GUIDE TO DEVELOPING AN INCIDENT RESPONSE PROGRAM
Featuring a Customizable Incident Response Plan Template
INTELLECTUAL PROPERTY NOTICE
Copyright © 2019 by CyberDefenses Inc.
All Rights Reserved.
This document contains work which is the subject matter of copyright held by CyberDefenses Inc. This document contains intellectual property and work product of CyberDefenses which may not be copied or provided to any person or entity other than for whom the template was prepared without the express written consent of CyberDefenses Inc.
# Table of Contents

**PREFACE**  
INTRODUCTION 1  
HOW THIS GUIDE IS ORGANIZED 1  

**THE INCIDENT RESPONSE PROGRAM**  
INCIDENT RESPONSE PROGRAM STAGES 3  
PREPARING TO HANDLE INCIDENTS 4  
DETECTION AND ANALYSIS 9  
CONTAINMENT, ERADICATION, AND RECOVERY 15  
POST-INCIDENT ACTIVITY 19  
PERFORMANCE METRICS 20  

**INCIDENT RESPONSE PLAN**  
DEVELOPING THE INCIDENT RESPONSE PLAN 20  
================================ INCIDENT RESPONSE POLICY TEMPLATE ====================

**INCIDENT RESPONSE PROGRAM POLICY**  
STATEMENT OF MANAGEMENT COMMITMENT 24  
PURPOSE 24  
SCOPE 24  
OBJECTIVES 24  
LEVELS OF AUTHORITY 25  
COMMUNICATION AND COORDINATION 25  

**APPENDIX A – SECURITY INCIDENT REPORT FORM**

**APPENDIX B – DOCUMENT SOURCE, BASELINE AND REFERENCES** 29
Introduction

While no organization sets out with the goal of seeing their cybersecurity defenses fail, it should be anticipated that eventually they will experience such an occasion. When a privacy or information security incident occurs, it is imperative that the organization is prepared to respond quickly, appropriately, and effectively to ensure that damages are minimized and that normal operations can be restored as soon as possible.

Because Information Security Incidents come in many varieties and potential levels of impact, Incident Response requires a multi-pronged approach. Implementing an effective incident response program that maintains a comprehensive plan for organization-wide response to a cybersecurity incident can make all the difference between mitigating the damage to keep your business operational or suffering irreparable consequences. Organizations that create and maintain an effective Incident Response Program anticipate that incidents will occur, have documented plans and procedures for responding to and handling the incidents, and learn from their experiences to continually improve.

The Incident Response Program will help you sustain the ongoing activities necessary to develop the right capabilities and prepare your organization for incident response. The program will enable improved detection of cybersecurity incidents and execution of a response plan with the goals of mitigating the event, communicating effectively during the course of the response, capturing all of the relevant information for useful analysis, and improving the program for the future with lessons learned along the way.

We’ll address the key elements of the program beginning with concise purpose and objectives, scope, roles, and responsibilities. We’ll further consider organizational coordination, compliance requirements, periodic review, prioritization, metrics and reporting. Most importantly we address how to develop your own plan for implementing a program and creating processes so that you’re prepared when the worst happens – with baselines for developing procedures for incidents that frequently occur.

An effective program is a living entity that requires buy-in, support and advocates throughout the organization. To that end, we also cover other important considerations such as mission, strategies and goals to ensure that senior management support is obtained and authorization provided. With the right roadmap, communications, and integration of incident response roles into every level of your organization, you will be prepared to respond when the eventual incident occurs.

How This Guide is Organized

This guide includes materials that are suitable for use as standalone documents, supporting materials for developing your own documents, or templates that can serve as a starting point. Much of the document structure is based on the National Institute of Standards and Technology Special Publication 800-61 Computer Security Incident Handling Guide Revision 2. As a template, this document allows organizations to customize specific passages commonly denoted with curly brackets and italics, i.e. {sample}.

Later sections that are meant to serve as templates include:
• Incident Response Policy
• Incident Response Plan
• Incident Response Procedures
• Incident Response Tabletop Exercise Simulation Run Book

This guide speaks generally to the requirements of a comprehensive Incident Response Program and is suitable for organizations of all sizes and types.

The Incident Response Program

In support of an overarching information security program, a resilient, sustained incident response comes from the organization developing the capability with the Incident Response Program. A program is “a planned, coordinated group of activities, procedures, etc., often for a specific purpose.” The Incident Response Program involves activities that occur in advance of an actual incident event with the goal of ensuring that the organization is prepared to respond. The prepared organization has anticipated the potential for their cybersecurity defenses to fail, or that an adversary will circumvent the defenses, and a set of actions will be necessary to protect critical assets and limit harm.

CyberDefenses helps organizations maintain “Military-Grade” levels of cybersecurity. Using disciplines and expertise built from extensive experience, the “Military-Grade” approach for incident response combines comprehensive preparedness and execution to move from reactive to responsive – anticipating likely outcomes and potential contingencies – while effectively executing to a plan that is purposely adaptable for adjustments that the field conditions may dictate. The Incident Response Program anticipates that practice makes perfect, and that perfect during practice may still need to adapt in order to overcome under live fire.

The Incident Response Program helps to improve and produce a capable defense while enabling a proactive response to attacks. The program will include developing a well-honed plan for the coordination of activities across the organization and within the teams that are responsible for incident response. The plan is used to ensure that communications are clear, timely and complete, enabling each of the team members to execute their distinct response processes. The processes, detailed steps executed to perform functions within the plan, must be replicable yet variable for the circumstances at hand.

“Military-Grade” isn’t the execution of rote process but instead the level-headed calm under extreme conditions that preparedness achieves. Execution like you’ve been through the event before occurs because you either have been there through training or experience. You are executing to a plan prepared for anticipated or predicted likely incident event types or otherwise adjusted as needed to adapt and overcome. The incident response program enables the organization to reach the end goals of mitigation of the active threat, remediation of the damages incurred, and restoration of normal operations for achieving mission objectives.

1 http://www.dictionary.com/browse/program
Incident Response Program Stages
There are well documented and modeled incident response program stages that define the essential functions that need to occur to define and maintain the program. The National Institute of Standards Special Publication 800-61 Computer Security Incident Handling Guide Rev. 2\(^2\) provides a well-articulated and concise model for stages of an incident response life cycle. Figure 1 below demonstrates the model.

The incident response program stages include:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post-Incident Activity

These stages help to emphasize that the program has a life cycle that begins in advance of any detected incident and continues after the threat of the active incident has abated. Each of the following topics within this section of the guide provides essential activities within each stage while highlighting tips and suggestions that will help the organization develop a capable incident response program.

Preparing to Handle Incidents

**Preparation**

Preparation for incident response extends on aspects of the information security program that are necessary to ensure that the incident response program is integrated into necessary program areas. A thorough understanding of the information security program functions along with the maturity and effectiveness will enable a comprehensive Incident Response Program that complements the organizations risk tolerance and current operational need. Information security program functions that should be considered include the below high-level categories and objectives:

**IDENTIFY** – Identification of information critical assets; network and system topologies; data flows, the supply chain and the extended business landscape; business risks and impact analysis; and vulnerabilities and cybersecurity weaknesses.

**PROTECT** – Protection capabilities to limit access to authorized entities; information asset protections for reducing risk to confidentiality disclosure, integrity corruption or manipulation, availability disruptions, privacy violations, and legal mandates; and countermeasures for defending weaknesses and deficiencies.

**DETECT** – Detection to continually observe organization events and activities and discover anomalous and suspicious occurrences; processes to investigate and analyze event activity occurring internal or external to the organization that may be a prelude to an attack or indicative of active incident activity; and the utilization of information and intelligence that will provide the basis for proactive investigation and adversary hunting.

**RESPOND** – Response processes created for required roles beyond the technology team to enable effective escalation, notification, and coordination; communications enabled to ensure that the internal and external stakeholder environment are appropriately included at the earliest possible stages of the event investigation or incident occurrence while protecting the privacy, confidentiality and operational integrity of the organization; analysis techniques are prepared to quickly remove speculation and determine facts; mitigation capabilities are identified within existing functions or supplemental resources.
RECOVER – Recovery processes designed to restore safe and secure operations once mitigation of the threat has been achieved; time allocated to analyze the incident response and incorporate lessons learned; and communications that ensure victims, external stakeholders and all impacted parties have a clear understanding of the events that transpired if appropriate.

Preventing Incidents
Preventing incidents and limiting harm is accomplished through functions of the organization information security program. Each of the examples listed below are relevant to the incident response capability. The people, processes, and technologies used to formulate controls in these areas become important detection and mitigation functions in the Incident Response Program. Relevant information security program functions include but are not limited to:

- Access Control
- Configuration Management
- Maintenance
- Vulnerability Management
- Business Continuity and Contingency Planning
- Risk Management and Risk Assessment
- System and Communications Protection
- Media Protection
- System and Services Acquisition
- System and Software Development
- Event Monitoring, Audit and Accountability

Additionally, other organizational functions can be key supporting functions to the Incident Response Program. Business Operations, Human Resources, Legal, Procurement and Purchasing, and many others can help in aspects of training and preparedness to prevent incidents or otherwise help in the eventual advent of a cybersecurity incident response. The Incident Response Program should seek to mature in capability to eventually work proactively throughout these areas to achieve objectives in preventing incidents through risk management or limiting the harm of an incident through effective response.
Incident Response Training

Incident response training is critical to implementing a successful Incident Response Program. It ensures that your team knows exactly what to do in the face of a cybersecurity attack. Training includes education opportunities to instruct the individuals directly responsible for incident response activities as well as organizational level training opportunities for the distinct processes that the Incident Response Program develops. The Incident Response Plan should include budget requirements for the appropriate level of training along with the schedule for obtaining the training or conducting the internal training events.

Internal training can include more expansive exercises and drills as well as smaller scale walkthroughs in the form of tabletop incident response exercises. Exercises should be used to instruct responsible personnel on how to perform activities during incidents and make sure that updates to processes based on lessons learned or other Incident Response Program continual improvement efforts keep the organization apprised of the most current response procedures.

The Incident Response Program should consider how best to involve executive leadership, corporate communications, and other key non-technical company resources such as general counsel in response exercises. Exercises can be an excellent opportunity to prepare the organization as a whole for response to a cybersecurity incident, but it is important to engage top level company personnel with a well-prepared exercise scenario that leverages their role and response requirements. Extend an extra level of effort in the preparation of these types of exercises to ensure that the time is maximized towards achieving its objectives.

A final point on incident response exercises and cybersecurity drills includes involving supply chain partners and outsourced providers. Organizations often outsource critical business functions to providers that have cybersecurity responsibilities for the resources they manage. What is often overlooked, however, is coordination during incidents or potential cybersecurity attacks between the organization and the external partners.

Outsourcing - Supplemental Services and Incident Response Contracts

Depending on the capabilities, skills and maturity of the organizational information security program functions, your organization may need to procure additional resources to supplement the internal resources and facilitate incident response on a contingency basis. Additional contracted resources to consider include but are not be limited to:

*Data Forensics and Incident Response (DFIR)* – Advanced digital and electronic forensics and evidence handling capabilities are available within many cybersecurity firms and consulting companies.

*Malware Reverse Engineering* - Malware disassembly, reverse engineering, and analysis is a specialized skillset requiring experience with software engineering techniques, assembly and disassembly of software, isolated laboratory systems and various tools that enable the analysis of malicious code and its behaviors. While there are toolkits and online resources available, such as malware sandboxes and file threat scanning solutions, increasing internal capabilities or otherwise supplement the internal personnel with services to adequately handle threats provides significant advantages and ensures true preparedness.
**Comprehensive Incident and Breach Response Services** – Retainer based services for full drop-and-insert incident response team consultants

**Call Center Services** - Call center services can be used to ensure that language considerations, customer support for hearing-impaired or other disabilities, extended operating hours, or other considerations that may extend beyond the organization’s current capacity or capabilities. Call center capacity should be considered for consumer and customer support during and after privacy breach incidents or other occurrences that result in disclosure requirements.

**Outbound Print Mailing Operations** – The ability to generate and mail printed materials at scale to affected/impacted consumers and customers may require services beyond the organization’s existing capability.

**Credit Monitoring Services** – In many personal or financial information disclosure incidents it is prudent to extend credit monitoring and protection services to impacted individuals. Obtaining these services from capable firms that are recognized as reputable and reliable partners should be considered in preparation and anticipation of a potential incident so that the services can be offered quickly and efficiently.

**Legal Counsel and Litigation Support** – Many organizations employ internal legal resources, but others may need to utilize expertise from external firms. Engaging early with legal counsel helps apply attorney-client privilege protections to incident response activities and communications. Having support from counsel with expertise in privacy considerations and cybersecurity specifics can help the incident response team and the organization proceed accordingly in the development of processes and the execution of response procedures.

**Additional Hardware and Software** - Determined as necessary. Consider the needs of additional disk storage, systems for laboratory type recovery testing, or the resources needed to recover from attacks that may require physical evidence retention.

**Cybersecurity Insurance Policies** – While insurance coverage may not be specific to incident response capabilities, the ability to leverage the insurance coverage for supplemental services during or after a cybersecurity event can have implications on the incident response process itself. Evaluating current coverage as part of the preparation process is advised, and if coverage doesn't currently exist then collaboration between the incident response program and the risk management organization to obtain the appropriate coverage is recommended.

**Law Enforcement Relationships**

There are numerous scenarios and incident types that may occur as the result of a criminal act. Cybersecurity incidents in many cases are caused by criminal actors in violation of a local, state, federal, or international laws. Additionally, when the attacker is part of a criminal or nation state group, law enforcement can be a useful and appropriate contact for information or action. As part of the incident response preparation stage establishing contacts and maintaining relationships with law enforcement agencies is an important component of the incident response program.

Law enforcement agencies at the federal level include organizations like the United States Secret Service Electronic Crimes Task Force (ECTF) and Financial Crimes Task Force (FCTF)³, the United States Secret Service Investigation Mission - [https://www.secretservice.gov/investigation/](https://www.secretservice.gov/investigation/)

States Federal Bureau of Investigations regional and local field offices that are accessible through the FBI InfraGard private sector partner program\(^4\), as well as numerous regional law enforcement fusion centers and public/private partnerships. In addition, most states have active cybersecurity investigation units within the attorney general’s office and local law enforcement organizations continue to evolve and refine capabilities to support in the area of electronic crimes.

Organizations should consider engaging with law enforcement in their area to best understand what capabilities are present and how to best interface in an ongoing capacity. The time to develop the contacts with law enforcement is during the Incident Response Program Preparation Stage, when the pressure of an active incident is not dictating the timeline.

**Third-Party and Supply Chain Partners**

Organizations often rely on third parties to provide significant portions of business functions and aspects of their supply chain. Partners that make up these extended parts of the organization should be considered when developing the Incident Response Program. An attack against an organization may likely be launched first against a third-party supplier or part of the organization’s supply chain.

When developing response processes, communications, and holding exercises and drills, these partners should be included to ensure that all parts of the organization’s operations are on the same page during an incident response. Additionally, detection of an incident that results as part of an attack against a third party may not be directly observed by the organization’s security operations, or in some cases may occur simultaneously against the third-party network and the organization’s technology resources. Coordination and information sharing are pivotal for effective detection and response.

During the preparation phase of the incident response program, the organization should include third-party suppliers and supply chain partners. While outsourcing of the functions that these suppliers provide is done to achieve efficiency and cost-effective operations, the cybersecurity operations cannot be completely abdicated to the third party while continuing to have an effective Incident Response Program.

**Cybersecurity and Breach Insurance**

The organization should consider maintaining Cybersecurity and Breach Insurance. Cybersecurity events can be incredibly costly. A good insurance policy could help protect the health of the organization in the aftermath of an incident.

---

\(^4\) US FBI InfraGard - [https://www.infragard.org](https://www.infragard.org)
Detection and Analysis

Detection
Detecting a cybersecurity incident can occur in a variety of forms. Primary detection mechanisms are alarms from cybersecurity protection measures or reports from personnel, but the warning of an incident may also come from an external organization. Capable organizations proactively seek indications of incident occurrences while others are relegated to receiving notification from law enforcement or other external entities.

Internal cybersecurity sources provide information on events and potential cybersecurity incidents in the form of alarms produced from configured countermeasures and detective measures. The maturity of the information security program and the effectiveness of the cybersecurity protective and detective measures determine how successful and timely incidents are detected.

The Vocabulary for Event Recording and Incident Sharing (VERIS)\(^5\) provides a framework for categorizing incident-related information and is the basis for the analysis that produces the Verizon Data Breach Investigations Report (DBIR)\(^6\). Evaluating this information and the analysis that accompanies the annual DBIR report should be considered an essential activity within the Incident Response Program. Numerous other cybersecurity incident and breach reports evaluate data from various reported and analyzed incidents. Consulting these reports is a useful exercise to evaluate the various ways detection should be considered as well as the effectiveness for reducing the time to detect incidents as they occur.

Attack Vectors
Most organizations are subject to malicious attack from multiple vectors (methods and methodologies). The Incident Response Program should evaluate exposure areas and the organization’s attack surface to ensure that potential attack vectors are considered when conducting incident response detection and analysis. During this analysis, the following areas should be

\(^5\) VERIS Framework - [http://veriscommunity.net/index.html](http://veriscommunity.net/index.html)

analyzed to determine the capabilities that enable detection of incidents or the inability to observe attacks or threats against each.

- Network Systems
- Web Services and Applications
- Data Interfaces
- Email
- Remote Access and VPN Systems
- Telecommunications Systems
- External/Removable Media
- Impersonation and Spoofing
- Social Engineering
- Social Networks and Public Information
- Insider Activities and Improper Usage
- Loss or Theft of Equipment
- Cybersecurity Tools and Utilities

Understanding which systems can be accessed by threat actors is a critical component of detection. Organizations should consider their partners and supply chain in the evaluation of attack vectors, as all of the vectors in the above list may be distributed across numerous vendors and participants in the organization’s supply chain. Capable attackers will find the weakest link in the chain and the attack vector may not be a direct route through the organization’s systems.

Signs of an Incident - Sources of Precursors and Indicators

Detecting possible incidents is accomplished through analyzing precursors and indicators. Precursors are signs that an incident may occur in the future. Indicators are signs that an incident has already occurred. Precursors such as web server log entries and announcement of new exploits should be monitored. Typical indicators to monitor include IDS sensor alerts, antivirus alerts, failed login attempts and deviations from typical network traffic flow. Anomalous indicators are more difficult to analyze but are perhaps more valuable in identifying signs of an incident related to stealthy threat actors. Common sources of precursors and indicators include:

- Intrusion Detection & Protection System (IDS / IPS)
- Security Information and Event Monitoring (SIEM)
- Event Logs
  - Operating system, service and application logs
  - Network device logs
  - Network flows
- Antivirus and antispam software
- File Integrity Checking Software
- Data Loss Prevention Software
- Managed Security Service Provider (MSSP)
- External Indicators and Threat Intelligence
- Third-party monitoring services of dark web forums
• Open Source Intelligence (OSINT) and Publicly Available Information
• Information on Newly Discovered or Disclosed Vulnerabilities and Exploits
• People

**Incident Analysis**

Incident analysis begins with the first notification or report of a possible incident, typically to the security monitoring team. Investigative activities and analysis can be elevated to the incident response program which will engage additional processes, procedures and participation when elements of the event indicate the potential of an incident. Operations analysts and IT personnel should be familiar with the incident process and handling techniques. Their processes should include the documentation and preservation requirements during these early stages to aide in the incident response process should the event later be declared an incident.

Preparation for incident analysis is enhanced through preparatory profiling of networks and systems to create a behavior baseline and then monitoring for deviations from the baseline.

**Incident Documentation**

Incident response actions should be carefully and thoroughly tracked using an Incident Response Report with detailed activity information on each incident captured and retained. Incident Response Reports should be stored on secure servers under access control with limited access by authorized personnel.

You can find an Incident Response Report template in Appendix A.

**Incident Activity Logging**

Participants in the incident response process should maintain a log of the activities they perform to ensure that activities are tracked accurately. Having an accurate account of each individual’s activities will help to develop the Incident Response Report and capture all of the efforts that have gone into the response effort. Having these details will help account for the costs and resource efforts that were part of the incident. Detailed activity information aides in the effective handling of the incident as well as ensuring that handlers and analysts can coordinate activities across time during incident response activities spanning longer timeframes. Additionally, the details can be used in the post incident review and analysis process to evaluate performance and improve response capabilities and procedures.

Another good reason to capture detailed activities is for use in potential law enforcement or criminal investigations. Contemporaneous notes in the form of an incident handler’s log can be used to meet evidentiary requirements and also help law enforcement officials understand other evidence and how it may have been handled or collected during the initial and ongoing incident response.
Incident Identification
At the initial stage of incident response, or the earlier stage investigation of events within the security operations center, precursors or indicators may lead analysts to suspect that an incident is occurring. General operations processes should include steps or linkage to the incident response procedures that at minimum include activities that will address identifying potential incidents by type, leading to execution of the incident response processes that can initiate notifications, escalations, and appropriate forming of the incident response team if and when the incident is formally declared.

Declaring an Incident – The Incident Response Policy should clearly indicate who has the authority to declare an incident. To ensure that the declaration can occur effectively and timely, operations processes should provide personnel the escalation process and necessary information related to the event to provide the authorized individual to appropriately determine and make the declaration. Events that may be indicative of incidents that are of lesser severity may be defined in a manner that permits the operations staff to categorize the incident and begin the response process. However, clear thresholds of impact or potential impact should be defined to make sure that escalations occur as needed.

Incident Types and Categorization
Because incidents can occur across the many areas of the threat profile and attack vectors mentioned previously, incident types and the thresholds for escalation may at minimum include:

- Denial of Service
- Unauthorized Access
- Malicious Code/Malware
- Improper Usage
- Scans/Probes/Attempted Access
- Phishing
- Ransomware

Within these incident types, incidents should be categorized by severity based on the impact to the organization. Consider the below example severity categories and criteria for determining levels of incident severity:

- Critical
  - A large number of organization users or customers specified in the Incident Response Program have been affected
  - A public-facing website or resource is unavailable or otherwise impaired and observable by external parties or publicly noticeable
  - A business or mission essential function is impaired or impacted
  - A VIP or Executive Leadership users are affected or impacted
A Privacy Breach or other reportable data type is at risk of inappropriate disclosure – although the number of records may be a determinant for the severity level. Input from the organization’s General Counsel should be used when defining.

- **High**
  - A smaller but still significant number of users or customers are affected
  - Important but not business or mission essential function is impaired or impacted

- **Moderate**
  - 2 to 10 users are affected

- **Low**
  - A single user is affected

The organization should expand upon this list during the development of the Incident Response Program and utilize the post-incident processes to expand upon the details to help customize and tailor as necessary.

**Insider Threat**

Preparing for and responding to internal threats is just as important as proactively handling the more publicized external threats. Whether malicious or simple human error, internal cybersecurity breaches can cause just as much damage as an outside actor. Be sure that the program includes how you will detect malicious activity, suspected insider threat, and potential internal security incidents.

**Incident Prioritization**

While severity is a good first stage method of prioritizing response activities, it should be contemplated that more than one critical incident may occur simultaneously. Most organizations have limited information and cybersecurity personnel, and the entire organization is likely focused on non-incident related activities as a normal course of business. Response efforts may have to be focused on the most significant incidents first, evaluating potential damage and impact to the organization to make sure that the incidents can be addressed accordingly.

**Incident Notification and Ongoing Communication**

Communicating information related to an incident is an area that should be carefully considered during the development of the Information Security Program. While the desire to keep important individuals in the organization “in the loop” and advised of incidents when they occur, it should also be tempered with the understanding that all events do not warrant the alarm bell to be rung at the highest level of the organization. Alternately, it is never a good idea to keep information under wraps or spring critical incident information on the leadership of the organization at the last minute – or later.

When defining the organization’s thresholds of severity, the team drafting the Incident Response Program should take the opportunity to consult senior level management to define the method of
communicating information appropriately across the various levels. Participants in these discussions and the formation of the communication processes should include the following roles in the organization:

- Chief Information Officer (CIO)
- Executive Leadership Team
- General Counsel
- Division Heads
- Human Resources
- Public Affairs
- Corporate Communications
- Government Relations

Incident notification should be initiated by the operations personnel as precursors or indicators of an incident are detected. The notification audience may include personnel at varying roles or levels specific to the organization and correspond to the severity level of the potential incident.

Initial notification should primarily consist of generating awareness to parts of the organization that may have a role in the response process. Namely, the individual designated as authorized to declare an incident – likely the CISO, or Security Operations Center Director should be the first contacted. If the organization does not maintain a full-time incident response team, then members of the stand-up team that is designated to be assembled during an incident should be notified using a call tree type process. Additionally, the IT Service Desk or Help Desk should also be notified with instruction to execute their corresponding response procedures.

**Notification Details** - Notification details should include but not be limited to:

- Incident type
- Incident classification
- A brief description of what happened
- When did the incident occur
- When was the incident detected
- How the incident was detected
- What current risks are present and what is the potential impact of the risk
- What data is potentially compromised or exposed
- How much data is compromised or exposed
- Whose data is compromised or exposed, (i.e., customer, client, third party, etc)
- What mitigation steps are currently being taken
- Anticipated next steps, if any
- Who to contact for additional information

**Incident Escalation/De-escalation**

As the incident response moves into next stages of analysis, containment, and eradication the severity of the incident may be determined to escalate or de-escalate. The incident response
processes need to include communication plans for escalating and including the appropriate audiences at the defined higher levels of the organization. Additionally, if information obtained during continued analysis, containment, and eradication determine that the severity is not as high as originally determined the processes should include de-escalation notification so that all parties are aware of the current status and expectations of future ongoing communications.

**Incident Handling Checklist**
The incident handling checklist provides the major steps to be performed in the handling of an incident. Actual steps performed may vary based on the type of incident and the nature of individual incidents. Annexes for specific incident types and related processes are included in this document.

**Public Press Releases**
Coordination with the organization’s public relations contacts will determine the communications strategy. Elements of a press release or public communication should include but not be limited to:

- What happened
- Is the incident considered a data breach as defined by regulations
- Who is affected/not affected
- What specific types of personal information are involved if any
- What are the (brief) details of the incident
- Whether or not evidence indicates data has been misused and what impact or harm may occur as the result of the incident
- Expression of regret and steps the institution is taking to prevent similar incidents from happening again
- Major actions taken
- Where to go for more information

**Containment, Eradication, and Recovery**
Containment and Eradication

Containment and Eradication will have varying steps and methodologies depending on the incident type. However, common objectives will always include driving activities towards determining facts and separating unknowns and speculation from known details that better enable decisions and next steps.

| Known Facts | Speculative Facts | Theories | Unknowns |

As the information begins to be gathered, tracking the information in terms of determined facts, theories and speculation with basic confidence levels, and next steps/necessary activities to prove out the facts and when those activities should be completed can help track the progress of the incident response.

Choosing a Containment Strategy

Containment strategy is directly related to the type of incident (e.g. denial of service, phishing, etc.). Containment may require cutting of network access, disabling traffic flows, and establishing aggressive traffic filtering. Additional containment methods may include deactivating systems or communications links. All of these techniques have implications to business activities and should be weighed in terms of the risk versus the reward.

The consideration of limiting damage or the impact of data disclosure or violating confidentiality, limiting the disruption of availability, or retaining the integrity or privacy of data during an active incident can sometimes result in decisions to take quick and decisive actions. These considerations should be evaluated during the planning stage and executed during the containment and eradication stages.

A logical network diagram is helpful for noting the points of attacker impact and tracking lateral movement in an active incident or for incidents where attackers have ceased activity. Rings of activity based on time/date can help to track the movement of the attacker, speculate on the motives and targets, and sometimes help to attribute to an attacker group type based on methods and tactics observed. Defenders should remember that they have the upper hand – they know the landscape better than the attacker, where the choke points are, and where the defenses are strong or weak.

Identifying Sources of Attacks and Attacking Hosts

In order to thwart an active attack, it is often necessary to identify the source of the attack and the resources utilized by the attacker. In order to fully determine how to stop the attack and prevent further attacker activities from succeeding, tracking the attack back to its origin will provide more comprehensive mitigation strategies.

Identifying attacking hosts typically includes:

- Validating the attacking host’s IP address
• Researching the attacking hosts through intelligence capabilities
• Using threat intelligence and indicator data
• Identifying Command & Control hosts and infrastructure
• Monitoring possible attacker communication channels

Attribution is debated and can be difficult to accurately determine. Identifying specific threat actors or even threat groups may not provide much value outside of law enforcement’s desire to arrest and prosecute. However, for the individual organization it is very useful to, at a minimum, determine the general attacker type in order to ensure that the attacker’s objectives can be fully defeated. Working to determine if the attacker(s) are part of a nation state, criminally or financially motivated, or disruptive activist-oriented will help to ensure that the techniques used to contain and mitigate the threat of the attackers during and after an incident were completely effective as well as how long to keep the incident response open to ensure complete mitigation.

Monitoring External Forums for Impact Analysis
Many organizations consider that an incident that includes infiltration of information systems and exfiltration of data as the final result of a successful attack and unsuccessful incident response. Organizations should consider monitoring dark web forums and other external channels to detect the entrance of company data into the criminal marketplaces. Doing so can help to determine how much data was exposed and potentially limit the damages caused. There is also a potential of identifying individuals involved so that apprehension might actually have an opportunity to occur.

Protecting Communications and Communication Channels
Organizations should consider their internal communications channels and have alternative means of communicating to ensure that attackers cannot eavesdrop or otherwise observe and obtain communications of the incident response team. Larger coordinated response efforts that include conference bridges should ensure that participants are all identified as authorized personnel. Encryption of email or removing email from the communications channels may be necessary during response to some incidents. Additionally, consider that helpdesk/ticketing systems may also have uninvited visitors. Lastly, some incidents may also include malicious insiders, so steps should be taken to consider that communications may need to be performed in a nontraditional manner.

Eradication and Recovery
Eradication may be necessary to eliminate components of the incident, such as deleting malware and disabling breached user accounts. Recovery may involve restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security. Eradication and recovery should be done in a phased approach so that remediation steps are prioritized.
Evidence Gathering and Handling

Evidence gathered in the process of incident response should be handled in a manner consistent with law enforcement requirements. Evidence collection includes documenting the chain of custody. Chain of custody refers to the chronological documentation or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence. Particularly important in criminal cases, the concept is also applied in civil litigation.

Incident response events likely include collection of evidence by non-law enforcement staffs. As a result, appropriate chain of custody procedures written in layman’s terms must be established and made available to incident response team members. Chain of custody procedures should address but not be limited to both a chronological and logical procedure, especially important when the evidence consists of items which can easily be substituted for items in evidence e.g. flash drives, laptops, etc.

Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs.
Post-Incident Activity

Lessons Learned
Upon closure, each incident is reviewed via a “lessons-learned” or “hotwash” meeting. Lessons-learned is essential to continuous improvement in incident response. Hotwash meetings should occur as soon as possible following an incident response completion to identify issue areas and process adjustments.

Access to hotwash documentation should be restricted to specific incident response technical personnel. Lessons learned should be reviewed and then included in iterative cycles of the preparation stage and for training events to ensure appropriate updates and changes are incorporated to the Incident Response Program and associated procedures.

Incident Summary Reports / Using Collected Incident Data
Incident data is used to develop metrics over time periods. Incident response information will be tracked and included in summary reports that may be issued on a periodic basis to evaluate overall incident trends.

Evidence Retention
Evidence is retained based on requirements for prosecution, data retention and cost. Evidence should be appropriately secured and provided to law enforcement as necessary when criminal behavior leads to opening a case with a law enforcement agency. Formal forensics processes and expert consultation should be sought to create forensically sound processes for potential court proceedings.
Performance Metrics
Performance metrics are used to capture level of effort, continuous improvement and future planning. Suggested Performance Metrics include:

- Number of events, alarms, and incidents per month per category:
- Total amount of labor spent working on investigating events, evaluating alarms, and responding to incidents.
- Elapsed time for activities related to incident response:
  - From the beginning of the incident to incident discovery
  - Time from discovery to the initial impact assessment
  - How long it took the incident response team to respond to the initial report of the incident
  - Time for each stage of the incident handling process (e.g., containment, recovery)
  - How long it took to report the incident to management if required
  - Time to include contacts with appropriate external entities (e.g., law enforcement,) if required
- Labor Effort Expended Per Incident
  - Hours
  - Costs

Incident Response Plan
The incident response plan provides the roadmap for implementing the Incident Response Program capabilities. The plan helps ensure that the program is sustained over time, matured for effectiveness, and improved to meet the ongoing needs of the organization.

The incident response plan accounts for the strategic goals of the information security program and organization’s mission, outlines the resource needs for executing on objectives, prioritizes the activities and defines the metrics for measuring progress for conducting the activities that are essential to how the response capabilities are enabled. The incident response plan should be a fundamental part of the information security program strategy as it relates to a foundational capability in the organization cybersecurity operation.

Developing the Incident Response Plan
As part of the Preparation Stage of the Incident Response Program, it is critical to develop the Incident Response Plan for implementing the necessary capabilities. Important steps for developing the plan will borrow from efforts of the overall information security program, specifically the risk management program and security policy for establishing the program with the appropriate authorization and prioritization. Additionally, the prelude to an incident response has the prerequisite
of detection produced from monitoring and the ability to contain the incident and mitigate damages relying on protection functions.

Leveraging the information provided in the previous sections, the following steps should be included in the execution of the incident response plan.

**Incident Response Preparation**

- Identify information resources and assets
- Evaluate risks associated with various information resources and assets, and perform an impact analysis to define the organization’s “crown jewels”
- Create the Incident Response Policy
- Garner Stakeholder Support
- Assemble the Response Team
- Define Incident Response roles and responsibilities
- Create a RACI\(^7\) chart with swim lanes for responsibilities and activities
- Develop the budget needs for the Incident Response Program and integrate into the organization budget process
- Identify role-required training and schedule participation for resources
- Schedule recurring internal team training
- Create recurring exercise schedule
- Identify location for incident response war room – a private conference room or area of the operations center that can serve as the central nerve center
- Ensure that system clocks are synchronized
- Establish a sharing center process for supply chain partners

**Detection and Response**

- Establish Incident Severity Levels – Consider Figure 1 as a guide

<table>
<thead>
<tr>
<th>Severity Classification</th>
<th>Users Impacted</th>
<th>VIP / Management Impact</th>
<th>Tier 1 Business Applications</th>
<th>Tier 2 or 3 Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^7\) Creating a RACI chart - [https://www.projectsmart.co.uk/how-to-do-raci-charting-and-analysis.php](https://www.projectsmart.co.uk/how-to-do-raci-charting-and-analysis.php)
• Establish incident types and classifications
• Define escalation levels
• Develop security operations processes for elevating investigations to incidents
• Establish hotline and reporting contacts for end user observations reporting
• Establish external contact mechanism and publish publicly
• Define threat hunting processes and attack vector analysis processes to continually improve detection and analysis
• Establish indicators and information types that the organization authorizes to be shared with information sharing groups
• Join relevant Information Sharing and Analysis Organizations (ISAOs) and/or Information Sharing and Analysis Centers (ISACs)
• Create the inventory of detection sources and methods – associate effectiveness metrics for timeliness, quality, and relevance
• Establish a baseline of normal network activity, workstation behavior, and data flow/transmission
• Integrate hunting processes into the ongoing exercise schedule
• Create the incident response activity log template for responders
• Create the incident response report – see Appendix A for example
• Create the template for incident progress status reports

**Containment, Eradication & Recovery**

• Determine the need for evidence preservation and a secure storage location
• Establish research laboratory – a network that analysts can research and evaluate potential attacker systems that is separate and not attributed to the organization
• Establish a segmented/protected area for analysis of systems that may need to be evaluated in a quarantined environment
• Continually evaluate backup retention status for key resources and document the means of gathering within the incident response processes
• Continually evaluate the workstation/server image status to ensure that the images are updated in conjunction with the change management processes

**Post-Incident Activity**

• Ensure that the incident activity log template includes notes areas for process observations and improvement notations
• Create an incident hotwash agenda template that includes discussion topics such as:
  o What went well?
  o What didn’t work well?
  o What information was needed sooner?
  o What information can we share with peers, partners, and industry sharing groups?
What protective measures, controls or countermeasures would prevent the incident in the future?
What detective measures would provide faster detection of the incident in the future?
What precursors or indicators should be watched for in the future to detect similar incidents?
How effective and timely were communications during the incident?

Ensure that the incident response report template accommodates useful data aggregated for analysis and reporting

Depending on the maturity level and operational capability, some of the recommended steps may not be approachable at the onset, but continual improvement and evolution of the Incident Response Program should anticipate these steps and will generate others.
Incident Response Program Policy

Statement of Management Commitment
The {organization name}’s leadership team is committed to information security and appropriate incident response to accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources. {Organization Name} has established the Incident Response Program to establish an actionable information security incident handling capability that includes preparation, detection, analysis, containment, recovery, and reporting for information security incidents.

The organization’s {responsible executive} oversees the Incident Response Program as a whole and ensures that resources are appropriately maintained for preparedness and training for response to incidents that are reasonably foreseen or identified through continual activities associated with the Information Security Program.

Purpose
The Information Security Program includes an Incident Response Program provided to establish and maintain consistent Incident Response capabilities and processes enabling the organization to respond to cybersecurity threats and attacks swiftly and effectively. The Incident Response Program is designed to address the many factors that comprise typical attacks and the wide variety of considerations that go into ensuring your organization is prepared to handle all possible scenarios.

Scope
The scope of the Information Security Incident Response Program includes the span of authority and requirements assigned by the organization’s executive leadership. All incidents impacting the confidentiality, integrity, availability of the organization’s information or information systems as well as the privacy of individuals associated with the organization within the assigned authority are considered within the scope of the Incident Response Program.

Objectives
The Incident Response Program include objectives to:

- provide a roadmap for implementing incident response capability
- describe the structure and organization of incident response capability
- provide a high-level approach for how incident response fits into the overall organization
- meet requirements of the organization to define specific capabilities, processes, or guidelines
- define reportable incidents
- provide metrics for measuring incident response capability
- define resources and management support for incident response capability
• establish review and approval process
• distribute the plan as appropriate based on incident response roles
• establish incident response plan review frequency
• establish a process to update the incident response plan as necessary
• communicate incident response plan changes to incident response personnel
• protect the incident response plan from unauthorized disclosure and modification
• create training opportunities and exercises to ensure personnel are prepared to perform their roles during an incident response

Levels of Authority

{Authority} has overall authority to
• Declare an information security or cybersecurity incident
• Authorize the confiscation or disconnection of equipment
• Communication with Management as necessary
• Establish requirements and guidelines for external communications and information sharing

{Incident Response Coordinator (IRC)} has overall authority to
• Activate incident response teams and resources as necessary
• Establish additional monitoring of suspicious activity
• Execute escalation processes

Incident Response Team Members
• Communicate among the activated teams and additionally as directed by the Incident Response Coordinator.

Communication and Coordination

Organizational Entities
Define the reporting structure for ongoing incident communications across the severity levels and impact analysis.

External Entities
Define the external organizations that are part of the communication and coordination center for the Incident Response Program.

List the elements of information, indicators, and other elements that are shareable during the active incident and after the incident concludes.
# Appendix A – Security Incident Report Form

## Information Security Incident Report

*Instructions: This form is to be completed as soon as possible following the detection or reporting of an Information Security incident. All items completed should be based on information that is currently available. The report should be updated and modified during the course of the incident response process.*

<table>
<thead>
<tr>
<th>Incident ID (yyyymmdd-xxxx)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

## 1. Incident Description.

Provide a brief description:

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

## 2. Incident Details

<table>
<thead>
<tr>
<th>Date and Time the Incident was discovered:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Has the incident been resolved?

<table>
<thead>
<tr>
<th>Physical location of affected system(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Number of sites affected by the incident:

<table>
<thead>
<tr>
<th>Approximate number of systems affected by the incident:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

Approximate number of users affected by the incident:

<table>
<thead>
<tr>
<th>Are third party vendor systems, such a business partners, affected by the incident? (Y or N – if Yes, please describe)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

## 3. Impact / Potential Impact

Check all of the following that apply to this incident.
Loss / Compromise of Data
Damage to Systems
System Downtime
Financial Loss
Other Organizations’ Systems Affected
Damage to the Integrity or Delivery of Critical Goods, Services or Information
Violation of legislation / regulation
Unknown at this time

Provide a brief description:

4. Sensitivity of Data/Information Involved Check all of the following that apply to this incident.

<table>
<thead>
<tr>
<th>Sensitivity of Data</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.</td>
</tr>
<tr>
<td>Internal Use Only</td>
<td>Internal Use information is information originated or owned by your organization or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.</td>
</tr>
<tr>
<td>Confidential</td>
<td>Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by your organization.</td>
</tr>
<tr>
<td>Restricted (Potential Privacy Violation)</td>
<td>Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.</td>
</tr>
<tr>
<td>Unknown/Other</td>
<td>Describe in the space provided</td>
</tr>
</tbody>
</table>

Provide a brief description of data that was compromised:
### 5. Who Else Has Been Notified?

Provide a log of the personnel notified during the course of the incident response. Include name, title, date and time of notification, as well as the method of communication.

### 6. What Steps Have Been Taken So Far? Examples of potential activities that may apply.

<table>
<thead>
<tr>
<th>No action taken</th>
<th>Restored backup from tape</th>
</tr>
</thead>
<tbody>
<tr>
<td>System disconnected from network</td>
<td>Log files examined (saved &amp; secured)</td>
</tr>
<tr>
<td>Updated virus definitions &amp; scanned system</td>
<td>Other – please describe:</td>
</tr>
</tbody>
</table>

Capture the ongoing log of activities taken during the incident response process, including date and time of the activity:
Appendix B – Document Source, Baseline and References

Portions of this Incident Response Program guide and the Incident Response Plan template materials leverage the National Institute of Standards and Technology (NIST) Special Publication 800-53.8 FedRAMP templates9 and documents10 are also used to include the necessary detail an organization needs to operate a comprehensive and effective information security program.

Each organization will need to tailor parts of the program to suit business objectives and priorities, relate to the identified and foreseeable risks that the organization is confronted with, and ensure compliance to applicable laws, regulations, and privacy mandates. You can enhance, edit, merge, rename, separate or modify individual components as necessary to meet your organizational requirements.

The Incident Response Program is modeled on the National Institute of Standards and Technology Special Publication 800-61 Computer Security Incident Handling Guide Revision 2.11 The program has been tailored to include specific guidance to deal with incidents as they relate to most organizations.

Statutory Requirements Regarding Data Breach Notification

Each state maintains state-specific requirements regarding data breach notification. In general, notification requirements include:

- Individuals impacted by the data breach if the organization owns the data
- The owner or license holder of the data if the organization does not own the data
- Consumer reporting agencies

Notification must be made as quickly as possible except

- When a law enforcement organization determines the disclosure would impede a criminal investigation
- As necessary to determine the scope of the breach and restore the reasonable integrity of the data system

At a minimum, organization procedures shall address requirements and applicability of the following –

- Gramm-Leach-Bliley Act (GLBA)
  - Financial Institutions and Customer Information: Complying with the Safeguards Rule
  - Health Insurance Portability and Accountability Act (HIPAA)
    - Breach Notification Rule

---

- Internal Revenue Service (IRS) Publication 1075
  - Section 10.0 Reporting Improper Inspections or Disclosures
- NIST SP 800-61 Rev 2
  - Section 3.2.7 Incident Notification
  - [http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
- Office of Management and Budget (OMB) Memorandum M-07-16
  - Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- Omnibus HIPAA Rulemaking
- Payment Card Industry Data Security Standard (PCI DSS)
  - [https://www.pcisecuritystandards.org/pci_security/](https://www.pcisecuritystandards.org/pci_security/)
- US Department of Health and Human Services (HHS)
  - Personally Identifiable Information (PII) Breach Response Team (BRT) Policy (Federal)
  - [http://www.hhs.gov/ocio/policy/20080001.003.html](http://www.hhs.gov/ocio/policy/20080001.003.html)
- Various state privacy laws as applicable
BE PREPARED FOR A CYBER ATTACK
Minimize the damage and disruption caused by a cyber attack by ensuring your organization is prepared to recover quickly from an incident. Our highly experienced team can help you take the next steps to validate that your plan is effective and your team is ready.

TABLETOP EXERCISES
$4900
Our cybersecurity experts will lead an onsite discussion-based session designed to help every employee understand their role in responding to a cybersecurity incident. Over the course of one day, our facilitators will guide participants through multiple customized scenarios to ensure everyone knows how to respond to a cyber attack. Plus, we'll deliver a full report after the exercise identifying gaps and recommendations for improvements.

VIRTUAL EXERCISES
$14900
Advance your team's cyber attack readiness further with virtual cyber attack exercises in the CyberDefenses virtual cyber range. Our cybersecurity experts will work onsite with up to 8 members of your team for two days to exercise your Incident Response Plan in response to relevant cyber attacks. Using our virtual environment, we'll assign each participant a role and we'll present a simulated threat to which they must respond using your established policies and protocols. Following the exercise, we'll provide you with a full report that outlines discovered gaps and improvement recommendations. It's an ideal way to work out any issues in a low-stakes environment so that everyone is ready for a real cyber threat event.

ONSITE EXERCISES
REQUEST QUOTE
Train your team where it matters most, in your own environment. CyberDefenses cybersecurity experts will come to your site to create simulated incidents that factor in the specific criteria and unique structure of your city, systems, network and culture. It ensures that every member of your response team knows exactly how to respond and that your processes are effective. We'll work closely with your leadership team to identify and design the specifics of your customized exercises.
OUR FULL SERVICE OFFERING

Guidance
- Organizational Review
- Operational Review
- Governance, Risk Mngmt, Compliance
- Incident Review
- CISO Advisory
- Board Advisor

Managed Security Service
- Data Protection
  - Backup and Recovery
  - Data Access and User Controls
- Defense Operations
- Vulnerability and Patch Management
  - Vulnerability Scanning, Patching
- Pen Testing
- External Threat Intelligence
  - Credential Tracking Services
- Continuous Monitoring
  - Securing Defense Monitoring
  - Identity Access Control
  - Server and User Endpoint

Threat Hunting and Response
- Advanced Detection
- Incident Response
- Forensics
- Forensics Accreditation
- Education and Skills

Academy
- Online, onsite and Austin Campus
  - cybersecurity training for individuals and groups. Courses include Threat Hunting, Incident Response, Compliance and many others.

Professional
- NIST SP 800-171 Assessments
- GDPR Assessments
- IAM Security Integration
  - Governance
  - Analysis
  - Unstructured
  - Solution Integration

ABOUT CYBERDEFENSES

Founded in 2001 by a team of returning military, cybersecurity veterans, the CyberDefenses staff is comprised of battle-tested cybersecurity professionals from the Big 5 consulting firms, Fortune 500 companies and the US Military. Our seasoned team holds credentials from the NSA, Endeca, SAP-BOBJ, Oracle - OBIEE, Microsoft, Cisco, Linux and many others. We are the only cybersecurity services firm that integrates cybersecurity oversight, comprehensive managed services and cybersecurity training to deliver top security services to businesses, associations, education associations and the military, among many other organizations.