Please Note: the sample RFP attachment isn't confidential
The plan that is created by a local entity using the sample will be confidential

Cyber Incident Response Plan

DATE

Version 1.0

NOTE: The following Incident Response Plan is intended to provide an example of how a policy and plan can be written. It is not intended to cover all possible situations. Each agency must evaluate their unique circumstances and incorporate those into their plan. The plan is not intended to be a "fill in the blank" plan. If an agency chooses to simply fill in the blanks, the plan may not be sufficient to cover the agency's unique requirements during a security incident and could potentially cause the agency additional harm.

This document was created from existing cyber response plans that were in use at several Michigan counties. Names were removed and replaced with *Our Organization*.

Please share your plan and experiences with colleagues to help improve these tools.

Use this with the accompanying Incident Response Planning Companion to Sample IR Plan PowerPoint presentation to guide your organization's development of a cyber response plan.

Table of Contents

SUMMARY

The elements of a traditional Information Security effort continue to be important and useful. Two trends necessitate the establishment of a Cyber Incident Response Plan:

1) Information Technology is widespread throughout *Our Organization*; *Our Organization* relies heavily on Information Technology and cannot afford denial of service.
2) *Our Organization* IT systems and networks are at much higher risk to threats such as computer viruses, intrusions, and exposures.

The following examples of cyber security incidents are now commonplace:

- A ransomware attack renders a municipality's systems inoperable until systems can be restored from backups (if available) or ransom is paid.
- A computer virus is copied to a LAN server; within minutes hundreds of other computers are infected; recovery takes several people and several days.
- Backups infected with viruses result in re-infected systems, requiring more time and expense.
- Vulnerabilities in software are discovered that permit unauthorized entry; explicit instructions on how to exploit the vulnerability become quickly known.
- System intruders copy password files and distribute them throughout large networks.
- Break-ins through international networks require cooperation of different government agencies.
- Outbreaks of viruses or system penetrations appear in the press, causing embarrassment and possible loss of public confidence.

These situations can cause *Our Organization* to face unnecessary expense in productivity, significant damage to systems, and damage to our reputation. Clearly, the need now exists to take action prior to suffering the consequences of a serious IT security problem.

Our Organization CYBER INCIDENT RESPONSE PLAN

1.0 Introduction

1.1 Purpose of the Cyber Incident Response Plan

A Cyber Incident Response Plan is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of *Our Organization* Information System Resources. This adverse event may be malicious code attack, unauthorized access to *Our Organization* systems, unauthorized use of *Our Organization* services, denial of service attacks, general misuse of systems, and accidental loss or hoaxes.

1.2 General Purpose of the Cyber Incident Response Team

The purpose of *Our Organization*'s Cyber Incident Response Team is to:

- Protect *Our Organization*'s Information assets
- Provide a central organization to handle incidents
- Comply with requirements
- Prevent the use of *Our Organization*'s systems in attacks against other systems (which could cause us to incur legal liability)
- Minimize the potential for negative exposure.

1.3 Operational Objectives of the Cyber Incident Response Team

The objectives of *Our Organization*'s Cyber Incident Response Team are to:

- Limit immediate incident impact to customers and partners
- Recover from the incident
- Determine how the incident occurred
- Find out how to avoid further exploitation of the same vulnerability
- Avoid escalation and further incidents
- Assess the impact and damage in terms of financial impact, loss of image etc.
- Update policies and procedures as needed
- Determine who initiated the incident
- Document al information, events, and efforts to provide to law enforcement.

2.0 Incidents

2.1 Incident Categories

An incident will be categorized as one of four severity levels. These severity levels are based on the impact to *Our Organization* and can be expressed in terms of financial impact, impact to services and/or performance of our mission functions, impact to *Our Organization*'s image or impact to trust by *Our Organization*'s customers, etc. Table 1 provides a listing of the severity levels and a definition/description of each severity level.

Severity Level	Description
0 (Low)	Incident where the impact is minimal. Examples are e-mail SPAM, isolated Virus infections, etc.
1 (Medium)	Incident where the impact is significant. Examples are a delayed ability to provide services, meet *Our Organization*'s mission, delayed delivery of critical electronic mail or data transfers, etc.
2 (High)	Incident where the impact is severe. Examples are a disruption to the services, and/or performance of our mission functions. *Our Organization* proprietary of confidential information has been compromised, a virus or worm has become wide spread, and is affecting over 1% of employees, Pubic Safety systems are unavailable or *Our Organization* Executive management has been notified.
3 (Extreme)	Incident where the impact is catastrophic. Examples are a shutdown of all *Our Organization* network services. *Our Organization* proprietary or confidential information has been compromised and published on a public site. Public safety systems are unavailable. Executive management must make a public statement.

Table 1: Severity Levels

3.0 Responding to an incident

There are generally six stages of response:

1. Preparation—one of the most important facilities to a response plan is to know how to use it once it is in place. Knowing how to respond to an incident BEFORE it occurs can save valuable time and effort in the long run.
2. Identification—identify whether or not an incident has occurred. If one has occurred, the response team can take the appropriate actions.
3. Containment—involves limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.
4. Eradication—removing the cause of the incident can be a difficult process. It can involve virus removal, conviction of perpetrators, or dismissing employees.
5. Recovery—restoring a system to its normal business status is essential. Once a restore has been performed, it is also important to verify that the restore operation was successful and that the system is back to its normal condition.
6. Follow-up—some incidents require considerable time and effort. Often once the incident appears to be terminated there is little interest in devoting any more effort to the incident. Performing follow-up activity is, however, one of the most critical activities in the response procedure. This follow-up can support any efforts to

prosecute those who have broken the law. This includes changing any company policies that may need to be narrowed down or be changed altogether.

3.1 Organization

To adequately respond to an intrusion or incident, predetermined teams will participate depending on the incident characteristics. As the situation develops and the impact becomes more significant, the various teams will be called to contribute. Figure 1 depicts the Cyber Incident Response organization.

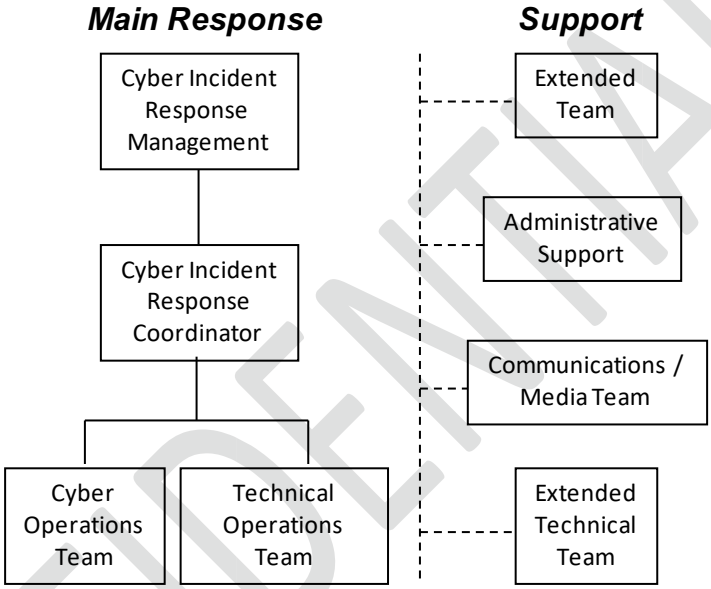


Figure 1: Cyber Incident Response Organization

Role	Responsibilities	Primary/Alternate(s)
Cyber Incident Response Management	Will have overall responsibility for directing activities in regard to the incident at Severity Level 2 and above. Will serve in advisory capacity for incidents at Severity Level 1.	
Cyber Incident Response Coordinator	Provides oversight to incident response. Requests resources as required to effectively contain and manage an incident response. Documents incident for purposes of law enforcement, lessons learned, and insurance.	
Cyber Operations Team / Technical Operations Team	Provide technical aspects of incident response.	
Communications / Media Team	Responsible for internal, external and media communications	
Extended Technical Team	Provides additional technical skill and capability to the Technical Operations team as required (ie. outside	

	vendor or agency)	
Admin Support	Provides requested administrative support.	
Extended Team	Provide additional visibility and support to incident response as required. Provide specific HR, legal, finance, etc. skills as required.	

Table 2: Roles and Responsibilities

3.2 Escalation Levels

	Main Response			Support			
Severity Level	**Technical Ops Team, Cyber Ops Team**	**Cyber Incident Response Coordinator**	**Cyber Incident Response Mgmt**	**Comms / Media Team**	**Extended Technical Team**	**Admin Support**	**Extended Team**
0	X						
1	X	X	X				
2	X	X	X	X	X		
3	X	X	X	X	X	X	X

Table 3: Severity Level Matrix

The escalation process will be invoked to involve appropriate resources as the incident has more impact (severity level increases). Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. Table 4 defines the escalation levels with the associated team involvement.

Escalation Level	Affected Team(s)	Description
0	• Technical Operations Team • Cyber Operations Team	Normal Operations. Engineering and cyber groups monitoring for alerts from various sources.
1	• Technical Operations Team • Cyber Operations Team • Cyber Incident Response Coordinator • Cyber Incident Response Management	*Our Organization* has become aware of a potential or actual threat. Determine defensive action to take. Message employees of required actions if necessary.
2	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Technical Operations Team • Cyber Operations Team • Extended Technical Team • Communications / Media Team	A threat has manifested itself. Determine course of action for containment and eradication. Message employees of required actions if necessary.
3	• Cyber Incident Response Management • Cyber Incident Response Coordinator • Extended Team	Threat is wide spread or impact is significant. Determine course of action for containment, mitigation and eradication.

	• Technical Operations Team • Cyber Operations Team • Extended Technical Team • Communications / Media Team • Administrative Support Team	Message employees. Prepare to take legal action. Prepare to make public statement.

Table 4: Escalation Levels

3.3 Escalation Considerations

Cyber Incident Response Management will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How wide spread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact to *Our Organization*?
- Will this affect *Our Organization*'s image negatively?

3.4 The Cyber Incident Response Process

The Cyber Incident Response Process is an escalation process where as the impact of the incident becomes more significant or wide spread, the escalation level increases bringing more resources to bear on the problem. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if and when they are needed.

Appendix B depicts the overall process, while paragraph 3.5 outlines the roles and responsibilities of individual teams. Team membership is contained in Appendix A.

In cases where Criminal Justice Information (CJI) is involved, *Our Organization* will contact the MSP ISO and fill out and submit the CJIS 016 document if the incident significantly endangers the security or integrity of CJIS data. (reference CJIS Security Policy section 5.3 and the Michigan Addendum)

3.5 Cyber Incident Response Team Roles and Responsibilities

3.5.1 Escalation Level 0

ii. Technical Operations Team / Cyber Operations Team

1. Monitors all known sources for alerts or notification of a threat.
2. Take appropriate defensive actions per known issues.
3. Escalate to Cyber Incident Coordinator if determined that Severity level may be greater than Level 0.

iii. Cyber Incident Coordinator

1. Escalate Cyber Incident Response to Level 1 if information is received that the incident is likely greater than Level 0.

3.5.2 Escalation Level 1

Our Organization has become aware of a potential or actual threat.

i. Technical Operations Team / Cyber Operations Team
   1. Determine initial defensive action required.
   2. Notify the Cyber Incident Coordinator.
   3. Determine appropriate course of action.

ii. Cyber Incident Coordinator
   1. Receive and track all reported potential threats.
   2. Start a chronological log of events.
   3. Escalate Cyber Incident Response to Level 2 if a report is received indicating that the threat has manifested itself.
   4. Determine relevant membership of the Technical Operations and Extended Technical teams.
   5. Alert other IT personnel and applicable support organizations of the potential threat and any defensive action required.
   6. Alert Cyber Incident Response Management of the potential threat. Seek advisory inputs as appropriate.
   7. Alert Communications Team

iii. Cyber Incident Response Management
   1. Provide advisory inputs as appropriate.

iv. Communications Team
   1. If employee action required, message employees of required action.

3.5.3 Escalation Level 2

The threat has manifested itself.

i. Cyber Incident Coordinator
   1. Notify Cyber Incident Response Management of the manifestation of the threat,
   2. Receive status from the Technical Operations Team and report to Cyber Incident Response Management,
   3. Start a chronological log of events.

      Note: The chronological log will be used to support possible follow on legal action as determined by *Our Organization*'s General Counsel and Executive Directors.

ii. Technical Operations Team

1. Determine best course of action for immediate containment of the incident,
2. Notify the Technical Support Team of any action that is required,
3. Report actions taken and status to the Cyber Incident Response Coordinator.

iv. Cyber Incident Response Management
1. Assume responsibility for directing activities in regard to the incident,
2. Coordinate discussion and analysis to determine best course of resolution,
3. Alert the Administrative Support Team of the incident,
4. Alert the Extended Team as applicable,
5. Determine whether Escalation Level 2 is appropriate or escalate to level 3,
6. Determine when the risk has been mitigated to an acceptable level.

v. Extended Technical Team
1. Take whatever action as determined by the Technical Operations Team
2. Report actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log

vi. Communications Team
1. Message *Our Organization* employee population informing them of the incident if deemed appropriate by Cyber Incident Response Management,
2. Message *Our Organization* employee population of any action they need to take as determined by the Technical Operations Team and directed by Cyber Incident Response Management.

3.5.4 Escalation Level 3

The threat has become widespread or has become a high severity level.

i. Cyber Incident Response Management
1. Direct the response team to:
   a. Set up communications channels between all teams.
   b. Assume occupancy of the command center if exists.
   c. Open a teleconference bridge for ongoing communications and team interaction or Initialize an incident voice mail box where status messages can be placed to keep *Our Organization* personnel statused
2. Organize scheduled team meetings. Define specific status update schedule.
3. Authorize initial communications to employees and executives. Use

Smart Message system as desired.
4. Alert the Extended Team of the incident notifying them of the Severity Level.
5. Status Executive Management as appropriate.
6. Determine when the risk has been mitigated to an acceptable level.

ii. Extended Team
1. Contact local authorities if deemed appropriate,
2. If local authorities are called in, make arrangements for them to be allowed into the building,
3. Ensure that all needed information is being collected to support legal action or financial restitution.

iii. Cyber Incident Response Coordinator
1. Continue maintaining the Chronological Log of Event,
2. Continue to manage incident response per direction of Cyber Incident Response Management.

iv. Communication Team
1. Message *Our Organization* population and external media as directed by Cyber Incident Response Management.

vii. Technical Operations Team
1. Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat,
2. Continue reporting status to the Cyber Incident Response Coordinator for the chronological log of events,
3. Monitor effectiveness of actions taken and modify them as necessary,
4. Provide status to Cyber Incident Response Coordinator and Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat.

viii. Extended Technical Team
1. Continue actions to eradicate the threat as directed by Cyber Incident
2. Response Coordinate and Cyber Incident Response Management and the Technical Operations team.
3. Continue to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

ix. Administrative Support Team
1. Provide administrative support to all persons and teams involved in incident

3.6 Special Circumstances

i. Email Communications are compromised or otherwise unavailable
   1. There could be a cyber security incident that compromises the ability to communicate via email. In this case, the backup will be communications via desk phone or cell phone. A phone directory of key persons on the response teams is given in Appendix A.

ii. Personal Identification Information / HIPAA or other Confidential Information is leaked via Internal Source
   1. The process defined above can also apply to the circumstance where information is leaked via an internal source by accident or maliciously. In this case, the steps in the response process would be very similar to the above process but would also include early determination of the type and quantity of data leaked, the source of the leak and the potential impact of the leak to the County or to the public at large.

4.0 Post incident

4.1 Cyber Incident Coordinator and Response Management

1. Report on:
   a) Estimate of damage/impact,
   b) Action taken during the incident (not technical detail),
   c) Follow on efforts needed to eliminate or mitigate the vulnerability,
   d) Policies or procedures that require updating,
   e) Efforts taken to minimize liabilities or negative exposure.
   f) Provide the chronological log and any system audit logs requested by the Extended Team,
   g) Document lessons learned and modify the Cyber Incident Response Plan accordingly.

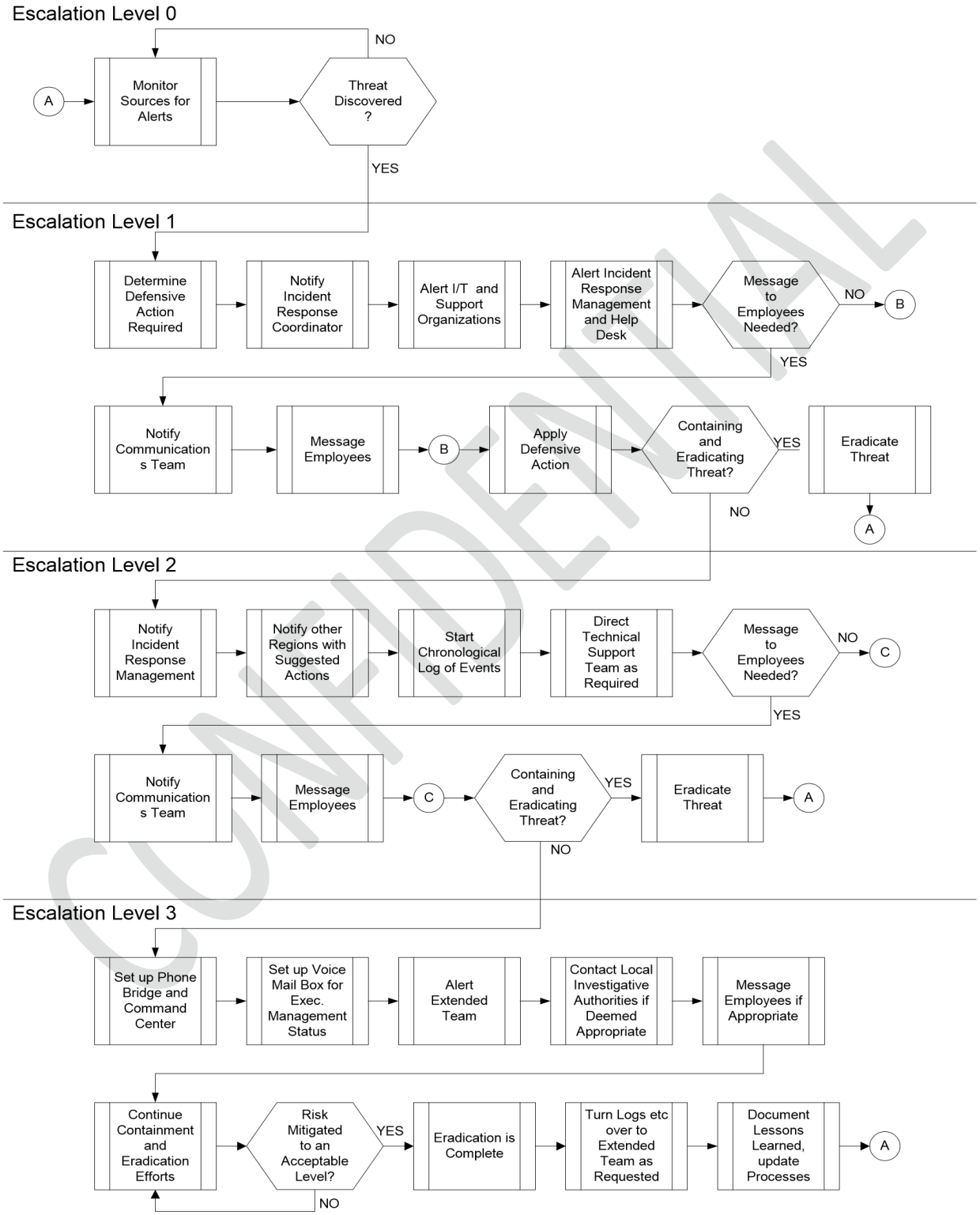
4.2 Extended Team

1. Legal and Finance work with the local authorities as appropriate in the case that the incident was from an external source,
2. HR and IT work with *Our Organization* management to determine disciplinary action in the case that the incident was from an internal source.
3. Homeland Security leveraged to support as necessary.

Appendix A. Cyber Incident Response Team

Team	Leadership / Members	Contact Information
Cyber Incident Response Management	CISO	
	Co-CISO	
Cyber Incident Response Coordinator	Security Operations	
Administrative Support Team	Administration	
	General	
Technical Operations Team	Infrastructure	
	Technical support	
	Applications	
Cyber Operations Team	Operations	
	Operations - Assigned technician	
Extended Technical Team	External Infrastructure and Applications personnel as needed	
Communications / Media Team	Communications	
Extended Team	Homeland Security	
	HHS (HIPAA)	
	Legal	
	HR	
	Finance	
	Sheriff	
	Treasurer	
	Clerk	
	Register of Deeds	
	Prosecutor	
Executive Management		

Appendix B: Incident Response Diagram and Examples



Threat Example 1: Server Software Vulnerability

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. A critical *zero-day* (discovered by its use in the wild) software vulnerability affects the operating system on a widely-used production server. The vulnerability allows for an unauthorized privilege escalation and therefore unauthorized data access. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the defensive action required is a patch of the operating system from the vendor.
2. Notifies the Incident Coordinator of the vulnerability.
3. Determines that employee action is not required.

INCIDENT COORDINATOR

1. Receives and tracks the status of the vulnerability.
2. Does not escalate the threat to Level 2, since the vulnerability has not manifested itself.
3. Determines relevant membership of the Technical Operations and Extended Technical team.
4. Alerts IT organizations and applicable support organizations of the vulnerability. The action required to contain the threat is a patch of the operating system from the vendor. This patch must be applied and tested on a development server before being propagated to the production server.
5. Alerts Cyber Incident Response Management of the vulnerability.
6. Alerts the Communications Team.

COMMUNICATIONS TEAM

1. Since employee action is not required, no message to employees is necessary.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

    a. Estimate of the impact of addressing the vulnerability and the potential cost of not doing so,

    b. Action taken during the vulnerability's assessment,

    c. Follow on efforts needed to eliminate or mitigate the vulnerability,

    d. Policies or procedures that may require updating (if applicable), and

    e. Efforts taken to minimize the liabilities of negative exposure of the vulnerability.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Not needed, because there was no manifestation of the vulnerability.

Threat Example 2: Ongoing Phishing Attack on Employees

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. Emails have been circulating to *Our Organization* employees that link users to a fraudulent website designed specifically to gather user authentication credentials from *Our Organization* employees. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the initial defensive action required is to notify employees of the phishing scam and educate them on avoiding these types of attacks.
2. Notifies Incident Coordinator.
3. Determines that employee action will be required, notifies Service Center.

CYBER INCIDENT COORDINATOR

1. Receives and tracks the phishing attack.
2. Escalates the threat to Level 2, since it has manifested itself.
3. Determines relevant membership of the Technical Operations and Extended Technical Team.
4. Alerts IT organizations and applicable support organizations of the phishing. The organizations begin modifying internal firewalls to block the offending website as well as initiating a system-wide password reset.
5. Alerts Cyber Incident Response Management of the phishing threat.
6. Alerts the Communications Team.

COMMUNICATIONS TEAM

1. A message is composed to all employees and sent system-wide. Additionally, all departmental managers are alerted to the phishing scam and asked to notify all employees in person immediately.

Escalation Level 2

CYBER INCIDENT COORDINATOR

1. Notifies Cyber Incident Response Management of the phishing attack.

2. Alerts the Cyber Incident Response Support Team of the phishing attack.

3. Alerts the Extended Team.

4. Receives status from the Technical Operations Team regarding the status of employee education. Reports the status to the Cyber Incident Response Management.

5. Starts a chronological log of the events, including logs of emails and, if possible, logs of users accessing the offending website.

TECHNICAL OPERATIONS TEAM

1. Determines that the best course of action for containing the attack is educating all employees about the attack and blocking any further emails from arriving on mail servers. Additionally, concludes that blocking the fraudulent website from being accessed internally. Finally, decides that a system-wide user password reset is necessary, since email is accessible from outside of *Our Organization*'s network and merely blocking the offending site will not be sufficient and the emails have been circulating for an unknown amount of time to only select employees.

2. Notifies the Extended Technical Team team of the above actions that are required.

3. Reports actions taken and status to the Cyber Incident Response Coordinator.

CYBER INCIDENT RESPONSE MANAGEMENT

1. Assumes responsibility for directing activities in regard to the phishing attack.

2. Determines that the attack does not need to be escalated to Level 3.

3. Determines when the risk has been mitigated to an acceptable level.

EXTENDED TECHNICAL TEAM

1. Takes the actions required by the Technical Operations Team.

2. Reports the actions taken, the number of personnel involved etc. to Cyber Incident Coordinator for the chronological log.

COMMUNICATIONS TEAM

1. Carries out the education of *Our Organization* employees by informing them of the incident and making sure everyone is aware of the scam as deemed appropriate by Cyber Incident Response Management.

2. Messages the *Our Organization* employees about the system-wide password reset, and how the employees must go about regaining access to their user accounts as determined by the Technical assessment team and directed by Cyber Incident Response Management.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

    a. Estimate of the impact of addressing the phishing attack and the potential cost of not doing so,

    b. Action taken during the attack's assessment,

    c. Follow on efforts needed to eliminate or mitigate the vulnerability presented by the phishing attack,

    d. Policies or procedures that may require updating, such as password change rules and procedures, and

    e. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Legal works with the authorities to present any information relating to the phishing party.

2. No disciplinary action will need to be taken.

3. Executive Management Team (EMT) leveraged to communicate to employees about the threat of phishing attacks and to be vigilant.

Threat Example 3: Stolen Asset, Leaked Confidential Information

Escalation Level 0

TECHNICAL OPERATIONS TEAM

1. An *Our Organization* employee has his or her laptop stolen, which contains unencrypted confidential personal information of *Our Organization* residents, including names, addresses, Social Security numbers, etc. The information has been found and posted on the public Internet. The threat is escalated to Level 1.

Escalation Level 1

TECHNICAL OPERATIONS TEAM

1. Determines that the attack has already taken place and that there is no initial technical defense possible in this circumstance. However, an internal data security practices audit is necessary to keep a data leak from happening again.

2. Notifies the Cyber Incident Coordinator.

3. Determines that employee action required to secure confidential data in the future through education. Contacts Service Center to arrange for instructions.

CYBER INCIDENT COORDINATOR

1. Receives and tracks the stolen data event.

2. Escalates to Level 2, because the threat has manifested itself.

3. Determines relevant membership of the Technical Operations and Extended Technical teams.

4. Alerts IT organizations and applicable support organizations of the situation. Defensive action that must be taken involves an audit of information security practices internally to ensure further data breaches do not occur.

5. Alert Cyber Incident Response Management of the data leak.

6. Alert the Communications team.

COMMUNICATIONS TEAM

1. Employee action is going to be required for the internal information security practices audit. The Communications Team notifies employees of

the data breach and the actions that are going to be taken to prevent such a leak in the future.

Escalation Level 2

CYBER INCIDENT COORDINATOR

1. Notifies Cyber Incident Response Management of the data leak.
2. Alerts the Cyber Incident Response Support Team of the data leak.
3. Alerts the Extended Team.
4. Receives status of the information security audit from the Technical Assessment Team and reports to Cyber Incident Response Management.
5. Starts a chronological log of events from the origin of the data to determine how the data ended up in a situation where it could be leaked. The chronological log will be used to support possible follow on legal action as determined by *Our Organization*'s General Counsel and Executive Directors.

TECHNICAL OPERATIONS TEAM

1. Determines that containment of the incident is going to be legal in nature, but that information security practices will need to be overhauled.
2. Notifies Extended Technical Team of the plan to audit and augment data security practices internally, including any technical measures that will need to be put into place to that end.
3. Reports actions taken and status to the Cyber Incident Response Coordinator.

CYBER INCIDENT RESPONSE MANAGEMENT

1. Assumes responsibility for directing activities in regard to the incident.
2. Determines that escalation Level 2 is not sufficient and escalates the incident to Level 3.
3. Determines when the risk has been mitigated to an acceptable level.

EXTENDED TECHNICAL TEAM

1. Takes action to begin comprehensive information security practices audit internally, as determined by the Technical Operations Team.
2. Reports actions taken, number of personnel involved etc. to Incident Coordinator for the chronological log.

COMMUNICATIONS TEAM

1. Messages *Our Organization* employee population informing them of the information leak and the ensuing legal action, as deemed appropriate by Cyber Incident Response Management.

2. Messages *Our Organization* employee population of the forthcoming comprehensive information security practices audit and the organization-wide practices that will be augmented as determined by the Technical Operations team and directed by Cyber Incident Response Management.

Escalation Level 3

CYBER INCIDENT RESPONSE MANAGEMENT

1. Directs the Cyber Incident Response Support team to:

    a. Set up communications between all Cyber Incident Response Team Managers, and the Extended Support Team in the field,

    b. Assume occupancy of the command center, and

    c. Initialize an incident voice mail box where status messages can be placed to keep *Our Organization* personnel statused.

2. Alerts the Extended Team of the incident notifying them of the Severity Level.

3. Determines when the risk has been mitigated to an acceptable level after the comprehensive information security data protection audit and overhaul.

4. Statuses Executive Management as appropriate.

EXTENDED TEAM

1. Contacts local, state, and federal authorities.

2. Makes arrangements for authorities to be allowed into the command center.

3. Ensures that all needed information is being collected to support legal action against the leaker and financial restitution for those affected by the breach of their personal information by *Our Organization* personnel.

CYBER INCIDENT RESPONSE COORDINATOR

1. Continues maintaining the Chronological Log of the event.

2. Posts numbered status messages in the incident voice mail box for statusing *Our Organization* Executive Management Team (if applicable).

COMMUNICATION TEAM

1. Messages *Our Organization* population as directed by Cyber Incident Response Management regarding the status of the information security data practices audit and any forthcoming changes to be made to policy.

TECHNICAL OPERATIONS TEAM

1. Continues to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat of further data being lost in any way, both internally and externally.

2. Continues reporting status to the Cyber Incident Response Coordinator for the chronological log of events.

3. Monitors effectiveness of the information security practices audit and subsequent changes and modifies them as necessary.

4. Statuses Cyber Incident Response Management on effectiveness of actions taken and progress in eliminating the threat of further information leakage.

EXTENDED SUPPORT TEAM

1. Continues the information security practices audit and changes to eradicate the further threat of data leaks as directed by Cyber Incident Response Management and the Technical Operations team.

2. Continues to report actions taken, number of personnel etc. to the Cyber Incident Response Coordinator for the chronological log.

Post Incident

CYBER INCIDENT RESPONSE MANAGEMENT

1. Prepare a report for *Our Organization* Executive Management to include:

    a. Estimate of the impact of addressing the data leak and the potential cost of not doing so,

    b. Action taken during the comprehensive information security practices audit and assessment,

    c. Follow on efforts needed to eliminate or mitigate any and all vulnerabilities that exist in terms of confidential data security,

d. Policies or procedures that may require updating to ensure strict oversight of sensitive data within *Our Organization*,

e. Efforts taken to minimize the liabilities of negative exposure of the attack.

2. Provides the chronological log and any system audit logs requested by the Extended Team.

3. Documents any lessons learned and modifies the Cyber Incident Response Plan accordingly.

EXTENDED TEAM

1. Legal works with the authorities to present any information relating to the leaking party that may lead to prosecution.

2. Human Resources and Information Services work with *Our Organization* management to determine disciplinary action for the negligent employee.

3. Executive Management Team leveraged to communicate to employees about the seriousness of keeping data safe and the costs of not doing so, as exemplified in this case.

Appendix C: ACIS Security Incidents Reporting Template*

Incident Detector's Information				
Date/Time of Report				
First Name				
Last Name				
Department/Division				
Title/Position				
Work Email Address				
Contact Phone Numbers	*Work*	*Mobile*	*Pager*	*Other*

Reported Incident Information	
Incident Location	
Incident Point of Contact (if different than above)	
Priority	*Level 1 / Level 2 / Level 3*
Data Breach?	*Yes / No*
Breach Category	
Incident Type	
US-CERT Category	*DoS / Malicious Code / Probes and Scans / Unauthorized Access / Other*
US-CERT Number	
Description	
Additional Support Action Requested	
Method Detected	*IDS/Log Review/ A/V Systems/ User Notification/ Other*
Configuration Item(s) Affected	
Department/ Division Impact	
Information Sharing	*Entities with which ACIS can share incident data*
System for Sharing	
Status	*Ongoing/ Resolved/ Etc.*

Attacking Computer(s) Information				
IP Address / Range	Host Name	Operating System	Ports Targeted	System Purpose

Victims Computer(s) Information				
IP Address / Range	Host Name	Operating System	Ports Targeted	System Purpose

Action Plan	
Action Description	
Requestor	
Assignee	
Time Frame	

Status	
Conclusion / Summary	
Entities Notified	
Resolution	*Include whether lost materials recovered as part of the solution*

CJIS Reporting Template

Other?
