The Utility Manager's Handy Reference Guide to Cyber Security

National Preparedness Leadership Initiative
Harvard University
October 2015

THE UTILITY MANAGER'S

HANDY REFERENCE GUIDE

TO

CYBER SECURITY

Developed by the students of Team Cyber, Cohort 13
fulfilling the requirements for executive training
during Harvard University's
National Preparedness Leadership Initiative

Brian D. Kelly
California Air National Guard

Mary T. Landers
Bay Area UASI

Steven R. Luczynski
Office of the Secretary of Defense

Annette L. Totten
National Counterterrorism Center

Thomas R. Welch
Bain Capital, LLC

Eric J. McNulty
Faculty Advisor

October 2015

ACKNOWLEDGEMENTS

Team Cyber would like to acknowledge the people who assisted us as we worked on this project:

- Our families and supervisors for their time and patience
- Our NPLI Faculty Advisor- Eric McNulty
- Drs. Leonard Marcus and Barry Dorn and all Cohort 13 Faculty Members

Mr. Mason Feldman, Emergency Services Assistant, Bay Area UASI

Mr. Brendan Fitzpatrick, Technical Manager, CERT Cyber Risk and Resilience Management, Carnegie Mellon Software Engineering Institute

Mr. Walter Grudzinski, Director, Information Security and Business Continuity, Vectren Corporation

Mr. Jarod Hysinger, Student Intern, Bay Area Urban Areas Security Initiative

CAPT John Kliem, PE, US Navy Deputy Director Renewable Energy Program Office

Mr. James Linn, Managing Director, Information Technology, American Gas Association

Ms. Elizabeth McCracken, Lead Cyber Analyst, Northern California Regional Intelligence Center

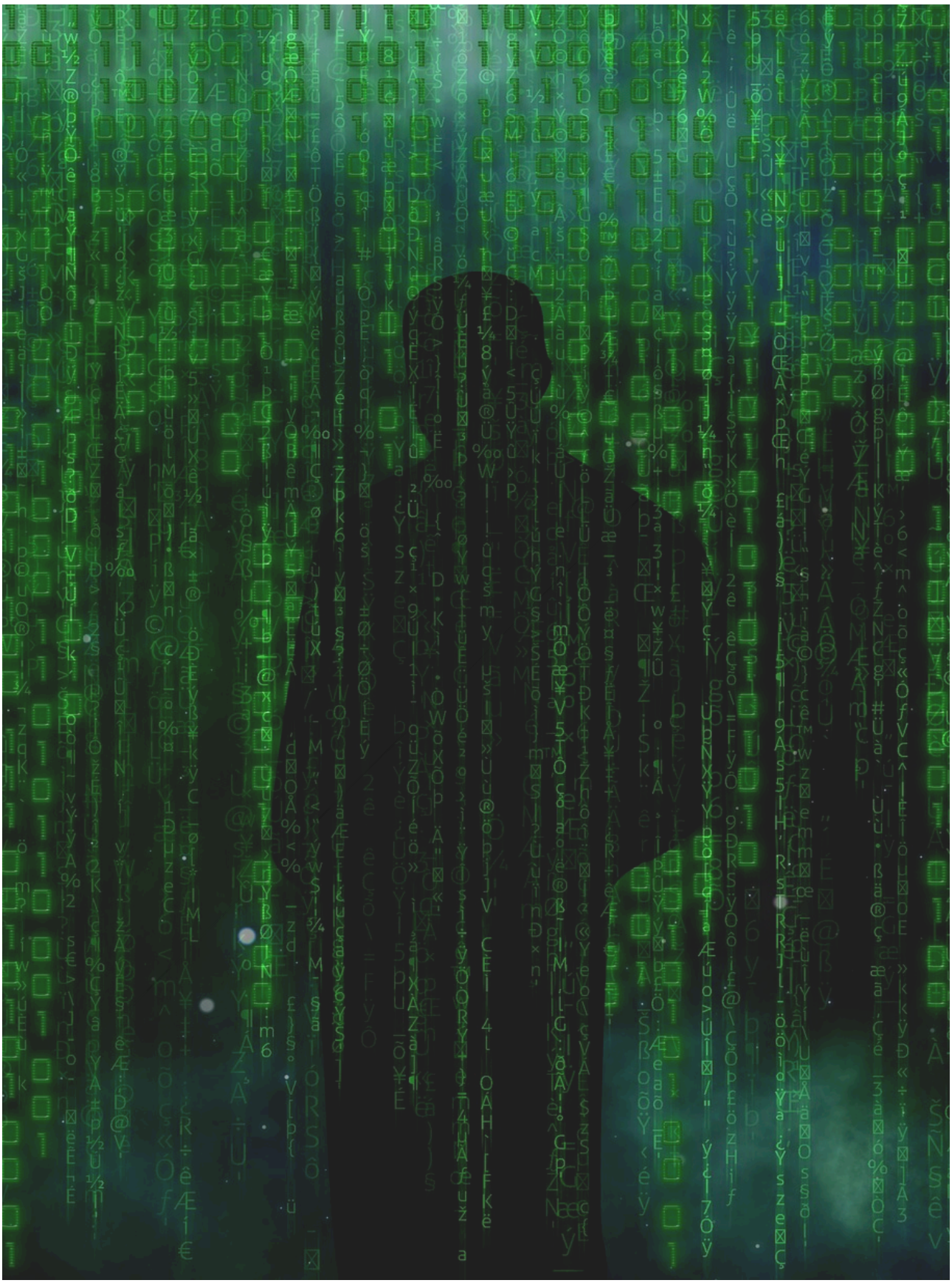
Mr. Deron McElroy, National Preparedness and Protection Division, Cyber Security Advisor for Region IX, U.S. Department of Homeland Security

Mr. James Sample, Executive Director, Ernst and Young, Americas Advisory Services

Mr. Chris Sawall, Director, Cyber Threat and Intelligence, Monsanto Information Security Office

Ms. Lisa Young, Senior Engineer, CERT Cyber Resilience Center, Carnegie Mellon Software Engineering Institute

TABLE OF CONTENTS



I. Introduction

Our nation relies on the essential services supplied by critical infrastructure such as utilities, which provide electricity, natural gas, and water vital to everyday life. While the largest utility companies may serve millions of customers in major metropolitan areas, smaller companies are an important component of this critical infrastructure. In fact, small companies, servicing cities and towns with populations under 10,000, make up 70% of our nation's critical infrastructure. Regardless of the size of the utility company, however, all face similar concerns regarding cyber security.

In today's cyber-enabled operating environment, utility companies have become increasingly vulnerable to malicious cyber activity. The reliance on computer networks for a company's operations requires that those networks be secured; but cyber security is a particularly complex responsibility. An incredible variety of resources are available to create and maintain an individualized cyber security program. These resources come from the federal and state, local, tribal, and territorial (SLTT) levels. Private industry also provides numerous resources. Even so, money and personnel to solve these problems are limited. Most importantly, companies face the threat of malicious cyber actors daily but the time available for managers and personnel to address these threats is limited. Furthermore, no matter the level of preparedness, if a cyber- attack were to occur today, an immediate response is necessary to ensure that the company stays in operation and quickly recovers. As a manager in one of those smaller utility companies, when time is of the essence, where do you start? What exactly are all those resources? And, to steal a line from a movie about other problem solvers, "Who ya gonna call"?

This guide will help you answer those questions, address concerns, and assist you in fulfilling your responsibilities. Beginning with a summary of cyber threats, to some of the industries comprising the nation's critical infrastructure, the guide will follow with a framework (using the term "Meta Leadership) for thinking about personal skills managers can utilize to solve complex problems under difficult circumstances. Next, the application of concepts to address your cyber security concerns are presented in detail. The particulars for how and when to use this guide are also included. Finally, the bulk of this guide contains best practices and resources from the federal and SLTT levels to help you begin creating your new, or improve your existing, cyber security program. In several instances, this guide denotes resources that only exist in the state of California. While limited to California, these are only examples of what your state may have available to help you overcome these issues. In the same manner, various examples of private company capabilities have been added in some volumes to illustrate additional resources that may be useful to your efforts. Inclusion of a company is not an endorsement of their services.

OF NOTE: Executive students who understand the complex problem you are facing created this guide; they are NOT cyber security experts. We wrote this guide for you to simplify the complexities of cyber security.

II. Cyber Threats to Critical Infrastructure

> "Overall, the unclassified information and communication technology (ICT) networks that support US Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure…we foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security."
>
> James Clapper, Director of National Intelligence,
> Congressional Testimony, September 2015[1]

As noted in the introduction, government and private sector operations are growing increasingly dependent on cyber-enabled operating environments. The Intelligence Community recognizes the vulnerabilities of all types of ICT networks, including those in the commercial sector. More telling, is the threat Director of National Intelligence (DNI) James Clapper presents as stemming from "low-to-moderate level cyber attacks." There should be little doubt in your mind about the importance of cyber security to even small utility companies.

Previously, you may have only focused on defending your computer networks from criminals. Now you should also consider providing cyber security sufficient to counter politically motivated cyber attacks since, "foreign actors are reconnoitering and developing access to US critical infrastructure systems, which might be quickly exploited for disruption if an adversary's intent became hostile."[2] Today you face a range of cyber threat actors from nation states (e.g. Russia, China or Iran), ideologically motivated hacktivists or extremists (e.g. Anonymous or ISIL), to profit-and motivated criminals.[3] DNI Clapper notably reported, "Russian cyber actors are developing means to remotely access industrial control systems (ICS) used to manage critical infrastructures." This is in addition to Russian efforts to compromise product supply chains of Industrial Control System (ICS) vendors allowing further exploitation of customers who purchase this equipment.[4]

Another way to view these sophisticated threats is through the standard cyber security model of Confidentiality, Integrity, and Availability. Typically, we defend against cyber espionage to ensure the confidentiality of our information or prevent denial-of-service and data-deletion attacks to ensure its availability. Increasingly, we must also defend against "cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e., accuracy and reliability) instead of deleting it or disrupting access to it."[5] In terms of your ICS and Supervisory Control and Data Acquisition (SCADA) systems, you may see these same thoughts expressed towards Process Control as Operability, Observability, and Controllability.[6] No matter which perspective you are dealing with, your leadership's decision-making

---

[1] Statement for the Record for the House Permanent Select Committee on Intelligence, *Worldwide Cyber Threats*, James R. Clapper, Director of National Intelligence, September 10, 2015.
[2] Ibid.
[3] Ibid.
[4] Ibid.
[5] Ibid.
[6] White paper, *Rocking the pocket book: Hacking chemical plans for competition and extortion*, Marina Krotofil and Jason Larsen, Hamburg University of Technology, August 2015.

capabilities will be severely impaired if they cannot trust the information they receive in order to make decisions about your company's operations.

Due to the diverse methods available to malicious cyber actors, eliminating cyber threats cannot be expected, but management of the risks they pose can be. This risk must now include the threats presented above. While important to the nation's critical infrastructure, implementing cyber security efforts of sufficient sophistication to counter threats of this type is an expensive, and difficult, business proposition.

III. Managers and Leadership Skills

Introducing Meta-Leadership

Successful organizations possess a number of key elements, including visionary leadership, innovative activities, and transparency at all levels. Another, perhaps even more important element, is a culture of trust. "Organizations with high levels of trust have more productive workforces, better employee morale and lower employee turnover. They also perform better financially than their industry peers."[7] So, why is a culture of trust important to your organization and to you in particular?

As a middle manager, you likely oversee a diverse array of departments that are responsible for multiple aspects of your company's operation. Chances are you may not be well versed in all the technical aspects of each department. In the area of information technologies, for example, you probably rely on your IT personnel to maintain the company's computer networks and execute the cyber security program without knowing every detail. Further, since your position is below the senior executive level, you must also rely on your leaders to provide the resources needed to accomplish your job. And yet, during a crisis, you are the one your subordinates look to for direction and the senior executives look to for answers. Understanding where you fit in both situations and the outcomes you can affect is crucial to the success of your company's operations. This is where a culture of trust becomes most important.

Normally, managers follow leadership patterns that include using their authority as defined by their formal role within the organization. However, during a complex situation or crisis, decision-making, control, and actions may be required that go beyond established roles and responsibilities. Meta-Leadership is a framework for thinking about these activities as they exceed established roles and responsibilities to seek creative solutions to problems.

The ML framework is a product of extensive and in depth research into the underlying reasons for the outcomes of extraordinarily difficult scenarios, such as the 2010 *Deep Water Horizon* oil spill in the Gulf of Mexico and the 2013 Boston Marathon bombing. It defines the various dimensions of Meta-Leadership and provides tools and techniques for the development of these leadership skills. Once learned, Meta-Leadership skills create confidence at all levels of an organization and help managers and other leaders face challenges that may arise.

As illustrated in Figure 1, the Dimensions of Meta-Leadership involve you as the manager and how you relate to others, both internally and outside your organization. The dimensions described below are broken down into three areas: the person, the situation, and connectivity.

---

[7] White paper, *How to Build Trust in an Organization*, Chris Hitch, PhD, UNC Kenan-Flagler Business School, 2012

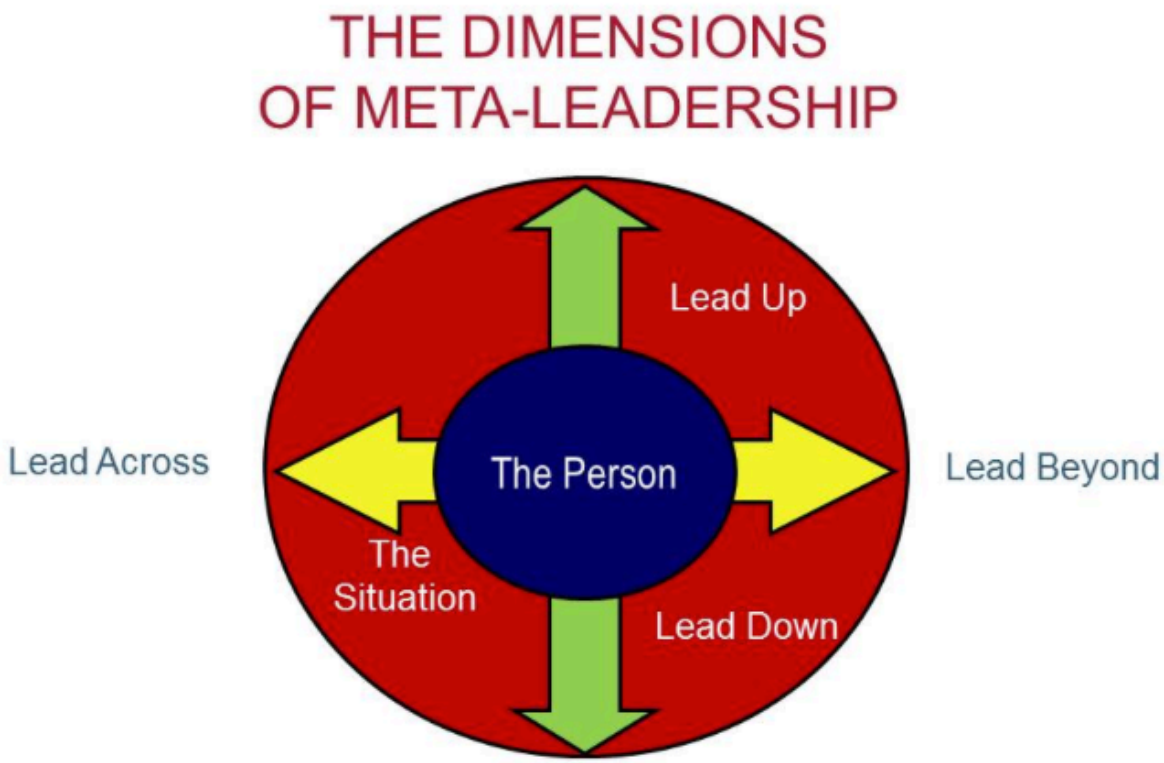


Figure 1. The Dimensions of Meta-Leadership[8]

The Person

A Meta-Leader is a person who has developed high levels self-awareness, self-knowledge, and self-regulation. They have an understanding of the impact of their personality and have developed ways to build trust between disparate groups both within and outside their organization. Meta-Leaders have developed an aura of calmness around them that subtly leads others to mimic that behavior. By building their capacity to confront fear, they lead themselves and others to higher levels of thinking and functioning.

The Situation

When a crisis situation occurs, decisions may have to be made with incomplete information. Frequently, the situation also requires collaboration with stakeholders who are not within a manager's area of control. Meta-Leaders must correctly map the situation to determine what is happening, identify the appropriate stakeholders, predict the next likely action, and create and foster a positive atmosphere in which problems can be successfully resolved.

[8] Marcus, Leonard J., Henderson, Joseph & Dorn, Barry C., & McNulty, Eric J., *Meta-Leadership: A Primer,* National Preparedness Leadership Institute (NPLI), Harvard School of Public Health, 2015.

Connectivity

To resolve a crisis, Meta-Leaders must successfully chart a course forward, make decisions, operationalize those decisions, and communicate effectively to obtain wide engagement and support. Meta-Leaders will navigate through personal dynamics and the complexities of the situation. There are four facets of leadership that create connectivity. Those four facets are:

Leading Down	This is the traditional leadership role in which a manager maintains formal authority towards his subordinates. It is important to maintain their support in order to achieve greater influence within other facets.
Leading Up	The manager, in the role of a subordinate, should know his boss' priorities, provide insight and information that they need, and ensure that the boss is kept connected and informed of necessary information.
Lead Across	Sometimes, necessary resources are found outside the organization. Meta-Leaders will engage peer groups and others not formally subordinate to them. These different entities may view the same information quite differently; their collaboration may provide successful solutions to problems.
Lead Beyond	Crisis resolution may involve interaction with a number of people and organizations including members of the community and the media. It is important to consider all possible stakeholders to provide for unity of effort.

The Dimensions of Meta-Leadership Applied to Cyber Security

At this point, you may be asking why the concept of Meta-Leadership is important to you as a middle manager in a utility company. This is best illustrated by applying the framework of Meta-Leadership to the complexities you will experience when dealing with your company's cyber security.

The Person

In a complex situation, such as a severe incident caused by malicious cyber activity, no one will have all the information. No one, including you, will fully understand the entire situation; yet, due to your position, everyone will look to you for answers. In a situation like this, it is important to be aware of your emotions and the behavior you exhibit. Under stressful situations, it is normal to instinctively resort to your most basic levels of thinking and functioning. This is called, going to your "emotional basement." It may cause you, and others in your organization, to behave in ways that will not only NOT resolve the situation, but may make matters worse.

This guide should help you understand this framework and increase your self-awareness and self-knowledge. As a result, you will be better prepared to confront that fear and lead yourself and others out of the "emotional basement" to higher levels of thinking and functioning.

The Situation

Knowing you may one day face this type of complex situation, you read this guide to prepare. While reacting to this type of complex situation, you refer back to this guide. This guide provides you with information about the key stakeholders involved with preparing for or reacting to a cyber incident. By following the best practices within this guide, you know better what to expect next, are able to identify the critical choice points, and develop options for action.

Connectivity

As stated earlier, help with cyber security is available from a wide variety of sources, but understanding where to start and which are the best to use is a monumental task. This guide provides you a starting point for the most useful resources. These resources provide assistance for training members of your organization both below and above you on cyber security concepts. These resources provide best practices for both on how to prepare for and react to malicious cyber activity. Resources consisting of agencies across and beyond your organization, from the federal to the state, local, tribal, and territorial levels are provided to help you with all facets of preparation and response.

IV. When and how do managers use this guide?

It is important for managers to create a culture of cyber security at all levels within their organization, Figure 2. That means they must identify their organization's current status and define their desired goals and objectives.

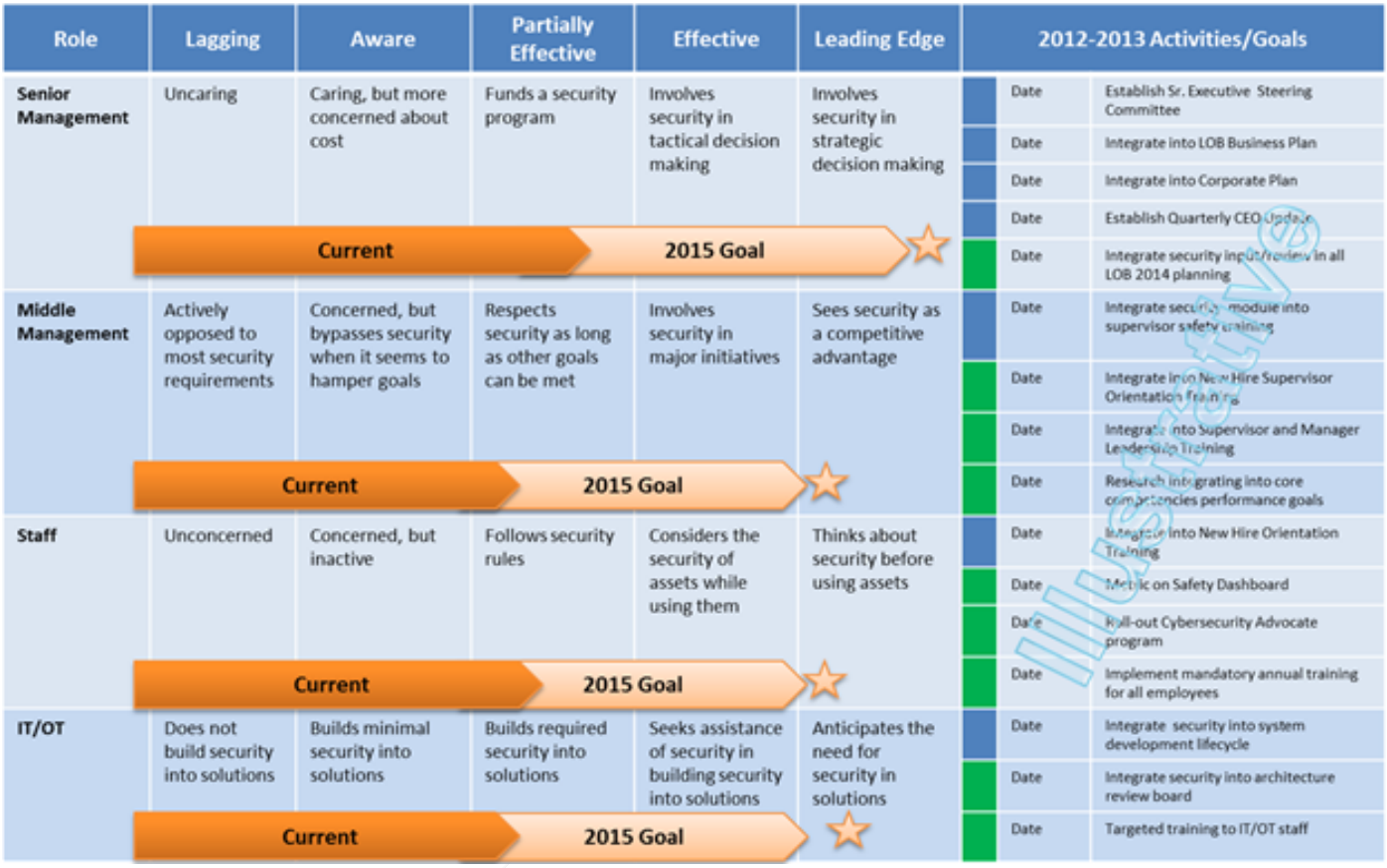


Figure 2. Culture of Security[9]

As stated, it is not possible to prevent malicious cyber activity, only to make the organization more resilient and able to recover more quickly when a cyber attack occurs. Therefore, managers are encouraged to use this guide as they create or revamp their cyber security plans, policies, and procedures.

Managers *should* refer to this guide when preparing to counter malicious cyber activities. This guide combines a vast array of existing resources into a single, simplified format in order to help increase a manager's understanding of the problem faced and simplify preparations. This guide also provides a detailed reference list of federal, state, and local resources and agencies available to provide assistance in those preparations.

[9] http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Creating-a-Culture-of-Security.aspx

Managers *could* refer to this guide when responding to or recovering from a cyber- incident. This guide provides a detailed reference list of federal, state, and local resources and agencies available to provide assistance during or after an incident caused by malicious cyber activity.

Managers *should* implement the best practices presented in the volumes of this guide. These volumes follow the format presented in the ten Cyber Resilience Review (CRR) Implementation Guides published by the Department of Homeland Security and summarize their content. The volumes of this guide also contain additional resources from State and Local agencies. While these are specific to the State of California, they are indicative of the types of resources you should look for in your particular State and locale. This guide ends with a list of each of the states and territories in which Fusion Centers are located as well as contact information by FEMA region.

Managers *must* develop and regularly update their own, customized cyber incident preparations and responses that may use this guide as a foundation for their creation. Cyber threats and response capabilities are constantly changing; this guide is only as accurate as the available information and materials at the time it of publishing. This guide is intentionally broad and somewhat generic; you must adapt it to your specific company and situation. *You must make this guide your own!*

In the pages that follow, ten volumes from the Cyber Resilience Review (CRR) developed by the Department of Homeland Security's Cyber Security Evaluation Program are synopsized. The volumes are divided by the following: Preparation- Technical Issues and End User Training and Response and Recovery- Immediate Response and Rapid Recovery. Resources that can provide further assistance are listed at the end of each volume.

V. Preparation – *Technical Issues*

Volume 1- Asset Management

Introduction:

Asset Management is one of the most important parts of any security program; it gives organizations an opportunity to identify all assets within their existing infrastructure and is the initial planning element within an organization. It is essential that a plan is developed and followed to ensure consideration and inclusion of all assets. An organization cannot truly safeguard what it hasn't identified or understand. One of the most important components is support from all levels of the management structure to ensure that the process receives the proper funding and staff support.

Planning:

To ensure that all the mission-critical equipment is identified and prioritized according to their potential to disrupt operations should they fail the organization should include the 4 following activities:

- Identification of critical assets
- Documentation of critical assets
- Prioritization of critical assets
- Establishment of a common definition of assets

Critical Asset Identification:

Successfully identifying your organization's critical assets and properly organizing them are key in this phase of the project. The list below provides 5 activities to be undertaken:

- Assign responsibility for asset identification
- Identify key people
- Identify key information assets
- Identify key technology assets
- Identify key facility assets

Asset Documentation:

Once all assets have been identified, organizing the documentation will allow for a better understanding of the relationships between the assets and lead to considerations for these assets throughout their lifecycle. The 9 components of the documentation should include:

- Define asset type (people, information, technology, or facilities)
- Prioritize asset by sensitivity level (generally for information assets only)
- Provide asset location (typically where the custodian is managing the asset)
- Identify asset owners and custodians (especially if assets are external to the organization)
- Indicate asset format or form (particularly for information assets that might exist on paper or electronically)
- Determine location of asset backups or duplicates (particularly for information assets)
- Define which services are dependent on these assets
- Assign a value to the asset (either qualitatively or quantitatively)
- Prepare asset protection and sustainment requirements

Value of this Volume:

Because this volume focuses on assets and their management, you should develop checklists for each step listed above and include definitions, suggestions, and the expected product when completed. Because assets change, it is important to have this baseline document and update it regularly. Pre-identifying the criteria for these changes ensure consistency for changes whether they are in the field, engineering, or personnel levels. The development of a schedule for performing these updates provides consistency and can lead to improved processes.

Asset Management Resources:

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
http://www.ics-cert.us-cert.gov

- Rinaldi et al. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control Systems Magazine*, 2001. http://ics-cert.uscert.gov/redirect?url=http%3A%2F%2Fwww.ce.cmu.edu%2F~hsm%2Fim2004%2Freadings%2FCII-Rinaldi.pdf

Information Systems Audit and Control Association (ISACA)
http://www.isaca.org

- Control Objectives for Information and Related Technology (COBIT) http://www.isaca.org/COBIT/Pages/default.aspx

Information Technology Infrastructure Library (ITIL)
http://www.itil-officialsite.com/Publications/Publications.aspx

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center http://csrc.nist.gov/
    - o NIST Special Publication 800-53, Recommended Security and Privacy Controls for Federal Information Systems and Organizations
    - o NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle
    - o NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook

Software Engineering Institute, CERT Division, http://www.sei.cmu.edu/

- CERT-RMM http://www.cert.org/resilience/rmm.html
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) http://www.cert.org/octave/

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- California IT Directory, http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html
- Holland, Kurtis "Incident Response Exercise Planning, Be Ready – Be Prepared" *SANS Institute*, 2014.

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

IBM, http://www.ibm.com/security

Ernst and Young, http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity

RSA, http://www.emc.com/services/index.htm

VI. Preparation – *Technical Issues*

Volume 2- Controls Management

Introduction:

Controls Management focuses on planning within an organization to define, analyze, and assess its internal controls. A good ongoing controls management program will ensure an organization's critical services can be sustained, it can meet its responsibilities to shareholders, and maintain critical infrastructure during times of stress. The goals of controls management should be an alignment with organizational priorities, operational controls which ensure the resiliency of assets and services, and enterprise controls for application across all levels of the organization. Before these controls can be established, however, the different types of controls that exist and different times when they should be used must be understood.

Planning:

Controls management planning should be supported by management and occur at all levels within an organization. Processes need to be defined to identify, implement, and assess these controls to provide for ongoing revisions, to ensure organizational resiliency.

The four (4) important activities while planning for controls management include the following:

- Develop a controls strategy
- Establish a controls identification process
- Utilize a controls analysis process
- Create a controls assessment process

Define Controls:

Each organization utilizes controls to define responsibilities in their enterprise, service, or asset areas. A process for identifying and defining these controls has three (3) important components, including:

- Assign responsibility and define enterprise-level controls
- Assign responsibility and define service- and asset-level controls
- Document these controls in a Security Requirements Traceability Matrix (SRTM)

Analyze Controls:

Organizations should first analyze the existing controls in place to ensure that they are meeting current needs. Next, they must develop controls in areas that are lacking these controls and deploy them.

Important activities for analyzing the controls management process include the six (6) following steps:

- Analyze existing controls against objectives
- Identify gaps in existing controls
- Create or update controls
- Establish linkages to the organization's risk management process
- Update the Security Requirements Traceability Matrix (SRTM)
- Deploy the controls

Assess Controls:

Organizations need to ensure that the deployed controls meet their needs from an internal control system standpoint as well as meeting resiliency requirements. There are six (6) important activities in this area:

- Identify stakeholders and begin the assessment process
- Establish a schedule
- Define the scope
- Perform the assessment
- Improve the process
- Update control objectives and controls

Controls Management Resources:

Information Systems Audit and Control Association (ISACA)
http://www.isaca.org

- Control Objectives for Information and Related Technology (COBIT)
  http://www.isaca.org/COBIT/Pages/default.aspx

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - NIST Special Publication 800-53, Recommended Security and Privacy Controls for Federal Information Systems and Organizations
  - NIST Special Publication 800-53A, Guide for Assessing the Security Controls in Federal Information Systems
  - NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security
  - NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
http://www.ics-cert.us-cert.gov

- Catalog of Control Systems Security: Recommendations for Standards Developers, April 2011, U.S. Department of Homeland Security National Cybersecurity and Communications Integration Center, ICS-CERT.
  http://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf
- Cyber Security Procurement Language for Control Systems, U.S. Department of Homeland Security National Cyber Security Division, September 2009.
  http://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

- CERT-RMM http://www.cert.org/resilience/rmm.html
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  http://www.cert.org/octave/

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- Risk Assessment Toolkit
  http://www.cio.ca.gov/OIS/Government/risk/toolkit.asp

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

IBM, http://www.ibm.com/security

SANS, https://www.sans.org/critical-security-controls

RSA, http://www.emc.com/services/index.htm

VII. Preparation – *Technical Issues*

Volume 3- Configuration and Change Management (CCM)

Introduction:

Another crucial planning component in cyber security is in the area of Configuration and Change Management (CCM). This volume assists organizations with the process of maintaining the integrity of hardware, software, and firmware. It also includes all documentation relating to this process. As systems and assets are added or changed, it is important to create processes that may reduce the possibility of errors and, in the event of an error, reduces the impact of that error on the organization.

Glossary of Terms:

Certain terms used in this configuration volume require explanation. These terms include:

- Configuration Item (CI)- asset or assets place under configuration management
- Baseline Configuration- represents the settings, software, and state of the Item; baseline is the formal review process and can only be changed through a formal review process
- Configuration and Change Management Plan (CCMP)- the process in which changes to CIs are developed and implemented, including requests, approvals, monitoring, and improvements
- Configuration Control Review Board (CCRB)- a group within the organization and made up of stakeholders who assess prioritize, authorize, and make/schedule changes to the CIs

Planning:

Creating a Configuration and Change Management Plan is important to an organization because it allows for the orderly control of changes to high-value assets. This benefits the organization through the mitigation of disruptions. Management support for this is critical as well as the following activities:

- Develop a budget
- Define roles and responsibilities
- Gather all existing policies, procedures, and documentation currently in effect within the organization
- Identify critical organizational services needing configuration and change management
- Validate critical services with stakeholders; establish a configuration change review board.
- Develop a change request process
- Develop mechanisms for the communication of changes to the organization
- Develop a training plan for this process
- Identify tools to use in the implementation of processes
- Prepare a plan for capacity management

Identify Configuration Items:

The following four (4) activities are important in identifying Configuration Items (CIs):

- Map critical organizational services to stakeholders and related services
- Identify assets related to the critical services
- Identify the CIs of the assets that will undergo change and require change and configuration management
- Determine a configuration baseline for each CI

Implement and Control Configuration Changes:

When all CIs have been identified and baselines have been tested and approved, the organization can make changes to the system. Here are the seven (7) activities to implementing configurations:

- Evaluate change requests and approvals
- Model configuration changes in a test environment
- Deploy changes
- Determine the success or failure of changes
- Change or eliminate unsuccessful changes
- Close out completed changes
- As necessary, change configuration baselines

Implement and Control Configuration Changes:

When CIs have been identified and baselines have been tested and approved, the organization can now implement them into the system. In information technology systems, organizations should use automated tools. The following seven (7) implementation activities should be performed:

- Evaluate change requests and approvals
- Test the configuration change process
- Put the changes into effect
- Analyze the success or failure of the changes
- Change or eliminate unsuccessful change processes
- Close out completed changes
- Change configuration baselines as necessary

Monitor Configuration Changes:

The monitoring of configuration changes poses a significant challenge to organizations. In order to be successful, perform the following six (6) activities:

- Identify systems or components not specified in documentation
- Identify disparities between authorized, approved baselines and actual, implemented baselines
- Monitor system logs for unauthorized changes
- Collect existing audits and configuration control records
- Define remediation action
- Execute monitoring plan

Outputs of Configuration Planning:

Resilient organizations have a variety of critical systems and assets that require configuration management. Changes to, or the introduction of, existing or new assets can pose a risk to the confidentiality, integrity, or the availability of data. With a reliable CCM, organizations can evaluate and control the impact of changes that might affect employees, assets, customers, or their security.

Configuration and Change Management Resources:

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp
- o Critical Capabilities for Configuration Management Database
  https://www.gartner.com/doc/2770917/critical-capabilities-configuration-management-database

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

ITIL (Requires a Fee)
http://www.itil-officialsite.com/

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html
- o NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - Special Publication 800-128 Guide for Security-Focused Configuration Management of
    Information Systems
    http://csrc.nist.gov/publications/nistpubs/800-128/sp800-128.pdf
  - NIST Special Publication 800-40r3, Guide to Enterprise Patch Management Technologies
    http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/
- o CERT Resilience Management Model
  http://www.cert.org/resilience/rmm.html
- o OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
  http://www.cert.org/octave/
- o Concepts in Configuration Management Systems
  ftp://ftp.sei.cmu.edu/pub/case-env/config_mgt/papers/cm_concepts.pdf

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov
- o Situational awareness information
  https://www.us-cert.gov/

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- California IT Directory
  http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

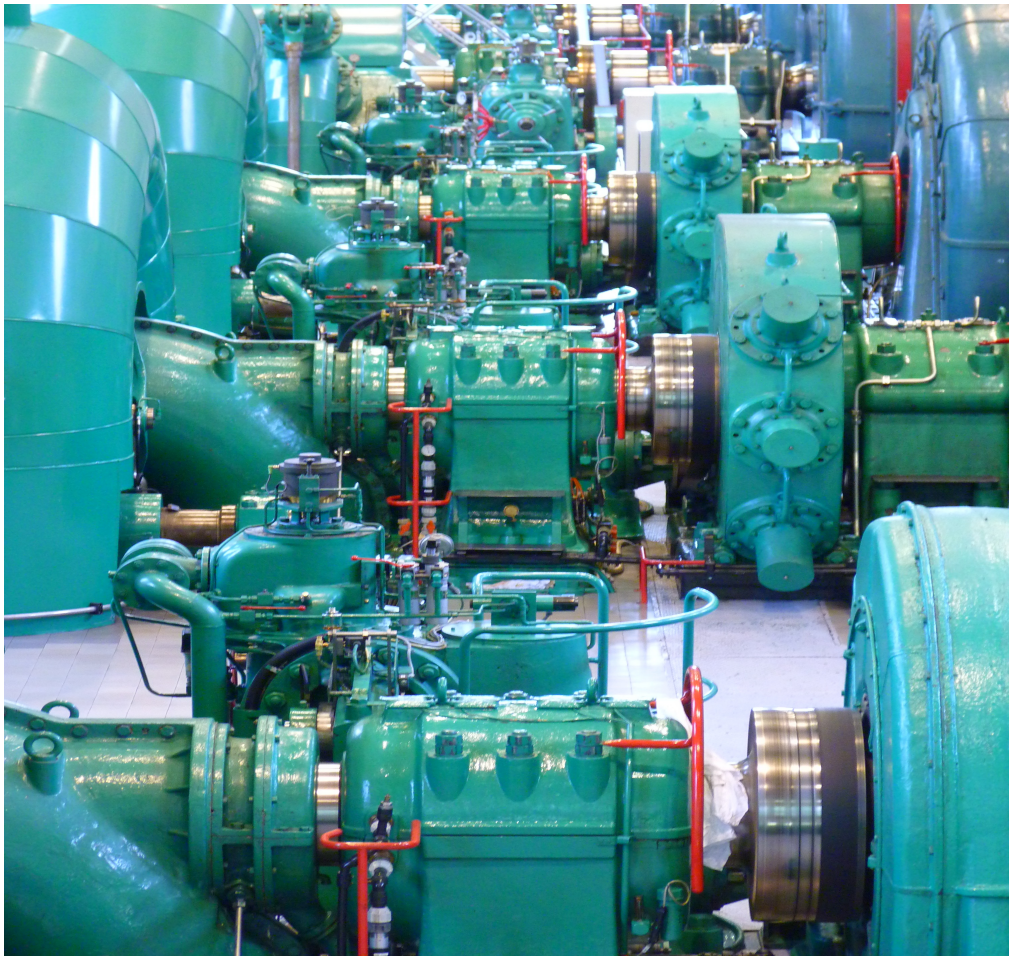
California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

IBM, http://www.ibm.com/security

SANS, https://www.sans.org/critical-security-controls

RSA, http://www.emc.com/services/index.htm



VIII. Preparation – *Technical Issues*

Volume 4- Vulnerability Management

Introduction:

This volume provides guidance on preparing for conditions within a particular organization that makes them susceptible to a threat and exposes them to risk. Asset vulnerability in the areas of people, information, technology, and facilities each has its own planning efforts within the organization. Managing these vulnerabilities is a key component for an organization when determining both the proper implementation of controls and risk management. After determining what the vulnerabilities are, the level of vulnerability, and the impacts of these vulnerabilities, risk management discussions and planning (Volume 7) begins.

Define a Strategy:

Preparing a vulnerability strategy involves defining the organization's goals and must align with the organization's requirements for success. Using input from all stakeholders, the strategy can be developed using these three (3) steps:

- Determine the scope of vulnerability management (i.e. what asset/services will be assessed and monitored)
- Determine and approve methods of the assessment
- Assign stakeholder responsibilities and develop a budget

Develop a Plan:
After the strategy is developed, it needs to be converted into a plan with rules and guidelines for the vulnerability management team. Use these eight (8) steps in the plan development process:

- Define and document the plan
- Define measures of effectiveness
- Provide training requirements
- Determine which tools will best align with the strategy
- Identify sources of vulnerability information
- Determine roles and responsibilities
- Ensure stakeholder Engagement
- Develop a plan revision process

Implementing Capabilities:

Implementing vulnerability management capabilities will be used to mitigate the organization's exposure to the vulnerability and is based on the timelines established in the strategy and the plan. The following seven (7) steps should be followed:

- Provide training to staff
- Conduct vulnerability assessment activities
- Record discovered vulnerabilities
- Categorize and prioritize all vulnerabilities
- Manage exposure to discovered vulnerabilities
- Determine effectiveness of vulnerability dispositions
- Analyze root causes of the vulnerabilities

Perform an Assessment to improve capabilities:

Organizations must assess the both the organization's vulnerabilities as well as analyze those that are pertinent. These discoveries must cover a comprehensive portion of the organization and the analysis must determine the extent of the vulnerability and the effect on the organization and its critical services. These three (3) steps should be used to assess and improve vulnerability management:

- Determine the state of the program
- Collect and analyze program information
- Improve capabilities

Vulnerability Management Resources

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp

- *Vulnerability Assessment Technology and Vulnerability Management Practices*
  https://www.gartner.com/doc/2664022?pcp=itg
  o MarketScope for Vulnerability Assessment
  https://www.gartner.com/doc/2586218?pcp=itg
  o Improve IT Security With Vulnerability Management
  https://www.gartner.com/doc/480703

Forrester
http://www.forrester.com/home/

- Vulnerability management articles, tools, and templates (some require a fee)
  http://www.forrester.com/search?tmtxt=vulnerability%20management&searchOption=10001&source=typed

FS-ISAC

- Cyber Intelligence Repository
  https://www.fsisac.com/CyberIntelligenceRepository

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

- ISO/IEC TR 20004:2012 Information technology -- Security techniques -- Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50951
  o ISO/IEC 30111:2013 Information technology -- Security techniques -- Vulnerability handling processes (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231
  o ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  o National Vulnerability Database http://www.nist.gov/itl/csd/stvm/nvd.cfm
  http://nvd.nist.gov/home.cfm
  o NIST IR 7946 DRAFT CVSS Implementation Guidance
  http://csrc.nist.gov/publications/drafts/nistir-7946/draft_nistir_7946.pdf
  o NIST NIST IR 7669 DRAFT Open Vulnerability Assessment Language (OVAL) Validation Program Derived Test Requirements
  http://csrc.nist.gov/publications/drafts/nistir-7669/draft-nistir-7669.pdf
  o NIST IR 7328 DRAFT Security Assessment Provider Requirements and Customer Responsibilities: Building a Security Assessment Credentialing Program for Federal

Information Systems http://csrc.nist.gov/publications/drafts/nistir-7328/NISTIR_7328-ipdraft.pdf
- o SP 800-40 v.2.0 Creating a Patch and Vulnerability Management Program http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
- o NIST Publication list http://csrc.nist.gov/publications/PubsFL.html

US Department of Energy- Office of Electricity Delivery & Energy Reliability- Electricity Maturity Model
http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

- Office of Electricity Delivery and Energy Reliability (OE) http://energy.gov/oe/services/cybersecurity

US Department of Energy- Office of Electricity Delivery & Energy Reliability- Oil and Natural Gas Maturity Model
http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/oil-and-natural-gas-subsector-cybersecurity

Payment Card Industry (PCI) Security Standards Council
https://www.pcisecuritystandards.org/index.php

- *Payment Card Industry (PCI) Data Security Standard, Navigating PCI DSS – Understanding the Intent of the Requirements v.2.0* See sections 5 and 6, *Maintain a Vulnerability Management Program* https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf
- *Payment Card Industry (PCI) Data Security Standard – Security Scanning Procedures* https://www.pcisecuritystandards.org/pdfs/pci_scanning_procedures_v1-1.pdf
- *PCI Quick Reference Guide* https://www.pcisecuritystandards.org/documents/pci_ssc_quick_guide.pdf
- PCI approved scanning vendors https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

SearchHealthIT
http://searchhealthit.techtarget.com/

- *Best of vulnerability management 2013* http://searchsecurity.techtarget.com/feature/Best-of-vulnerability-management-2013
  - o Access "Vulnerability management programs: A handbook for security pros" http://searchsecurity.techtarget.com/ehandbook/Vulnerability-management-programs-A-handbook-for-security-pros

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

- CERT Resilience Management Model http://www.cert.org/resilience/products-services/cert rmm/index.cfm
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) http://www.cert.org/resilience/products-services/octave/index.cfm
  - o Vulnerability analysis topics at CERT http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Analysis
  - o Vulnerability discovery topics at CERT http://www.cert.org/blogs/blog_categories.cfm?getCat=Vulnerability%20Discovery

United States Computer Emergency Readiness Team (US-CERT) http://www.us-cert.gov

- *Getting Started for State, Local, Tribal, and Territorial (SLTT) Governments* http://www.us-cert.gov/ccubedvp/getting-started-sltt
- *Exploit and Vulnerability Databases* https://buildsecurityin.us-cert.gov/swa/resources/exploit-and-vulnerability-databases
- Analytical Tools and Programs http://www.us-cert.gov/government-users/tools-and-programs
- National Cyber Awareness System https://www.us-cert.gov/ncas

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- Incident Management, http://www.cio.ca.gov/OIS/Government/incident.asp#Inci_Othr_Res
- Information Security Incident Reporting Roadmap for State Government http://www.cio.ca.gov/OIS/Government/documents/pdf/ISO_Incident_Notify_Roadmap.pdf
- Technology Recovery Management http://www.cio.ca.gov/OIS/Government/disaster.asp
- California IT Directory, http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html
- Holland, Kurtis "Incident Response Exercise Planning, Be Ready – Be Prepared" *SANS Institute*, 2014.

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force, http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf
- California National Guard Cyber Knowledge HUB https://ngcamy.ng.army.mil/SitePages/Cyber.aspx

Dell Secure Works, http://www.secureworks.com

FireEye, http://www.fireeye.com

IBM, http://www.ibm.com/security

Rapid7, http://www.rapid7.com

DFLabs, http://www.dflabs.com/professional-services/

RSA, http://www.emc.com/services/index.htm

IX. Preparation – *End User Training*

Volume 9- Training and Awareness

Introduction:

This volume focuses on training and awareness activities to teach staff members their roles in an organization's cyber resilience efforts. Specific training, focusing on cyber resilience activities, should be integrated into and support the organization's overall training and awareness program. If the organization already has training or awareness programs, it is important that they include cyber resilience. These existing programs can use their established information gathering processes, building capabilities, evaluation methods, record keeping, and improvement activities to support cyber resilience training and awareness. Training activities teach skills to support cyber resilience programs; awareness activities focus on developing staff members' understanding of issues, policies, plans, and practices.

Planning:

Planning for training and awareness is important for the successful development of the program. Management support is vital at all levels of the organization to identify, implement, and assess these activities on an ongoing basis to create skilled employees. Planning for training and awareness activities should include the following:

- Establish a training and awareness program strategy.
- Establish an approach to building a training capability.
- Establish an approach to building an awareness capability

Assess Training and Awareness Needs:

If the organization does not already have a training and awareness program, a needs analysis should be conducted. Identifying needs for specific cyber resilience courses and activities can be derived from various other organizational plans like controls management and risk management. Using these plans, a list of critical skills needed to perform job duties and functions can be developed to educate staff members and close gaps. Important activities for the identification of training and awareness needs include:

- Obtain support for training and awareness needs assessment
- Develop a strategy for identifying training needs
- Develop a strategy for identifying awareness needs
- Establish a process for training and awareness needs analysis

Conduct Training and Awareness Activities:

Because each organization will have unique needs, different methods of course delivery must be developed. Establishing capabilities for cyber resilience training and awareness includes identifying and developing the program's educational vehicles (courses, presentations, etc.). In some instances, organizational training and awareness needs common to other companies, will allow for the use of third party providers. In order to build training and awareness capabilities, the following important activities must be conducted:

- Establish and maintain support functions (e.g., library for storing materials and a record tracking system)
- Develop training and awareness materials
- Procure third-party provider services
- Conduct training and awareness activities

Improve Training and Awareness Capability:

Following the development of the program, the organization should evaluate activities to ensure that they meet objectives. Criteria should be developed, data collected, and an analysis of the program will allow for improvements. Desirable outcomes of this evaluation should include: improved employee job performance, increased ability of supervisor assessments, and increased confidence that organizational goals and objectives are being met. To ensure continual improvement in the training and awareness program, data should be collected and evaluated on a regular cycle and updated materials should be incorporated as needed. The following important activities should be included:

- Establish a plan to evaluate the training and awareness program
- Evaluate training and awareness program and analyze results
- Improve the process
- Update training and awareness materials

Training and Awareness Resources

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center http://csrc.nist.gov/
  - NIST Special Publication 800-16 Revision 1 (2nd Draft Version 2), A Role-Based Model For Federal Information Technology/Cyber Security Training

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

CERT-RMM
http://www.cert.org/resilience/rmm.html

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- California IT Directory
  http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html
- Holland, Kurtis "Incident Response Exercise Planning, Be Ready – Be Prepared" *SANS Institute*, 2014.

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf
- California National Guard Cyber Knowledge HUB
  https://ngcamy.ng.army.mil/SitePages/Cyber.aspx

California Highway Patrol Emergency Notification and Tactical Alert Center (ENTAC)
https://www.chp.ca.gov/notify-chp/computer-crime-reporting-for-state-agencies

Rapid7, http://www.rapid7.com

Palo Alto Networks, https://www.paloaltonetworks.com/

RSA, http://www.emc.com/services/index.htm

X. Response and Recovery – *Immediate Response*

Volume 5- Incident Management

Introduction:

Incident management is the process an organization uses to detect, analyze, respond to, and recover from a disruptive event. Organizations need to develop processes to address these events. The four (4) steps to establish this process includes:

- Detect and identify events
- Triage and analyze events to determine whether an incident is underway
- Respond to and recover from an incident
- Improve the organization's capabilities for responding to a future incident

Detect Events:

An "event" is defined as an occurrence affecting an organization's assets and having the potential to disrupt its operations. To be effective, an organization must have an incident management plan and monitor and identify incidents as they occur. Although there are many units within an organization that can perform this activity, typically help desks or network operations centers have been assigned this responsibility. To be effective, all organizations need the capability to detect, report, log, track, and collect and store event evidence. An inability to perform these actions reduces an organization's ability to recover rapidly from an incident. The steps required for event detection include these four (4) steps:

- Event detection and reporting
- Logging event data in an incident database or similar mechanism
- Event status tracking
- Event data handling in accordance with laws, rules, regulations, policies, etc.

Triage and Analyze

Unlike an event, an "incident" is described as a high-magnitude event or series of events that significantly affect an organization's assets and requires a response to either prevent or limit its impact. In the triage portion of the incident, the organization must determine how to categorize and evaluate whether it is declarable as an incident. This threshold is different for each organization and depends on multiple factors.
Once an organization determines that an incident has occurred, additional analysis is performed to determine the appropriate response. Depending on the organization, either a response has already been planned or the organization will collect data from stakeholders before responding. The five (5) important steps in this phase include:

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

Respond and Recover

To prevent or contain the impact of an incident, organizations must respond. The amount of resources used will depend on the extent of the incident and will be guided by analysis. Due to the broad range of possible incidents, responses may also vary widely. Moreover, as each organization has a unique operating environment, their response to an incident will determine their response. The four (4) practices in the area of response and recovery include:

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

Improve Capability

After the resolution of the incident, organizations should conduct a review to consider its performance. This will help the organization understand why the incident occurred and what can be done to prevent future incidents. The review process should include stakeholders who participated in the incident and those whose assets were involved. After the incident has been reviewed, it is necessary to close it, an indication that no further action needs to be taken.

Incident Management Resources

US Computer Emergency Readiness Team (US-CERT)
https://www.us-cert.gov/ccubedvp/getting-started-business

- Links to various security organizations, https://www.us-cert.gov/related-resources

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- Incident Management, http://www.cio.ca.gov/OIS/Government/incident.asp#Inci_Othr_Res
- Information Security Incident Reporting Roadmap for State Government http://www.cio.ca.gov/OIS/Government/documents/pdf/ISO_Incident_Notify_Roadmap.pdf
- Technology Recovery Management, http://www.cio.ca.gov/OIS/Government/disaster.asp
- California IT Directory, http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html
- Holland, Kurtis "Incident Response Exercise Planning, Be Ready – Be Prepared" *SANS Institute*, 2014.

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf
- California National Guard Cyber Knowledge HUB https://ngcamy.ng.army.mil/SitePages/Cyber.aspx

California Highway Patrol Emergency Notification and Tactical Alert Center (ENTAC)
https://www.chp.ca.gov/notify-chp/computer-crime-reporting-for-state-agencies

State of California Department of Justice
Office of the Attorney General
http://oag.ca.gov/privacy

Dell Secure Works, http://www.secureworks.com

FireEye, http://www.fireeye.com

IBM, http://www.ibm.com/security

Rapid7, http://www.rapid7.com

DFLabs, http://www.dflabs.com/professional-services/

XI. Response and Recovery – *Immediate Response*

Volume 7- Risk Management

Introduction:

Organizations manage multiple risks and the processes by which they identify, analyze, and mitigate those risks allows them to remain effective and achieve their desired objectives. Operational risks can occur under a variety of circumstances and an organization's ability to manage these risks will affect their capability to respond and adapt when disruptions occur.

Identify Risks:

Organizations must first identify their risks in order to manage them successfully. Risk identification tasks include the following four (4) areas:

- Establish various categories for risk
- Identify all risk stakeholders
- Identify sources of risk to operations dependent on technology and information assets
- Log identified risks in a risk register or other tracking mechanism to organize and record information on identified operational risks

Analyze Risk and Assign Disposition:

Analysis will provide an organization with an understanding of a risk's potential impact and allow for the development of appropriate strategies and responses. The first step is assessing and prioritizing identified risks based on potential impact, likelihood of occurrence, and other potential factors. After these determinations are made, an organization must decide how to deal with their risks. This disposition of risk may include: avoiding, accepting, or mitigating. Creating registers or tracking mechanisms allows the organization to keep track of events. The seven (7) activities to take in risk analysis and disposition assignment include:

- Establish and prioritize impact areas for risk
- Create risk tolerance parameters for each impact area
- Establish risk tolerance thresholds for each risk category
- Analyze identified risks to determine potential operational impacts
- Categorize and prioritize identified risks based on operational impact and risk tolerance thresholds
- Assign a disposition to all identified risks
- Update risk register or other tracking mechanism with analysis and disposition information

Control Risks:

To control risks, organizations must design and implement a process that reduces the likelihood of risk and their impact if an event occurs. Risk management strategies should ensure that risks are reduced to an acceptable level and are managed in a way that allows an organization to meet its mission. Although some risks will require changes to control strategies, not all risk can be mitigated. However, no matter how an organization deals with risks, it is important to develop processes to track and address risk. There are five (5) plans that will assist in managing operational risks.

- Develop plans for managing identified operational risks
- Communicate plans and status to stakeholders
- Validate risk management plans
- Develop mitigation plans for organization-identified risks
- Track identified risks to closure

Plan for Risk Management:

Risk management plans provide an organization with a defined process for its effective operation. These plans must address the risks faced by the organization that may disrupt their ability to deliver services. These seven (7) steps should, minimally, be used when developing a risk management plan:

- The organization's approach to risk management
- Provide adequate financial and organizational resources
- Develop a risk management process structure
- Identify the requirements and objectives of the risk management process
- Describe how the organization will identify, analyze, and mitigate risks, and monitor and improve its risk management capabilities over time
- Define roles and responsibilities necessary to carry out the plan
- Provide for applicable training needs and requirements

Risk Management Resources:

DHS

- Office of Risk Management and Analysis
  http://www.dhs.gov/about-office-risk-management-and-analysis
  - **Risk Management Fundamentals: Homeland Security Risk Management Doctrine**
    http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf
  - **Threat and hazard identification and risk assessment guide**
    http://www.state.nj.us/njhomelandsecurity/grants/grants-main/06-21-12-thira-guide.pdf

Federal Emergency Management Agency (FEMA)
http://www.fema.gov/

- PS-Prep—Voluntary program, primarily serving as a resource for private and nonprofit entities interested in instituting a comprehensive business continuity management system. The program adopted the following three preparedness standards. For more information, see http://www.fema.gov/about-ps-preptm.
  - **ASIS International (PDF 1.2 MB)**
    http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.asisonline.org%2Fguidelines%2FASIS_SPC.1-2009_Item_No._1842.pdf
  - **British Standards Institution (BSI)**
    http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.bsiamerica.com%2Fen-us%2FAssessment-and-Certification-services%2FManagement-systems%2FStandards-and-schemes%2FBS-25999%2F
  - **National Fire Protection Association (NFPA)**
    http://www.fema.gov/redirect?url=http%3A%2F%2Fwww.nfpa.org%2Faboutthecodes%2FAboutTheCodes.asp%3FDocNum%3D1600%26cookie%255Ftest%3D1
  - **Business Continuity Planning (BCP) Suite**
    http://www.ready.gov/business-continuity-planning-suite
  - **BCP resources to assist businesses with preparedness**
    http://www.ready.gov/business
  - **Exercise Design Materials**
    http://www.training.fema.gov/emiweb/IS/is139lst.asp

Federal Financial Institutions Examination Council (FFIEC)
http://www.ffiec.gov/

- Management
  http://ithandbook.ffiec.gov/it-booklets/management.aspx

Gartner (requires subscription)
http://www.gartner.com/technology/home.jsp

- Operational Risk Blog
  http://blogs.gartner.com/business-continuity/tag/operational-risk-management/

Forrester
http://www.forrester.com/home/

- Risk management articles, tools, and templates (some require a fee)
  http://www.forrester.com/search?tmtxt=Risk%20management&searchOption=10001&source=typed

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

- ISO 31000 Risk management - Principles and guidelines (fee)
  http://www.iso.org/iso/home/standards/iso31000.htm
- ISO 31010 Risk management - Risk assessment techniques (fee)
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51073
- ISO 27002 outlines potential cybersecurity controls and control mechanisms (fee)
  http://www.27000.org/iso-27002.htm

Information Systems Audit and Control Association (ISACA)
http://www.isaca.org

- Control Objectives for Information and Related Technology (COBIT) 4.1
  http://www.isaca.org/COBIT/Pages/default.aspx
- Control Objectives for Information and Related Technology (COBIT) 5
  http://www.isaca.org/COBIT/Pages/default.aspx

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

- NIST Computer Security Division, Computer Security Resource Center
  http://csrc.nist.gov/
  - **NIST Special Publication 800-30, Guide for Conducting Risk Assessments**
    http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
  - **NIST Special Publication 800-37, Risk Management**
    http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
  - **NIST Special Publication 800-39, Managing Information Security Risk**
    http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
  - **NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations"**
    http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

Software Engineering Institute, CERT Division
http://www.sei.cmu.edu/

- CERT Resilience Management Model http://www.cert.org/resilience/rmm.htmlie
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) http://www.cert.org/octave/
- *Measures for Managing Operational Resilience* (CMU/SEI-TR-2011-019) http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10017

United States Computer Emergency Readiness Team (US-CERT)
http://www.us-cert.gov

- Situational awareness information https://www.us-cert.gov/

U.S. Department of Health and Human Services (HHS)
http://www.hhs.gov/

- The basics of risk analysis and risk management http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- Risk Management http://www.cio.ca.gov/OIS/Government/risk/default.asp
- California IT Directory http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html

California Governor's Office of Emergency Services (CAL OES) Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

BT,
http://www.globalservices.bt.com/us/en/products_category/security_and_risk_management

Sera-Brynn, https://sera-brynn.com/

XII. Response and Recovery – *Immediate Response*

Volume 10- Situational Awareness

Introduction:

The purpose of this volume is to provide organizations with methods to develop their own common operating picture for the collection, fusion, and analysis of data. Such efforts will improve communication, support critical decision-making, and guide appropriate actions to provide for operational stability and security. The following situational awareness activities should include:

- collecting and analyzing data from external threats
- identifying suspicious behavior of potential internal threats
- communicating threat information
- participating in threat-sharing communities

Planning:

Planning is the first step and is essential for a situational awareness program. This program will support staff members and external stakeholders by providing information needed to perform their duties. Regardless of whether the situational awareness is at the enterprise level (for all organizational needs) or in specific areas of need, management support is crucial. Planning will document program objectives, create a strategy to reach these objectives, and ensure that the appropriate resources are obtained. The following are important planning requirements for situational awareness activities:

- Develop a situational awareness program strategy
- Establish an approach to collecting and analyzing data
- Create an approach for communicating information
- Prepare a plan

Collect and Analyze Situational Awareness Data:

If an organization already has an established situational awareness program, previously identified requirements should be reviewed to ensure they include cyber resilience. Vulnerability management, incident management, and service continuity management plans will all provide specific requirements to aid in the addition of this requirement. Once these requirements have been identified, an organization must analyze its gaps and the steps needed to resolve them. The following activities should be included:

- Establish data collection and analysis requirements
- Develop an approach to collecting and analyzing data
- Provide and maintain an infrastructure to support monitoring activities
- Collect, record, and analyze information

Communicate Information Needed to Make Appropriate Decisions:

Information collected through situational awareness activities must be effectively communicated to any stakeholder needing the information so they can make informed decisions. The following activities for communicating this information include:

- Establish communication requirements
- Develop communication standards and guidelines
- Create and maintain an infrastructure to support communication activities
- Communicate information

Improve Situational Awareness Process and Technology:

Organizational risks to critical services are best managed when an organization has effective situational awareness processes and technology. Due to increasing threats through cyber or physical attacks, organizations must continually improve its situational awareness capabilities. The following activities should be included in the improvement of situational awareness processes:

- Review overall program effectiveness
- Identify updates and improvements to the program
- Make improvements to the processes and technology

Situational Awareness Resources

United States Computer Emergency Readiness Team (US-CERT)

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.

US-CERT: http://www.us-cert.gov/
National Cyber Alert System: http://www.us-cert.gov/ncas

Critical Infrastructure Cyber Community or C³ (pronounced "C Cubed")

Voluntary program to assist the enhancement of critical infrastructure cybersecurity and to encourage the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.
http://www.nist.gov/cyberframework/

Getting Started for Business resources: http://www.us-cert.gov/ccubedvp/getting-started- business
Cyber Resilience Review (CRR) assessment resources: http://www.us-cert.gov/ccubedvp/self-service-crr

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

ICS-CERT provides a control system security focus in collaboration with US-CERT. ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts.

ICS-CERT: http://www.us-cert.gov/control_systems/ics-cert/
SCADA and Control Systems Procurement Language Project, September 2009, U.S. Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf
CSSP Training: http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Traning-v12.pdf
Cyber Security Evaluation Tool (CSET): http://ics-cert.us-cert.gov/Assessments

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 center responsible for the production of a common operating picture for cyber and communications across federal, state, and local government; intelligence; law enforcement communities; and the private sector.

NCCIC: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

Daily Open Source Infrastructure Report

Each business day, the DHS collects a summary of open-source published information concerning significant critical infrastructure issues.

Daily Open Source Infrastructure Report: http://www.dhs.gov/dhs-daily-open-source-infrastructure-report

Homeland Security Information Network (HSIN)

HSIN is a national secure and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

HSIN: http://www.dhs.gov/homeland-security-information-network

Multi-State Information Sharing and Analysis Center

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

MS-ISAC: http://msisac.cisecurity.org/resources/videos/free-training.cfm

United State Secret Service (USSS) Electronic Crimes Task Force (ECTF)

The USSS ECTF is a partnership of not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. Its common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures.

USSS ECTF: http://www.secretservice.gov/ectf.shtml

Federal Bureau of Investigation (FBI) InfraGard

InfraGard, a partnership between the FBI and the private sector, is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members.

InfraGard: https://www.infragard.org/

Internet Crime Complaint Center (IC3)

The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). The IC3 provides a central point for internet crime victims to report to and alert an appropriate agency online at www.ic3.gov. The IC3 collects, reviews, and refers internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts and identify current crime trends across the internet.

IC3: http://www.ic3.gov/default.aspx

iGuardian

The iGuardian portal, currently in its pilot stage, is available to 58,000 companies that make up the FBI's InfraGard network. If the pilot succeeds, the FBI plans to open it up to more organizations, probably at first in critical infrastructure sectors. Participating companies can submit a form online in the instance of a cybersecurity breach to their networks. The National Cyber Investigative Joint Taskforce (NCI-JTF) handles the information provided by these companies.

iGuardian: http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view
NCI-JTF: http://www.fbi.gov/about-us/investigate/cyber/ncijtf

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- California IT Directory
  http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

California Highway Patrol Emergency Notification and Tactical Alert Center (ENTAC)
https://www.chp.ca.gov/notify-chp/computer-crime-reporting-for-state-agencies

Dell Secure Works, http://www.secureworks.com

FireEye, http://www.fireeye.com

IBM, http://www.ibm.com/security

Rapid7, http://www.rapid7.com

MITRE Corporation, http://www.mitre.org/capabilities/cybersecurity/situation-awareness

Northrop-Grumman,
http://www.northropgrumman.com/Capabilities/Cybersecurity/Pages/FullSpectrumCapabilities.aspx

XIII. Response and Recovery – *Rapid Recovery*

Volume 6- Service Continuity Management

Introduction:

This volume provides for the process of preparing for and responding to disruptive events of any type. These disruptions may be small, with little impact, or so large, that they affect the operation of the entire organization. This planning allows pre-defined procedures to sustain essential operations- the first priority for an organization. By assessing, prioritizing, planning and responding to, and improving plans, organizations prepare to maintain service continuity. The goal of this is mitigating the impact of disruptive events.

Establish and Maintain your Program:
Developing a plan for service continuity allows for the preparation of appropriate actions in the event of a disruption. The plan should not only document strategies but should also be used during the design of new services or systems. The plan should also be managed by each particular unit in order to provide for accountability.

After ensuring support for service continuity planning, the following four (4) steps should be taken:

- Manage program design and supporting documentation
- Oversee the business impact analysis process
- Monitor service continuity training and awareness activities
- Establish linkages to the incident response and recovery process

Planning:

After establishing your program, continuity plans are developed to document the steps taken in response to a disruption. The most important point is the identification of essential services, the establishment of service continuity requirements, and a guide to the recovery process during disruptions. This risk management activity depends heavily on both a Business Impact Analysis (BIA) and a risk assessment process. There are many forms of service continuity plans and each organization must determine the documents needed. These plans should be as detailed as necessary but should also be useable so that all personnel can carry out the activities when needed.

The following five (5) steps are key activities in developing a service continuity plan:

- Identify what type of service continuity plans to be developed
- Conduct service continuity planning activities
- Assign staff
- Establish a service continuity plan repository
- Define procedures for service continuity plan activation and execution

Validate and Exercise:

Once the plans have been developed, they should be validated to ensure they achieve resiliency requirements for the organization. The plans must be consistent, accurate, complete, and effective to meet standards and guidelines. An exercise strategy should be developed with determinations of rigor, frequency, stakeholder involvement, and which units or groups should participate together. The following six (6) key components of plan validation and exercise should include:

- Establish a plan review process
- Develop an exercise strategy, process, and schedule
- Exercise/execute service continuity plans
- Evaluate exercise/execution results
- Conduct an after-action review of plan activations and execution
- Perform service continuity training

Improve:

In order for service continuity to be successful, they require careful management. Regular reviews of strategies, standards, and methodologies will ensure that they also meet the organization's needs. As changes occur within the organization, modifications to the plans should be performed. Conducting regular exercises will allow for the consideration of various scenarios and provide a means for plan improvements. Service continuity improvement planning should include the following three (3) components:

- Review effectiveness of overall service continuity program
- Proactively identify conditions for revising service continuity plans
- Update and modify Plans

Service Continuity Management Resources

US Computer Emergency Readiness Team (US-CERT)
https://www.us-cert.gov/

- Continuity Planning
  https://www.us-cert.gov/sites/default/files/c3vp/csc-crr-question-set-and-guidance.pdf

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

- Incident Management
  http://www.cio.ca.gov/OIS/Government/incident.asp#Inci_Othr_Res
- Technology Recovery Management
  http://www.cio.ca.gov/OIS/Government/disaster.asp
- California IT Directory
  http://www.cio.ca.gov/Government/It_Directory/ITDirectory.html

California Governor's Office of Emergency Services (CAL OES)
Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

Ernst and Young
http://www.ey.com/GL/en/Services/Advisory/EY-cybersecurity-cyber-breach-response-management

XIV. Response and Recovery – *Rapid Recovery*

Volume 8- External Dependencies Management (EXD)

Introduction:

This volume focuses on establishing controls between organizations and their relationships with outside entities (including vendors, suppliers, shared public infrastructure, or other public services). These controls assist in the management of risks that come from or are related to the organization's dependence on these external entities. An important external dependency is the supply chain- while outsourcing of some purchases provides certain advantages; it may also introduce a certain level of uncertainty concerning operational resilience. Challenges exist between monitoring and controlling vulnerabilities and threats that may be introduced by external entities.

Develop a Plan for External Dependencies

Developing an External Dependency (EXD) plan requires extensive input and support at all levels in the organization. Once the organization's critical services and key assets have been identified, the plan can be developed. It should be widely reviewed, documented, distributed, and frequently updated. The following five (5) steps should be followed in the development of an EXD plan:

- Establish external dependencies support and strategy
- Plan the relationship formation process
- Plan a process for identifying and prioritizing external dependencies
- Plan relationship management
- Plan an information management process

Form Relationships and Implement Plan:

Organizations must establish strong working relationships with clearly defined agreements to clarify organizational needs and to aide vendors in understanding the organization's mission. Suppliers need to be monitored closely, organizations must approach these relationships as a reflection of the importance of the vendor, and the potential for failure should the supplier not meet requirements. Plan implementation should include all organizational resources and teams to integrate the plan. These teams may include: business units, project managers, contracts/legal teams, and asset management groups (among others).

The four (4) steps in this section include:

- Assign responsibility for implementing the plan
- Establish and maintain implementation measurements
- Formalize relationships with external entities
- Identify and prioritize dependencies

Managing Relationships:

Once the plan has been developed, the process is heavily dependent on managing relationships between the organization and the supplier. The structure of the relationships must be consistent and in accordance with the EXD plan and managed by the appropriate unit of the organization. These units should closely monitor external suppliers to ensure they are meeting defined needs. They should also always be prepared to take appropriate action when necessary, including changing vendors or bringing the activity back in-house.

Monitoring and Improving:

The EXD plan should include the program's objectives, policies, and standards as well as a process for monitoring performance. Consistent monitoring should verify that external vendors/suppliers are satisfactorily performing established requirements. These measures should be documented, tracked, and reviewed by the appropriate stakeholders. The four (4) components of this plan should include:

- Define effectiveness measures
- Detect, analyze, and correct process exceptions
- Report and review the program with stakeholders
- Improve the EXD program, plans, and procedures

Relationship and Cyber Information Resources:

United States Computer Emergency Readiness Team (US-CERT)

US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans.

US-CERT: http://www.us-cert.gov/
National Cyber Alert System: http://www.us-cert.gov/ncas

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

ICS-CERT provides a control system security focus in collaboration with US-CERT. ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts.

ICS-CERT: http://www.us-cert.gov/control_systems/ics-cert/
SCADA and Control Systems Procurement Language Project, September 2009, U.S. Department of Homeland Security National Cybersecurity and Communication Integration Center, ICS-CERT: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809.pdf
CSSP Training: http://ics-cert.us cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Traning-v12.pdf
Cyber Security Evaluation Tool (CSET): http://ics-cert.us-cert.gov/Assessments

National Cybersecurity and Communications Integration Center (NCCIC)

The NCCIC is a 24x7 center responsible for the production of a common operating picture for cyber and communications across federal, state, and local government; intelligence; law enforcement communities; and the private sector.

NCCIC: http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

Daily Open Source Infrastructure Report

Each business day, the DHS collects a summary of open-source published information concerning significant critical infrastructure issues.

Daily Open Source Infrastructure Report: http://www.dhs.gov/dhs-daily-open-source-infrastructure-report

Homeland Security Information Network (HSIN)

HSIN is a national secure and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

HSIN: http://www.dhs.gov/homeland-security-information-network

Multi-State Information Sharing and Analysis Center

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

MS-ISAC: http://msisac.cisecurity.org/resources/videos/free-training.cfm

United States Secret Service (USSS) Electronic Crimes Task Force (ECTF)

Partnership of not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. Its common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures.

USSS ECTF: http://www.secretservice.gov/ectf.shtml

Federal Bureau of Investigation (FBI) InfraGard

InfraGard, a partnership between the FBI and the private sector, is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members.

InfraGard: https://www.infragard.org/

Internet Crime Complaint Center (IC3)

The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). The IC3 provides a central point for internet crime victims to report to and alert an appropriate agency online at www.Ic3.gov. The IC3 collects, reviews, and refers internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts and identify current crime trends across the internet.

IC3: http://www.ic3.gov/default.aspx

iGuardian

The iGuardian portal, currently in its pilot stage, is available to 58,000 companies that make up the FBI's InfraGard network. If the pilot succeeds, the FBI plans to open it up to more organizations, probably at first in critical infrastructure sectors. Participating companies can submit a form online in the instance of a cybersecurity breach to their networks. The National Cyber Investigative Joint Taskforce (NCI-JTF) handles the information provided by these companies.

iGuardian: http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view
NCI-JTF: http://www.fbi.gov/about-us/investigate/cyber/ncijtf

Other Resources
DHS

National Strategy for Global Supply Chain Security:
http://www.dhs.gov/national-strategy-global-supply-chain-security

Office of Cybersecurity and Communications:
http://www.dhs.gov/office-cybersecurity-and-communications

Critical Infrastructure Cyber Community C³ Voluntary Program:
https://www.us-cert.gov/ccubedvp

Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach:
http://www.dhs.gov/publication/executing-critical-infrastructure-risk-management-approach
Office of Cyber & Infrastructure Analysis:
http://www.dhs.gov/office-cyber-infrastructure-analysis

Federal Emergency Management Agency (FEMA)
http://www.fema.gov/

Federal Financial Institutions Examination Council (FFIEC)
http://www.ffiec.gov/

Supervision of Technology Service Providers:
http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_SupervisionofTechnologyServiceProviders(TSP).pdf

Federal Reserve Board Guidance on Managing Outsourcing Risk
http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

Gartner (requires subscription)
Operational Risk Blog: http://www.gartner.com/technology/home.jsp

Forrester
Risk management articles, tools, and templates (some require a fee):
http://www.forrester.com/home/

International Organization for Standardization (ISO)
http://www.iso.org/iso/home.html

ISO/IEC 27036:2013+ — IT Security — Security techniques — Information security for supplier relationships (parts 1, 2 & 3 published, remainder in draft.
http://www.iso27001security.com/html/27036.html

ISO 28000 series of standards on supply chain security management system
http://www.iso.org/iso/home/search.htm?qt=28000&sort=rel&type=simple&published=on

27002: Outlines potential cybersecurity controls and control mechanisms (fee)
http://www.27000.org/iso-27002.htm

Information Systems Audit and Control Association (ISACA)
http://www.isaca.org
Control Objectives for Information and Related Technology (COBIT) 5, AP008 – Manage Relationships
http://www.isaca.org/COBIT/Pages/default.aspx

Information Technology Infrastructure Library (ITIL) 2011, Service Strategy, Supplier Design
http://www.itil-officialsite.com/

National Institute of Standards and Technology (NIST)
http://www.nist.gov/index.html

NIST Computer Security Division, Computer Security Resource Center
http://csrc.nist.gov/

NIST Special Publication 800-161, "Supply Chain Risk Management Practices for Federal Information Management Systems"
http://csrc.nist.gov/publications/drafts/800-161/sp800_161_draft.pdf

NISTIR 7622, "Notional Supply Chain Risk Management Practices"
http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf

NIST Special Publication 800-30, Guide for Conducting Risk Assessments for Federal Information Systems and Organizations
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

NIST Special Publication 800-39, Managing Information Security Risk http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NIST Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations"
http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

NERC/FERC
http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Software Engineering Institute, CERT Division
http://www.cert.org
CERT Resilience Management Model
http://www.cert.org/resilience/rmm.html

CMMI for Acquisition, Version 1.3
http://www.sei.cmu.edu/reports/10tr032.pdf

California Department of Technology Information Security Office
http://www.cio.ca.gov/ois/

California Governor's Office of Emergency Services (CAL OES) Cyber Security Task Force
http://www.caloes.ca.gov/Cal-OES-Divisions/Cybersecurity-Task-Force

- California IT Directory

California National Guard

- California National Guard Cyber Network Defense
  http://www.calguard.ca.gov/J6/Pages/Cyber-Network-Defense.aspx
- California National Guard Cyber Defense, Support Services Brochure
  http://www.calguard.ca.gov/J6/Documents/CND%20InfoFlyer.pdf

XV. Appendices

Appendix 1: Terms and Definitions

Appendix 2: Sample Cyber Security Training Presentation

Appendix 3: Sample Incident Management Templates

Appendix 4: Fusion Centers by FEMA Region

Appendix 1: Terms and Definitions

Access Control Mechanism – Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system. SOURCE: CNSSI-4009.

Active Attack – An attack that alters a system or data. SOURCE: CNSSI-4009. An attack on the authentication protocol where the Attacker transmits data to the Claimant, Credential Service Provider, Verifier, or Relying Party. Examples of active attacks include man-in-the-middle, impersonation, and session hijacking. SOURCE: SP 800-63.

Advanced Encryption Standard (AES) –The Advanced Encryption Standard specifies a U.S. government approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. SOURCE: FIPS 197.

Advanced End Point Threat Detection – Advanced end point threat detection services provide monitoring support for endpoints to detect signs of advanced threat actor activity. In addition, threat intelligence is maintained in real time and updates such as virus signatures, are updated automatically. In the event of a breach, forensic analysis services and provided and resolution recommendations are communicated.

Advanced Malware Protection and Detection – Advanced malware protection services provide 24x7 monitoring by a dedicated team of analysts. The analysts leverage real and historical visibility into the network traffic to detect malware signatures, events and trends. Event analysis and compliance reporting is supplied. Custom services integrate with existing security devices and critical information assets.

Advanced Persistent Threats (APT) – An adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. SOURCE: SP 800-39.

Anomaly-Based Detection – The process of comparing definitions of what activity is considered normal against observed events to identify significant deviations. SOURCE: SP 800-94.

Attack Signature – A specific sequence of events indicative of an unauthorized access attempt. SOURCE: SP 800-12 A characteristic byte pattern used in malicious code or an indicator, or set of indicators, that allows the identification of malicious network activities. SOURCE: CNSSI-4009.

Baseline Configuration – A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. SOURCE: SP 800-128.

Business Impact Analysis (BIA) – An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. SOURCE: SP 800-34. An analysis of an enterprise's requirements, processes, and interdependencies used to characterize information system contingency requirements and priorities in the event of a significant disruption. SOURCE: CNSSI-4009.

Chief Information Security Officer (CISO) - the senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected. The CISO directs staff in identifying, developing, implementing and maintaining processes across the organization to reduce information and information technology (IT) risks. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance.

Compensating Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system. SOURCE: SP 800-37 The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253, that provide equivalent or comparable protection for an information system. SOURCE: SP 800-53A; SP 800-53.

Configuration and Change Management Plan (CCMP) - the process in which changes to CIs are developed and implemented, including requests, approvals, monitoring, and improvement.

Configuration Control Review Board (CCRB) - a group within the organization and made up of stakeholders who assess prioritize, authorize, and make/schedule changes to the CIs.

Configuration Item (CI) - asset or assets place under configuration management.

Contingency Plan – Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. SOURCE: CNSSI-4009.

Critical Infrastructure - PPD 21 defines the meaning of critical infrastructure as provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. PPD -21 identifies 16 Critical Infrastructure Sectors: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams;Defense Industrial Base; Emergency Services; *Energy*; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste, Transportation Systems; *Water and Wastewater Systems*.

Cyber Security Managed Services - Many organizations lack the appropriate skills necessary to define, implement and operate appropriate levels of data protection and privacy-specific security controls. This lack of skills leads organizations to contract security consulting firms that specialize in data protection and security risk management to address regulatory compliance demands and enhance their security postures. A significant portion of organizations are shifting existing resources away from the operational aspects of security technologies, such as security device administration and monitoring, toward mitigation and incident response. This new dynamic has given rise to significant growth throughout the globe for managed security services. Managed security services provide a systematic approach to managing an organization's security needs. The services may be conducted in-house or outsourced to a service provider that oversees other companies' network and information system security. Functions of a managed security service include round-the-clock monitoring and management of intrusion detection systems and firewalls, overseeing patch management and upgrades, performing security assessments and security audits, and responding to emergencies. SOURCE: Gartner.

Data Encryption Standard (DES) – Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard (FIPS) Publication 46. (FIPS 46-3 withdrawn 19 May 2005) See Triple DES. SOURCE: CNSSI-4009.

Defense-in-Depth – Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. SOURCE: CNSSI-4009; SP 800-53.

Disaster Recovery Plan (DRP) – A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities. SOURCE: SP 800-34 Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days. See Continuity of Operations Plan and Contingency Plan. SOURCE: CNSSI-4009.

Distributed Denial of Service (DDoS) - A Denial of Service technique that uses numerous hosts to perform the attack. SOURCE: CNSSI-4009

Downstream Natural Gas - IInformation Sharing Analysis Center (DNG-ISAC) - The DNG-ISAC serves natural gas utility (distribution) companies by facilitating communications between participants, the federal government, and other critical infrastructures. Specifically, the DNG-ISAC coordinates very closely with the ES (Electricity Sector) ISAC and shares information back and forth between electric, combination (natural gas and electric) and natural gas utilities. The DNG-ISAC promptly disseminates threat information and indicators from government and other sources and provides analysis, coordination and summarization of related industry-affecting information. (https://www.dngisac.com/)

Electricity Sector - Information Sharing Analysis Center (ES-SAC) - The ES-ISAC serves the Electricity Sector by facilitating communications between electricity sector participants, federal governments, and other critical infrastructures. It is the job of the ES-ISAC to disseminate promptly threat indications, analyses, and warnings, together with interpretations, to assist electricity sector participants take protective actions. (https://www.esisac.com/SitePages/Home.aspx)

Enterprise Risk Management – The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures as necessary. SOURCE: CNSSI-4009.

External Security Testing – Security testing conducted from outside the organization's security perimeter. SOURCE: SP 800-115

Federal Departments and Agencies - Per PPD21 this means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

Full Disk Encryption (FDE) – The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. SOURCE: SP 800-111.

Honeypot – A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators. SOURCE: CNSSI-4009.

Incident Response Plan – The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyberattacks against an organization's information system(s). SOURCE: SP 800-34. The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of an incident against an organization's IT system(s). SOURCE: CNSSI-4009.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works to reduce risks within and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among Federal, state, local, and tribal governments and control systems owners, operators, and vendors. Additionally, ICS-CERT collaborates with international and private sector Computer Emergency Response Teams (CERTs) to share control systems-related security incidents and mitigation measures. (https://ics-cert.us-cert.gov/)

Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA) - According to National Institute of Standards (NIST) Special Publication 800-82 ICS, Guide to Industrial Control Systems (ICS) Security, ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control.

Managed Vulnerability Scanning and Penetration Testing – Managed vulnerability scanning and penetration testing services provide vulnerability assessments for servers, network hardware and software on both the internal and external network segments. Detailed reports are provided to identify vulnerabilities and remediation options. Physical, virtual and cloud environments can be scanned. Penetration testing utilizes targeted attempts to reach network resources using multiple attack vectors. Penetration testing reports identify vulnerabilities and provide recommendations to resolve. Scanning complies with requirements to satisfy PCI, HIPAA, and GLBA.

National Cybersecurity and Communications Integration Center (NCCIC) - a division of the Department of Homeland Security's (DHS) National Protection and Programs Director(NPPD). NCCIC's mission is to operate at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities, applying unique analytic perspectives, ensuring shared situational awareness, and orchestrating synchronized response efforts while protecting the Constitutional and privacy rights of Americans in both the cybersecurity and communications domains. (ww.dhs.gov/about-national-cybersecurity-communications-integration-center)

National Cyber Investigative Joint Task Force (NCIJTF). The FBI is responsible for the operation of the NCIJTF. NCIJTF serves as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations, with representation from DHS, the Intelligence Community (IC), the Department of Defense (DOD), and other agencies as appropriate. The Attorney General and the Secretary of Homeland Security shall collaborate to carry out their respective critical infrastructure missions. (www.fbi.gov/about-us/investigate/cyber/ncijtf)

National Infrastructure Protection Plan (NIPP 2013) - outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. The 2013 update is informed by significant evolution in the critical infrastructure risk, policy, and operating environments, as well as experience gained and lessons learned since the NIPP was last issued in 2009. The *National Plan* builds upon previous NIPPs by emphasizing the complementary goals of security and resilience for critical infrastructure. To achieve these goals, cyber and physical security and the resilience of critical infrastructure assets, systems, and networks are integrated into an enterprise approach to risk management. (http://www.dhs.gov/national-infrastructure-protection-plan)

Oil and Natural Gas - Information Sharing Analysis Center (ONG-ISAC) - ONG-ISAC is the central reservoir of cyber threat information for the oil and natural gas industry. It protects the industry's exploration and production, transportation, refining, and delivery systems from cyber-attacks through the analysis and sharing of timely and trusted cyber intelligence. As an industry owned and operated organization, ONG-ISAC provides a pipeline for members to share information anonymously across its membership, increasing the speed, quality, and flow of cyber intelligence. (www.isaccouncil.org)

Presidential Policy Directive 21 (PPD-21), "Critical Infrastructure Security and Resilience" - The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. (www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

Resilience - PPD-21 defines resilience as the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Sector-Specific Agency - SSA is the Federal department or agency designated under PPD-21 to be responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

Secure and Security - Refer to reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or manmade disasters according to PPD-21.

Water Information Sharing and Analysis Center (WaterISAC) – The WaterISAC was authorized by Congress in 2002 and created and managed by the water sector. Its mission is to keep drinking water and wastewater utility managers informed about potential risks to the nation's water infrastructure from contamination, terrorism, and cyber threats. The mission has been expanded to help utilities respond to and recover from all hazards. Funded by subscriber fees and matching federal funds, WaterISAC links members through a secure online portal. The subscriber base includes water utilities and state and federal agencies dealing with security, law enforcement, intelligence, the environment, and public health. (www.isaccouncil.org)

Appendix 2: Sample Cyber Security Training Presentation

From this course you will NOT:

- Learn to code and read Binary
- Know how to jailbreak your Iphone
- Configure a firewall
- Know the difference between SQL Injections and Cross-Site Scripting

You Will…

- Understand the need for Cyber Awareness programs at your agency
- Know the various ways end-users are targeted by the bad guys
- Have the tools to establish a Cyber Awareness program at your agency

We have an IT Department, isn't that enough?

A Few Facts to Illustrate the Threat to End-Users:

- 23% of users open "phishing" emails and 11% open the attachments*
- The top three industries affected by data breaches are Public, Information, and Financial Services, but no industry is immune*
- The theft/loss of electronic devices is a significant vector for data loss and breaches. Most theft occurred within a victim's work area (55%) but, employee-owned vehicles (22% of incidents) were also a common location*
- The Twitter and YouTube accounts of the US Central Command were most likely hacked because the military was using simple passwords.

*2015 Verizon Data Breach Report

Why target the end-user?

- Low hanging fruit
- Lack of training and awareness
- Use access to escalate privileges or deliver malware to the network

You ARE a Target

- SOCIAL ENGINEERING
- CREDENTIALS (PASSWORDS!)
- THEFT/LOSS/MISUSE OF DEVICES

Social Engineering – manipulating people to give up confidential information

WHALING

SHOULDER SURFING

PHISHING

IMPERSONATION

BAITING

SMISHING

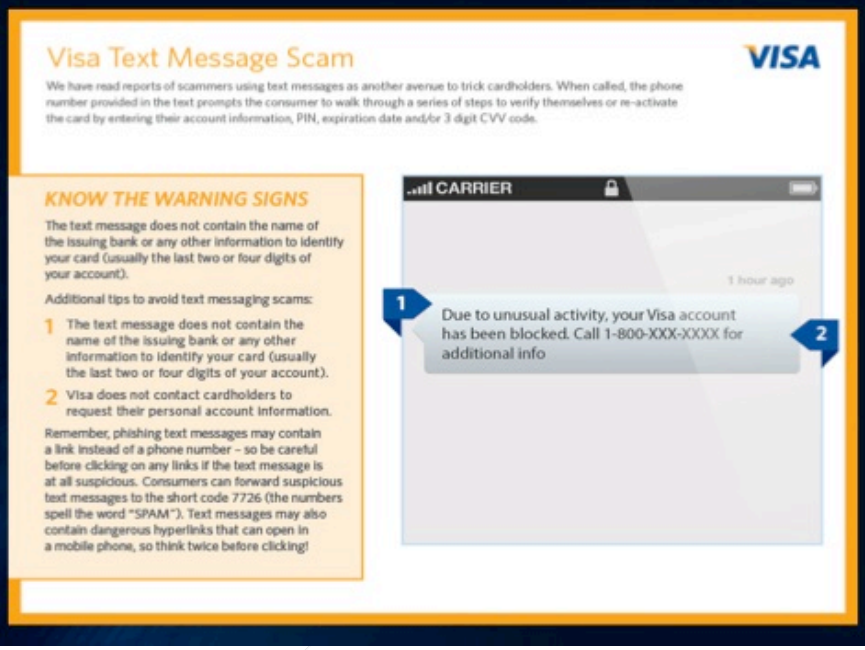
TAILGATING

VISHING

SPEAR-PHISHING

Vishing

Smishing



Visa Text Message Scam

VISA

We have read reports of scammers using text messages as another avenue to trick cardholders. When called, the phone number provided in the text prompts the consumer to walk through a series of steps to verify themselves or re-activate the card by entering their account information, PIN, expiration date and/or 3 digit CVV code.

KNOW THE WARNING SIGNS

The text message does not contain the name of the issuing bank or any other information to identify your card (usually the last two or four digits of your account).

Additional tips to avoid text messaging scams:

1. The text message does not contain the name of the issuing bank or any other information to identify your card (usually the last two or four digits of your account).
2. Visa does not contact cardholders to request their personal account information.

Remember, phishing text messages may contain a link instead of a phone number – so be careful before clicking on any links if the text message is at all suspicious. Consumers can forward suspicious text messages to the short code 7726 (the numbers spell the word "SPAM"). Text messages may also contain dangerous hyperlinks that can open in a mobile phone, so think twice before clicking!

CARRIER

1 hour ago

1 Due to unusual activity, your Visa account has been blocked. Call 1-800-XXX-XXXX for additional info 2

Phishing

CHASE

Dear Customer,

Currently we are trying to upgrade our on-line security measures. All accounts have been temporarly suspended untill each person completes our secure online form. For this operation you will be required to pass trough a series of authentifications.

We won't require your ATM PIN number or your name for this operation!

To begin unlocking your account please click the link below.

https://www.chase.com/security/do_auth.jsp

Please note:
If we don't receive your account verification within 72 hours from you, we will further lock down your account untill we will be able to contact you by e-mail or phone.

2006 JPMorgan Chase & Co.

TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Spam vs Phishing:

- Phishing is a specific type of spam… unsolicited emails
- Not all SPAM is malicious…but assume it is
- SPAM can be used to spread malware like viruses, trojans, and worms
- SPAM can misdirect end-users to spoofed websites

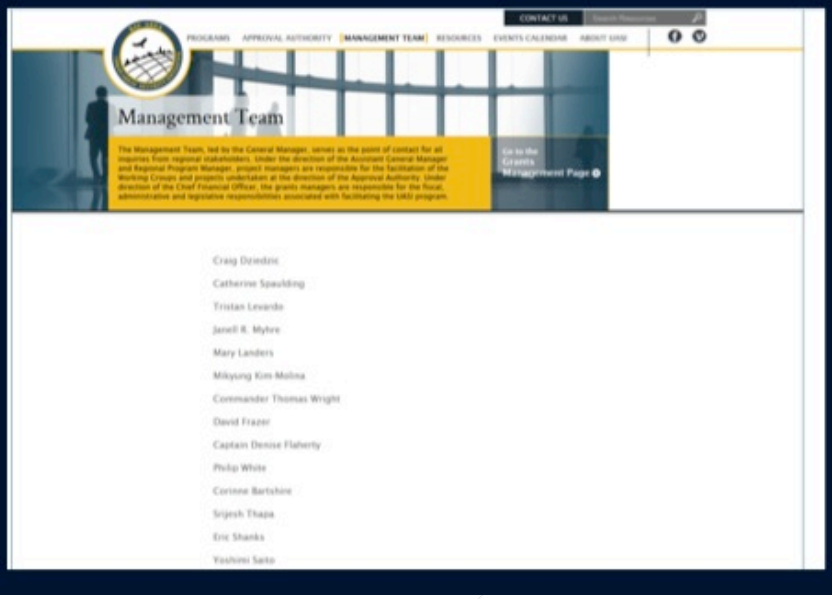
Managing Your Online Presence:

- Know your Social Media Footprint
  - Name, family, hobbies, employment, location

- What is PRIVATE and what is PUBLIC – you may be surprised

- People Search websites- like Spokeo, piple, etc. aggregate personal information

For Example the Bay Area UASI…

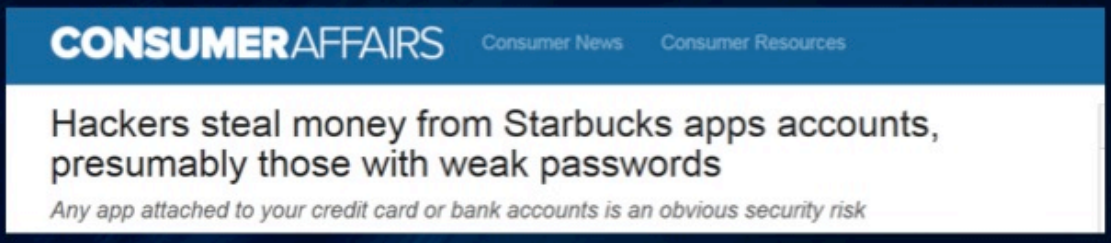


How to Combat Social Engineering:

- End-Users need to be aware of these tactics
  - Recognize Social Engineering attempts
  - Look out for spoofed emails or websites
  - Think before you link.
- End-Users need to understand the value of the information they have access to
- End-Users need to know who to report to regarding potential social engineering attempts

COMPLEX and PROTECTED PASSWORDS

- Social Engineering
- Guessing
- Dictionary Attacks

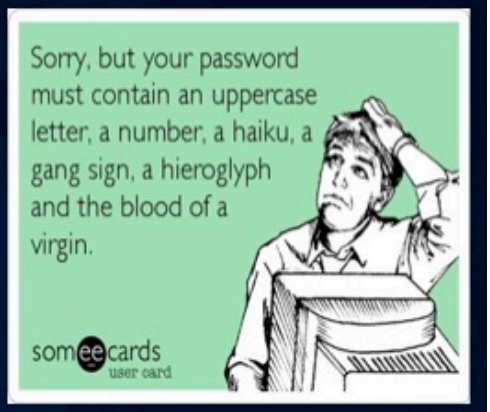


The Top 25 Passwords from 2014:

Rank	Password
1	123456
2	password
3	12345
4	12345678
5	qwerty
6	123456789
7	1234
8	baseball
9	dragon
10	football
11	1234567
12	monkey
13	letmein
14	abc123
15	111111
16	mustang
17	access
18	shadow
19	master
20	michael
21	superman
22	696969
23	123123
24	batman
25	trustno1

What does a strong password look like?

- Numb3Rs, L#tT3R$, Sp#c1@1 cHArAcT3R$
- 8+ characters in length (passphrase)
- Unique for every site/program/platform
- Two-Factor Authentication when possible
- Changed regularly



What to avoid:

- Using pet names, birthdays, spouse name, anniversaries, etc… Remember Social Engineering
- Complete words
- Writing it on a sticky note and put it on your monitor (this still happens far too frequently)
- Sharing passwords

Managing multiple accounts/passwords

- Use a base or template for your passwords
- Password Management Tools

Securing Devices

- BYOD Concerns
- Connecting to WiFi
- Theft or loss of devices
- Securing the data

What's being plugged into the Agency Network?

- Infected USB or disks
- Same security practices for home and office being enforced?
- Where is sensitive data residing?

- What is your Agency's Policy
- Do your employees know the policy?
- Have they been taught the policy?

Public WiFi Risks

- Man-in-the-Middle Attacks
- Distribution of malware

- Does your agency offer VPN?
- Does you Agency have policies about remote access?
- Have they been taught the policy?

Theft/Loss/Neglect of Devices

- The theft of two unencrypted laptop computers from Horizon Blue Cross Blue Shield of New Jersey resulted in the breach of information of nearly 840,000 individuals.
- The Insider Threat must also be considered—is your desktop locked when you walk away?
  - Who should an employee report lost or stolen devices to? Do they know?
  - Are your portable devices encrypted or have the capability for remote swiping
  - How secure are your offices and server rooms?

Better Preparing The End-User

- Creating Policies and Expectations
- Training to those Policies and Expectations
- Reinforcing that training periodically

Policies and Expectations

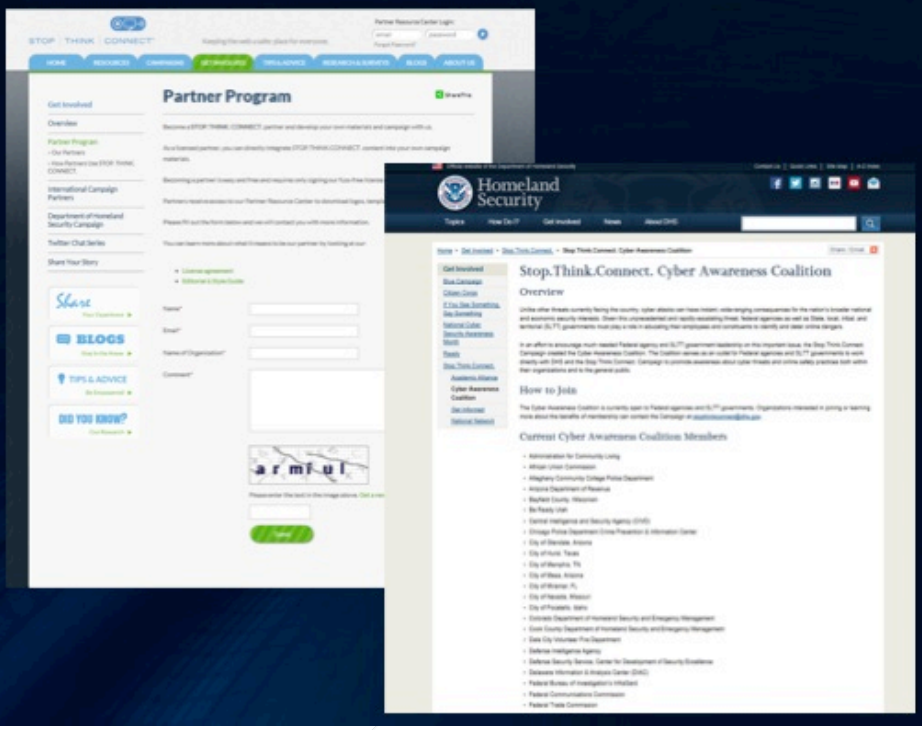
- Agencies will differ but the need for basic cyber security awareness is universal for all employees who are provided access the Agency's Network
  - Awareness campaign-flyers, posters, email reminders
  - Training, online or class based
- Is there a policy or guidance in place already or does one need to be created
  - SecuringtheHuman.org provides an example roadmap
- Who is responsible for leading the cyber security awareness program in your agency- IT, Security, Human Resources, etc.?

Resources

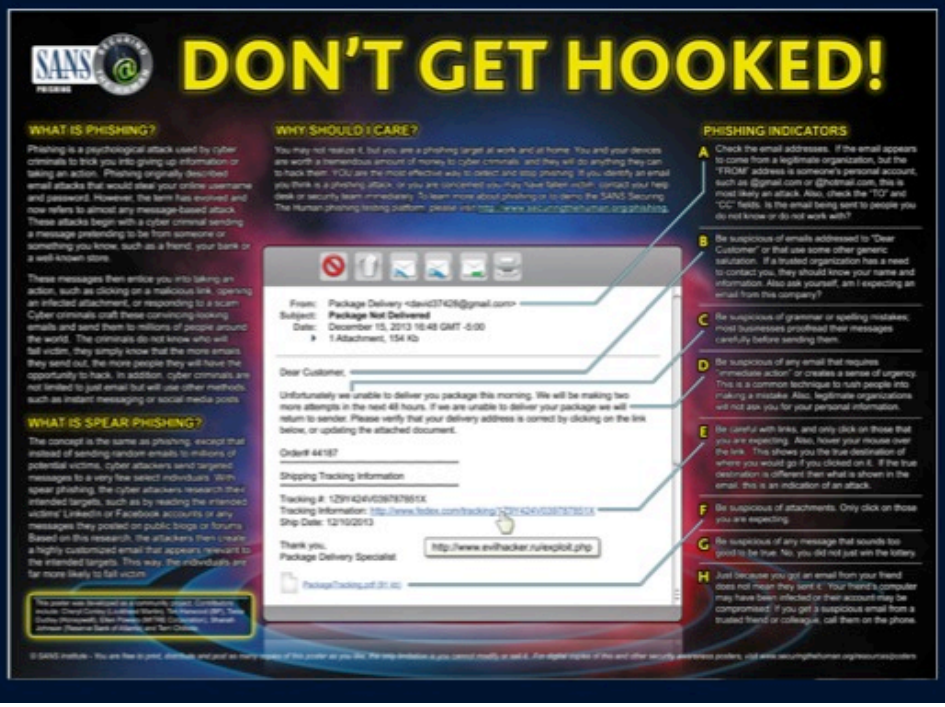
- StopThinkConnect Program
- SecuringtheHuman.org from SANs—free and paid services
- DHS/FEMA Funded Online Courses through TEEX (AWR175 Information Security for Everyone)
- National Cyber Security Alliance StaySafeOnline.org
- Multi-State Information Sharing & Analysis Center
- US-CERT-Protect Your Workplace Campaign

StopThinkConnect.org

Posters, Tip Sheets, Videos and more



Free Resources from SANS Securingthehuman.org



TEEX

StaySafeOnline.org

MS-ISAC

- Discounted Training for Public Sector Organizations (SANS SecuringtheHuman)
- Cyber Security Training Vidoes—Awareness and Cyber Security for Business Managers
- Cyber Security Guides

US-CERT
Protect Your Workplace Campaign

Physical Security Guidance

Monitor and control who is entering your workplace: current employees, former employees, commercial delivery, and service personnel.

Check for identification and ask individuals to identify the purpose of their visit to your workplace.

Report broken doors, windows, and locks to your organization's or building's security personnel as soon as possible.

Back up or copy sensitive and critical information and databases.

Store, lock, and inventory your organization's keys, access cards, uniforms, badges, and vehicles.

Monitor and report suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, garages, and immediate vicinity.

Report suspicious packages to your local police. DO NOT OPEN or TOUCH!

Shred or destroy all documents that contain sensitive personal or organizational information that is no longer needed.

Keep an inventory of your most critical equipment, hardware, and software.

Store and lock your personal items such as wallets, purses, and identification when not in use.

Cybersecurity Guidance

Employees

- Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
- Change your passwords regularly (every 45 to 90 days).
- Do NOT give any of your usernames, passwords, or other computer/ website access codes to anyone.
- Do NOT open emails, links, or attachments from strangers.
- Do NOT install or connect any personal software or hardware to your organization's network without permission from your IT department.
- Make electronic and physical back-ups or copies of all your important work.
- Report all suspicious or unusual problems with your computer to your IT department.

Leadership & IT Professionals

- Implement Defense-in-Depth: a layered defense strategy includes technical, organizational, and operational controls.
- Establish clear policies and procedures for employee use of your organization's information technologies.
- Implement Technical Defenses: firewalls, intrusion detection systems, and Internet content filtering.
- Update your system's anti-virus software daily.
- Regularly download vendor security "patches" for all of your software.
- Change the manufacturer's default passwords on all of your software.
- Monitor, log, analyze, and report successful and attempted intrusions to your systems and networks.

Report Suspicious Behavior and Activity

Surveillance: Are you aware of anyone recording or monitoring activities, taking notes, using cameras, maps, binoculars, etc., near a key facility?

Deploying Assets: Have you observed abandoned vehicles, stockpiling of suspicious materials, or persons being deployed near a key facility?

Suspicious Persons: Are you aware of anyone who does not appear to belong in the workplace, neighborhood, business establishment, or near a key facility?

Suspicious Questioning: Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding a key facility or its personnel?

Tests of Security: Are you aware of any attempts to penetrate or test physical security or procedures at a key facility?

Acquiring Supplies: Are you aware of anyone attempting to improperly acquire explosives, weapons, ammunitions, dangerous chemicals, uniforms, badges, flight manuals, access cards, or identification to a key facility? Are you aware of anyone attempting to legally obtain items under suspicious circumstances that could be used in a terrorist act?

Dry Runs: Have you observed any suspicious behavior that appears to be preparation for terrorist activity, such as mapping out routes, playing out scenarios with other people, monitoring key facilities, timing traffic lights and traffic flow, or other suspicious activities?

Report Suspicious Cyber Incidents

System Failure or Disruption: Has your system or website's availability been disrupted? Are your employees, customers, suppliers, or partners unable to access your system or website? Has your service been denied to its users?

Suspicious Questioning: Are you aware of anyone attempting to gain information in person, by phone, mail, email, etc., regarding the configuration and/or cybersecurity posture of your website, network, software, or hardware?

Unauthorized Access: Are you aware of anyone attempting (either failed or successful) to gain unauthorized access to your system or data?

Unauthorized Changes or Additions: Has anyone made unauthorized changes or additions to your system's hardware, firmware, or software characteristics without your IT department's knowledge, instruction, or consent?

Suspicious Email: Are you aware of anyone in your organization receiving suspicious emails that include unsolicited attachments and/or requests for sensitive personal or organizational information?

Unauthorized Use: Are unauthorized parties using your system for the processing or storage of data? Are former employees, customers, suppliers, or partners still using your system?

Cyber Security Takeaways:

- The IT Department cannot do it alone. Everyone connected to a network has a role to play in maintaining security.
- Give your end-users the knowledge to act responsibly. Do not assume they know the dangers lurking in the cyber realm.
- There are free resources out there to get any agency, large or small, started in creating a cyber awareness program. Placing a poster in break rooms about phishing scams is a start. An email reminder about using strong passwords takes minutes.

Appendix 3: Sample Incident Management Templates

Sample Incident Management Plan Template

<Organization name> Incident Management Plan

Date: _____ Name of person completing this form: _____

Executive Support

List the executives who had input to this document and endorse its development and applicability.

Name of executive	Date	Signature
Sponsor		
Incident Manager		

Process Description

Explain the incident management process in a manner that provides a high-level understanding to personnel who must implement this plan.

Critical Services

Indicate the priority of critical services.

Priority level	***Service restoration time objective***

Plan Activation Criteria

Describe conditions that must be met before the incident management plan can be executed.

Assignment of Responsibility

List employees at your organization who are responsible for developing and maintaining this plan.

Name of employe	Date	Signature	Responsibility

Communication Channels

Identify communication channels to be used to notify stakeholders if this plan is to be executed.

Key Contacts

List the key contact information essential to the service and this plan. Include the service owner as well as internal and external technical support (examples embedded).

Name	Role	Company name	Phone 1	Phone 2
	Service owner			
	Internal technical support for information assets			
	Internal technical support for technology assets			
	External support for information assets			
	External technical support for technology assets			
	Hardware vendor			
	Primary software vendor			
	Fire company			
	Police			
	Alternate processing site contact			
	Electric utility POC			
	Telecommunications POC			
	Water utility POC			
	Executive management			
	Legal counsel			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Internal resource for continuity plan execution			
	Stakeholder who requires notification of plan activation			

	Stakeholder who requires notification of plan activation			
	Stakeholder who requires notification of plan activation			
	Regulatory organizations that require notification if this plan is activated			
	Healthcare providers who should be notified if this plan is activated			
	Other organizations that should be notified if this plan is activated			

Service Owner(s)

List the business owner(s) responsible for critical services.

Name of employe	Date	Signature	Role

Essential Roles and Alternates

Identify roles essential for incident management, as well as primary and backup/alternate personnel to perform those roles.

Role	Primary personnel	Alternate personnel

Essential Information Assets

List the information assets essential to incident management.

Information asset name	Description	Logical location	Physical location	Backup strategy and schedule

Special Considerations for Information Assets

Identify any special considerations for handling information assets in the event of plan activation.

Essential Technology Assets

List the technology assets essential to incident management.

Asset name	Description	Physical location	Backup strategy/location

Primary and Alternate Site(s)

Identify the location(s) for command, control, and communication.

Site name	Physical location

Incident Management Checklist

List the steps to follow when obtaining an incident status (examples embedded).

Issue	Responsible party	Guidance	Status
Safety	Security, HR, Facilities		
Physical damage			
Business impact			
Immediate actions			
Media attention			

Plans of Action

List the predetermined plans and procedures to be relied on during an incident (examples embedded).

Fire and evacuation	Instruct personnel to evacuate the immediate area. Locate available fire extinguishers if possible and contact fire department.
Communications/media	
Health and safety	
Disaster recovery	
Service continuity	
Cybersecurity	
Physical security	
Pandemic	
Emergency procurement and transportation	

Schedule for testing this plan
This plan will be tested <at a defined frequency> Date of last test <YYYY/MM/DD>

Identify any support plans that are related to this plan.

Plan name	Relationship

Appendix 4: Fusion Centers by FEMA Region

Another cyber security resource for utility managers is the region's Fusion Center. Fusion Centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and coordination between agencies within the Federal Government like the Federal Bureau of Investigation (FBI) and the Drug Enforcement Agency (DEA) and state, local, tribal, territorial (SLTT) and private sector partners.

They are located in states and major urban areas throughout the country to assist front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel. Fusion centers also provide interdisciplinary expertise and situational awareness to inform decision-making at all levels of government. They conduct analysis and facilitate information sharing while assisting in preventing, protecting against, and responding to crime and terrorism.[10]

A national network of fusion centers (78 in all) exist in the United States and its Territories. Many of these centers are developing Cyber Integration Plans to provide assistance to local and state jurisdictions to prepare for and respond to malicious cyber activity. Produced in May 2015, the "Cyber Integration for Fusion Centers" plan was developed. In the plan are recommended actions and guidance for state and major urban area fusion centers (fusion centers) to integrate information technology, cybersecurity, and cybercrime prevention (cyber) intelligence and analytic capabilities. The plan contains protocols to be followed and seeks collaboration with all potential cyber partners. It also defines the skill set required by fusion center analysts and has developed a Fusion Center Cyber Toolkit. This document can be found at: http://www.cisecurity.org/documents/CyberIntegrationforFusionCenters_000.pdf. For more information on the national network of fusion centers, please see: http://www.dhs.gov/national-network-fusion-centers-fact-sheet.

[10] Department of Homeland Security Website

FEMA Region 1	Connecticut Maine Massachusetts New Hampshire Rhode Island Vermont	FEMA Region 6	Arkansas Louisiana New Mexico Oklahoma Texas
FEMA Region 2	New Jersey New York Puerto Rico U.S. Virgin Islands	FEMA Region 7	Iowa Kansas Missouri Nebraska
FEMA Region 3	Delaware Maryland Pennsylvania Virginia Washington, DC West Virginia	FEMA Region 8	Colorado North Dakota South Dakota Utah
FEMA Region 4	Alabama Florida Georgia Kentucky Mississippi North Carolina South Carolina Tennessee	FEMA Region 9	Arizona California Guam Hawaii Nevada
FEMA Region 5	Illinois Indiana Michigan Minnesota Ohio Wisconsin	FEMA Region 10	Alaska Idaho Montana Oregon Washington

FEMA Region 1 Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, Vermont		
Connecticut Intelligence Center (CTIC)	**Maine Information and Analysis Center (MIAC)**	**Commonwealth Fusion Center (CFC)**
Hartford, Connecticut	Augusta, Maine 04330-0164	Maynard, Massachusetts
Phone: (860) 706-5500	Phone: (207) 624-7280	Phone: (978) 451-3711
Fax: (806) 706-5535	Toll-Free: (877) 786-3636	Alt Phone: (978) 451-3700
ctic@ct.gov	intel.msp@maine.gov	fusion@massmail.state.ma.us
http://www.ct.gov/demhs		
Boston Region Intelligence Center (BRIC)	**New Hampshire Information and Analysis Center (NHIAC)**	**Rhode Island State Fusion Center (RISFC)**
Boston, Massachusetts	Concord, New Hampshire	Providence, Rhode Island
Phone: (617) 343-4328	Phone: (603) 271-0300	Phone: (866) 490-8477
bric.bpd@cityofboston.gov	nh.iac@dos.nh.gov	Fax: (401) 458-1173
http://www.mbhsr.org/	http://www.nh.gov/safety/information-analysis-center	fusion@risp.dps.ri.gov
Vermont Intelligence Center (VIC)		
Williston, Vermont		
Phone: (802) 872-6110		
dps.VIC@state.vt.us		
http://www.dps.state.vt.us		

FEMA Region 2 New Jersey, New York, Puerto Rico, U.S. Virgin Islands		
New Jersey Regional Operations Intelligence Center (NJROIC)	**New York State Intelligence Center (NYSIC)**	**National Security State Information Center (NSSIC)**
West Trenton, New Jersey	East Greenbush, New York	Hato Rey, Puerto Rico
Phone: (609) 963-6900	Phone: (866) 723-3697	Phone: (787) 793-1234
roic@gw.njsp.org	ciu@nysic.ny.gov	nssic@policia.pr.gov
U.S. Virgin Islands Fusion Center		
St. Thomas, Virgin Islands		
Phone: (340) 776-3013		
fusioncenter@vitema.vi.gov		

FEMA Region 3 Delaware, Maryland, Pennsylvania, Virginia, Washington, DC, West Virginia		
Delaware Information and Analysis Center (DIAC)	**Maryland Coordination and Analysis Center (MCAC)**	**Delaware Valley Intelligence Center (DVIC)**
Dover, Delaware	Woodlawn, Maryland	Philadelphia, Pennsylvania
Fax: (302) 739-1609	Phone: (800) 492-8477	Phone: (267) 322-4131
Alt Phone: (302) 739-5996	mdwatch@leo.gov	Fax: (215) 717-3263
Toll-Free: (800) 367-2312	http://www.mcac.maryland.gov	dvic@phila.gov
mailto:diac@state.de.us		Phone: (800) 492-8477
www.dediac.org		mdwatch@leo.gov
Pennsylvania Criminal Intelligence Center (PaCIC)	**Southwestern Pennsylvania Region 13 Fusion Center**	**Northern Virginia Regional Intelligence Center (NVRIC)**
Harrisburg, Pennsylvania	Pittsburgh, Pennsylvania	Fairfax, Virginia
Phone: (877) 777-6835	Phone: (412) 473-2550	Phone: (703) 212-4590
sp-intelligence@pa.gov		fcpdnvric@fairfaxcounty.gov
http://www.psp.pa.gov		
Virginia Fusion Center (VFC)	**Washington Regional Threat Analysis Center (WRTAC)**	**West Virginia Intelligence Fusion Center (WVIFC)**
North Chesterfield, Virginia	Washington, DC, Washington DC	Charleston, West Virginia
Phone: (804) 674-2196	Phone: (202) 481-3075	Phone: (304) 558-4831
vfc@vsp.virginia.gov	wrtac@dc.gov	wvfusion@wv.gov
http://www.vsp.state.va.us/Fusion Center		http://www.fusioncenter.wv.gov

FEMA Region 4 Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, Tennessee		
Alabama Fusion Center	**Florida Fusion Center (FFC)**	**Central Florida Intelligence Exchange (CFIX)**
Montgomery, Alabama	Tallahassee, Florida	Orlando, Florida
Phone: (334) 517-2660	Phone: (850) 410-7645	Phone: (407) 858-3950
Fax: (334) 517-2746	Toll-Free: (800) 342-0820	cfix@ocfl.net
Toll-Free: (866) 229-6220	ffcenter@fdle.state.fl.us	http://www.cfix.fl.net
fusioncenter@alacop.gov	http://www.fdle.state.fl.us	
http://www.fusion.alabama.gov		
Southeast Florida Fusion Center (SEFFC)	**Georgia Information Sharing and Analysis Center (GISAC)**	**Kentucky Intelligence Fusion Center (KIFC)**
Miami, Florida	Atlanta, Georgia	Frankfort, Kentucky
Phone: (305) 470-3900	Phone: (404) 486-6420	Phone: (502) 564-2081
ioc@mdpd.com	generalinfo@gisac.gbi.ga.gov	fusioncenter@ky.gov
http://www.mdpd.com		http://www.homelandsecurity.ky.gov
Mississippi Analysis and Information Center (MSAIC)	**North Carolina Information Sharing and Analysis Center (NS ISAAC)**	**South Carolina Information and Intelligence Center (SCIIC)**
Pearl, Mississippi	Raleigh, North Carolina	Columbia, South Carolina
Phone: (601) 933-7200	Phone: (919) 716-1111	Phone: (866) 472-8477
MSAIC@dps.ms.gov	Toll-Free: (888) 624-7222	Toll-Free: (803) 896-7133
http://www.homelandsecurity.ms.gov/msaic.html	ncisaac@ncdoj.gov	sciic@sled.sc.gov
		http://www.sled.sc.gov
Tennessee Fusion Center (TFC)		
Nashville, Tennessee		
Phone: (877) 250-2333		
tfc@tn.gov		
http://www.tennessee.gov/homelandsecurity		

FEMA Region 5 Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin		
Illinois Statewide Terrorism and Intelligence Center (STIC)	**Crime Prevention and Information Center (CPIC)**	**Indiana Intelligence Fusion Center (IIFC)**
Springfield, Illinois	Chicago, Illinois	Indianapolis, Indiana
Phone: (877) 455-7842	Phone: (312) 745-5669	Phone: (866) 400-4432
stic@isp.state.il.us	cpic@chicagopolice.org	iifc@iifc.in.gov
		http://www.in.gov/iifc
Michigan Intelligence Operations Center (MIOC)	**Detroit and Southeast Michigan Information and Intelligence Center (DSEMIIC)**	**Minnesota Fusion Center**
Lansing, Michigan	Detroit, Michigan	St. Paul, Minnesota
Phone: (517) 241-8000	Phone: (313) 967-4600	Phone: (651) 793-3730
Toll-Free: (877) 616-4677	DSEMIIC@michigan.gov	Fax: (651) 793-3731
mioc@michigan.gov		Toll-Free: (800) 422-0798
http://www.michigan.gov/mioc		info@icefishx.org
		http://www.icefishx.org
Ohio Strategic Analysis and Information Center (SAIC)	**Cincinnati/Hamilton County Regional Terrorism Early Warning Group**	**Northeast Ohio Regional Fusion Center (NEORFC)**
Columbus, Ohio	Cincinnati, Ohio	Cleveland, Ohio
Phone: (614) 799-3555	Phone: (513) 263-8000	Phone: (216) 515-8477
saic@dps.state.oh.us	Fax: (513) 263-8225	Toll-Free: (877) 515-8477
http://www.homelandsecurity.ohio.gov/index.stm	tewg@hamilton-co.org	info@neorfc.us
	http://www.hamiltoncountyohio-tewg.org	http://www.neorfc.us
Southeastern Wisconsin Threat Analysis Center (STAC)		
Madison, Wisconsin		
Phone: (608) 242-5393		
wsic@doj.state.wi.us		
http://www.doj.state.wi.us/dci		

FEMA Region 6 Arkansas, Louisiana, New Mexico, Oklahoma, Texas		
Arkansas State Fusion Center (ASFC)	**Louisiana State Analytical and Fusion Exchange (LA-SAFE)**	**New Mexico All Source Intelligence Center (NMASIC)**
Little Rock, Arkansas	Baton Rouge, Louisiana	Santa Fe, New Mexico
Phone: (501) 618-8001	Phone: (225) 925-4192	Phone: (505) 476-9600
Toll-Free: (866) 787-2332	Toll-Free: (800) 434-8007	intelligence.fusion@state.nm.us
arfusioncenter@asp.arkansas.gov	lafusion.center@dps.la.gov	www.nmdhsem.org
	www.la-safe.org	
Oklahoma Information Fusion Center (OIFC)	**Texas Joint Crime Information Center (TX JCIC)**	**Dallas Fusion Center**
Oklahoma City, Oklahoma	Austin, Texas	Dallas, Texas
Phone: (405) 842-8547	Phone: (866) 786-5972	Phone: (214) 671-3482
Alternate Phone: (405) 848-6724	TXJCIC@dps.texas.gov	dallas.fusion@dpd.ci.dallas.tx.us
fusion@osbi.ok.gov		
http://www.okfusion.ok.gov		
Southwest Texas Fusion Center (SWTFC)	**North Central Texas Fusion Center (NCTFC)**	**MATRIX - El Paso Multi-Agency Tactical Response Information eXchange**
San Antonio, Texas	McKinney, Texas	El Paso, Texas
Phone: (210) 207-7680	Phone: (972) 548-5537	Phone: (915) 680-6500
swtxfusion@sanantonio.gov	NCTFC@co.collin.tx.us	pdintel@elpasotexas.gov
	http://www.co.collin.tx.us	

FEMA Region 7 Iowa, Kansas, Missouri, Nebraska		
Iowa Division of Intelligence and Fusion Center (DOI/FC)	**Kansas Intelligence Fusion Center (KIFC)**	**Kansas City Regional TEW Interagency Analysis Center**
Des Moines, Iowa	Topeka, Kansas	Kansas City, Missouri
Phone: (800) 308-5983	Phone: (785) 274-1805	Phone: (816) 413-3601
intel@dps.state.ia.us	intelligence.fusion@ksag.org	kctew@kcpd.org
http://www.dps.state.is.us/intell/index.shtml		http://www.kctew.org
Missouri Information Analysis Center (MIAC)	**St. Louis Fusion Center (STLFC)**	**Nebraska Information Analysis Center (NIAC)**
Jefferson City, Missouri	St. Louis, Missouri	Lincoln, Nebraska
Phone: (866) 362-6422	Phone: (314) 615-4839	Phone: (402) 479-4049
miac@mshp.dps.mo.gov	info@sltew.org	Fax: (402) 479-4950
http://www.miacx.org	http://www.sltew.org	nefusioncenter@nebraska.gov

FEMA Region 8 Colorado, North Dakota, South Dakota, Utah		
Colorado Information Analysis Center (CIAC)	**North Dakota State and Local Intelligence Center (NDSLIC)**	**South Dakota Fusion Center**
Lakewood, Colorado	Bismarck, North Dakota	Sioux Falls, South Dakota
Phone: (877) 509-2422	Phone: (866) 885-8295	Phone: (605) 367-5940
ciac@ciac.co.gov	ndslic@nd.gov	sdfusioncenter@state.sd.us
http://www.dhsem.state.co.us	http://www.nd.gov/des/homeland/fusion-center	
Utah Statewide Information and Analysis Center (SIAC)		
Sandy, Utah		
Phone: (801) 256-2360		
SIAC@utah.gov		
http://www.publicsafety.utah.gov/investigations/siac.html		

FEMA Region 9 Arizona, California, Guam, Hawaii, Nevada		
Arizona Counter Terrorism Information Center (ACTIC)	**California State Threat Assessment Center (STAC)**	**Northern California Regional Intelligence Center (NCRIC)**
Phoenix, Arizona	Sacramento, California	San Francisco, California
Phone: (602) 644-5805	Phone: (916) 874-1100	Phone: (866) 367-8847
Toll-Free: (877) 272-8329	Fax: (916) 874-2484	dutyofficer@ncric.org
actic@azdps.gov	STAC@caloes.ca.gov	http://www.ncric.org
http://www.azdps.gov	http://www.calstas.org	
Central California Intelligence Center (CCIC)	**Joint Regional Intelligence Center**	**Orange County Intelligence Assessment Center (OCIAC)**
McClellan, California	Norwalk, California	Santa Ana, California
Phone: (916) 808-8383	Phone: (562) 345-1100	Phone: (714) 289-3949
Toll-Free: (888) 884-8383	Fax: (562) 345-1766	Fax: (714) 289-1025
info@sacrtac.org	jric@jric.org	ociac@ociac.org
http://www.sacrtac.org	http://www.jric.org	http://www.ociac.org
San Diego Law Enforcement Coordination Center (SD-LECC)	**Mariana Regional Fusion Center (MRFC)**	**Hawaii State Fusion Center (HSFC)**
San Diego, California	Agana Heights, Guam	Honolulu, Hawaii
Phone: (858) 495-5730	info@mlrin.org	Phone: (916) 356-4467
info@sd-lecc.org		pacclear@hi.hidta.net
		http://www.pacclear.org
Nevada Threat Analysis Center (NTAC)	**Southern Nevada Counter-Terrorism Center (SNCTC)**	
Carson City, Nevada	Las Vegas, Nevada	
Phone: (775) 687-0450	Phone: (702) 828-2200	
ntac@dps.state.nv.us	ansec@lvmpd.com	
	www.snctc.org	

FEMA Region 10 Alaska, Idaho, Montana, Oregon, Washington		
Alaska Information and Analysis Center (AKIAC)	**Idaho Criminal Intelligence Center**	**Montana All-Threat Intelligence Center (MATIC)**
Anchorage, Alaska	Meridian, Idaho	Helena, Montana
Phone: (907) 269-8900	Phone: (208) 846-7676	Phone: (406) 444-1330
Toll-Free: (855) 692-5425	ICIC@fusion.idaho.gov	dojintel@mt.gov
AKIAC@alaska.gov	www.isp.idaho.gov/icic	doj.mt.gov
Oregon Terrorism Information Threat Assessment Network (TITAN)	**Washington State Fusion Center (WSFC)**	
Salem, Oregon	Seattle, Washington	
Phone: (503) 378-6347	Phone: (877) 843-9522	
oregonfusioncenter@doj.state.or.us	intake@wsfc.wa.gov	
www.oregonfusioncenter@doj.state.or.us		

National Preparedness Leadership Initiative
Harvard University
October 2015