Incident Report Plan for Johned and Davis

Drafted By Oyindamola Olayiwola

Executive Summary

The Incident Response Plan (IRP) is designed to safeguard the integrity, confidentiality, and availability of data and systems within critical business processes, specifically focusing on Customer Account Management and Transaction Processing. As Jones & Davis integrates with Garden City Wealth Management, these processes are particularly vulnerable to security threats such as data breaches and unauthorized access. The IRP aligns with the NIST Cybersecurity Framework and outlines structured responses to security incidents, ensuring a rapid and effective response to mitigate risks and restore normal operations.

Incident Response Plan Goals:

The primary objectives of this Incident Response Plan are:

- Minimize Damage: Swift identification and containment of threats to reduce potential financial and reputational harm.
- Data Protection: Safeguard sensitive customer information and transaction data from unauthorized access or exposure.
- Ensure Business Continuity: Maintain the availability of critical services and systems during and after an incident.
- Comply with Regulatory Standards: Ensure all actions align with industry regulations and compliance requirements.
- Continuous Improvement: Learn from each incident to improve security posture and incident handling procedures.

Revision History

The Incident Response Plan has been modified as follows:

Date	Version	Modification	Modifier
18th Octobber, 2024	v1.01		Oyindamola

TESTING & REVIEW CYCLE

Testing of the Incident Response Plan is necessary to ensure the CSIRT (Cyber Security Incident Response Team) is aware of its obligations. Unless real incidents occur, which test the full functionality of the process, this can be achieved using walkthroughs and practical simulations of potential incidents.

1. The Incident Response Plan will be tested at least once semi-annually.
2. The Incident Response Plan Testing will test your business response to potential incidents, identifying process gaps and improvement areas.
3. The CSIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and aspects that need improvement.
4. The Incident Handler will ensure the Security Incident Response Plan is updated and distributed to CSIRT members.

HOW TO RECOGNIZE A CYBER INCIDENT

A cyber security incident may not be recognized straightaway; however, there may be indicators of a security breach, system compromise, unauthorized activity, or signs of misuse within your environment, or that of your third-party service providers.

Look out for any indication that a security incident has occurred or may be in progress. Some of these are outlined below:

1. Excessive or unusual log-in and system activity, in particular from any inactive user IDs (user accounts)

2. Excessive or unusual remote access activity into your business. This could relate to staff or third-party providers

3. The occurrence of any new wireless (Wi-Fi) networks visible or accessible from your environment

4. The presence of or unusual activity in relation to malware (malicious software), suspicious files, or new/unapproved executable files and programs. This could be on your networks or systems, including web-facing systems

5. Hardware or software key-loggers found connected to or installed on systems

6. Suspicious or unusual activity on, or behavior of web-facing systems, such on as e-commerce websites

7. Point-of-Sale (POS) payment devices, payment terminals, chip & PIN/signature devices, or dip/swipe card readers showing signs of tampering

8. Any card-skimming devices found in your business

9. Lost, stolen, or misplaced merchant copy receipts or any other records that display a full payment card number or card security code (the three- or four-digit number printed on the card)

10. Lost, stolen, or misplaced computers, laptops, hard drives, or other media devices that contain payment card data or other sensitive data

CSIRT Structure

CSIRT Role	Role Definition
Executive	IT Security Team
Incident Handler	The Incident Handler is the main triage role of the CSIRT. This role organizes the team and initiates the Incident Response Plan to investigate and respond to cyber security incidents.
Communication Expert	The Communications Expert is responsible for both public relations and internal communications. They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashio

Note Taker	The note-taker records the progress of the CSIRT, including anything from meeting minutes, to post-mortem reports.
Infrastructure Team	The Infrastructure Team are responsible for identifying and addressing technical issues, restoring compromised systems, and implementing preventative measures to reduce the likelihood of future incidents.
IT Security Team	They are responsible for leading incident response teams, assessing the scope and impact of breaches, implementing technical countermeasures, and communicating with stakeholders throughout the process.
Soc Analyst	They monitor network traffic, analyze logs, and investigate alerts to identify potential threats. Upon detection, SOC analysts coordinate with other teams to contain the incident, eradicate the threat, and restore normal operations. They also contribute to post-incident analysis and improvement efforts, helping to strengthen the organization's overall security posture.
Legal & Compliance Team	They provide guidance on data privacy laws, incident reporting obligations, and potential legal consequences of security breaches.
Stakeholders	Partners, vendors, customers, and regulatory bodies who may be affected by security incidents.
Forensics Team	is responsible for collecting, preserving, and analyzing digital evidence to identify the root cause of security incidents, determine the extent of damage, and gather intelligence for future prevention.
Audit Team	The Audit Team within a CSIRT is responsible for conducting regular security audits and assessments to identify vulnerabilities, assess compliance with security standards, and evaluate the effectiveness of security controls.
DR Engineer	Ensures that a company can quickly recover from a disruptive event and resume normal operations.
IT support Team	Acts as the first line of defense in identifying and reporting security incidents, provides technical assistance during incident response, and serves as a liaison between the CSIRT and end-users.
End-Users	The individuals who use the organization's IT systems and are impacted by security incidents.

CSIRT Responsibility

The responsibilities described below are organized by role within Bright Minds Learning Center.

Executive

The Executives are/is responsible for:

1. Meeting with the board of directors to best understand what is needed from a security point of view based of the organization’s business needs.
2. Regularly reporting any incidents and necessary cyber security actions to the board of directors and other executives.
3. Making decisions on the best way forward based on information provided by the CSIRT team.
4. Making sure that the roles within the CSIRT team are filled and the necessary tools/training are provided for employees to do their jobs.
5. Meeting with key roles within the CSIRT team to better understand what improvements can be

Incident Handler

The Incident Handler is responsible for:

1. Making sure that the Incident Response Plan and associated response and escalation procedures are defined and documented. Ensure the handling of security incidents is timely and effective.
2. Making sure that the Incident Response Plan is up-to-date, reviewed and tested, at least once each year.
3. Making sure that staff with Incident Response Plan responsibilities are properly trained, at least once each year.
4. Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.
5. Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as required.
6. Authorising on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required. This includes authorising access to/removal of evidence from the site.

Communication Expert

The Communications Expert is responsible for:

1. Writing and sending internal and external communications about any incident that occurred.
2. Reporting any cyber incidents to the authorities if needed.
3. Interfacing with executives and other board members to provide information.
4. Interfacing with customers to provide regular updates about any incidents that may affect their experience.

5. Collecting customer responses for impact of incidents, how they were handled and any tips/suggestions.
6. Collecting lessons learned from members of the CSIRT team and updating management.

CSIRT Team

Cyber Security Incident Response Team (CSIRT) members are responsible for:

1. Making sure that all staff understand how to identify and report a suspected or actual security incident.
2. Advising the Incident Handler of an incident when they receive a security incident report from staff.
3. Investigating each reported incident.
4. Taking action to limit the exposure of sensitive information or payment card data and to reduce the risks that may be associated with any incident.
5. Gathering, reviewing, and analysing logs and related information from various central and local safeguards, security measures and controls.
6. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
7. Reporting each security incident and findings to the appropriate parties. This may include the acquirer, card brands, third party service providers, business partners, customers, etc., as required.
8. Helping law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
9. Resolving each incident to the satisfaction of all parties involved, including external parties.
10. Initiating follow-up actions to reduce the likelihood of recurrence, as appropriate.
11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

Note Taker:

1. Document all incident-related activities and decisions.
2. Maintain a detailed record of the incident response process.
3. Provide support to the incident handler and other team members.
4. Assist in the creation of incident reports.
5. Maintain a secure repository for incident-related documentation.

Infrastructure Team:

1. Identify and isolate compromised systems.
2. Restore systems and data to a secure state.
3. Implement security patches and updates.
4. Monitor network and system activity for suspicious behavior.
5. Provide technical support to the incident response team.

IT Security Team:

1. Conduct security assessments and audits.
2. Identify and address vulnerabilities.
3. Implement security controls and best practices.
4. Investigate security incidents and analyze root causes.
5. Provide technical expertise and guidance to the incident response team.

Soc Analyst:

1. Monitor networks, systems, and logs for suspicious activity.
2. Detect and investigate security incidents.
3. Analyze threat intelligence and identify emerging threats.
4. Provide alerts and notifications to the incident response team.
5. Assist in incident containment and eradication.

Legal & Compliance Team:

1. Provide legal advice and guidance during incidents.
2. Ensure compliance with relevant regulations and standards.
3. Conduct legal investigations and document evidence.
4. Coordinate with law enforcement agencies as needed.
5. Manage legal proceedings related to security incidents.

Forensics Team :

1. Collect, preserve, and analyze digital evidence.
2. Identify the root cause of security incidents.
3. Provide expert testimony in legal proceedings.
4. Assist in incident investigation and analysis.
5. Develop best practices for digital forensics within the organization.

Audit Team:

1. Conduct regular security audits and assessments.
2. Evaluate the effectiveness of security controls.
3. Identify vulnerabilities and recommend corrective actions.
4. Review incident response plans and conduct tabletop exercises.
5. Ensure compliance with industry regulations and standards.

IT suppoort Team :

1. Provide technical support to end-users during incidents.
2. Identify and report suspicious activity to the CSIRT.
3. Assist in incident containment and recovery.
4. Provide information and updates to end-users.
5. Ensure that systems and applications are up-to-date with security patches.

End-Users:

1. Report suspicious activity or incidents to the CSIRT.
2. Follow security best practices and avoid clicking on suspicious links or downloading attachments from unknown sources.
3. Comply with security policies and procedures.
4. Provide feedback on security awareness training and incident response processes.

Incident Severity Matrix

The CSIRT will determine the severity of the incident. They will consider:

1. whether a single system is affected or multiple
2. the criticality of the system(s) affected
3. whether impacting a single person or multiple
4. whether impacting a single team/department, multiple teams/departments, or the entire organization

The Incident Handler must consider the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remedial action.

The CSIRT will consider the available information to determine the known magnitude of impact compared with the estimated size, along with likelihood of the effect spreading and the potential pace of such spread. The CSIRT will determine the potential impacts to the organization, including financial damage, brand and reputational damage, and other types of harm.

The incident may be the result of a sophisticated or unsophisticated threat, an automated or manual attack, or may be nuisance/vandalism.
The CSIRT will determine:

1. whether there is evidence of the vulnerability being exploited
2. whether there is a known patch
3. whether this is a new threat (for example, zero day) or a known threat
4. the estimated effort to contain the problem

OTHER STAKEHOLDER CONTACTS

Role	Organization	Name	Title	Phone	Email

INCIDENT TYPES

Type	Description
Unauthorized Access or Usage	Individual gains physical or logical access to network, system, or data without permission.
Phishing Attack	Attempts to trick users into revealing sensitive information through deceptive emails or messages.
Service Interruption or Denial of Service	Attack that prevents access to the service or otherwise impairs normal operation.
Malicious Code	Installation of malicious software (for example, virus, worm, Trojan, or other code).
Ransomware	A specific type of malicious code that infects a computer and displays messages demanding a fee be paid in order for the system to work again.

Distributed Denial of Service (DDoS)	Distributed denial-of-service attacks target websites and online services. The aim is to overwhelm them with more traffic than the server or network can accommodate. The goal is to render the website or service inoperable. Symptoms are widespread connectivity failures or system unavailable errors.
Network System Failures (widespread)	An incident affecting the confidentiality, integrity, or availability of networks.
Application System Failures	An incident affecting the confidentiality, integrity, or availability of applications or systems.
Unauthorized Disclosure or Loss of Information	An incident affecting the confidentiality, integrity, or availability of data.
Information Security/Data Breach	An incident that involves real or suspected loss of sensitive information.
Account Data Compromise	A data breach incident specific to payment card data. Such events result in unauthorized access to or exposure of payment card data (cardholder data or sensitive authentication data).
Configuration ErroR	Incorrect settings leading to security vulnerabilities or data loss.
Human Error	Mistakes or errors made by employees that lead to security incidents.
Other	Any other incident that affects networks, systems, or data.

Incident Severity Matrix

The CSIRT will determine the severity of the incident. They will consider:

1. whether a single system is affected or multiple
2. the criticality of the system(s) affected
3. whether impacting a single person or multiple
4. whether impacting a single team/department, multiple teams/departments, or the entire organization

The Incident Handler must consider the relevant business context and what else is happening with the business at the time to fully understand the impacts and urgency of remedial action.

The CSIRT will consider the available information to determine the known magnitude of impact compared with the estimated size, along with likelihood of the effect spreading and the potential

pace of such spread. The CSIRT will determine the potential impacts to the organization, including financial damage, brand and reputational damage, and other types of harm. The incident may be the result of a sophisticated or unsophisticated threat, an automated or manual attack, or may be nuisance/vandalism.
The CSIRT will determine:

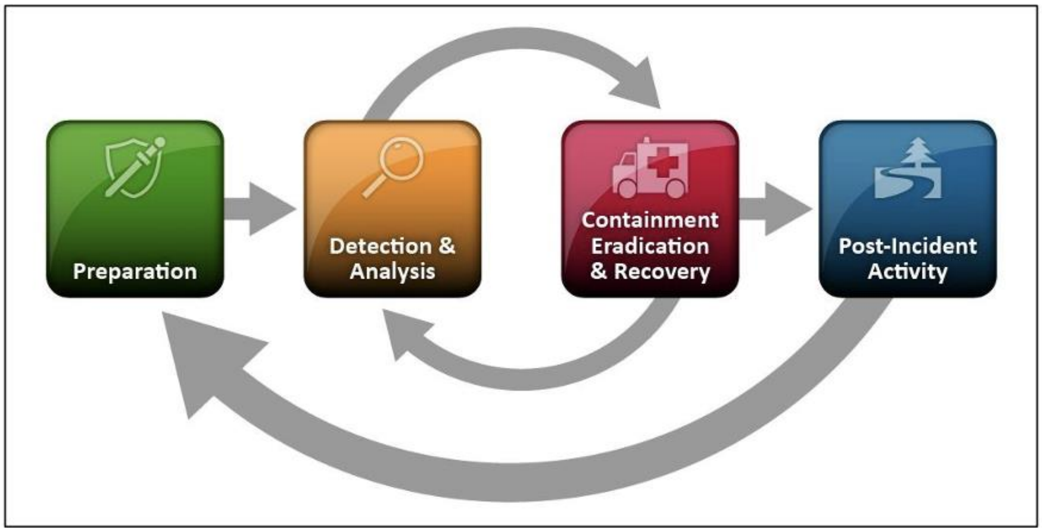
1. whether there is evidence of the vulnerability being exploited
2. whether there is a known patch
3. whether this is a new threat (for example, zero day) or a known threat
4. the estimated effort to contain the problem

Category	Indicators	Scope	Action
1 – Critical	Data loss, Malware	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
2 – High	Theoretical threat becomes active	Widespread and/or with critical servers or data loss, stolen data, unauthorized data access	Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide
3 – Medium	Email phishing or active spreading infection	Widespread	Implement CSIRT, Incident Response Plan, create Security Incident, Organization-wide
4 - Low	Malware or phishing	Individual host or person	Notify CSIRT, create Cyber Security Incident

Incident Handling Process

Incident Handling Process Overview

In the event of a Cyber Security Incident the Cyber Security Incident Response Team will adhere to the Nist Incident Response process as follows.



PREPARATION

In preparation for a cyber security incident my organization commits to:

- Build an Incident Response Plan
  - Establish mandate, delegate authority decision making process and chain of command
- Create a soft and hard copy of the Incident Response Plan
- The hard copy of the plan is located at Head Office, on the Office Manager's Desk
- Review/update the incident response plan annually. Record the last revision date on the Revision History section
- Ensure a cyber security incident response team is created
  - Dedicated, virtual, or on-retainer
  - Provide training as necessary
- Document roles and responsibilities
  - Delegate authority
  - Provide training as necessary
- Conduct exercises, drills regularly
  - Consider that most incident types are known in advance
  - Prepare for the known so the CSIRT can focus on the unknown
  - Test the plan, team and tools
- Understand the environment
  - Diagrams, location of critical systems and data
  - Ensure adequate visibility into networks and systems to respond to an incident
  - Vendor environment
  - Understand dependencies

- Understand what controls are in place
    - Are they sufficient to mitigate risk to an acceptable level?

- Understand impacts
    - Determine Maximum Tolerable Downtime (MTD) (max. time a business can be disrupted without causing significant harm) and Acceptable Interruption Window (AIW) (max. time a system can be unavailable)
    - Prioritized list of assets and downtime

- Prepare war room and/or conference bridge(s)
    - Determine and prepare a location to convene, physically or digitally
    - Ensure location is secure and appropriately equipped

- Establish communications plan in advance

- Establish agreements in advance
    - Incident Response Contacts on retainer
    - Ensure annual plan review/update
    - Regular exercises
    - Familiarity with environment in advance
    - Preferred pricing
    - Established service-level agreement (SLA), response times

- Ensure a central point of contact exists for employees to report real or suspected cyber security incidents

- Ensure all employees are required to report cyber security events
    - Information security incidents must be reported, without delay, to the Incident Handler (preferable) or to another member of the Cyber Security Incident Response Team (CSIRT). The member of the CSIRT receiving the report will advise the Incident Response Handler (or the Backup) of the incident
        - In the event that a security incident or data breach is suspected to have occurred, staff member shall discuss their concerns with their line manager, who in turn may raise the issue with a member of the CSIRT
    - Ensure all employees know they are required to report cyber security incidents and how
    - Ensure all employees report cyber security incidents in a timely fashion

IDENTIFICATION

In the event that a cyber security incident is identified, my organization commits to:

- Bring together those who are aware of the incident

- Engage Cyber Security Incident Response Team members

- Remind all with responsibility to maintain need-to-know
    - Failure to do so leads to managing misinformation

- Communicate effectively and efficiently
- Convene in war room or conference bridges
    - Ensure location is secure and appropriately equipped
- Often more than one location is required for different needs (for example, the management and technical team)
- CSIRT to investigate and determine whether an incident has occurred
    - Is it an event or an incident?
    - Search for correlating information to increase confidence there is a real incident
- Perform triage and ensure common understanding of how it was detected and who is aware
- Analyze the precursors and indicators
- Perform research (for example, search engines, knowledge base)
- Document the investigation and evidence gathering
- Prioritize handling of incident based on relevant factors (functional impact, information impact, recoverability effort, etc.)
    - Please execute special response steps, if the following cyber security incidents are confirmed. Please consult the sections below for each specific incident type
- Determine severity, urgency and initial impact
- Review information and actions taken to date
- Report incident to appropriate internal personnel and external organizations

CONTAINMENT

In the event of a cyber incident my organization commits to:

- Invoke a communications plan respecting need-to-know
- Develop stakeholder relationship map, to determine the level of stakeholder involvement
- Ensure reported information is factual based on evidence available at the time
- Ensure a point of contact knows the current status at all times
- Implement incident response playbook
- Prevent further damage by containing the incident
- Determine the source, what vulnerability was exploited and implement repairs
- Continue impact/damage assessment and confirm the scope of the incident
- Determine what was changed (for example, files, connections, processes, accounts, access)
- Acquire, preserve, secure and document evidence and preserve the chain of custody

- Continue taking notes, ensuring a detailed log about what was found and what you did about it

For additional assistance:
In the event that CSIRT requires help in containment, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will help with additional expertise.

ERADICATION

In the event of a cyber incident my organization commits to:

- Eradicate the incident
- Remove all traces of the infection or other incident
  - Identify and mitigate all vulnerabilities that were exploited
  - Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (for example, new malware infections), perform the identification steps on the newly identified examples, then contain
- Ensure the incident cannot re-occur
- Further understand the attack method and exploited vulnerabilities
- Continue taking notes, ensuring a detailed log
- Ensure any compromised machines are removed or formatted before placing back into service
  - Ensure necessary evidence has been collected

For additional assistance:

- In the event that the CSIRT requires help in eradication, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will provide additional help and expertise

RECOVERY

In the event of a cyber incident my organization commits to:

- Eradicate the incident
- Remove all traces of the infection or other incident
  - Identify and mitigate all vulnerabilities that were exploited
  - Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (for example, new malware infections), perform the identification steps on the newly identified examples, then contain
- Ensure the incident cannot re-occur
- Further understand the attack method and exploited vulnerabilities

- Continue taking notes, ensuring a detailed log
- Ensure any compromised machines are removed or formatted before placing back into service
    - Ensure necessary evidence has been collected

For additional assistance:

- In the event that the CSIRT requires help in eradication, contact Network Security Vendor Support Lead or Helpdesk (see External Contact List). They will provide additional help and expertise

LESSONS LEARNED

In the event of a cyber security incident my organization commits to:

- Hold a meeting to discuss lessons learned within 2 weeks
- Create a follow up report
- Walk through and review play-by-play of incident report
    - How the incident was detected, by whom, and when
    - Scope and severity of incident
    - Methods used in containment and eradication
- Identify opportunities for improvement to better prepare for next time
- Ensure accountability to follow up on identified opportunities for improvement

[*] Multiple sources including NIST Special Publication 800-61 revision 2 and SANS

INCIDENT SPECIFIC HANDLING PROCESSES

DATA BREACH

If CSIRT investigations confirm that a Data Breach security incident has occurred, please execute the following additional steps:

1. Containment: Immediately isolate affected systems to prevent further data exposure.
2. Assessment: Evaluate the scope of the breach, identifying the type of data compromised and the number of affected individuals.
3. Notification: Notify affected individuals and regulatory bodies as required by law (e.g., GDPR, CCPA).
4. Investigation: Conduct a thorough investigation to determine the cause of the breach and how it occurred.
5. Remediation: Implement measures to address vulnerabilities that led to the breach and strengthen data protection protocols.

RANSOMWARE

If CSIRT investigations confirm that a Ransomware security incident has occurred, please execute the following additional steps:

1. Isolation: Immediately isolate infected systems from the network to prevent further spread.
2. Assessment: Identify the ransomware variant and assess the extent of the infection.
3. Communication: Inform relevant stakeholders and law enforcement if necessary.
4. Recovery Options: Evaluate options for data recovery, including restoring from secure backups or decryption tools, if available.
5. Post-Incident Review: Analyze how the ransomware infiltrated the systems and implement measures to prevent future attacks.

TAMPERING OF PAYMENT TERMINALS

If CSIRT investigations confirm that tampering of pin pads or payment terminals has occurred, please execute the following additional steps:

1. Immediate Shutdown: Disable the affected terminals to prevent further transactions.
2. Investigation: Conduct a thorough forensic investigation to determine the extent of tampering and any compromised data.
3. Communication: Notify affected customers and stakeholders regarding the potential compromise.
4. Secure Replacement: Replace compromised terminals with secure devices and ensure they are installed correctly.
5. Review Security Measures: Evaluate and strengthen physical security controls for payment terminals.

WIDESPREAD SERVICE INTERRUPTION

If CSIRT investigations confirm that a widespread service interruption security incident has occurred, please execute the following additional steps:

1. Diagnosis: Identify the cause of the interruption (e.g., DDoS attack, system failure).

2. Communication: Notify affected users and provide updates on the situation and estimated resolution time.
3. Mitigation: Implement measures to restore services as quickly as possible, including rerouting traffic or increasing server capacity.
4. Post-Incident Review: Conduct an analysis of the incident to determine root causes and any necessary infrastructure improvements.
5. Service Monitoring: Increase monitoring of services to detect future interruptions early.

NETWORK SYSTEM FAILURE

If CSIRT investigations confirm that a Network System Failure security incident has occurred, please execute the following additional steps:.

1. Containment: Isolate affected network segments or devices to prevent further spread or failure across other systems.
2. Diagnosis: Identify the root cause of the network failure (e.g., hardware malfunction, software failure, misconfiguration, or cyberattack).
3. Communication: Notify all affected users, stakeholders, and IT teams, providing regular updates on the resolution progress and expected recovery time.
4. Restoration: Restore network services by repairing or replacing faulty components (e.g., switches, routers, firewalls) or rolling back configuration changes.
5. Investigation: Conduct a detailed investigation to determine the cause of the failure and assess the extent of the outage's impact on business operations.
6. Mitigation: Apply corrective actions to ensure the issue does not reoccur, such as upgrading hardware, fixing software bugs, or updating network configurations.
7. Post-Incident Review: Analyze the incident, including the timeline of failure and recovery efforts, to identify potential areas for improvement in network resilience.
8. Backup and Redundancy: Review and improve network failover systems, ensuring redundancy in critical network paths to minimize the impact of future failures.

APPLICATION SYSTEM FAILURE

If CSIRT investigations confirm that an Application System Failure security incident has occurred, please execute the following additional steps:

1. Assessment: Evaluate the failure's impact, identifying which services, processes, or data were affected by the system crash.
2. Root Cause Analysis: Investigate the underlying cause of the failure (e.g., software bugs, configuration errors, hardware malfunctions) to understand why the system failed.

3. Communication: Notify relevant users, stakeholders, and affected departments, providing updates on the outage and estimated recovery time.
4. Recovery: Implement measures to restore the application, such as applying patches, rolling back to previous stable versions, or rebooting servers.
5. Data Integrity Check: Ensure that no data has been lost or corrupted during the failure. Restore affected data from backups if necessary.
6. Post-Incident Review: Analyze the failure to determine any underlying systemic issues and plan for long-term fixes to avoid recurrence.
7. System Hardening: Improve system resiliency by addressing the root causes, adding redundancy, and optimizing error-handling mechanisms within the application.

Malicious Code

1. Containment: Isolate infected systems and remove the malicious code.
2. Assessment: Identify the type of malware and affected systems.
3. Communication: Notify IT staff and affected users about the infection.
4. Remediation: Update antivirus definitions and apply security patches.
5. Post-Incident Review: Review security measures and user education to prevent recurrence.

Distributed Denial of Service (DDoS)

1. Containment: Implement traffic filtering or rerouting strategies to mitigate the attack.
2. Assessment: Analyze attack patterns and identify affected services.
3. Communication: Update users on service status and mitigation efforts.
4. Remediation: Deploy DDoS protection services and review capacity planning.
5. Post-Incident Review: Analyze the incident for weaknesses and improve response capabilities.

Network System Failures (Widespread)

1. Containment: Isolate affected systems to prevent further impact.
2. Assessment: Identify the cause of the failure (hardware, software, etc.).
3. Communication: Notify affected users and stakeholders about the outage.
4. Recovery: Implement fixes or restore systems from backups.

5. Post-Incident Review: Analyze root causes and implement measures to prevent recurrence.

Unauthorized Disclosure or Loss of Information

1. Containment: Isolate affected systems to prevent further data leakage.
2. Assessment: Identify the nature and extent of the disclosed information.
3. Communication: Notify affected parties and regulatory bodies if required.
4. Remediation: Strengthen access controls and data protection measures.
5. Post-Incident Review: Evaluate the incident and enhance data handling policies.

Configuration Error

1. Containment: Roll back to a previous stable configuration if possible.
2. Assessment: Identify the nature and impact of the configuration error.
3. Communication: Notify relevant IT teams and stakeholders.
4. Remediation: Implement corrective actions and adjust configuration management practices.
5. Post-Incident Review: Analyze the error's cause and improve configuration change processes.

Human Error

1. Containment: Assess the impact of the error and implement corrective actions immediately.
2. Assessment: Identify the specific error and affected systems or data.
3. Communication: Inform relevant teams and stakeholders about the error.
4. Remediation: Provide training or refreshers for staff on procedures to minimize future errors.
5. Post-Incident Review: Analyze the incident to improve training and operational protocols.

Phishing Attack

1. Containment: Warn users to avoid clicking on suspicious links and quarantine affected devices.

2. Assessment: Identify the phishing method and any compromised credentials.
3. Communication: Inform affected users and provide guidance on securing their accounts.
4. Remediation: Implement security awareness training and email filtering solutions.
5. Post-Incident Review: Analyze the attack vector and enhance user training.

Security Tooling Overview:

1. SIEM (Security Information and Event Management): Continuous monitoring and alerting.
2. Intrusion Detection and Prevention Systems (IDPS): Detects and blocks unauthorized access.
3. Data Loss Prevention (DLP): Ensures data security and prevents data leaks.
4. Endpoint Detection and Response (EDR): Identifies suspicious activity on devices.
5. Backup and Recovery Solutions: Secures offsite data storage and restores services quickl

APPROVALS

RESPONSIBLE PARTY

Responsibility for the security of company and customer information resides with the following Responsible Party:

Responsible Party Name and Title	Responsible Party Signature	Version	Date
CISO			
CIO			
CSIRT			

HR			
Communication Lead			

The Responsible Party has reviewed the Incident Response Plan and delegates the responsibility for mitigating harm to the organization to the Incident Handler.

During times when a high or critical cyber security incident is underway this responsibility is entrusted to the Incident Handler or their delegate.

INCIDENT HANDLER

The Incident Handler has reviewed the Security Incident Response Plan and acknowledges that, when a high or critical cyber security incident is underway, responsibility for managing the incident is entrusted to the Incident Handler or their delegate.

The Incident Handler or their delegate is expected to handle the incident in a way that mitigates further exposure of the organization. The incident will be handled according to process including identification, containment, eradication, recovery, and lessons learned.

Incident Handler Name and Title	Incident Handler Signature	Version	Date
John Doe			20th October,2024

Conclusion

Incident response planning is a critical component of a robust cybersecurity strategy. A well-developed plan outlines the steps an organization should take to respond to security incidents effectively, minimizing damage, protecting sensitive data, and restoring operations quickly.

Key takeaways from the incident response plan:

- Proactive Preparation: The plan emphasizes the importance of being prepared for incidents by developing clear procedures, training staff, and conducting regular testing.

- Swift Response: The plan outlines steps for rapid identification, containment, eradication, and recovery from incidents.
- Data Protection: Protecting sensitive customer data is a key priority. The plan includes measures to safeguard data and prevent unauthorized access.
- Regulatory Compliance: The plan aligns with industry regulations and ensures compliance with data privacy and security standards.
- Continuous Improvement: Regular testing and updates of the plan are essential for ensuring its effectiveness and identifying areas for improvement.

By implementing and maintaining a well-developed incident response plan, organizations can significantly reduce their risk of experiencing security incidents and mitigate their impact if they do occur.