ENTERPRISE SECURITY INCIDENT RESPONSE PLAN

2025

ITS

Mississippi Department of
Information Technology Services

TABLE OF CONTENTS

PURPOSE & SCOPE

This document seeks to reduce the risks to state government from cybersecurity incidents by providing practical guidelines on responding to cybersecurity incidents effectively and efficiently. This document provides insight, guidance, and awareness on identifying, responding to, and reporting a cybersecurity incident that could impact state agencies from achieving their missions.

When a cybersecurity incident occurs, it is imperative that state agencies follow documented procedures for managing the incident. Incident management is the process of detecting, analyzing, responding to, and improving from an incident. An Incident Response Plan (IRP) is intended to contain the procedures and plans for such incidents when they occur. The IRP should be in both hard copy and electronic formats and be readily available to any standing member of the Incident Response Team (IRT).

Two principles guide the establishment of the IRP:

1. Every agency must establish in advance and maintain a plan for cybersecurity incident management, and
2. Every agency must test and update the operation of the IRP periodically to ensure that it meets agency objectives and is functional.

This document is established to clarify roles and responsibilities in the event of a cybersecurity incident involving one or more state agencies. It is also intended to be a framework for state agencies in creating their own IRP that meets the business needs of the agency, as well as established Enterprise Security Program requirements.

The MS Department of Information Technology Services (ITS) is responsible for routine maintenance and review of this IRP. Routine maintenance and review are required to ensure that this plan is up to date with respect to the technological advances and changes in the business requirements of state agencies, potential threats, applicable legislation, and other changes that impact cybersecurity incident management.

Roles and Responsibilities

ITS

ITS administers the Enterprise Security Program to execute the duties and responsibilities of Mississippi Code Ann. § 25-53-201. Duties and responsibilities related to cybersecurity incidents include, but are not limited to:

- Assisting with cybersecurity incidents that are of severity or scope to pose a hazard to the Enterprise State Network as a whole
- Gathering, aggregating, tracking, and reporting cybersecurity incident information
- Analyzing enterprise IT systems and sharing information that may assist in state agency incident response efforts
- Implementing appropriate controls in enterprise IT systems to reduce the likelihood of the cybersecurity incident impacting other state agencies
- Sharing threat intelligence with appropriate stakeholders to limit the size and scope of the cybersecurity incident
- Interacting with public and private stakeholders as it relates to the cybersecurity incident

State Agencies

State agencies are responsible for the security of their data and IT resources and as such, are required to develop and maintain an IRP for responding to cybersecurity incidents. Agency duties and responsibilities for responding to cybersecurity incidents include:

- Reporting cybersecurity incidents to ITS
- Reporting cybersecurity incidents to appropriate legal and regulatory entities
- Performing data breach notification responsibilities according to applicable data breach laws and regulations
- Identifying and assessing cybersecurity incidents and providing recommendations to the Agency Head
- Detecting, analyzing, containing, eradicating, and recovering from cybersecurity incidents impacting their agency
- Cooperating with ITS and other state agencies on cybersecurity incidents that have the potential to impact other state agencies

Incident Reporting

Per the requirements of the State of Mississippi Enterprise Security Program and state law[1], state agencies must report all cybersecurity incidents involving their information and information systems, whether managed by the state agency, contractor, or other source no later than the close of the next business day following the discovery of the incident.

Reporting incidents to a central group promotes collaboration and information sharing with other entities that may be experiencing the same or similar problems. Reporting to a central group provides the ability to:

- Coordinate activities among agencies experiencing similar incidents to help identify and resolve the problem more quickly than if done separately
- Share threat intelligence to help agencies protect themselves from similar attacks
- Share information between public and private stakeholders, and other appropriate entities
- Collaborate with key entities that can provide the necessary cybersecurity expertise to assist when necessary
- Collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack

Reportable Incidents

A cybersecurity incident is an event that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or a violation or imminent threat of violation of cybersecurity policies, acceptable use policies, or standard cybersecurity practices. This also includes cyberattacks where there is an attempt to gain illegal access, including any data breach, to a computer, computer system or computer network for purposes of causing damage, disruption or harm as well as ransomware.[2] Examples of incidents include, but are not limited to:

- Email/Phishing: An attack executed via an email message or attachment

    Exploit code disguised as an attached document, or a link to a malicious website in the boy of an email message

[1] Miss. Code Ann. § 25-53-201.
[2] Miss. Code Ann. § 25-53-201(5).

- Impersonation/Spoofing: An attack involving replacement of legitimate content/services with a malicious substitute

  Spoofing, man in the middle attacks, rogue wireless access points, and structured query language injection in attacks all involve impersonation

- Attrition: An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services

  Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.

- Web: An attack executed from a website or web-based application

  Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.

- Malware: An attack using software, firmware, or hardware to gain unauthorized access to and/or adversely impact the confidentiality, integrity, or availability of a system

  A virus, worm, and/or Trojan used to steal data, disrupt system services, damage networks, and/or access to system(s) for harmful purpose(s).

- External/Removable Media: An attack executed from removable media or a peripheral device

  Malicious code spreading onto a system from an infected flash drive.

- Improper Usage: Any incident resulting from violation of an organization’s acceptable usage policies by an authorized user, excluding the above categories

  User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.

- Ransom: Any incident resulting in a demand for a designated sum of money or other consideration

  Malicious code spreading onto a system that obtains and/or encrypts or restricts access to sensitive information, information systems, or information networks, including information, systems, and networks managed by third-parties

- Unknown: Cause of attack is unidentified

  This option is acceptable if cause (vector) is unknown upon initial report. The attack vector may be updated in a follow-up report.

- Other: An attack method that does not fit into any other vector

  This option could include theft of physical devices, physical break-in, malicious actions taken by employee such as intentional deletion/destruction of state property and/or state data, misconduct/negligence

- User Error: An incident resulting from user mistakes or violation of policies and security best practices

This option could include misconfiguration, sensitive data shared, accessed, and/or used inappropriately, compromised user credentials, *etc*.

- Breach: An incident resulting from unauthorized access, disclosure, exposure, use, acquisition and/or loss, compromise, or any similar occurrence or term where person(s) other than authorized user accesses or potentially accesses to sensitive information (e.g., personally identifiably information *etc*.) or where authorized user takes actions other than authorized purposes

  This option could include ransom attack and/or intentional actions taken by malicious actors; errors such as emailing sensitive information, uploading/inputting sensitive information into open/public technology solutions (e.g. open-source artificial intelligence *etc*.)
- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host
- An attacker obtains sensitive data and threatens that the details will be destroyed and/or released publicly if the organization does not pay a designated sum of money
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services

Incident Classification

Cybersecurity incidents classified as low, medium, or high must be reported to ITS. Cybersecurity incident severity classifications are provided below.

- **None (Green)**: Malicious activity has been identified with little to no impact on agency operations, agency assets, or individuals
  - Result in no impact to confidentiality, integrity, or availability to information or information systems
  - Result in no financial loss
  - Result in no harm to individuals

- **Low (Yellow):** Malicious activity has been identified with minor impact on agency operations, agency assets, or individuals. Minor impact could

- Cause a degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is noticeably reduced
- Result in minor damage to agency assets
- Result in minor financial loss
- Result in minor harm to individuals

➢ **Medium (Orange):** Malicious activity has been identified with a moderate level damage or disruption on agency operations, agency assets, or individuals. Moderate impact could

- Cause a significant degradation in mission capability to an extent and duration that the agency can perform its primary functions, but the effectiveness of the functions is significantly reduced
- Result in significant damage to agency assets
- Result in significant financial loss
- Result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries

➢ **High (Red):** Malicious activity has been identified with a severe level of damage or disruption on agency operations, agency assets, or individuals. Severe impact could

- Cause severe degradation in or loss of mission capability to an extent and duration that the agency cannot perform one or more of its primary functions
- Result in major damage to agency assets
- Result in major financial loss
- Result in severe harm to individuals that may involve loss of life or serious life-threatening injuries

Reporting Incidents

Each agency must report cybersecurity incidents classified as low, medium, or high to ITS no later than the close of the next business day following the discovery of the incident using the online web form. The form is accessible at the following location:

Cybersecurity Incident Reporting Form

For detailed information about how to report incidents to ITS, please refer to the Enterprise Cybersecurity Incident Reporting Guidelines that can be found on the ITS website (www.its.ms.gov).

INCIDENT ESCALATION

The NIST 800-61 Computer Security Incident Handling Guide provides advisement on escalation of security incidents. Section NIST 800-61, 3.2.7 (Incident Notification) outlines important contacts and modes of communications.

- Agency Head
- Chief Information Office (CIO)
- Agency Information Security Officer (ISO)
- CPO or Privacy Officer
- Other incident response teams within the agency
- External (contractor) incident response teams, if appropriate
- System Owner
- Human Resources
- Public Affairs
- Legal Department
- Law enforcement, if appropriate

- **Contact Methods:** Agencies may need to provide status updates to certain external and internal parties. Among communication methods to be considered are:
  - Email (Preferred)
  - Telephone (Alternate)
  - Website (internal, external, or portal)
  - In person (e.g., daily briefings)
  - Voice mailbox greetings (e.g., set up a separate voice mailbox for incident updates and update the greeting message to reflect the current incident status; use the help desk's voice mail greeting)
  - Paper (e.g., post notices on bulletin boards and doors, hand out notices at all entrance points)

Laws Pertaining to Data Breach Notifications

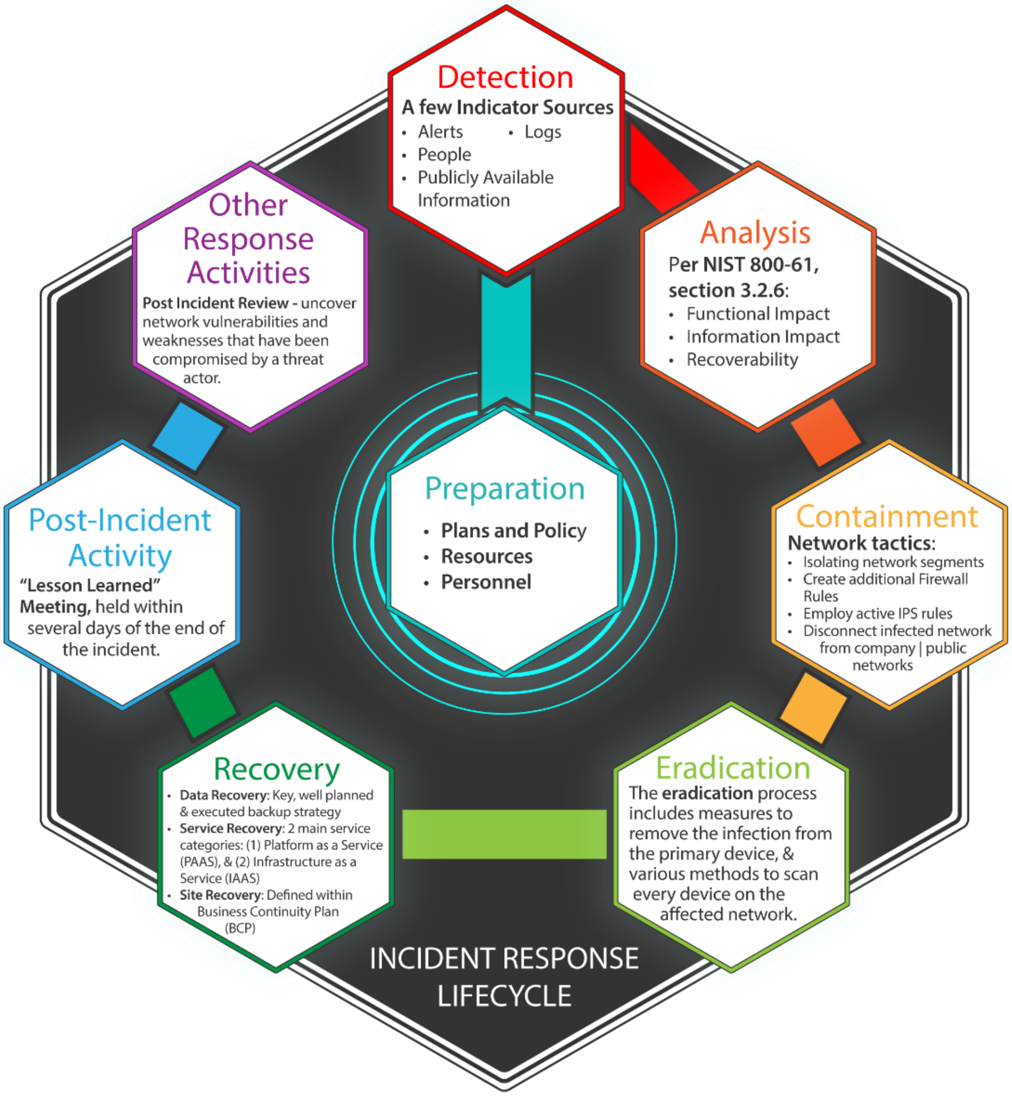
Certain types of breaches carry legal notification responsibilities. While this non-exhaustive section includes references to breach notification statutes and rules, agencies are ultimately responsible for knowing and abiding by any applicable state and/or federal laws/regulations relating to their data including laws, regulations, and/or obligations not listed below.

- **State of Mississippi Data Breach Law:** Miss. Code Ann. § 75-24-29
- **State of Mississippi Enterprise Security Program:** Miss. Code Ann. § 25-53-201
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA):** 45 CFR § Part 164.400 *et seq.*
- **Internal Revenue Service (IRS):** IRS Publication 1075
- **Social Security Administration (SSA):** IRS Publication 1075
- **Federal Trade Commission (FTC):** Health Breach Notification 16 CFR Part 318
- **Family Educational Rights and Privacy Act (FERPA):** 20 U.S.C. § 1232g; 34 CFR Part 99
- **The Privacy Act of 1974:** 5 U.S.C. § 552a

INCIDENT RESPONSE LIFECYCLE

Each agency must develop and implement a security incident management capability for handling cybersecurity incidents. An incident management capability should include a defined plan and address the following stages of incident response:

- Preparation
- Detection
- Analysis
- Containment and Eradication
- Recovery
- Post-Incident Activity
- Other Response Activities



Detection

A few Indicator Sources

- Alerts
- Logs
- People
- Publicly Available Information

Analysis

Per NIST 800-61, section 3.2.6:

- Functional Impact
- Information Impact
- Recoverability

Containment

Network tactics:

- Isolating network segments
- Create additional Firewall Rules
- Employ active IPS rules
- Disconnect infected network from company | public networks

Eradication

The **eradication** process includes measures to remove the infection from the primary device, & various methods to scan every device on the affected network.

Recovery

- **Data Recovery:** Key, well planned & executed backup strategy
- **Service Recovery**: 2 main service categories: (1) Platform as a Service (PAAS), & (2) Infrastructure as a Service (IAAS)
- **Site Recovery**: Defined within Business Continuity Plan (BCP)

Post-Incident Activity

"Lesson Learned" Meeting, held within several days of the end of the incident.

Other Response Activities

Post Incident Review - uncover network vulnerabilities and weaknesses that have been compromised by a threat actor.

Preparation

- **Plans and Policy**
- **Resources**
- **Personnel**

INCIDENT RESPONSE LIFECYCLE

The agency is responsible for understanding the indicators, interpreting internal and external inputs, as well as conducting all required coordination necessary to support cybersecurity incidents reported to the agency.

The agency receives, reviews, and analyzes the event indicators from multiple sources to determine the nature and severity of the event(s) in question. The information derived from the data analysis is then used to inform their partners of the potential or current threats, as well as coordinate all necessary remedial efforts required to return operational stability to the agency.

Preparation

Incident handling requires great consideration and coordination prior to event handling to ensure as many circumstances as possible are addressed prior, during and after the event. These include, but are not limited to plans and policy, resources, and personnel.

Plans and Policy

Planning begins with the development of the IRP and training an Incident Response Team (IRT). The IRP defines the process for identifying, analyzing, responding to, and learning from incidents that interrupt an agency's operations. The IRP provides a consistent response to cybersecurity incidents and ensures that objectives are met when handling an incident. The objective of the IRP should be translated into specific actions assigned to individuals or groups to perform when an incident occurs. The IRP should address, at a minimum.

- The agency's approach to incident management
- The structure of the incident management process
- The requirements and objectives of the incident management process
- A description of how the agency will detect incidents, analyze incidents, contain, and eradicate incidents, recover from incidents, and improve its response capabilities over time
- The roles and responsibilities necessary to carry out the plan
- Applicable training needs and requirements

- Resources that will be required to meet plan objectives
- Relevant costs and budgets associated with incident management activities

In addition to relying on internal staff for incident management, agencies may decide to leverage outside resources for a third-party IRT. When outsourcing an IRT, the third-party organization should be pre-identified and contracted. Ideally the contract should be in place before a cyber incident occurs. Prior to an incident, the third party should perform a review of the agency's IT infrastructure, review and test the IRP, and clearly establish a service level agreement (SLA) between all parties.

The Planning phase also includes training for all agency employees as well as supervisors and managers. They should be trained to identify suspicious behavior, whether it is computer related or other device behavior or an interaction with another person such as a phone call that may be an attempt at social engineering. Employees should also understand the appropriate use for information systems and know the steps necessary should they observe another employee or contractor's behavior inconsistent with agency policies. Consider that insider threats are still a common source of cybersecurity incidents, including data breaches, theft of intellectual property and sensitive information, and damage to networked systems.

Part of the planning process should include establishing an ongoing effort for maintaining, testing, and improving the IRP to ensure that the agency is prepared to manage cybersecurity incidents.

RESOURCES

Internal resources exterior to the agency are most often very vital to the success of incident handling. Internal resource commitments should be included in your agency's Business Continuity Plan (BCP) and therefore have roles and responsibilities defined. Inner-agency departments (e.g., human resources, logistics, finance and communications) are required at the fundamental level to provide support for standard and contingency operations.

External resources are just as important as your internal resources. Having a comprehensive list of all partner agencies to ensure continuous communication is key to establishing and maintaining effective partnerships to foster open information sharing. Example partner agencies are listed below.

- MS Department of Information Technology Services
- Law Enforcement Entities
- Incident Response Partners
- MS Attorney General's Office

Personnel

When developing an IRT, it is critical to identify the various roles that make up the team: Cybersecurity personnel, IT staff, management, public relations personnel, human resources, legal, and perhaps facilities personnel if the event involves Industrial Control Systems (ICS) or Supervisory Control and Data Acquisition (SCADA) systems. Once your IRT personnel are identified, you need to ensure they are well trained in their respective roles, which should include formal training and certification and continuing education.

Detection

One of the largest concerns when reporting an incident is the amount of time it takes between detecting a suspected or actual incident and notifying appropriate parties. Time sensitivity is of great concern when reporting an incident and can become critical where personally identifiable information (PII) or sensitive information is involved.

Effectively detecting incidents relies on the agency's ability to monitor and identify events as they occur. An event is one or more occurrences that affect agency assets and have the potential to disrupt operations. Events may include, but are not limited to, a user logging into an account, a web server receiving a request for a specific web page, a user accessing files on network share, and a firewall blocking a connection attempt. Agencies should have capabilities to detect, report, log, track, collect, and store event evidence. The inability to identify events in a timely manner can significantly increase the agency's recovery costs and effort. Important activities in event detection include:

- Event detection and reporting
- Logging of event data in an incident database or similar mechanism

- Event status tracking
- Handling of event data in accordance with laws, rules, regulations, policies, etc.

An effective plan should consider and implement methods to ensure information gathered from multiple sources is effectively utilized. Information, also known as indicators, is derived from various types of sources, both systematic and from monitored open-source information. Below are a few examples of indicator sources.

- **Alerts:** Agency security solutions (firewall, IPS, anti-malware, security monitoring, etc.) detect suspicious events and generate alerts for agencies to review and investigate
- **Logs:** Logs from agency IT systems are frequently of great value when an incident occurs. Agencies should require a baseline level of logging on all systems and a higher baseline level on critical systems
- **Publicly Available Information:** Information gathered from publicly available sources such as news web sites, government web sites, books, and periodicals
- **Threat Intelligence:** Information that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors
- **People:** People internal and external to the agency may report signs of incidents and the agency should review and validate all reports

Understanding how to begin to triage an event greatly depends on the characteristics of the incident and/or events in question. There is a myriad of contributing characteristics which may demand various responses and levels of escalation.

- **Authentication –** unusual or unauthorized logon attempts, logon activities after hours, remote session attempts, unauthorized privilege escalation, etc
- **Data Handling –** abnormal ad-hoc requests, unauthorized access or attempted access, inappropriate disclosure, inappropriate destruction of sensitive data, etc
- **Data Exfiltration –** large amounts of data leaving the network by an authorized (or unauthorized) user
- **System Availability –** web defacements, denial of services, hacking activities, modification of software or systems, suspicious activities
- **Physical –** power outages, physical damage, sabotage, physical loss or theft of information or systems
- **Other –** social engineering, Trojan or virus infections, harassment, elevated data disclosure, improper disposal of documents

Next, to properly triage an event, you must understand the impact to the operations, security classification of the information, legal implications and value of the information. Examples of some typical initial exploratory methods are below.

- **Authentication:** The system administrator could simply review the Security Information and Event Management (SIEM) logs to understand the account in question and reason for error and advise the ISO
- **Data Handling:** The administrator can review SIEM and Active Directory logs to understand the nature of the requests – this could simply be the case of user rights management issues, or it could lead to an investigation
- **Data Exfiltration:** The system administrator may immediately cease all applicable activities related to the incident in question, secure their workstation or area and contact the appropriate ISO or their representative to begin preserving the information or evidence of questionable activities. Do not turn off power to the device in order to allow cybersecurity personnel to conduct forensics.
- **System Availability:** The administrator may review SIEM logs to understand the activity in question and prepare to restore services from a backup and actively review firewall logs.
- **Physical:** Coordinate with the ISO and the facility infrastructure team to understand the nature of the event and understand how to implement secondary power and possibly provide security personnel to protect the physical perimeter and sensitive areas
- **Other:** Disable the user account, take a screenshot and turn in, unplug the computer from the network, actively log authentication and access actions, etc.

There are a range of suspect security-based events which could warrant an investigation based on probable cause: Authentication issues, malformed large data requests, system outages or unexplained degradation, single or multiple victims, as well as many other unexplained events. These types of events should be addressed in your IRP. In addition, your IRT should have special training to identify and respond appropriately to the many different types of cyber incidents such as a phishing attack, ransomware, malware, Distributed Denial of Service (DDOS).

Analysis

The investigation of the incident should include an event threat and impact analysis in order to understand the scope of the incident and categorize the impact of the event on the agency. Once the event's impact level is understood it may be appropriate to escalate the incident response and contact other entities.

Analyzing event artifacts is the first step in a process through which an agency recognizes that an incident is underway. The agency analyzes the event to determine how to categorize it, how to evaluate it, and whether the event reaches the threshold of a declarable incident. The threshold for when an incident has occurred, is occurring, or is imminent and requires a response depends on factors such as agency structure, mission requirements, and laws and regulations. Important activities in analysis include:

- Event categorization
- Event prioritization
- Event data correlation and analysis
- Incident declaration
- Incident analysis and response determination

The National Institute of Standards and Technology (NIST) Special Publication NIST 800-61, Computer Security Incident Handling Guide, provides advisement on prioritizing the handling of security incidents. These incidents may be applicable to computer systems as well as paper or other media. Per NIST 800-61, section 3.2.6 (Incident Prioritization) relevant factors for event threat and impact/escalation criteria include:

- **Functional Impact:** Incidents targeting IT systems typically impact the business functionality that those systems provide, resulting in some type of negative impact to the users of those systems
- **Information Impact:** Incidents may affect the confidentiality, integrity, and availability of the agency's information
- **Recoverability:** The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident

While there is no single model for determining event impact, the items below in the impact analysis section provide guidance on defining impact to agency systems, agency information (business impact), and the agency ability to recover from an event (possible responses). Agencies should consider each category to assure proper response and recovery from these events.

IMPACT ANALYSIS

- Examples of functional impact categories include:
  - **None:** No effect to the agency's ability to provide all services to all users
  - **Low:** Minimal effect; the agency can still provide all critical services to all users but has lost efficiency
  - **Medium:** Agency has lost the ability to provide a critical service to a subset of system users
  - **High:** Agency is no longer able to provide some critical services to any users

- Examples of information impact include:
  - **None:** No information was exfiltrated/leaked, disclosed, changed, deleted, used, or disclosed by or for unauthorized persons or purposes, or otherwise compromised
  - **Privacy Breach:** Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc., was accessed or exfiltrated/leaked, or protected health information (PHI) of individuals was used or disclosed by or for unauthorized persons or purposes, or otherwise compromised
  - **Proprietary Breach:** Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed, exfiltrated/leaked, or used or disclosed by or for unauthorized persons or purposes
  - **Integrity Loss:** Sensitive or proprietary information was changed or deleted accidentally or intentionally

- Examples of recoverability effort categories include:
  - **Regular:** Time to recovery is predictable with existing resources
  - **Supplemented:** Time to recovery is predictable with additional resources
  - **Extended:** Time to recovery is unpredictable; additional resources and outside help are needed
  - **Not Recoverable:** Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation

TYPES OF THREAT

Analysis of the incident should include considerations relative to the specific type of threat. Each type of attack may require a different response. For example, a ransomware attack involves a much different response than a Distributed Denial of Service attack.

PHYSICAL CONSIDERATIONS

Cybersecurity incidents could impact physical systems or critical infrastructure. Physical considerations extend beyond the immediate physical and boundary of the agency. Physical considerations encompass any and all physical and/or mechanical features directly or indirectly required to support business operations.

Incidents involving physical infrastructures have additional considerations than those with typical cyber related attacks. Agencies may have to consider more than simply network protection principles; they must also take into consideration the acquisition and replacement of physical systems that are connected to the network.

Containment and Eradication

Containing and eradicating an incident requires an agency to take actions to prevent or contain the impact of an incident and remove the source of the incident. This requires that agency response be escalated to the stakeholders who are best able to implement and manage the response and bring the incident to a close. The number of resources and level of effort required for the agency response will vary with the extent of the incident and should be informed by incident analysis. Because there are a broad range of potential incidents, agencies must consider a broad range of potential responses. Each agency's unique operating environment determines the appropriate containment and eradication effort and should be used by the agency to set incident response performance requirements. Important practices in containment and eradication include:

- Incident escalation to stakeholders
- Response development and implementation
- Incident status communication
- Incident tracking

CONTAINMENT

Agencies are responsible for developing and employing sufficient methodologies to contain the incident in order to minimize continued impact and / or disruption of services to the agency as well as reducing the possibility of continued contamination to other services. Tactics supporting the immediate local isolation and containment are vital to slowing, and hopefully stopping the proliferation of the attack. However, this approach is only one part of a multi-faceted approach.

The containment plans are usually based on the findings of the security team's investigation of the incident. Often, the plan relies on limited information gathered during the preliminary detection. Information is acquired from multiple sources based on the attack vector.

A risk management strategy should address the risk at every level, starting with the infected computing device all the way to examining the viability of the network. During the investigative phase and beyond, the affected computing devices may require immediate isolation or removal from the network in order to support the required efforts. Some commonly employed network tactics involve disconnecting or isolating network segments, creating additional firewall rules, employing active IPS rules or simply disconnecting the infected network from the company and / or public networks.

ERADICATION

Beyond the identification and containment, there is the requirement to determine how to effectively and safely remove the source of the incident from the computing device and ensure another node in your network is not affected in the future. Many organizations stop at removing the device from the network and stop there; remember malware spreads silently and very rapidly. The eradication process must include measures to not only remove the infection from the primary device, but various methods to scan every device on the affected network segment to ensure the relevant risk is addressed.

Recovery

Today's technological and business environments are dynamic and utilize multiple platforms for information management. Agencies must ensure they understand their technological boundaries and consider recovery principles and methodologies for every environment. Information Technology Recovery Plans are essential and should align with the Incident Response Plan.

DATA RECOVERY

The key to an effective data recovery strategy begins with a well planned and executed backup strategy. A back-up strategy may vary from agency to agency based on the data type, location, sensitivity, availability requirements, and / or data owners. Other variables may come into play such as location of the backup media or the statement of work (SOW) with an external data recovery vendor. Prior to any data restoration activities, the data owners should confirm with the data custodians of all the previous and current locations of any live or backup data. Agencies should also include periodic testing of data backups to ensure the data backups were successful and contain the expected data to be backed up.

SERVICE RECOVERY

Recovery expectations and deliverables are typically spelled out within the Service Level Agreement (SLA) in a service contract. There are two main service categories organizations should have situational knowledge of, Platform as a Service (PAAS) or Infrastructure as a Service (IAAS).

SITE RECOVERY

Site recovery is typically defined within your Business Continuity Plan (BCP) and may be needed in the Data Recovery Plan (DRP) or Technology Recovery Plan (TRP). The actions required for site recovery are based upon what type of recovery site is defined in the BCP, e.g., cold site, warm site or hot site.

Post-Incident Activity

Often overlooked, one of the most important parts of incident response is learning and improving. After remediating an incident, agencies should take steps to identify and implement any lessons learned from the event, and to pursue or fulfill any legal action or requirements. This process requires a cross-functional effort from all employees and technologies connected to the incident to truly understand the root cause and full scope of the attack. Important practices in improving the incident management capability include:

- Root cause analysis
- Incident closure

Holding a “lessons learned” meeting with all involved parties after a major incident, and optionally periodically after lesser incidents as resources permit, can be extremely helpful in improving security measures and the incident handling process itself. This meeting provides a chance to achieve closure with respect to an incident by reviewing the root cause of what occurred, what was done to intervene, and how well intervention worked. The meeting should be held within several days of the end of the incident.

By completing a post-incident review, security teams are able to uncover network vulnerabilities and weaknesses that have been compromised by a threat actor. Post-incident reviews can result in a list of practical actions that address each of the issues that allowed the threat actor to succeed. These actions should minimize the impact of an attack and teach the security team, the security tools, and the wider enterprise how to prevent, detect, and respond to a similar attack in the future.

Testing the Incident Response Plan

By completing a post-incident review, security teams are able to uncover network vulnerabilities and weaknesses that have been compromised by a threat actor. Post-incident reviews can result in a list of practical actions that address each of the issues that allowed the threat actor to succeed. These actions should minimize the impact of an attack and teach the security team, the security tools, and the wider enterprise how to prevent, detect, and respond to a similar attack in the future.

- Root cause analysis
- Incident closure

Sample Incident Response Policy

This is a sample policy that agencies can use to develop their agency-specific policy.

Purpose	The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with the {AGENCY POLICIES} and State of Mississippi policies. This document sets forth the policy for incident management within the Agency.
Scope	This policy applies to and must be complied with by all {AGENCY} Users. The User agrees to abide by this policy while employed or contracted with the {AGENCY}. Roles and responsibilities of each function pertaining to the protection of {AGENCY}-owned systems and data are documented in {AGENCY} policy. The User is responsible for understanding the terms and conditions of this policy. Exemptions to this policy shall follow the process defined in {AGENCY} policy. This policy is subject to change. This policy applies to any computing device owned or leased by the {AGENCY}. It also applies to any computing device regardless of ownership, which either is used to store {AGENCY}-owned Confidential or {AGENCY}-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.
Policy	The {AGENCY} shall establish an Incident Response Team (IRT) for overseeing incident investigations. The {AGENCY} Information Security Officer (ISO) shall recommend the IRT members to the {AGENCY} for approval. The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that fall under one or the following categories: • Propagation to external systems • Violation of applicable federal and/or state laws which will require involvement from law enforcement • Potential modification or disclosure of Confidential Information as defined in the Agency Data Classification Policy.

	The {AGENCY} shall • develop an Incident Response Plan (IRP) that: o provides a roadmap for implementing its incident response capability o describes the structure and organization of the incident response capability o provides a high-level approach for how the incident response capability fits into the overall organization o meets the unique requirements of the {AGENCY}, which relate to mission, size, structure, and functions o defines reportable incidents o provides metrics for measuring the incident response capability o defines the resources and management support needed to effectively maintain and mature an incident response capability o is reviewed and approved by designated {AGENCY} officials • review incident response plans and procedures at least annually • revise the incident response plan/procedures to address system/organizational changes or problems encountered during implementation, execution, or testing • distribute copies of the incident response plan/procedures to incident response personnel • communicate incident response plan/procedure changes to incident response personnel and other organizational elements as needed • when required by information system changes and annually thereafter, provide incident response training to information system users consistent with their assigned roles and responsibilities before authorizing access to the information system or performing assigned duties • test the incident response capability of the information systems they support at least annually o use {AGENCY}-defined tests and/or exercises to determine incident response effectiveness. Document the results. • implement an incident handling capability for cybersecurity incidents that includes preparation, detection and analysis, containment, eradication, and recovery • coordinate incident handling activities with contingency planning activities • incorporate the lessons learned from prior and ongoing incident handling activities into incident response procedures, training, and testing/exercises

	• track and document information system security incidents; retain and safeguard cybersecurity incident documentation as evidence for investigations, corrective actions, potential disciplinary actions, and/or prosecutions • promptly report cybersecurity incident information to appropriate authorities in accordance with State or {AGENCY} incident reporting procedures • provide an incident response support resource, integral to the {AGENCY} incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents o Possible implementations of incident response support resources in an {AGENCY} include a help desk or an assistance group and, when required, access to forensics services. The {AGENCY} shall notify appropriate individuals (which must include the ITS) as soon as possible if it is believed that personal information owned by the Agency has been used or disclosed by or for unauthorized persons or purposes. The {AGENCY} shall establish an Incident Criticality matrix. This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants. The {AGENCY} shall establish and document appropriate procedures, standards, and guidelines regarding Incidents. The {AGENCY} is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by the Agency may be subject to seizure and retention. The {AGENCY} will work directly with law enforcement regarding any Incidents that may have violated federal or state laws. The {AGENCY} will develop a summary report for each valid Security Incident.
Disciplinary Acton	Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law. Any User who has violated this policy may be subject to disciplinary action, up to and including termination of employment.

	The {AGENCY} will cooperate with appropriate law enforcement if any User may have violated federal or state law.
Document Change Management	All changes to this document shall follow the process defined in {AGENCY} policy. The ISO will be responsible for communicating the approved changes to the {AGENCY}.

Incident Handling Checklist

This checklist provides the major steps to be performed in the handling of an incident.

Detection and Analysis

- Determine whether an incident has occurred
    - Analyze the precursors and indicators
    - Look for correlating information
    - Perform research (e.g., search engines, knowledge base)
    - As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence
- Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)
- Report the incident to the appropriate internal personnel and external organizations

Containment, Eradication, and Recovery

- Acquire, preserve, secure, and document evidence
- Contain the incident
- Eradicate the incident
    - Identify and mitigate all vulnerabilities that were exploited
    - Remove malware, inappropriate materials, and other components
    - If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them
- Recover from the incident
    - Return affected systems to an operationally ready state
    - Confirm that the affected systems are functioning normally
    - If necessary, implement additional monitoring to look for future related activity

Post-Incident Activity

- Create a follow-up report
- Hold a “lessons” learned meeting (mandatory for major incidents)

Initial-Incident Triage Checklist

Incident Response Team: Assemble Incident Response Team (IRT) in response to an actual or suspect event/incident. Meet daily if necessary, with priority over other work, possibly requiring after-hours activities.

Secure data: Secure data and confidential information and limit immediate consequences of the event. Suspend access and secure/image assets as appropriate, e.g. harden or disable system or contact internet search engines if appropriate to clear internet cache.

Data elements: Determine the types, owners, and amounts of confidential information that were possibly compromised.

Data source: Identify each location where confidential information may have been compromised and the business owner of the confidential information.

Scope and escalation: Confirm the level and degree of unauthorized use or disclosure (includes access) by the named or unidentified individuals or threats.

Number of individuals impacted: Determine the number of individuals impacted. The number may implicate breach notification requirements, e.g. individual or media notice.

Discovery date: Determine the date the agency or contractor knew or should have known about the event/incident.

Management alert: Advise appropriate internal management.

External communications, as required: Advise external contacts, such as ITS, legislative leadership, the Office of the Inspector General, the Office of the Attorney General, Secretary of State (SOS) (if election data involved), law enforcement, outside counsel, and applicable regulatory authorities.

Investigate:

- Interview: Identify and interview personnel with relevant knowledge, e.g., determine whether and by whom access may have been approved, who discovered the risk, etc.
- Documents: Gather and review contracts and provisioning documents (documents authorizing access or restricting use or disclosure).
- Root Cause Analysis: Prepare RCA which describes how and why the event occurred, what business impact it had, and what will be done to prevent reoccurrence.
- Event and Threat Impact Analysis.

Mitigation: Revise policies, process, or business requirements, sanction workforce, enforce contracts, etc. to reduce the likelihood of event reoccurrence. Set timeline and assign responsibility to ensure accountability. Follow-up to ensure corrective action initiated and completed on time or decision to accept the risk of reoccurrence, and report appropriately.

POST-INCIDENT CHECKLIST

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Relevant factors for post-incident and root cause analysis include the items below.

Learning and improving: Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:

Follow-up reporting. An important post-incident activity is creating a follow-up report for each incident. Report considerations include:

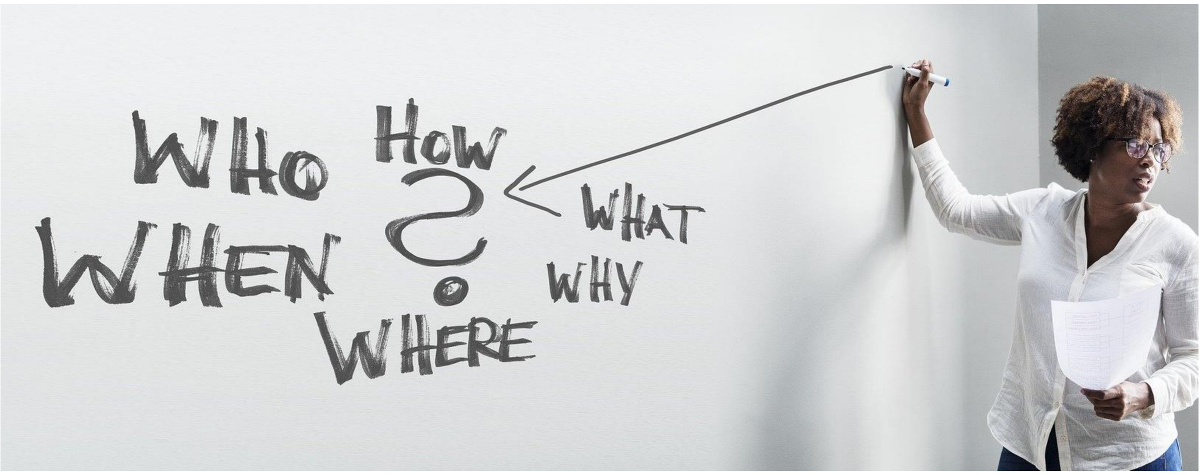
- Creating a formal event chronology (including time-stamped information from systems).
- Compiling a monetary estimate of the amount of damage the incident caused.
- Retaining follow-up reports as specified in retention policies.

Data collected. Agencies collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event. Accountable authorities should make a determination on data retention and disposition.

Root Cause Analysis. Agencies performing root cause analysis should focus on relevant objective assessment activities including:

- Reviewing of logs, forms, reports, and other incident documentation.
- Identifying recorded precursors and indicators.
- Determining if the incident caused damage before it was detected.
- Determining if the actual cause of the incident was identified.
- Determining if the incident is a recurrence of a previous incident.
- Calculating the estimated monetary damage from the incident.

- Measuring the difference between initial impact assessment and the final impact assessment.
- Identifying measures, if any, that could have prevented the incident.



ITS Contact Information

Executive Director	Craig P. Orgeron, Ph.D craig.orgeron@its.ms.gov
Chief Information Security Officer	Jay White jay.white@its.ms.gov
Chief Administration Officer	Stephanie Hedgepeth stephanie.hedgepeth@its.ms.gov
Chief Operations Officer	Brian Norwood brian.norwood@its.ms.gov
Data Services	Steve Patterson steve.patterson@its.ms.gov
Internal Services	Holly Savorgnan holly.savorgnan@its.ms.gov
Procurement Services	Tabatha Baum tabatha.baum@its.ms.gov
Telecom Services	Lisa Kuyrkendall lisa.kuyrkendall@its.ms.gov
Mississippi Department of Information Technology Services	3771 Eastwood Drive Jackson, MS 39211 (601) 432-8000

ITS Mississippi Department of
Information Technology Services

Craig Orgeron, Ph.D, Executive Director

3771 Eastwood Drive
Jackson, Mississippi 39211
Telephone (601) 432-8000
Fax (601) 713-6380
Web site: www.its.ms.gov
State Portal: www.mississippi.gov