Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
Unknown	100%

Report Generated: Tuesday, April 15, 2025 at 12:08 PM

Guided Exercises

Part 1: Research Incident Response Plans

3. **Describe** the key components within the incident response plan you identified. Be sure to cite the plan by including a link.

The State of Michigan Sample Cyber Incident Response Plan has several key components. Here is a list derived from key sections of the plan:

General Purpose of the Incident Response Team

The IRT protects the organization's information assets, acts as a central hub for incident handling, maintains regulatory compliance, prevents system misuse in attacks to prevent legal liability, and minimizes harmful exposure.

Incident Response Methodology: The Six Stages

Preparation – Develop and train on the IRP before an incident happens.
Identification – Detect and confirm if an incident has occurred.
Containment – Limit the scope and impact immediately.
Eradication – Eliminate the root cause, such as malware, compromised accounts, etc.
Recovery – Restore systems and validate they are clean.
Follow-up – Document lessons learned, update policies, and support legal actions.

Incident Severity Levels

Incidents are categorized into four severity levels:
Low – Minimal impact, such as spam
Medium – Service delays, operational disruptions
High – Compromise of confidential info, major disruptions
Extreme – Catastrophic loss, public disclosure, complete service outages

Incident Response Team Members

The plan emphasizes a multidisciplinary team with the following roles:
Cyber Incident Response Management - the CISO or identified IT leadership position.
Cyber Incident Response Coordinator - a security operations lead who provides oversight of the response.
Technical Operations & Cyber Ops Teams – Hands-on incident containment and resolution
Communications/Media Team – Internal and external messaging
Extended Technical Team – Vendors or external specialists
Administrative Support - an administrative assistant trained in emergency procedures for documentation, scheduling, compliance tasks, etc.
Extended Team – Includes Legal, HR, Finance, Risk Management, Executive Management, Cyber Insurance provider, and local law enforcement

Escalation Levels

Incidents escalate based on severity and impact:
Low > Medium > High > Extreme
As severity increases, more teams get involved, and higher-level decisions are made.

Roles & Responsibilities by Escalation Level

Each level includes specific roles for detection, communication, and response. Detailed logs are maintained to support legal or compliance needs.

Special Circumstances

Includes procedures for email system unavailability, leaked personal/health information, and the use of alternative communication methods like phone trees

Post-Incident Activities

Reporting on damages, actions taken, and future mitigations
Policy updates are adjusted based on lessons learned

Appendices and Examples

incident response diagrams and examples,
detailed scenarios include a server vulnerability, a phishing attack, and a stolen device with leaked PII
incident reporting template

https://www.michigan.gov/dtmb/-/media/Project/Websites/dtmb/Services/Cybersecurity/MI_Sample_CyberSecurity_Incident_Response_Plan.docx?rev=0724fd209e0c47e583625868586e7ccb&hash=A80455AAFDA48F98A7A762031F558F23

6. **Outline** the six-step methodology for performing incident response. **List** each step and its purpose. How closely does the plan that you reviewed follow this methodology?

The SANS Six-Step Incident Response Methodology

Preparation -Establish policies, procedures, and tools to handle incidents, form a Computer Security Incident Response Team (CSIRT) with defined roles, conduct risk assessments, and provide training to ensure readiness
Identification -Detect potential security incidents through monitoring and alerts, analyze events to confirm if they constitute actual incidents, document findings, and notify appropriate stakeholders
Containment -Implement short-term measures to limit the spread of the incident, develop long-term strategies to prevent recurrence while maintaining business operations, and preserve evidence for further analysis
Eradication -Remove the root cause of the incident, such as malware or unauthorized access, apply necessary patches and updates to affected systems, and ensure all threats are completely eliminated
Recovery -Restore systems to normal operation in a controlled manner, monitor systems for any signs of weakness or further compromise, and validate that systems are functioning correctly and securely
Lessons Learned -Conduct a post-incident review to analyze the response, identify improvements, update policies and procedures based on insights gained, and share findings with relevant parties to enhance future readiness.

The Michigan Sample Cybersecurity Incident Response Plan does align closely with the SANS six-step methodology:

Preparation -The plan emphasizes readiness through defined roles, training, and resource allocation.
Identification - It outlines procedures for detecting and confirming incidents using monitoring tools.
Containment - The plan details both immediate and long-term containment strategies to mitigate impact.
Eradication - It includes steps for removing threats and addressing vulnerabilities.
Recovery - The plan provides guidance on restoring systems and verifying their integrity.
Lessons Learned - It mandates post-incident analysis to improve future response.

The Michigan plan effectively incorporates the SANS framework, providing a comprehensive approach to incident response.

Part 2: Create an Incident Response Policy

2. **Describe** how this policy would be associated with an incident response plan.

The SANS Security Response Plan Policy acts as a governance framework that requires every business unit to create and maintain a tailored Incident Response Plan (IRP). While the policy sets high-level expectations, the IRP is the tactical document that outlines exactly how the organization will respond when a security incident occurs.

The policy emphasizes that each business unit is responsible for developing the plan in coordination with the organization's information security team. This collaboration provides consistency while allowing each plan to be specific to the systems, products, or services it supports.
The policy requires key elements in every IRP, including accurate contact information for after-hours response, clearly defined triage and mitigation steps, and a tested process for resolving incidents. It also mandates that response timelines be aligned with a security event's severity and potential impact, whether to customer trust, brand reputation, or operational continuity.

The policy enforces accountability by requiring plans to be documented, version-controlled, and available online. Without a proper plan in place in the event of an incident, non-compliance can lead to delays in product and/ or service development and disciplinary action.

The policy acts as the blueprint, and the IRP is the execution. Together, they guarantee that the organization is prepared to respond to cyber threats and does so consistently, coordinated, and effectively.

Policy Statement
Insert policy verbiage here.

Policy Statement

Bankwise Credit Union is committed to protecting its information systems, customer data, and physical infrastructure from cybersecurity threats, breaches, and other security incidents. The organization establishes this Incident Response Team - Access and Authorization Policy to detect, contain, and recover from such events.

This policy formally grants the Bankwise Credit Union Incident Response Team (IRT) full authority to act on behalf of the organization during any verified or suspected cybersecurity incident. The IRT is empowered to take all necessary actions, including collecting and preserving digital and physical evidence, to maintain the investigation's integrity and provide compliance with legal, regulatory, and organizational requirements.

During an incident, the IRT shall have unrestricted access to all organization-owned physical facilities, IT assets, systems, applications, and data. This authority includes but is not limited to isolating affected systems, conducting forensic investigations, performing content and email filtering audits, and securing physical or digital evidence in a manner that maintains an unbroken chain of custody.

This policy applies to all departments, employees, contractors, and business units. This policy shall be reinforced through annual security awareness training as part of the organization's compliance with the Gramm-Leach-Bliley Act (GLBA) and industry best practices.

Purpose/Objectives

Insert the policy's purpose as well as its objectives; use a bulleted list for the policy definition. Define the incident response team members and the authorization and authority granted to them during a crisis or while securing an incident situation.

Purpose / Objectives

This policy aims to define the roles, responsibilities, and authority of the Bankwise Credit Union Incident Response Team (IRT) in the event of a cybersecurity incident or security breach. The policy ensures the IRT has the necessary access and authorization to act swiftly, effectively, and in accordance with regulatory requirements, particularly the Gramm-Leach-Bliley Act (GLBA), to contain, investigate, and recover from incidents while preserving evidence and minimizing organizational impact.

Policy Objectives

*Ensure a rapid, coordinated, and effective response to security incidents.
*Establish clear authority for the Incident Response Team.
*Enable the IRT to secure, investigate, and document incidents while preserving the chain of custody for all physical and digital evidence.
*Minimize risk to critical systems, sensitive data, and customer trust.
Support compliance with GLBA and industry cybersecurity best practices.
*Provide enterprise-wide enforcement and accountability through defined roles and authority.

Incident Response Team Definition and Authority

The Bankwise Credit Union Incident Response Team (IRT) is a cross-functional group composed of members from the following units:
- Information Security (lead)
- IT Operations
- Legal and Compliance
- Human Resources
- Executive Management
- Communications and Public Relations

During an active incident, IRT members are granted full authority to:
*Access and secure any physical or logical IT asset or location owned by the organization.
*Isolate affected systems or networks to prevent further harm.
*Monitor, review, and log all relevant digital activity.
*Collect, preserve, and analyze physical and electronic evidence while maintaining a chain of custody.
*Communicate with internal and external stakeholders as required.
Direct staff actions necessary for incident containment and recovery.

All organizational units must fully cooperate with the IRT during an incident, and no individual may interfere with or obstruct the team's activities.

Scope

Define this policy's scope and whom it covers. What elements, IT assets, or organization-owned assets are within the scope of this policy? What access and authority are granted to the incident response team members that may be outside of standard protocol?

Scope

This policy applies to all employees, contractors, consultants, vendors, and temporary personnel who access, manage, or utilize Bankwise Credit Union's information systems, networks, data, or physical assets. It covers all business units and branch locations under the organization's control, including remote operations and cloud-based services.

The scope of this policy includes, but is not limited to, the following elements:
*All organizational IT systems, including servers, workstations, laptops, mobile devices, networking equipment, and virtual infrastructure.
*All software and applications, including core banking systems, customer relationship management tools, and third-party integrations.
*All data, including customer financial records, internal business communications, email systems, audit logs, and backup data.
*Internet usage systems, including web content filtering platforms and activity monitoring tools.
*Email systems and associated security controls, including spam filtering, encryption, and usage logging.
*Physical assets and facilities, including data centers, branch offices, communication equipment, and storage areas where evidence or sensitive systems may reside.

Expanded Access and Authority During an Incident

In the event of a security incident, breach, or declared crisis, members of the Incident Response Team shall be granted elevated authority beyond standard operating protocol. This access and authority shall include full access to any system, device, facility, or dataset required for investigation, regardless of data ownership or departmental boundaries, the authority to bypass standard change control, access control, or escalation procedures if necessary to contain or mitigate an active threat, permission to seize and isolate organizational devices or systems suspected of compromise, authorization to monitor and log user activities on organizational assets as part of forensic analysis, access to personnel records, access logs, and internal communications when required for investigation, in coordination with HR and Legal, and the authority to take control of communication channels, such as email, intranet messaging, or public relations notices, to ensure consistent messaging and limit the spread of misinformation.

This policy guarantees that the IRT can act without delay or obstruction during an incident, enabling a speedy and legally proper response to protect the organization, including its employees, assets, and customers.

Standards

Does this policy point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards

Standards

This policy aligns with and supports the implementation of specific hardware, software, and configuration standards critical to the success of incident response activities at Bankwise Credit Union. These standards guarantee that incident detection, containment, forensics, and recovery can be performed effectively and in compliance with internal protocols and regulatory compliance such as the Gramm-Leach-Bliley Act (GLBA). These standards support a consistent, secure, and legally defensible approach to incident response.

Implemented Standards

Endpoint Detection and Response Standards
All organizational endpoints must be equipped with approved EDR software to allow real-time monitoring, threat detection, and historical event analysis. The IRT is authorized to query, isolate, or retrieve logs from any endpoint supporting an investigation.

Centralized Logging and SIEM Configuration
All servers, applications, and network devices must forward security and event logs to a centralized Security Information and Event Management (SIEM) system. This allows the IRT to access logs from a single source to perform correlation and threat analysis.

Network Segmentation and Access Control Standards
All critical systems must be segmented and protected via access control lists and firewall rules. During an incident, the IRT may override or reconfigure segmentation boundaries to isolate affected systems or trace lateral movement.

Email and Web Content Filtering Standards
All incoming and outgoing emails shall be filtered for malicious content using approved email security gateways, and internet access shall be controlled through content filtering. The IRT has the authority to review, modify, or disable specific filters to investigate or contain email or web-based attacks.

Encryption and Data Handling Standards
Sensitive data shall be encrypted in transit and at rest, and the IRT may decrypt and access encrypted communications or files as part of evidence collection and forensic investigation in coordination with legal and compliance teams.

Chain of Custody Documentation Standards
All digital or physical evidence collected during an incident must be documented following internal chain of custody procedures to ensure admissibility and integrity. This policy grants the IRT authority to initiate and manage that documentation process.

Procedures

Explain how you intend to implement this policy across the organization. Also, define and incorporate the six-step incident response approach here along with how the chain of custody must be maintained throughout any evidence collection process.

Procedures

To implement this policy effectively across Bankwise Credit Union, the Information Security team will integrate incident response procedures into workflows, employee training, and system configurations. These procedures shall be part of the annual security awareness program and implemented through established response protocols aligned with industry standards and regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA). All business units must cooperate fully with the Incident Response Team during the execution of these procedures. Regular incident response drills will validate readiness, clarify roles, and maintain organizational resilience.

Six-Step Incident Response Process

Bankwise Credit Union adopts the industry-standard six-step incident response model to manage and respond to security events:

Preparation
Establish roles, train staff, configure detection tools, and ensure all systems are aligned with security standards. The IRT shall be activated when a potential threat is identified.

Identification
Detect and confirm an incident using SIEM alerts, EDR tools, or user reports. The IRT assesses the severity, scope, and nature of the threat.

Containment
Short-term containment isolates affected systems; long-term containment may involve segmentation, rule changes, or temporary shutdowns. The IRT acts with full authority to limit the threat's spread.

Eradication
The IRT identifies root causes and removes malware, unauthorized access, or other malicious artifacts. Root causes may include applying patches, updating signatures, or disabling compromised accounts.

Recovery
Systems are restored to operational status under IRT supervision. Verification steps will be taken to confirm that the systems are clean.

Lessons Learned
A formal review assesses what happened, how it was handled, and what improvements are needed. Documentation is updated, and training or policy changes begin as required.

Maintaining Chain of Custody

The IRT is responsible for maintaining an unbroken chain of custody throughout any evidence collection effort, digital or physical. All evidence handling must meet legal standards for integrity and admissibility, supporting potential legal or regulatory actions. Chain of custody collection effort includes:

*logging who collected the evidence, when, and how.
*documenting storage, access, and any transfers.
*ensuring evidence is tamper-proof and stored securely.
*using standardized forms and secure evidence containers.

Guidelines

Explain any roadblocks or implementation issues that you must address in this section and how you will overcome them per defined policy guidelines.

Guidelines

Implementing a comprehensive incident response policy across all Bankwise Credit Union locations and business units involves addressing several operational and procedural challenges. These guidelines outline potential roadblocks to successfully implementing this policy and strategies for overcoming these roadblocks.

Cross-Departmental Cooperation
Challenge: Some departments may resist granting the Incident Response Team full access to their systems, data, or facilities, particularly if they perceive it as a disruption or overreach.
Solution: This policy mandates full organizational compliance during an incident. Annual training and tabletop exercises will emphasize the critical importance of unified response. Department heads will understand the legal and operational need for unrestricted IRT access.

Privacy and Access to Sensitive Information
Challenge: Accessing employee communications, HR records, or customer data for forensic purposes may raise concerns about privacy and confidentiality.
Solution: Access is granted only during a verified or suspected incident and must follow documented chain-of-custody protocols. All actions are logged and subject to oversight by the Legal Department and Compliance Officers to ensure that data privacy laws and internal ethics policies are followed.

Lack of Incident Awareness or Delayed Reporting
Challenge: Security incidents may go unreported or be delayed due to a lack of awareness, fear of consequences, or uncertainty about what constitutes an incident.
Solution: The policy is reinforced through required annual security awareness training, which includes clear incident identification criteria and non-punitive reporting guidelines. Employees are encouraged to report any suspicious activity without fear of blame.

Technical Barriers to Response
Challenge: Limited resources or outdated systems may hinder timely incident detection, containment, or evidence collection.
Solution: This policy aligns with hardware, software, and configuration standards that ensure forensic readiness. To support policy execution, the organization will continue investing in SIEM tools, endpoint monitoring, and secure evidence-handling processes.

Policy Enforcement During Crises
Challenge: Normal policies and change control procedures may slow response efforts during an active threat.
Solution: This policy grants the IRT pre-defined authority to override standard protocols as needed to contain threats, protect assets, and preserve evidence. All deviations will be documented and justified post-incident.

Challenge Exercise

Identify and define an incident scenario for Bankwise Credit Union. The incident must involve some type of cybersecurity issue.

Scenario

On a Monday morning, several employees at multiple Bankwise Credit Union branches report being locked out of their workstations. A pop-up message on their screens demands a cryptocurrency ransom in exchange for decrypting their files. Simultaneously, the IT helpdesk receives alerts that customer service representatives cannot access critical banking applications, and some file servers appear encrypted. Internal monitoring tools report unusual network traffic overnight, including outbound data transfers to external IP addresses overseas.
As the investigation unfolded, the Incident Response Team discovered that the initial point of compromise was a phishing email that bypassed spam filters and was sent to employees in the customer service department. The email impersonated an internal IT request for a mandatory software update. At least one employee clicked the malicious link and entered their login credentials on a spoofed Bankwise login page. The attacker used the stolen credentials to move laterally across the network, escalate privileges, and deploy ransomware to high-value systems, including customer databases and internal file shares.

Complicating the situation, backup systems were partially affected when the attacker gained access to network-attached storage devices. The public relations team begins receiving media inquiries after customers report being unable to access their online banking accounts. Executives request immediate impact assessment and mitigation updates, while the legal team raises concerns about potential GLBA violations due to the exfiltration of customer data.

This scenario is **defined** by challenging the incident response team to coordinate initial detection, containment, and eradication activities, communicate effectively across departments and with external stakeholders, preserve forensic evidence and maintain chain of custody, navigate regulatory and reputation risks, especially concerning GLBA, and evaluate the effectiveness of email filtering, endpoint detection, and backup resilience.

Create a brief abstract of the scenario to be approved by C-level executives.

To: Executive Leadership Team
Subject: Tabletop Exercise Scenario Approval – Cybersecurity Incident Simulation

The proposed cybersecurity incident simulation tabletop exercise scenario simulates a coordinated cybersecurity attack targeting Bankwise Credit Union's customer service department. The incident begins with a sophisticated phishing campaign that results in credential theft and unauthorized access to internal systems. The attacker uses these credentials to deploy ransomware across multiple branches, encrypting critical systems and disrupting online banking services.

The exercise will evaluate Bankwise's readiness to respond to real-world threats, including the effectiveness of technical controls, the coordination of the Incident Response Team, and communication strategies across departments and with external stakeholders. It will also test the organization's ability to preserve forensic evidence, comply with regulatory obligations under the Gramm-Leach-Bliley Act, and maintain business continuity under crisis conditions.

The goal is to identify strengths, expose gaps in the current incident response plan, and reinforce Bankwise's commitment to security, compliance, and customer trust.