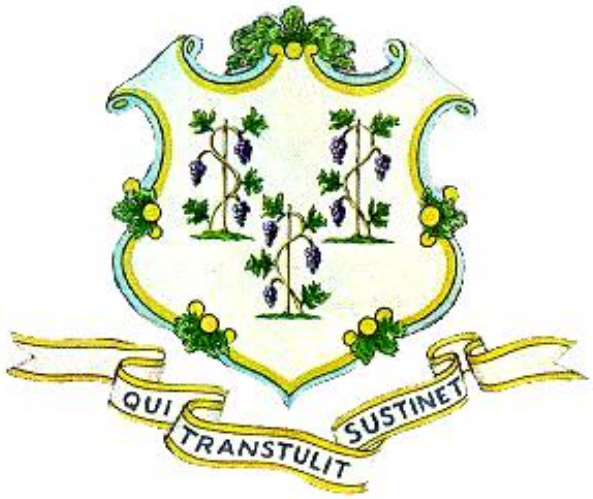
7/11/2019

Incident Response Plan



State of Connecticut

Release 1.5

Table of Contents

Executive Summary

{This document is designed as a template for State of Connecticut Executive branch agencies to use developing agency-specific Incident Response Plans. Other state branches, local and municipal government agencies may also use this template, but some references to DAS/BEST as a central response resource may need to be modified.}

The State of Connecticut utilizes a Distributed and Centralized Computer Security Incident Response Teams (CSIRTs)[1] model compliant with the National Incident Management System (NIMS)[2]. In this model, a dedicated, centralized CSIRT (The DAS/BEST Security Division) interacts with the DAS/BEST supported agencies who are distributed in various geographic sites and divisions. The DAS/BEST Security Division provides high-level analysis, recommends recovery and mitigation strategies and co-ordinates with the various Divisions of DAS/BEST. The DAS/BEST Security Division also provides incident and vulnerability response support for the agencies. The agencies and other DAS/BEST Divisions implement the strategies and provide expertise in their areas of responsibility.

This model maximizes the utilization of existing staff in strategic locations through the organizations with the centrally located coordinating capability of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency. It has management support in assigning needed resources during times of crisis.

The model builds on the infrastructure and expertise in the local areas where the agencies facilitate incident analysis and response (working with others in their own organization and at DAS/BEST –systems, network, and security administrators, software developers, LAN/WAN managers, etc. – who are not part of the CSIRT). The CSIRT responds to reports of abnormal activity or other incident reports, participates in incident and vulnerability analyses, lends expertise in testing or assessing the security of the enterprise, and plays a proactive role in promulgating computer security awareness and training throughout the organization.

The model provides a centralized team that can collect information from a wide variety of constituent sources and quickly synthesize and disseminate it across the enterprise.

The combined team works best if it has full authority to analyze activity and shared authority to respond to incident activity as it occurs. No enterprise-wide action is taken or recommended without the approval of the CSIRT manager and possibly upper management such as the CIO or ITSecurity Director. The team also has the authority to enforce the recovery and mitigation strategies with the approval and consent of

[1] Organization Models for Computer Security Incident Response Teams (CSIRTs), December 2003, Carnegie Mellon Software Engineering Institute
[2] Governors Directive 10

management. Divisional and functional unit managers are notified of any action to be taken in their areas and are involved in the decision-making process to determine how to implement a response.

The team has the authority to release organization-wide advisories and other documents, including best-practices, response and recovery steps, and security updates. The team can also be responsible for reviewing and analyzing all IDS or other network, system or application logs.

The Incident Response Plan covers all information security incidents that occur at DAS/BEST and the State of CT agencies, including those that need to comply with Federal regulatory compliance mandates including but not limited to SSA, HIPAA, FTI, CMS, etc.

Definitions

For the purposes of the Incident Response Plan, the following terms have been defined.

1. Access – The ability or the means necessary to read, write, modify or communicate data/information or otherwise use any system resource.
2. Access Control – The process that limits and controls access to resources of a computer system; a logical or physical control designed to protect against unauthorized entry or use.
3. Access Control Mechanisms – Hardware, software, or firmware features and operating and management procedures in various combinations designed to permit authorized, and detect and prevent unauthorized access to a computer system.
4. Access Rights – Also called "permissions" or "privileges", these are the rights granted to users by the Agency. Access rights determine the actions users have been authorized to perform (e.g., read, write, execute, create and delete).
5. *Agency* – *see covered entity*.
6. Agency Security Official – The individual designated by the Agency who is responsible at that Agency for the development and implementation of the policies and procedures.
7. Application – A computer program or set of programs that processes records for a specific function.
8. Application Controls – These refer to the transactions and data relating to computer-based applications whose purpose is to ensure the completeness and accuracy of records and the validity of the entries in the records. Applications controls may be manual or programmed, and the records and entries may result from both manual and programmed processing. Examples of application controls include, but are not limited to, data input validation, agreement of batch totals and encryption of data transmitted.
9. Audit – A methodological examination and review of an Agency's implementation of Security Policies and Procedures, including but not limited to FTI, HIPAA, PCI, etc…
10. Authentication – The corroboration that a person is the one claimed. Authentication is the act of verifying the identity of a user and the user's eligibility to access computerized information. Authentication is designed to protect against fraudulent logon activity. It also can refer to the verification of the correctness of a piece of data.
11. Backup – Exact copies of files and data, and the necessary equipment and procedures available for use in the event of a failure of applications or loss of data, if the originals are destroyed or systems are not functioning.
12. Business Continuity Plan – Also known as contingency plan. A document describing how an organization responds to an event to ensure critical business functions continue without unacceptable delay or change.
13. Business Continuity Planning – Business continuity is the ability to maintain the constant availability of critical systems, applications, and information across the enterprise.
14. Centralized Procedures – Procedures that are developed and administered by the ITSU pertaining to the Federal regulatory compliance and must be implemented by all Agencies.

15. CIO – State of Connecticut Chief Information Officer and the administrative head of the DAS/BEST.
16. CSO – Chief Security Officer.
17. Data Owners – Individuals employed by state agencies, who have been given the responsibility for the integrity, accurate reporting, and use of computerized data.
18. Decentralized Procedures – Procedures that are developed, administered and implemented by the Agencies that are Agency specific.
19. Detection and Analysis: First reports of an incident, may come from a customer complaint or report, a monitoring tool such as IDS or log, or other method.
20. Disaster Recovery Plan – A documented plan that provides detailed procedures to facilitate recovery of capabilities at an alternate site.
21. Disaster Recovery Planning – Disaster recovery refers to the immediate and temporary restoration of critical computing and network operations after a natural or man-made disaster within defined timeframes. An organization documents how it will respond to a disaster and restart the critical business functions within a predetermined period of time; minimize the amount of loss; and repair, or replace, the primary facility to resume data processing support.
22. Electronic Protected Health Information (ePHI) – Agency information that is individually identifiable health information that is transmitted by electronic media or maintained in electronic media.
23. Encryption – A technique (algorithmic process) used to transform plain intelligible text by coding the data so it is unintelligible to the reader.
24. Health Care Clearinghouse – A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value added" networks and switches, that either processes or facilitates the processing of health information.
25. HIPAA – The Health Insurance Portability and Accountability Act of 1996 and the rules and regulations promulgated thereunder.
26. Information Security – Administrative, physical and technical controls that seek to maintain confidentiality, integrity and availability of information.
27. Information Technology (IT) Resources – IT resources are tools that allow access to electronic technological devices, or are electronic technological devices themselves that service information, access information, or are the information itself stored electronically. These resources include all state-supplied computers and servers; desktop workstations, laptop computers, handheld computing and tracking devices; cellular and office phones; network devices such as data, voice and wireless networks, routers, switches, hubs; peripheral devices such as printers, scanners and cameras; pagers, radios, voice messaging, computer generated facsimile transmissions, copy machines, electronic communication including email and archived messages; electronic and removable media including CD-ROMs, tape, floppy and hard disks; external network access such as the Internet; software, including packaged and internally developed systems and applications; and all information and data stored on State equipment as well as any other equipment or communications that are considered IT resources by DAS/BEST.

28. Information Technology Security Division (ITSD) – The unit within DAS/BEST under the direction of the CIO that is responsible for overall information security functions for the executive branch of State government. Information security functions include policy administration, security audits and assessments, security tools, security operations, security investigations, security awareness training, and risk management pertaining to the potential loss or unauthorized disclosure of IT resources and electronic information.
29. Logical Access Control – The policies, procedures, organizational structure and electronic access controls designed to restrict access to computer software and data.
30. Malicious Software – Software, for example, a virus, designed to damage or to disrupt a system.
31. Password – A protected, generally computer-encrypted string of characters that authenticate an IT resource user to the IT resource.
32. Preparation for Incidents: The time prior to the incident that is spent planning for a potential event. For each incident response, several things need to be in place prior to the occurrence of an incident such as: contact information and methodologies for command staff and team members; facilities for meetings, work, storage, and other activities related to the incident response; hardware and software tools needed for the recognition and handling of the incident; as well as documentation and other knowledge bases needed for effective response to the incident.
33. Preventive Controls – Controls designed to prevent or restrict an error, omission or unauthorized intrusion to IT resources.
34. Risk Analysis – An assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of IT resources.
35. Risk Management – The process of identifying, measuring, controlling and minimizing or eliminating security risks that may negatively affect information systems.
36. Security Incident – The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with systems operations in an information system.
37. Unique User Identifier – A unique set of characters assigned to an individual for the purpose of identifying and tracking user identity.
38. Workforce Member (User of an Information Technology Resource) – Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

0. Mission Statement

The mission of this plan is to define a National Incident Management System (NIMS) and National Institute of Standards and Technology (NIST) compliant incident response plan for use by *Your Agency*. The purpose of this plan is to make incident response more simplistic and consistent for all potential types of incidents.

NIMS and NIST compliance enhances the scalability of the framework, allowing interaction with local, state and federal resources using common methods and terminology defined at the federal level. This framework is a plan by which to develop response procedures for general and specific incident types. Material here is based on NIST special publication 800-61 and the NIMS 9.0 document published by the Department of Homeland Security.

Incidents response occurs in four phases.

1. Preparation: Preparation has to be completed before effective response to an incident can occur. Different incident types require different preparation. For each incident response, several things need to be in place prior to the occurrence of an incident such as: contact information and methodologies for command staff and team members; facilities for meetings, work, storage, and other activities related to the incident response; hardware and software tools needed for the recognition and handling of the incident; as well as documentation and other knowledge bases needed for effective response to the incident.

2. Detection and Analysis – First reports of an incident – may come from a customer complaint or report, monitoring tools or other methods. At this step the incident is vetted for validity and categorized for type and severity. Preliminary notifications and communications are established. Appropriated response procedures, personnel, and tools are assembled.

3. Containment, Eradication, and Recovery – Based on the results of recognition, the proper response procedure is implemented. Immediate steps are taken as appropriate to limit loss from the incident. Evidence is preserved. Impact of this containment to customers and the enterprise is communicated to those affected. A long term resolution of the incident is developed and implemented. This step may include policy alteration or development, system redesign, introduction of new systems or technologies, training, or other actions deemed necessary to permanently resolve an incident. As necessary, systems are restored and brought back online, data is restored, and appropriate parties are notified.

4. Post Incident Activity – Report of the incident from start to conclusion is finalized. Updated incident response procedures, lessons learned, and documentation of any permanent changes to systems as a result of the incident are generated. Incident data

collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

General points about implementing the framework:

1. Communication to appropriate parties will be maintained throughout the incident. Critical communication paths are between response team members, between the response team and command staff, and between command staff and customers. Some of these communication paths may need to be secure. Communication procedures should be developed to be consistent across incident response procedures.

2. All procedures should be available and accessible. This means that all procedures should be maintained through several different methods in case an incident renders one or more methods unavailable. All updates must be communicated to all those who may be involved in a response.

1. Preparation Phase

PREPARATION PLANNING

As part of information security risk assessment and management, DAS/BEST and its supported agencies identify potential threats. While DAS/BEST and its supported agencies make an effort to prevent most incidents, it is impossible for DAS/BEST or its agencies to prevent all incidents from occurring at all times. Therefore, DAS/BEST and its supported agencies need to prepare for incidents which may occur.

Critical to this preparation is the identification and development of the appropriate trained staff to support the response to any incident and to implement incident prevention technologies and protocols as necessary.

STAFF SUPPORT

Background: It is important to pre-identify the necessary roles for the purpose of incident response. Required knowledge and skill sets should be in place prior to the need for an incident response. Individuals with the required knowledge and skill sets should be available at all times to respond to an incident. A single individual may perform several roles concurrently. Members of an incident response group may or may not participate in a similarly labeled group in their day to day work. Specific incident response will dictate which roles are necessary and activated. These roles are in alignment with National Incident Management System (NIMS) guidelines as per the NIMS 9.0 document.

Roles:

1) Command Staff (Incident Management Team)
    a) Incident Commander - Management level person(s) with the authority to make high level decisions and approve actions to be taken by the incident response team.
    b) Information Officer – Person who disseminates public and non-sensitive information to interested parties.
    c) Liaisons – Persons who are the point of contact for other governmental and non-governmental agencies and organizations.
    d) Safety Officer – Person who monitors incident operations and advises on matters related to operational safety.
    e) Legal - Advises incident command on legal matters

2) General Staff
    a) Operations staff – responsible for the functional aspects of the incident command structure
        i) Operations Chief and deputies
            (1) Directly manages all incident tactical activities

ii) Divisions, Groups, and Resources **(NOTE – REMOVE – Agencies should establish operational groups appropriate for their Agency business function(s) REMOVE)**

(1) *Agency Division* Group – Incident response team members responsible for functional aspects of IT security policies, and procedures
   (a) *Agency* group lead – oversees IT security group team members
   (b) *Agency* security analysts and specialists – team members with incident analysis and handling skills and experience.
   (c) *Agency* Security SME/Analysts
      (i) Intrusion and Monitoring SME and Analysts – Person(s) with firewall, IPS, and monitoring tool experience.
      (ii) Forensic SME - Person(s) with systems analysis and forensic ability and experience

(2) *Agency* Network Group – Incident response team responsible for functional aspects of network management
   (a) Network group supervisor - oversees network group team members
   (b) Network SMEs (local area networks, area specialists) – Persons with experience and authorization necessary to manage affected local area networks.

(3) *Agency* Database Group – Incident response team responsible for functional aspects of database systems
   (a) Database group supervisor – oversees database team members
   (b) Database SMEs – person(s) with experience and authorization necessary to manage affected database systems.
      (i) Oracle
      (ii) Microsoft SQL
      *(iii)*DB2

(4) *Agency* Platform Group – Incident response team responsible for functional aspects of server and workstation platforms
   (a) Platform group supervisor – oversees platform group team members
   (b) Server Platform SMEs - person(s) with experience and authorization necessary to manage affected server platforms
      (i) Windows
      (ii) Linux
   (c) Workstation Platform SMEs - person(s) with experience and authorization necessary to manage affected workstation platforms
      (i) Windows

(5) *Agency* Application Group - Incident response team responsible for functional aspects of server and client applications
   (a) Application group supervisor – oversees application group team members
   (b) Web Application SMEs - person(s) with experience and authorization necessary to manage affected web server applications

(c) Management Application SMEs - person(s) with experience and authorization necessary to manage affected management information systems
    (i) Antivirus
    (ii) Patch Management
    (iii) Email
    (iv) Other incident affected applications
(d) Desktop Application SMEs - person(s) with experience and authorization necessary to manage affected workstation based applications.

(6) *Agency* Continuity of Operations Group – Team responsible for continuity of operations – responsible for maintenance and implementation of disaster recovery and business continuity procedures should they be necessary
    (a) COOP planner

b) Planning staff
   i) Planning section Chief and deputies
      (1) Oversees all incident related data gathering and analysis regarding incident operations and assigned resources, develops alternatives for tactical operations, conducts planning meetings, and prepares the incident action plan for each operational period.

   ii) Resources Unit – Team responsible for assuring that all assigned personnel and other resources are available at the incident
      (1) resource managers
         (a) Human resource manager – responsible for human resource availability
         (b) Equipment manager – responsible for equipment maintenance and availability
         (c) Facilities manager – responsible for facilities maintenance and availability

   iii) Situation Unit – Team responsible for collecting, preparing, organizing, processing, and disseminating ongoing incident information
      (1) Situation report specialist

   iv) Documentation Unit – Team responsible for maintaining accurate and complete incident records including major steps taken to resolve an incident. Also maintains and stores incident information for legal, analytical, and historical purposes
      (1) Incident documenters

   v) Demobilization Unit – Team responsible for the creation and dissemination of an incident wide demobilization plan.
      (1) Demobilization planner

   vi) Technical Specialists – Team responsible for advising other incident response personnel on their respective areas of expertise, including but not limited to:
      (1) Legal specialist
      (2) IT specialists
      (3) Medical / healthcare specialist
      (4) Human resources specialist
      (5) Environmental specialist
      (6) Structural specialist
      (7) Industrial hygienist
      (8) Transportation specialist

c) Logistics staff – Responsible for providing all support needs for the incident.
   i) Logistics Section Chief and deputies
      (1) Responsible for all support needs for the incident, including coordination of procurement for required resources, providing facilities, transportation,

supplies, food service, communications, and medical services for incident personnel.

ii) Supply Unit – Team responsible for receiving, storing, and processing all incident related resources, personnel, and supplies.
   (1) Supply specialist
   (2) Human Resources specialist
   (3) Procurement specialist

iii) Facilities Unit – Team responsible for set-up, maintenance, and demobilization of all facilities used in the support of incident operations including food and water service, sleeping, sanitation and showers, and staging.
   (1) Facilities manager
   (2) Facilities specialist

iv) Communications Unit – Team responsible for developing, implementing, and maintaining a communication plan for the incident.
   (1) Communications specialist

v) Food Unit – Team responsible for determining food and water requirements, developing menus, ordering food, providing cooking facilities, cooking, serving, maintaining food service areas, and managing food security and safety concerns.
   (1) Food service specialist

vi) Medical Unit – Team responsible for developing an incident medical plan, providing medical care, the transportation of sick or injured personnel, and tracking of incident personnel patients.
   (1) Medical specialist

d) Finance / Administration staff
   i) Finance / Admin Chief and deputies
      (1) Responsible for determining current and anticipated requirements for the establishment of specific incident response units.

   ii) Time Unit – Team responsible for ensuring proper daily recording of personnel time.
      (1) Personnel time tracking specialist (CoreCT)
      (2) Equipment time tracking specialist

   iii) Procurement Unit – Team responsible administering all financial matters pertaining to vendor contracts.
      (1) Procurement (purchasing) specialist

   iv) Compensation and Claims Unit – Team responsible for documenting and investigating injury compensation claims.
      (1) Injury compensation and claims specialist

(2) Human resource specialist

v) Cost Unit – Team responsible for cost analysis data for the incident. Also provides input on cost estimates to the planning unit.
(1) Accountant

INCIDENT PREVENTION

Agencies will carry out incident prevention activities, including patch management, , training, etc. as part of its ongoing risk assessment and risk management activities. Periodic review of potential risks through a risk assessment and audit process will occur. As a result of this risk assessment and audit process, additional procedures and roles will be identified in the incident management plan.

2. Detection and Analysis

INCIDENT DETECTION

Incidents may be detected by DAS/BEST or by DAS/BEST's supported agencies. Once a security incident is identified it is classified and prioritized. Depending on the priority of the incident, the IT Security Division will determine if the agency needs support in its incident response. All incidents should be entered into the incident log at the time of classification and prioritization.

INCIDENT IDENTIFICATION

Incidents may be detected either by DAS/BEST or by DAS/BEST's supported agencies and trusted partners. Incident detection will in general occur as a report to the help desk or through ongoing system monitoring by the IT security Division. In some cases, other DAS/BEST Divisions or Agencies may identify a potential security incident.

When an agency identifies a potential security incident, the security incident should be reported by the security officer to the DAS/BEST IT Security Division as soon as possible.

INCIDENT CLASSIFICATIONS

All incidents are classified according to the following criteria. An incident may fit into more than one defined type. A 'security incident' can be defined as any security related event that has an actual or potential adverse effect on any computing resource or the data contained therein; or the violation of an explicit or implied security policy.

Incident Types:

Denial of Service: An incident by which authorized access to systems or data is prevented or impaired. Usually a denial of service (DoS) incident is a security event if the DoS is due to malicious intent. Not all events that prevent or hinder authorized access to systems or data are security incidents. The mechanical, electrical, or administrative failure of a system or access mechanism may not be a security incident.

Unauthorized Access: An incident where unauthorized access is attempted or gained to systems or data. This access can be logical or physical in nature. Unauthorized access is any access for which permission has not been granted. Such permissions would include connect, authenticate, read, write, create, delete, modify, etc. This unauthorized access can be by an individual or another system.

Inappropriate Usage: An incident by which acceptable use policies are violated. Acceptable use policies may include what types of data may be accessed or transmitted, how information may be accessed or transmitted, and where information may be received from or transmitted to.

Conclusion: Although references to many other incident types can be found in documentation, they seem to all fall in one of the three categories noted above. For example, malicious code such as a virus or trojan will be first recognized as a denial of service, unauthorized access, or inappropriate usage, depending on the payload of the malicious code. Using these three incident types, responses can be developed to cover any incident that might affect the enterprise.

References:

1. RFC 2350 “Expectations for Security Incident Response” http://www.ietf.org/rfc/rfc2350.txt
2. CERT incident Reporting Guidelines http://www.cert.org/tech_tips/incident_reporting.html#I.A
3. RFC 2196 “Site Security Handbook” http://www.ietf.org/rfc/rfc2196.txt?Number=2196
4. NIST Special Publication 800-61 “Computer Security Incident Handling Guide” http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf

INCIDENT SEVERITY

Once the incident is categorized it is prioritized according to its severity level. The appropriate response to an incident is dependant on the severity rating of the incident.

Method for Determining Severity:

By adding the scores from the following evaluation criteria, a severity rating is established:

1. Potential number of affected parties:
   How much productivity is impacted by this incident?
   1.1. Less than 1% of systems; less than 1% of workforce = 1
   1.2. More than 1%, but less than 10% of systems; more than 1% but less than 10% of workforce = 2
   1.3. More than 10% of systems; more than 10% of workforce = 3
2. Probability of widespread escalation:
   Does this incident have the potential to spread to as yet unaffected systems?
   2.1. Minimal = 1
   2.2. Moderate = 2
   2.3. High = 3
3. Commonality:
   Has this occurred in the past; is there experience in mitigating this particular incident?
   3.1. Commonly Seen = 1
   3.2. Occasionally happens = 2
   3.3. Rare = 3
4. Potential for damage or loss[1]
   How expensive is the incident expected to be, both in lost production and in mitigation costs.
   4.1. Minimal = 1
   4.2. Moderate = 2
   4.3. High = 3
5. Business impact[1]
   What is the expected negative impact on the overall health of the enterprise both in short and long term contexts?
   5.1. Minimal = 1
   5.2. Moderate = 2
   5.3. High = 3, Certain types of data, due to regulatory and/or legal definitions are always classified as 'High'. One example would be HIPAA covered Electronic Protected Health Information

This score can be used to determine the severity as follows:

Priority Guideline	Score	Initial Action	Containment Goal
Severity Level 1: Severe impact on	13-15	Immediately	ASAP

enterprise			
Severity Level 2: Loss of a major service	11-12	Immediately	<24 Hours
Severity Level 3: Some impact some portion of enterprise	8-10	Within 4 hours	<72 Hours
Severity Level 4: Minor impact on a a small portion of enterprise	5-7	Within 24 hours	<7 Days

(1. Reference: SANS Incident Handling and Intrusion detection)

INCIDENT ANALYSIS

All incidents of level 3 or higher should automatically involve the DAS/BEST IT Security Division. Level 4 incidents may be addressed by the agency without direct involvement of the IT Security Division. The IT Security Division coordinates incident analysis at a high level to understand what is occurring across the state and the work with the agency security officers to implement incident response actions ad required.

The Incident Response team uses resources through the State to conduct analysis. Tasks such as reviewing logs or monitoring intrusion detection systems can be assigned to distributed team members or handled by the central team. If handled at the local level, the results of these reviews are then shared with the centralized team members, who consolidate the data to determine patterns and trends across the organization and identify any additional work or follow-up actions to be passed back to the distributed team members for implementation.

Results of analysis should be archived in an incident folder for daily operations and for future reference by all team members.

3. Containment, Eradication and Recovery

INCIDENT RESPONSE SUPPORT AND COORDINATION

Once the incident has been categorized and an appropriate severity level has been identified, the process enters the phase of Containment, Eradication and Recovery.

Agency Incident Response team members, provide incident information to the DAS/BEST ITSecurity team. For example, once solutions are identified and distributed by the agency Incident Management team, team members communicate the appropriate information the to DAS/BEST ITSecrity team who will provide guidance and assistance on implementing recovery procedures for the reported activity to other supported agencies.

IT Security Division staff develop and document mitigation and recovery strategies to address the immediate threat for distribution to the rest of the agencies as necessary. This notification can be achieved through secure mailing list aliases, secure web intranet or extranet servers, or even via phone or fax. Timely information that is important for all organizational staff to receive can be distributed via internal employee mailing lists if necessary.

Response coordination is provided primarily by the agency Incident management team. The team members confirm that local administrators have implemented the appropriate actions and relay this information back to the agency Incident mangement team.

Containment, Eradication, and Recovery – Based on the results of recognition, the proper response procedure is implemented. Immediate steps are taken as appropriate to limit loss from the incident. Evidence is preserved. Impact of this containment to customers and the enterprise is communicated to those affected. A long term resolution of the incident is developed and implemented. This step may include policy alteration or development, system redesign, introduction of new systems or technologies, training, or other actions deemed necessary to permanently resolve an incident. As necessary, systems are restored and brought back online, data is restored, and appropriate parties are notified

FORM RESPONSE TEAM

The first step in creating and executing the incident response plan is activation of the IMT and response teams when necessary. Team members are assigned based upon the required rolls as listed in the preparation phase of incident response.

CREATE COMMUNICATION PLAN

A communication plan is created for each phase of containment, eradication and recovery identifying who within DAS/BEST and *your Agency* will be contacted once each phase is complete.

CONTAINMENT

Containment processes can include:

- Disconnect suspected subnet
- Terminate operation
- Observation and assessment
- Run full system backup
- Determine duration of termination
- Notify help desk
- Change the passwords on the compromised systems
- Vulnerability analysis to identify the root cause
- Encapsulation of incident
- Any action deemed necessary to mitigate the incident

Containment times vary according to the level of severity of the incident. Containment steps will be carried out in different order and concurrency depending on the nature of the incident.

ERADICATION AND RECOVERY

Eradication and recovery occurs concurrently and involves the following activities:

- Eradication actions for specific incident type
- Follow change management procedures
- Perform recovery procedures
- System verification
- Remove malicious code/virus
- Assess the impact on operating systems
- Harden the operating systems
- Remove dormant user ID’s
- Tighten access rights
- Shut down and restart systems/services for DoS
- Software/Hardware configuration changes
- Restoration from previous backup
- Re-installation.

RESUME OPERATION

Once eradication and recovery have been completed successfully, normal operations can resume. Appropriate agency and interagency communication will occur at this time.

4. Post Incident Review

The IT security Division focus' on analyzing patterns of activity across the enterprise. They support comprehensive tracking, recording, and dissemination of information to the enterprise. By consolidating the information collected, the team is better able to identify similar attacks, artifacts, exploits, trends and patterns. Potential new threats to the enterprise can also be identified. *Your Agency* will focus on patterns of activity within the LAN and agency applications. In this model, it is important that the team have expertise or familiarity with all platforms and operating systems used in the organization. If this does not exist within the centralized team component, then there must be mechanisms in place to collaborate with the distributed team members or other organizational experts who can provide the required knowledge.

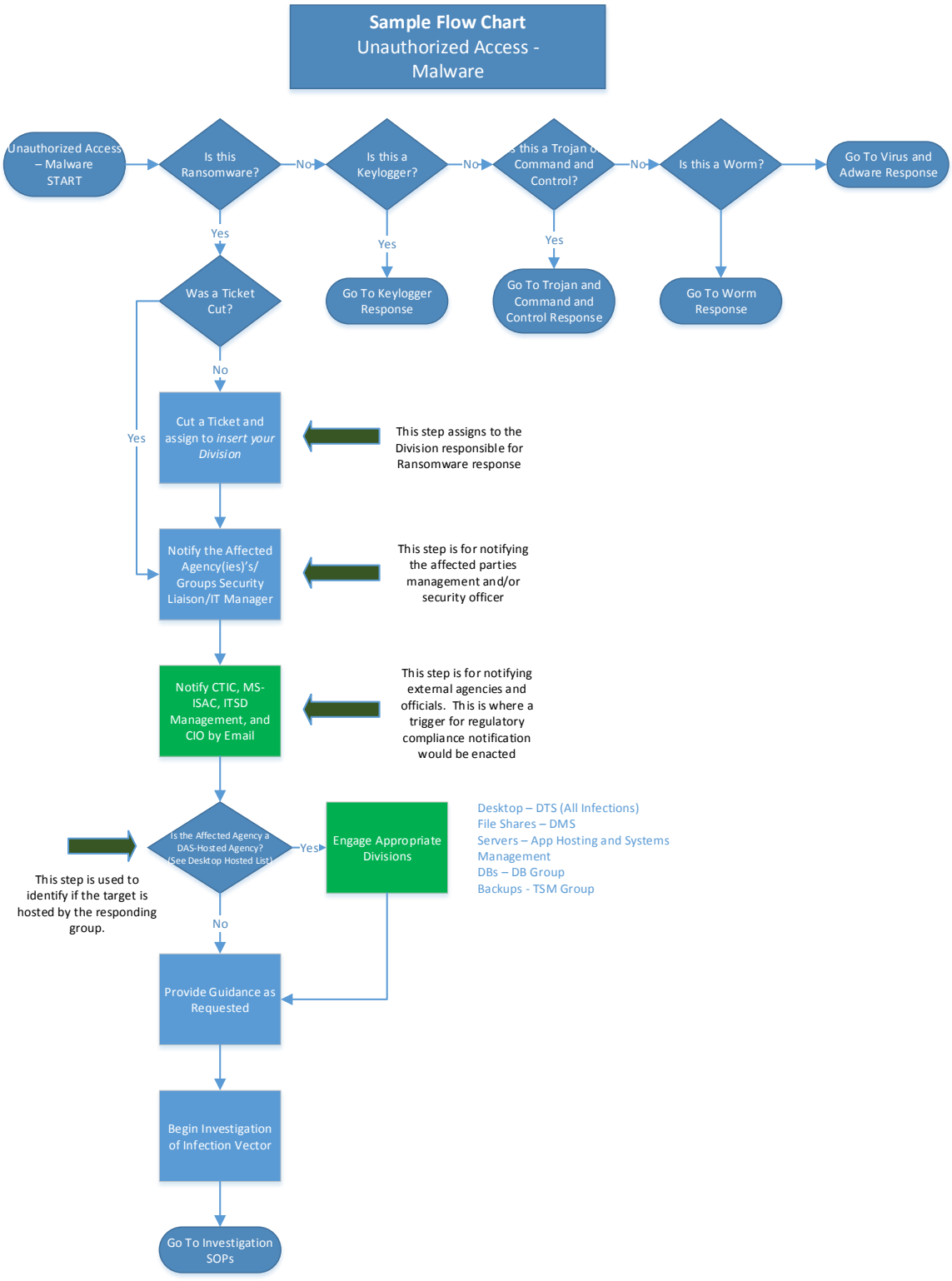
Based on the results of the analysis of any vulnerability or artifact information, the IT security Division coordinates the release of remediation, detection, and recovery steps throughout the enterprise as required.

Post Incident Activity – The IMT and response team(s) will attend a debriefing meeting and an After Action Report (AAR) of the incident from start to conclusion is developed which will include an improvement plan. Documentation of any permanent changes to systems as a result of the incident are generated. Incident data collected is analyzed to determine such things as the cost of the incident in money, time, etc. Evidence retention policies and procedures are implemented.

FOLLOW UP

Specific follow up activities include

- Monitor affected systems
- Update incident log
- Perform post-mortem
- Incident documentation
- Media-Handling
- Update incident response procedures


Sample Flow Chart
Unauthorized Access - Malware
Unauthorized Access – Malware START
Is this Ransomware?
No
Is this a Keylogger?
No
Is this a Trojan or Command and Control?
No
Is this a Worm?
Go To Virus and Adware Response
Yes
Was a Ticket Cut?
Yes
Go To Keylogger Response
Yes
Go To Trojan and Command and Control Response
Go To Worm Response
No
Yes
Cut a Ticket and assign to insert your Division
This step assigns to the Division responsible for Ransomware response
Notify the Affected Agency(ies)'s/ Groups Security Liaison/IT Manager
This step is for notifying the affected parties management and/or security officer
Notify CTIC, MS-ISAC, ITSD Management, and CIO by Email
This step is for notifying external agencies and officials. This is where a trigger for regulatory compliance notification would be enacted
Is the Affected Agency a DAS-Hosted Agency? (See Desktop Hosted List)
Yes
Engage Appropriate Divisions
Desktop – DTS (All Infections)
File Shares – DMS
Servers – App Hosting and Systems Management
DBs – DB Group
Backups - TSM Group
This step is used to identify if the target is hosted by the responding group.
No
Provide Guidance as Requested
Begin Investigation of Infection Vector
Go To Investigation SOPs