appropriate members of cybersecurity and leadership.

Source - CyberAlberta

PRE-APPROVED COMMUNICATION TEMPLATES.

INTERNAL COMMUNICATION TEMPLATES

RANSOMWARE INCIDENT - INTERNAL NOTIFICATION

Subject: Internal Alert: Ransomware Incident Detected

Body:

Dear [Team/Department],

We have detected a ransomware incident affecting certain systems within our network. Our IT and security teams are actively working to contain and mitigate the impact. As a precaution, please refrain from accessing shared drives and sensitive systems until further notice.

Immediate actions you can take:

- Do not open suspicious emails or attachments.
- Report any unusual system behaviour to the IT help desk immediately.

We will provide regular updates as we progress in resolving this issue. Your cooperation and vigilance are crucial during this time.

Thank you for your understanding.

Best regards,
[Your Name/IT Security Team]

PHISHING INCIDENT - INTERNAL NOTIFICATION

Subject: Internal Alert: Phishing Attempt Detected

Body:

Dear [Team/Department],

A phishing attempt has been identified targeting our organization. Please be extra cautious with emails requesting sensitive information or containing suspicious links.

To protect yourself and the organization:

- Do not click on links or download attachments from unknown sources.
- Report any suspicious emails to the IT help desk immediately.

Our team is monitoring the situation closely and will keep you informed of any developments.

Thank you for your attention to this matter.

Best regards,
[Your Name/IT Security Team]

EXTERNAL COMMUNICATION TEMPLATES

RANSOMWARE INCIDENT - EXTERNAL NOTIFICATION

Subject: Important Notice: Security Incident Update

Body:

Dear [Customer/Partner],

We are writing to inform you of a recent security incident involving ransomware that has affected some of our systems. Our team is working diligently to resolve the issue and ensure the security of our network.

At this time, we have no evidence that any customer data has been compromised. We are taking all necessary steps to protect your information and will keep you updated as more information becomes available.

If you have any questions or concerns, please do not hesitate to contact our support team.

Thank you for your understanding and trust.

Sincerely,
[Your Name], FlowerPower HQ

PHISHING INCIDENT - EXTERNAL NOTIFICATION

Subject: Security Advisory: Phishing Alert

Body:

Dear [Customer/Partner],

We want to make you aware of a phishing attempt that has been targeting our organization. Please be cautious of any emails that appear to be from us requesting sensitive information or containing suspicious links.

To protect yourself:

- Verify the sender's email address before responding.
- Do not click on links or download attachments from unexpected emails.

We are actively addressing this issue and appreciate your vigilance. If you have any questions or need assistance, please contact our support team.

Thank you for your cooperation.

Sincerely,
[Your Name], FlowerPower HQ