INCIDENT RESPONSE PLANS FOR STATE GOVERNMENT: A PRELIMINARY CONTENT ANALYSIS

An Applied Research Project

By Corey L. Banks

CLBanks23@gmail.com

Submitted to the Department of Political Science

Texas State University-San Marcos

In Partial Fulfillment for the Requirements for the Degree of

Master of Public Administration

Spring 2019

Committee Members:

Patricia M. Shields, Ph D

William DeSoto, Ph D

Travon Earl, MPA

TABLE OF CONTENTS

CHAPTER V: CONCLUSION

BIBLIOGRAPHY

Abstract

Purpose:

With cyberattacks on the rise state government need to be prepared for cyber incidents. Therefore, the purpose of this preliminary research is to first identify key elements of a cyber incident response plan using the literature; second, assess available state cyber incident response plans using the key elements and lastly, make recommendations to improve state incident response plans using the results of the assessment.

Methodology:

Incident response plans were broken down into three major categories derived from the literature: incident response team structure, handling an incident, and coordination and information sharing. A content analysis was completed to compare the National Institute of Standards and Technology's (NIST) framework to the state incident response plans.

Findings:

The finding showed that there was significant involvement from the states' governors; that the state plans were generic but had a diversity of names. The incident response plan was broken down into three major categories which were incident response team structure, handling an incident and coordination and information sharing. The first category incident response team structure six states had a minimal discussion, and two had no reference to "Chief Information Officer." The second category handling an incident eight of the ten states were rated as "well done" or "adequate" for "Preparation, "Detection and Analysis" and "Containment Eradication and Recovery." Lastly, coordination and information sharing nine of the ten states were rated as "well done" or "adequate."

With limited manpower, it is imperative that IT teams be highly proficient in their duties. The governors have given these agencies the freedom to tailor policies, plans, and team models

according to their manpower. Most plans cited the NIST framework and tailor it to their own organizations. Overall the state of Texas had the best incident response plan; however, there is much work needed to be done to strengthen state incident response plans.

About the Author

Corey Banks was born and raised in Suffolk, Virginia. He graduated with a Bachelor of Science in Industrial Technology Management from Virginia State University in 2008. Corey will complete the Master of Public Administration degree from Texas State University in May 2019. Corey is currently serving in the United States Army as a Signal Officer; if you have any questions you may contact Corey at CLBanks23@gmail.com.

Acknowledgments

I want to thank God, my family, and my friends for their unwavering support. I also thank my late great aunt Maddie D. Vann for motivating me to reach for the stars. I thank Dr. Shields, editor of *Armed Forces and Society*, for her guidance, encouragement, and assisting me throughout the process. I thank the rest of the MPA faculty for their assistance.

Chapter I: Introduction

Introduction:

The compromise or violation of an organization's security is a matter of when, not if. Cyber-attacks are on the rise, from Fortune 500 companies to local and state governments. Criminals are using vulnerable access points and leaving malware to capture debit and credit card data, names, mail and email addresses, and phone numbers. State governments are targets for hackers because of the valuable data that they store and the big networks they are connected to, and because they lack the resources to fight back. In some organizations, one full-time person may be doing all the work to meet IT and cybersecurity requirements (Small Towns, 2017, p. 2).

Lou Romero, the cyber-liability and risk-practice lead for Pivot Point Security, surveyed 200 municipalities in New Jersey and reported that 78% lacked a password management policy, 97% lacked a disaster recovery plan, 46% of backup files and records were kept onsite rather than in the cloud, which is more secure, and 90% of local governments did not encrypt sensitive emails. Historically, local governments have not outsourced cybersecurity; about 61% keep it in-house. There are signs of organizations that do not practice basic cyber-hygiene (Small Towns, 2017, p. 3).

In 2015, the Nonprofit Municipal Research and Services team surveyed 200 small local governments in Washington State and found that only 25% updated their security policies annually. Steve Sedore, the executive director of operations of Allegan County, Michigan, reported, "The lack of good policies and practices can be traced to some fundamental problems that plague government at every level" and that the problems they face include inability to pay competitive salaries for cyber personnel, lack of training and end-user accountability, and lack of funds (Small Towns, 2017, p. 3).

According to Newman, 38% of state and federal government cyber incident that occur agencies are unable to identify the attacker. They also have grueling time figuring out how the hacker perpetrated the attack. Chris Wysopal, of the CTO of Veracode stated that "The Whole Key of incident response is understanding what happened. If you can't plug the hole the attacker is just going to come back in again." (Newman, 2018, p.2)

State Government Cyber Security

State government agencies are vulnerable to attacks primarily due to the lack of advanced technology and manpower to monitor their systems. With the growing popularity of e-government services the internet portals become a target for cyber attackers and terrorists. Cyber intrusions into the e-government network can significantly impair systems and services of government (Zhao & Zhao, 2010, p50.) Due to the rapid changes in technology and the increasingly sophisticated methods of attacks, it is difficult for all organizations to constantly fight and detect signs of a data breach. Private companies with more financial and manpower resources are being hacked daily and governmental organizations are notorious for having less resources to protect their technology, making them a constant target. The systems that many state governments have in place are inferior or obsolete and do not provide complete visibility of their entire networks. State governments need to allocate more funds to the cybersecurity budget in order build strong incident response plans.

Approximately 76% of e-government attacks in the United States are vulnerable to common web application attacks such as denial of service (DoS), unauthorized access to networks, theft of employee data, breaching customer information, online financial fraud, web-application attacks and system penetration (Zhao & Zhao, 2010, p50.) The threat of these attacks

would be reduced with risk assessment imbedded in state plans and the impact of an actual breach would be minimized by having an incident response plan intact.

An incident response plan needs to be comprehensive and updated on an annual basis. Good incident response plans limit damage to organizations, protect citizen's data, and allow users to act quickly and notify respective personnel and regulators in an orderly manner. One key element to a robust incident response plan is collaboration from respective governmental departments including health, technology, legal and security. By bringing these departments together we easily can identify each department's critical reporting requirements and avoid having employees work in silos. All employees should also understand that in the event of a breach of certain types of sensitive health information they are required by law to report within 72 hours to General Data Protection Regulation (GDPR). Agencies should also invite external organization such as the local law enforcement and digital forensics teams. It is important to have their names and contact numbers because these agencies bring a wealth of knowledge and will play an instrumental role in recovering from a data breach.

Research Purpose:

The inspiration for this research was to determine if state governments had incident response plans in place to combat cyber attacks. All organizations, including governments, need a plan to reduce the risk of a cyber security attack and a plan of action if an attack occurs. Hence, state governments need a formal cyber security plan. The literature does not provide information on the state of cyber security planning among state governments. Cichonski et al, of National Institute of Standards and Technology's (NIST) have developed a useful and widely recognized cyber security plan model that can be adapted for state governments. Given these conditions the purpose of this preliminary research is, first, to identify the key elements of a cyber incident response plan using the literature; second, to assess the available state cyber incident response

plans using these elements; and, last, to recommend improvements to the plans using the assessment

Chapter Summaries:

Chapter one provides an introduction to the research on incident response plans and state the research purpose. Chapter two examines scholarly literature on the history of cybersecurity and the threats to organizations. A summary of the conceptual framework is present at the end of this chapter. Chapter three describes the research methodology used to assess different state plans. This chapter also discusses the operationalization of the conceptual framework. It also examines some of the advantages and disadvantages of using content analysis. Chapter four provides the results of the content analysis and illustration of *well-done* plans. Chapter five provides findings, recommendations and a conclusion based on the content analysis. It also, additional recommendation for future state plans.

Chapter II: Literature Review

Chapter Purpose:

This chapter, examines the literature and policies on cybersecurity in state government. Cybersecurity is a complicated process, and large organizations need plans to ensure they carry it out in a systematic manner. The conceptual framework for cybersecurity planning in state governments is introduced at the end.

Cyber Security:

Cybersecurity is the protection of the network, programs, and data on a computer from unauthorized personnel to safeguard the availability, integrity, and confidentiality of people's personally identifiable information (Kamar, 2017, p. 8). Craigen (2014, p. 18) defined cybersecurity as "the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights." The Department of Homeland Security (DHS; 2014, p. 11) defined cybersecurity as "the activity or processability or capability or state whereby information and communications systems and the information contained therein are protected from and/or defended against unauthorized damage use or modification or exploitation."

History of Cybersecurity:

Cybersecurity dates to the 1970s, when the U.S. Department of Defense separated major elements of the design and management of networks from the design and management of network security. This was because military needed a network on which it could send classified data, though many other technologies would benefit because other vendors could also use it to send classified data. This factor played an instrumental role in the design and management of the internet because through the mid-1980s, the infrastructure and management of the civilian

internet was a part of the military's Defense Data Network. The split of networks from network security was critical for the development of the civilian internet (Fidler, 2017, p. 449).

As U.S. infrastructure, mechanisms, and policies were evolving, three major cyber incidents occurred. The first period was the realization phase in the early era of the internet. The second period was before and after the September 11, 2001 attacks, and the last is the modern militarization phase, in which cyberwarfare causes damage to capabilities and critical infrastructure. The Morris worm attack acted as the wake-up call to the U.S. intelligence community, academics, and policymakers. The first significant cyberespionage event happened in 1986, however, with the Cuckoo's Egg attack involving the Soviet KGB. This was considered the first large-scale attack, and the worm crashed 6,000 computers. The U.S Government Accountability Office assessed the damage at between $100,000 and $10,000,000. This also shows the difficulty of genuinely assessing the damage of a cyberattack. The Morris worm attack played a vital role as a catalyst for the first steps toward a regulated cyberspace.

The Moonlight Maze incident caused the U.S. cyber-defense forces to rethink their strategies on cyberwarfare attribution, deterrence, and sensitive networks such as the Non-secure Internet Protocol Router Network, "NIPRNet." The government and agencies realized that there were no clear policies or strategies for these problems. This remained so until the legislature put together Presidential Decision Directive 63, which had two significant strategic implications: The National Incident Protection Center (NIPC) and the Joint Task Force Computer Network Defense (JTF-CND). The history of cyberwarfare is an important tool for assessing mistakes and projecting the future (Haizler, 2017, p. 33).

Threats to organizations

Reputation

The first threat to an organization in the event of a cyberattack is to its reputation. Eckert (2017, p.147) defined a reputation as "a perceptual representation of a company's past actions and future prospects that describes the firm's overall appeal to all of its key constituents when compared with other leading rivals." Fombrun (2012, p. 95) defined it as "a collective assessment of a company's attractiveness to a specific group of stakeholders relative to a reference group of companies with which the company competes for resources."

Cyberattacks can damage a company's reputation, and some unprepared organizations never recover. Reputational loss can affect organizations in multiple ways, such as a decrease in market value, which is a significant concern for companies that trade publicly. Other cascading effects are loss competitiveness and loss of confidence in the company's ability to protect itself. But organizations can overcome reputation loss by conducting annual risk assessments. This gives them the ability to look at their shortfalls and mitigate risks that they can't remove. It also forces them to implement better policies and best practices (Dhillon, 2015, p. 4). It the responsibility of a company's vice president to manage its reputational risk and to conduct assessments to evaluate problems that could affect this reputation, including pending lawsuits, weak product-testing procedures, and product liability (Eccles, etal, 2007, p. 4).

Financial Losses

The second threat is financial loss. This is sometimes hard to measure and can be either direct or indirect. Direct loss is the monetary loss and damage suffered by the victim; examples include money withdrawn from company or individual accounts and the time and effort required to reset the accounts. Indirect losses are monetary-equivalent losses and the opportunity costs

imposed on society. These are not normally attributed to individuals and are very difficult to quantify. Examples include lack of trust in a company's online banking systems because consumers doubt that it will work (Böhme, 2016). According to Acquisti, Friedman, and Telang (2006, p. 1563), organizations suffer significant financial losses as a result of security breaches. There are a large, negative market reactions to information-security breaches involving unauthorized access to confidential data, but no significant reactions to breaches that don't include access to sensitive data (Campbell, et al, 2003, p. 3).

Critical Information Ransomware

The third threat is loss of critical information to ransomware if organizations fail to pay the demanded ransom. Ransomware has become a billion-dollar industry for cybercriminals. Organizations need to develop benchmarks to measure the costs of recovery and cleanup after attacks and productivity and revenue lost to downtime. These benchmarks underpin a model that permits better estimations from the data Computer Economic Inc CEI collects (Cashell, K. et al, 2004, p. 5).

In March 2018, a ransomware attack shocked the city of Atlanta in demanding $50,000 to allow victims to unlock their own data and network connections. The attack affected internet systems and government employees citywide, forcing them to turn off computers, disable airport Wi-Fi, and restrict the functionality of the city's website. Residents were unable to pay utility bills or parking tickets or to report potholes and graffiti because of the cyber-hostage situation. Employees of the Atlanta Municipal Court were unable to retrieve and validate warrants. Employees had to complete many tasks manually for about five days, shutting down the city's productivity and spreading fear and chaos as the rest of the state and country wondered what would happen next (Deere, 2018, p. 2).

Researchers and third-party investigators believe this attack came from the SamSam hacking crew and are unsure if this is a group of cybercriminals working together or an individual. Judging from the broken English in the communication from the hackers, it was assumed but not confirmed that the suspects were from a third world country (Deere, 2018, p. 5).

iv. Addressing Threat

Cyberattacks happen so often that it is imperative for organizations to respond quickly. But when breaches are announced, there is not always clear or specific information on what information was attacked, the identity of the hacker, and how the stolen information will be used. Delays in announcing a breach can be a result of law enforcement investigations or of companies needing more time to determine what kind of disclosure is needed for financial or medical data.

The model of developing an incident response plan has been widely accepted and applied all across the United States (Connell, n.d.). The benefits of having an incident response plan in place include ensuring that appropriate steps are taken, reduced costs investigation costs, targeted security monitoring, giving clients and investors confidence in the system, and helping agencies avoid penalties. That is why all organizations need incident response plans (Cichonski, P, et al, 2012, p. 1).

Overview of Conceptual Framework

The next sections of this paper identify key elements of a cyber-incident response plan, including an incident response team structure; incident response policy, plan and procedures; handling an incident; and coordination and information sharing.

II. **Incident Response Team Structure** (Category 1)

A cyber incident is a matter of when, not if, so it is imperative that organizations have the right incident response teams to plan for any such situation. This team should be available to anyone who discovers or suspects a cyberattack in the organization. It is important to establish roles and responsibilities in an IRT, as this gives the team the ability to coordinate a myriad of details simultaneously and determine their impacts so that members can act appropriately to limit the damage and restore the system in a timely matter (Killcrece, 2003, p. 11-12). Each phase of the IRT's activity is important, from preparation to lessons learned.

Chief Information Officer (1.1)

The CIO plays an instrumental role in the information technology department in any organization. The CIO is the senior executive in this department who is responsible for establishing information policy and IT standards and ensuring that information assets are effectively protected and managed (Hütter & Riedl, 2017, p. 2). The CIO is also responsible for managing the IT portfolio and IT investment and for planning a continuity and disaster recovery plan. According to Lawry, Waddell, and Singh (2007), in the public sector the "increasing importance of governance will require the CIO to develop a deeper understanding and intuitive grasp of corporate finance and accounting processes; CIOs will assume a greater leadership role with a focus on shaping and creating a world economy fuelled by information." The CIO must be a business leader who has strong organizational skills and the ability to quickly identify a problem, formulate a solution, and take corrective action to retain the organization's competitive advantage. The CIO also has to delegate authority effectively to his IT staff and not run a one-person operation. He has to recruit the best employees who demonstrate great creative thinking skills and innovate problem solving.

Incident Response Policy and Procedures (1.2)

The reason an organization should have an incident response policy and procedures is that this prepares it with the tools necessary for responding to cyberattacks in a timely matter. An incident response plan is an organized way to manage cyberattacks and reduce recovery time and costs. Organizations also need to establish an incident response team (IRT) with a list of key names and titles posted visibly and available 24/7 in the event of a cyberattack. The IRT must establish an alert status and be ready to take preventative measures once notified. There also needs to be a checklist of procedures to be carried out in such a case. The IRT must have the contact information of local law enforcement and other agencies, such as the FBI, and pertinent technology professionals. There needs to be a contact roster of key local government officials who might be affected. Organizations should conduct a risk analysis on the IRT and develop and rehearse contingency plans in the event the team is unavailable (Killcrece, 2003, p. 211).

Team Models and Selection (1.3)

It is imperative that IT personnel understand their composition and the disposition to create the right structure for their organizations. The two most common types of team are central IRTs and distributed IRTs. Central IRTs are common in small organizations with limited resources and geographic dispersal. Distributed IRTs are mostly used in large organizations with extensive computing resources. They will establish one team per region and one per major facility (Cichonski, P, et al., 2012, p.14).

III. **Handling an Incident** (Category 2)

Instruction on handling an incident provides an IRT team with the basic tools necessary to deal with a cyber-incident step by step.

A. Preparation (2.1)

Preparation is the most important stage of handling an incident. It means that everyone on the team is ready to handle a cyber-incident at a moment's notice. An incident can arise from a simple power outage or hardware failure. According to Wright, there are several key elements that organizations must put in place to mitigate problems that could hinder people's ability to handle such an incident. The first is policy: a policy is a written set of rules, principles, and practices for an organization. Without clear policies and procedures, an organization could be left vulnerable to lawsuits. The second is a response plan. This gives the organization the ability to set priorities regarding organizational impact, which helps it gain buy-in from stakeholders and management. The third element is a communication plan. This is vital because a specific person may need to be notified immediately, such as the CIO or FBI. Lack of a communication plan could result in a delayed response or the wrong person being contacted.

The fourth element is to have is a good filing system for documentation. Documenting things pays large dividends and is a life saver when it comes to incident response. The most important reason organizations should document cyber-incidents is so they can use the documentation in court as evidence of what the IRT team has done. The fifth element is that the IRT should consist of people of different disciplines so they can handle the various problems that can arise in the event of a cyber-incident. The sixth element is strong access control to ensure that only the right people have access to the network. The final element is proper training; the last thing anyone needs is a team that is unprepared to carry out its tasks. It is imperative to conduct regular battle drills to ensure team proficiency (Wright, 2011, p. 2-3).

B. Detection and Analysis (2.2)

It has been said that the hardest part of an incident response plan is detecting the cyber-incident and verifying whether it actually occurred. This requires the IT specialist to gather information through log files monitoring intrusion detection systems and firewalls. If an event is identified, it should be reported and documented and the IRT allowed to collect data. In this phase, the IRT should also analyze the incident to validate it and notify and relevant members of the team (Wright, 2011, p.5). The majority of attacks do not have identifiable or detectable precursors because if those had been detected, the organization could prevent the attack by changing its security posture. An example of a precursor is a web server log that presents usage vulnerability.

C. Containment Eradication and Recovery (2.3)

Containment and eradication are custom-tailored strategies for an organization. First, it is necessary establish priorities for which systems and services need to be shut down without hurting the business workflow. Containment and eradication strategies vary with the type of incident, and these decisions are easier to make when priorities are known. It is also important to document all evidence for legal proceedings (Kelly, 2016).

The primary purpose of containment is to limit the damage to systems and prevent further losses. The first thing the organization should do is establish a short-term containment. This involves isolating the system or taking it off the network. The second step is to back up and take forensic images of the affected systems. This captures the state of the system during the cyber-incident and can be used as evidence. The third step is long-term containment: affected systems are temporarily fixed to be used on the network if necessary, and the IRT focuses on removing

backdoor malware left by the attackers or the affected system by installing new security patches. This limits the chance of further incidents while retaining productivity (Wright, 2011, p. 6).

The eradication phase involves the removal and restoration of the affected systems. In this phase, the IRT continues to document all actions, ensures that all proper steps are taken to remove malicious software, and calculates the cost of working hours, miscellaneous resources, and anything else that made a significant impact. The IRT takes extra measures to improve the situation by learning what really caused the incident and ensuring the system will not be compromised again. This can be done by updating the system and installing patches. At the end of this phase, the original images that were created before the attack should be on the computers, and all affected systems and files should be monitored and scanned (Wright, 2011, p.7).

The recovery phase involves the IRT restoring all systems to normal operation and patching any vulnerabilities to prevent future incidents. Recovery includes but is not limited to restoring systems, rebuilding systems from scratch, installing patches, and changing passwords. The primary goal is to be vigilant and prevent another incident (Cichonski et al., 2012, p.37).

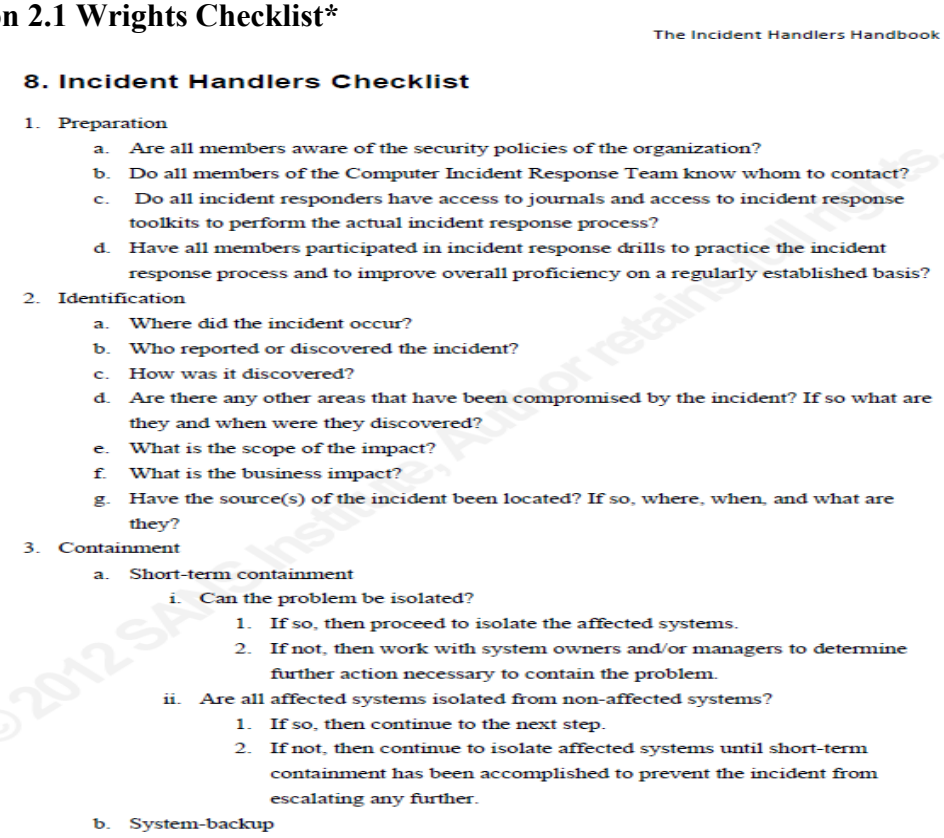
D. Post- Incident Activity (2.4)

Post-incident activities such as identifying the lessons learned give an organization the opportunity to identify, collect, and analyze data and develop practices for preventing the incident from happing again. This is also a way to bring the team together and let employees provide input. Organizations should document the things that were not done during the incident in a written report. This report should ask the questions who, what, where, why, and how (Cichonski et al., 2012.p. 38)

E. Incident Handling Checklist (2.5)

Checklists play an instrumental role in our everyday lives, as they remind us of all the steps needed to complete a task. A checklist should be clear and concise to take the work off your mind; they're often a simple "brain dump" in chaotic lives in which people are always multitasking. As Gawande (2009) noted, checklists help organizations set standards and benchmarks for performance evaluation. They can also improve medical care significantly: in one case, patients' average length of stay was reduced by fifty percent. Gawande also notes that checklists can be either "do-confirm" or "read-do." With a do-confirm checklist, employees perform their jobs from memory and experience. In Illustration 2.1 -2.3 Wright provides examples in a checklist of critical events that need to happen in each phase of an incident.

Illustration 2.1 Wrights Checklist*



The Incident Handlers Handbook

8. Incident Handlers Checklist

1. Preparation
   a. Are all members aware of the security policies of the organization?
   b. Do all members of the Computer Incident Response Team know whom to contact?
   c. Do all incident responders have access to journals and access to incident response toolkits to perform the actual incident response process?
   d. Have all members participated in incident response drills to practice the incident response process and to improve overall proficiency on a regularly established basis?
2. Identification
   a. Where did the incident occur?
   b. Who reported or discovered the incident?
   c. How was it discovered?
   d. Are there any other areas that have been compromised by the incident? If so what are they and when were they discovered?
   e. What is the scope of the impact?
   f. What is the business impact?
   g. Have the source(s) of the incident been located? If so, where, when, and what are they?
3. Containment
   a. Short-term containment
      i. Can the problem be isolated?
         1. If so, then proceed to isolate the affected systems.
         2. If not, then work with system owners and/or managers to determine further action necessary to contain the problem.
      ii. Are all affected systems isolated from non-affected systems?
         1. If so, then continue to the next step.
         2. If not, then continue to isolate affected systems until short-term containment has been accomplished to prevent the incident from escalating any further.
   b. System-backup

Source * https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Illustration 2.2 Wrights Checklist*

i. Have forensic copies of affected systems been created for further analysis?
ii. Have all commands and other documentation since the incident has occurred been kept up to date so far?
    1. If not, document all actions taken as soon as possible to ensure all evidence are retained for either prosecution and/or lessons learned.
    2. Are the forensic copies stored in a secure location?
        a. If so, then continue onto the next step.
        b. If not, then place the forensic images into a secure location to prevent accidental damage and/or tampering.

c. Long-term containment
    i. If the system can be taken offline, then proceed to the Eradication phase.
    ii. If the system must remain in production proceed with long-term containment by removing all malware and other artifacts from affected systems, and harden the affected systems from further attacks until an ideal circumstance will allow the affected systems to be reimaged.

4. Eradication
    a. If possible can the system be reimaged and then hardened with patches and/or other countermeasures to prevent or reduce the risk of attacks?
        i. If not, then please state why?
    b. Have all malware and other artifacts left behind by the attackers been removed and the affected systems hardened against further attacks?
        i. If not, then please explain why?
5. Recovery
    a. Has the affected system(s) been patched and hardened against the recent attack, as well as possible future ones?
    b. What day and time would be feasible to restore the affected systems back into production?
    c. What tools are you going to use to test, monitor, and verify that the systems being restored to productions are not compromised by the same methods that cause the original incident?

Source * https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Illustration 2.3 Wrights Checklist*

d. How long are you planning to monitor the restored systems and what are you going to look for?
e. Are there any prior benchmarks that can be used as a baseline to compare monitoring results of the restored systems against those of the baseline?

6. Lessons Learned
   a. Has all necessary documentation from the incident been written?
      i. If so, then generate the incident response report for the lessons learned meeting.
      ii. If not, then have documentation written as soon as possible before anything is forgotten and left out of the report.
   b. Assuming the incident response report has been completed, does it document and answer the following questions of each phase of the incident response process: (Who? What? Where? Why? And How?)?
   c. Can a lessons learned meeting be scheduled within two weeks after the incident has been resolved?
      i. If not, then please explain why and when is the next convenient time to hold it?
   d. Lessons Learned Meeting
      i. Review the incident response process of the incident that had occurred with all CIRT members.
      ii. Did the meeting discuss any mistake or areas where the response process could have been handled better?
         1. If no such conversations occurred, then please explain why?

Source * https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

IV. **Coordination and Information Sharing** (Category 3)

It is imperative for organization to communicate effectively with law enforcement about cyber-attacks. On February 13, 2015, President Obama issued Executive Order 13691 (White House, 2015), which read, "In order to address cyber threats to public health and safety, national security, and economic security of the United States, private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible." Knowledge is power, and by not letting others know you do yourself an injustice.

A. Coordination (3.1)

In the event of a cyber-incident, it is critical that all parties be notified and on the same page. There must be coordination in contacting outside agencies, such as local law enforcement, the FBI and CIA, and internet service providers. The incident response team should plan before an event occurs to ensure that all parties know their roles and responsibilities (Cichonski et al., 2012, p. 45). NIST used the chart below as a baseline for coordinating with teams.

Table. 2.1 NIST Coordination Relationship *

Category	Definition	Information Shared
Team-to-team	Team-to-team relationships exist whenever technical incident responders in different organizations collaborate in the incident-handling life cycle. The organizations that participate in this type of relationship are usually peers without any authority over each other and choose to share information, pool resources, and reuse knowledge to solve problems common to both.	The information shared in team-to-team relationships is mostly tactical and technical (e.g., technical indicators of compromise, suggested remedies) but also includes other matters (plans, procedures, lessons learned) if conducted as part of the preparation phase.
Team–to–coordinating team	Team–to–coordinating team relationships exist between an organizational IRT and a separate organization that acts as a central point for coordinated incident response and management, such as US-CERT or an ISAC. The coordinating body may require some degree of reporting from the member organizations and expect the coordinating team to disseminate timely and useful information to participating organizations.	Teams and coordinating teams frequently share tactical and technical information and information on threats, vulnerabilities, and risks to the community served by the coordinating team. The coordinating team may also need specific impact information about incidents to decide where to focus its resources and attention.
Coordinating team–to–coordinating team	Relationships between coordinating teams, such as US-CERT and the ISACs, let them share information on the nature and scope of cross-cutting incidents that affect multiple communities, and on reusable mitigation strategies to assist in inter-community response. The coordinating teams act on behalf of their communities' member organizations.	Coordinating teams often share periodic summaries during "steady state" operations, punctuated by the exchange of tactical and technical details, response plans, and impact- or risk-assessment information during coordinated incident-response activities.

Source * https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

B. Information Sharing Techniques (3.2)

Information sharing plays a vital role in communicating and coordinating access with multiple organization. Regardless of the size of an incident, information must be shared with colleagues to handle it effectively. Organizations should be proactive in establishing an incident-

response life cycle to distribute information quickly. The most common approaches are the ad hoc method and the partially automated method.

The ad hoc method includes sending emails and instant messages and making telephone calls to notify people. This relies on individuals talking with employees and IRT teams. Organizations should make an effort to fix their information strategies through formal agreements. The partially automated method is used when organization have pre-made messages to distribute. Organizations should generate as much as information as possible automatically to make the sharing process seamless, and strive for a balance between automated information sharing and direct human communication. To do this effectivity, they must first identify the kind of information they want to communicate to their partners and then construct a formal data dictionary numbering all the entities and relationships (Cichonski et al., 2012).

C. Granular Information Sharing (3.3)

This is sharing information with organizations on a need-to-know basis. It is imperative that organizations balance the sharing of sensitive information that can have an impact on business. Business-impact information is frequently shared within teams to build relationships. This information involves how an incident affected the organization's finances and mission. Other organization can use it to make decisions about their own cyber-attacks. Sharing business-impact information is only useful with organizations that have an invested interest in one's own organization (Cichonski et al., 2012, p. 47-48).

V. Summary of the Conceptual Framework

Table 2.1 summarizes the conceptual framework in this chapter of the content analysis. Also, it combines the framework with the relevant literature. These descriptive categories are drawn from multiple scholars who have conducted research on this topic.

Table 2.1 Conceptual Framework Table

Conceptual Framework Table	
Title: Cyber Incident Response Plan for State Government **Purpose:** The purpose of this preliminary research is to first identify key elements of a cyber incident response plan using the literature, second assess available state cyber incident response plans using the key elements and lastly make recommendations to improve state incident response plans using the results of the assessment.	
Incident Response Team Structure ➢ Chief Information Officer ➢ Incident Response Policy and Procedures ➢ Team Models and Selection	Cichonski, P et al. (2012), Dutta & McCrohan (2002), Killcrece (2003), Lawry et al. (2007), Wright (2011).
Handling an Incident ➢ Preparation ➢ Detection and Analysis ➢ Containment, Eradication and Recovery ➢ Post- Incident Activity ➢ Incident Handling Checklist	Cichonski, P et al. (2012), Dutta & McCrohan (2002), Killcrece (2003), Lawry et al. (2007), Wright (2011).
Coordination and Information Sharing ➢ Coordination ➢ Information Sharing Techniques ➢ Granular Information Sharing	Cichonski, P et al. (2012), Dutta & McCrohan (2002), Killcrece (2003), Lawry et al. (2007), Wright (2011).

Chapter III: Methodology

Chapter Purpose:

This chapter describes the methodology used to analyze the incident response plan in the state government. The conceptual framework was developed from the literature and involved identifying the key elements of a cyber incident response plan. One of the most common modes of data collection for description is content analysis (Shields & Rangrajan, 2013); the framework was also used to develop a coding sheet for the content analysis. Issues around sampling are also discussed.

Operationalization Table/ Coding Sheet:

An Incident Response Plan should fully describe the notification procedures, roles, and responsibilities of respective personnel in the event of a cyber-attack. The relationship between the descriptive categories and the content analysis is displayed in the operationalization table (Shields & Rangrajan, 2013). The categories are used to code the content of the state plans, and it considers the level of discussion found in the plan.

Table 3.1 Operationalization of the Conceptual Framework Table: Content Assessment Coding Sheet

Operationalization Table

Title: Cyber Incident Response Plan for State Government. **Purpose:** The purpose of this preliminary research is, first, to identify the key elements of a cyber incident response plan using the literature; second, to assess the available state cyber incident response plans using these elements; and, last, to recommend improvements to the plans using the assessment.

Variable	Assessment Category	Well Done	Adequate	Minimal	No Discussion
Incident Response Team Structure					
1	Chief Information Officer	WD	A	M	ND
2	Incident Response Policy, Plan and Procedures	WD	A	M	ND
3	Team Models and Selection	WD	A	M	ND
Handling an Incident					
1	Preparation	WD	A	M	ND
2	Detection and Analysis	WD	A	M	ND
3	Containment Eradication and Recovery	WD	A	M	ND
4	Post- Incident Activity	WD	A	M	ND
5	Incident Handling Checklist	WD	A	M	ND
Coordination and Information Sharing					
1	Coordination	WD	A	M	ND
2	Information Sharing Techniques	WD	A	M	ND
3	Granular Information Sharing	WD	A	M	ND

Evaluation Criteria:

The Assessment Categories are evaluated off a rubric from *Well Done, Adequate*, *Minimal* and *No Discussion*. *Well Done* indicates that a substantial amount of material was cover in the state's plan and it exceeds the standard. *Adequate* indicates that a sufficient amount of information was cover in the state plan and it meets the standard. *Minimal* indicates that some material was mention in the state plan but needs more information to meet standards. *No Discussion* indicates that no information at all was mention in the state plan and needs substantial improvement.

Content Analysis:

Content analysis is the primary collection tool used in this study. It is used to identify the key elements of an incident response plan for a state government.

Content analysis has many advantages and disadvantages. One advantage is "economy in terms of both time and money" (Babbie, 2010, p. 344). Babbie argued that this technique does not require research staff or special equipment, so it is cost-efficient and time-consuming as long as one has access to the material. Another is "correction of errors" (p. 344): if a mistake is made due to an experimental design, it is sometimes impossible to redo the project. With content analysis, however, it is easy to redo a section of a project without doing the entire experiment again. A third is that content analysis "permits the study of the process occurring over a long time" (p. 344). The final advantage is "all unobtrusive measures, namely that the content analyst seldom has any effect on the subject being studied" (p. 344)—that is, once the book has been published, content analysis cannot have an effect on these.

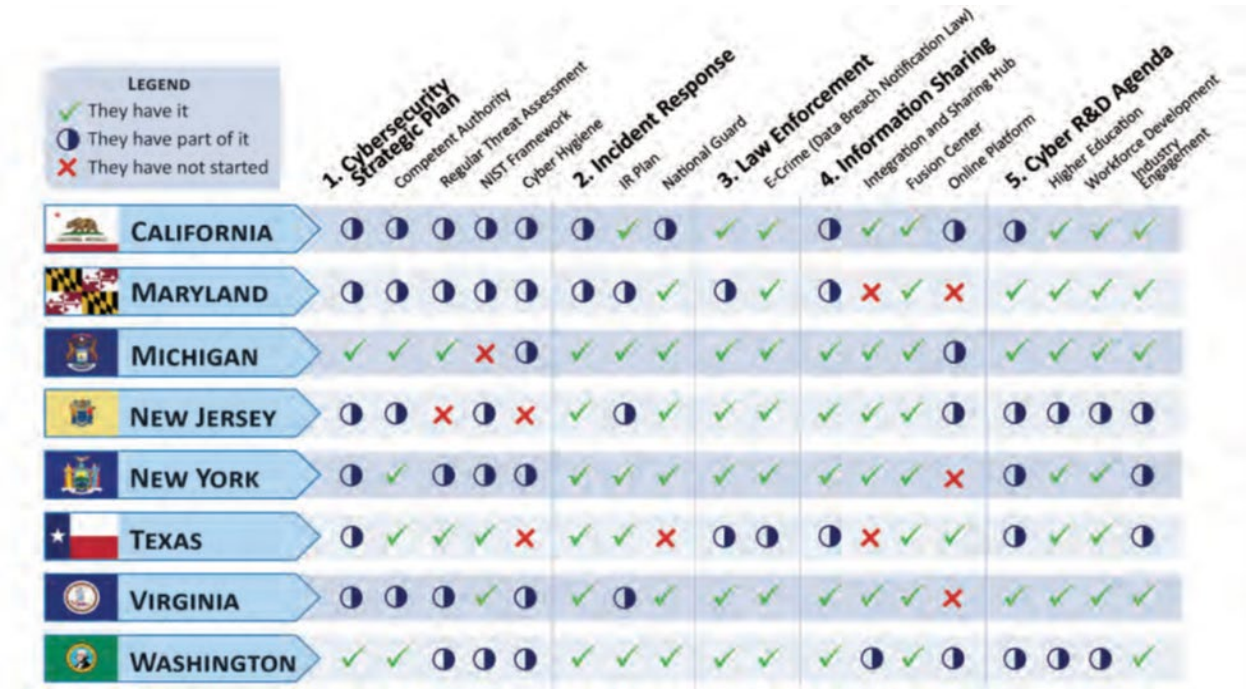
The disadvantage of content analysis is that it is "limited to the examination of recorded communications" (Babbie, 2010, p. 344). Examples include written and oral recordings and

graphics. These must be filed in the same manner to permit analysis. Another disadvantage is lack of validity and reliability (p. 344).

State Plans:

State plans were identified using the *State of States on Cybersecurity* document (Spidalieri, 2015, p8). Table 3.2 illustrates the level of cyber security among the states. States are rated on their cyber security plans, incidence- response plans, law enforcement, information sharing and cyber research and development. This document identified eight states with incident response plans. After an extensive review of state website two more states were identified as having incident response plans.

Table 3.2 State of State on Cybersecurity*



Source * https://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/

The ten state plans used in the study are identified in Table 3.3, along with their titles of plan and corresponding URLs.

Table 3.3 State Plans

State Plans

State	Document Title	URL
California	California Joint Cyber Incident Response Guide	https://www.caloes.ca.gov/LawEnforcementSite/Documents/California-Joint%20Cyber%20Incident%20Response%20Guide.pdf
Connecticut	Cybersecurity Action Plan	https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en
Maryland	State of Maryland Information Security Policy	https://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf
Michigan	Michigan Cyber Disruption Response Strategy	https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf
New Jersey	Executive Branch of New Jersey State Government: Statewide Information Security Manual	https://static1.squarespace.com/static/555b2d4ee4b011aa38092227/t/5b118de388251bb8d2b35995/1527877092177/NJ_Statewide_Information_Security_Manual.pdf
New York	Cyber Incident Response	https://its.ny.gov/document/cyber-incident-response-standard
Oregon	Statewide Information Security Plan	https://www.oregon.gov/das/OSCIO/Documents/StatewideInformationSecurityPlan.pdf
Texas	Texas Department of Information Resources (DIR)	https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf
Virginia	Information Technology Resource Management Information Security Standard	https://www.vita.virginia.gov/media/vitavirginiagov/resources/presentations/pdf/InformationSecurityIncidentResponseProcedure.pdf https://www.vita.virginia.gov/commonwealth-security/awareness-toolkit/faqs/
Washington	Washington State Significant Cyber Incident Annex	https://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf

Summary of Methodology:

This chapter discussed the research methodology used in this study. A content analysis was used to operationalize the conceptual framework. The next chapter will provide the results of this analysis.

Chapter IV: Results

Chapter Purpose:

The purpose of this chapter is to see the results of the content analysis examining how close ten state incident response plans are to the practical model the National Institute of Standards Technology (NIST). The analysis includes the frequency of discussion of the different categories and elements of each state plan as defined in the conceptual framework. The results are organized and categorized by the framework.

State Incident Response Plans

This content analysis shows that incident response plans emerged as one of the most important issues for governments and businesses in the twentieth century. States have a number of different names for their incident response plans, including “Action Plan,” “Disruption Response Strategy,” “Information Security Plan,” and “Joint Cyber Incident Response Guide.” State governments’ reliance on advanced technology has come with a price: not having the right measures in place to prevent disruption of critical computer systems, denial-of-service attacks, and exposure of citizens’ data to hackers and terrorists.

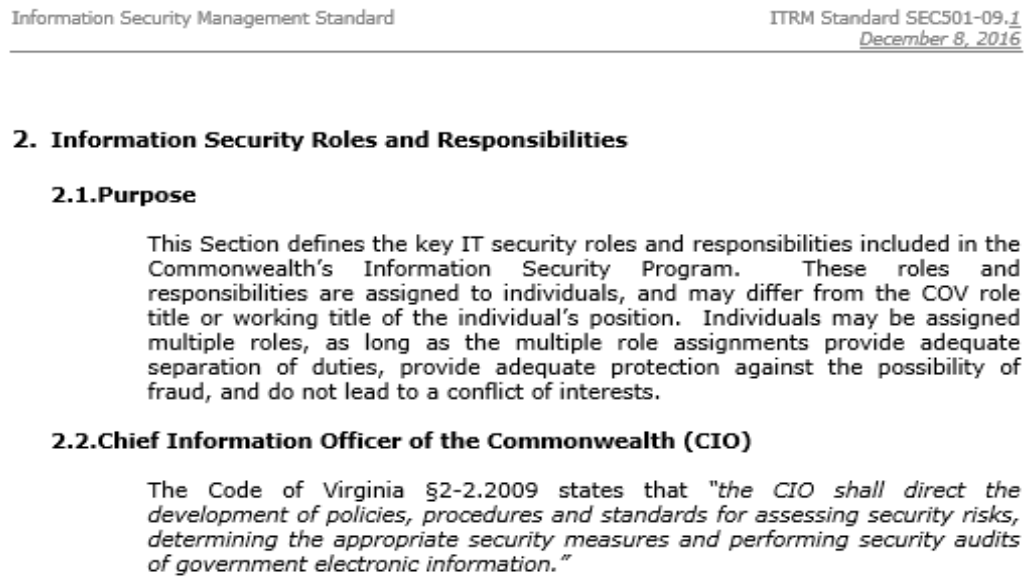
Table 4.1 Incident Response Team Structure

Assessment Category	Well Done	Adequate	Minimal	No Discussion	Total
Chief Information Officer	2	0	6	2	10
Incident Response Policy, Plan and Procedures	5	4	1	0	10
Team Models and Selection	4	5	1	0	10

On two of the three "Team Structure" categories, the states were doing fairly well. Nine of the ten states (See Table 4.1) were rated as "*well done*" or "*adequate*" for "Incident Response Policy, Plan and Procedures" and Team Models and Selection. Only two of the ten states identified the "Chief Information Officer" clearly (six had a minimal discussion, and two had no reference to the Chief Information Officer. There does seem to be room for improvement on this category particularly for the identification of the Chief Information Officer.

For example, Virginia was rated "*well done"* because it clearly defined the CIO's role and responsibilities and gave the CIO the power to develop response policies and procedures for assessing cyber threats (Illustration 4.1). Illustration 4.2 shows that Texas was rated "*well done"* for "Incident Response Policy, Plan and Procedures." Texas provided a well-developed template and often referred to the NIST model for government agencies. Illustration 4.3 shows that Texas's did "Team Models and Selection" were also rated "*well done*". The team model's contact roster was clearly defined with the key leader, which will enable team members to assimilate information in a timely manner and stay ahead of unfolding situations.

Illustration 4.1 Virginia Chief Information Officer *



Information Security Management Standard — ITRM Standard SEC501-09.1 December 8, 2016

2. Information Security Roles and Responsibilities

2.1. Purpose

This Section defines the key IT security roles and responsibilities included in the Commonwealth's Information Security Program. These roles and responsibilities are assigned to individuals, and may differ from the COV role title or working title of the individual's position. Individuals may be assigned multiple roles, as long as the multiple role assignments provide adequate separation of duties, provide adequate protection against the possibility of fraud, and do not lead to a conflict of interests.

2.2. Chief Information Officer of the Commonwealth (CIO)

The Code of Virginia §2-2.2009 states that *"the CIO shall direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government electronic information."*

Source *
https://www.vita.virginia.gov/media/vitavirginiagov/resources/presentations/pdf/InformationSecurityIncidentResponseProcedure.pdf

Illustration 4.2. Texas Incident Response Policy, Plan and Procedures *

SECTION 2

Incident Response Policy

Each agency should have a policy to address compliance with privacy and security breach management. Below is a sample policy which should be replaced by each agency and should be consistent with the agency's incident response plan.

2.1 Sample Security Incident Response Policy

Purpose

The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with the Texas Administrative Code, Title 1, Chapter 202. This document sets forth the policy for incident management within the Agency.

Scope

This policy applies to and must be complied with by all Agency Users.

The User agrees to abide by this policy while employed or contracted with the Agency.

Roles and responsibilities of each function pertaining to the protection of Agency-owned systems and data are documented in Agency policy.

The User is responsible for understanding the terms and conditions of this policy.

Exemptions to this policy shall follow the process defined in Agency policy.

This policy is subject to change.

This policy applies to any computing device owned or leased by the Agency. It also applies to any computing device regardless of ownership, which either is used to store Agency-owned Confidential or Agency-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.

Policy

The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Information Resources Manager (IRM) for approval. 1 TAC §202.26

The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that fall under one or the following categories: 1 TAC §202.26

- Propagation to external systems
- Violation of applicable federal and/or state laws which will require involvement from law enforcement

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.2.-1 Texas Incident Response Policy, Plan and Procedures *

	• Potential modification or disclosure of Confidential Information as defined in the Agency Data Classification Policy.	
	The Agency shall notify appropriate individuals (which must include the State CISO and the State Cybersecurity Coordinator) within 48 hours if it is believed that personal information owned by the Agency has been used or disclosed by or for unauthorized persons or purposes.	TGC §2054.1125, TBC §521.053
	The ISO shall establish an Incident Criticality matrix. This matrix will define each level of escalation, detail the appropriate response for various incidents, and establish the appropriate team participants.	1 TAC §§202.21-22
	The ISO shall establish and document appropriate procedures, standards, and guidelines regarding Incidents.	1 TAC §202.21
	The ISO is responsible for determining the physical and electronic evidence to be gathered as part of the incident investigation. Any electronic device containing data owned by the Agency may be subject to seizure and retention by the ISO.	
	The Chief Information Security Officer, Chief Privacy Officer, or Agency General Counsel (as appropriate) will work directly with law enforcement regarding any Incidents that may have violated federal or state laws. If an Incident is determined to be the result of a privacy violation by a User, the ISO shall notify the User's supervisor and Human Resources of the violation(s), or the Inspector General's Office, as applicable, for appropriate action.	
	The ISO shall provide a summary report for each valid Security Incident to the IRM within five business days after the incident has been closed.	
Disciplinary Action	Management reserves the right to revoke access at any time for violations of this policy and for conduct that disrupts the normal operation of agency information systems or violates state or federal law.	
	Any User who has violated this policy may be subject to disciplinary action, up to and including termination of employment or contract with DIR.	
	The Agency will cooperate with appropriate law enforcement if any User may have violated federal or state law.	
Document Change Management	All changes to this document shall follow the process defined in Agency policy.	
	The ISO will be responsible for communicating the approved changes to the organization.	1 TAC § 202.21

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.3 Texas Team Models and Selection*

7.2 IRT Charter

Information Privacy or Security Incident Response Team Charter

Charter Purpose:

This Incident Response Team (the "IRT") Charter establishes membership, subject matter experts, roles, responsibilities, and activities of the [agency] IRT to respond to an actual or suspected information privacy or security event/incident.

IRT Mission:

The IRT mission is, first, to prevent incidents by reasonably anticipating, detecting, and planning for actual and suspected privacy or security events; and second, to respond to and mitigate privacy or security events.

Overview:

The Incident Response Team (the "IRT") is a standing team of internal personnel established by [Executive Management] in this [Charter] with expertise in responding to a significant actual or suspected privacy or security event or incident. The IRT operates on behalf of [Executive Management] and engages, informs, and receives support from [Executive Management]. There [is/is not] a set protocol to initiate the IRT activities in response to an actual or suspected event/incident. Once activated, the IRT has authority to [request cooperation/establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours].

Responsibilities and Roles:

Responsibilities:

1) **Anticipate and prepare** [the agency] for privacy or security events/incidents which can be reasonably anticipated;
2) **Respond** to actual or suspected events/incidents on behalf of [the agency] as needed, with activities such as:
    a. Triage (see section 2);
    b. Communication, internal and external, as needed according to [agency's] communications protocol (e.g. funneled to the top from a deputy, for example) (see communications templates)
    c. Track and document IRT activities and discoveries; and
    d. Prepare post-event/incident analysis and lessons learned.

Examples of significant events/incidents within IRT responsibility:

- Uncontained or escalating malware attack on system (computer virus, worm, bot, or Trojan);
- Abuse, theft, misuse, or loss of data or hardware (including unauthorized use, disclosure, or access to computer accounts, systems, or data; hacking; human error);

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.3-2 Texas Team Models and Selection *

- Improper use or disclosure of information or information resources as outlined in [agency] standards or contracts including e-mail, equipment, Internet, and acceptable data use (includes human resources or contractor misuse or error);
- Many individuals or a large amount of sensitive data impacted; or
- Events likely to be high-profile or create a significant risk of individual harm (e.g., risk of financial harm, reputational harm, or medical identity theft).

Roles:

1) **The IRT Lead.** The Lead of the IRT may:
    a. Be designated by and reporting to [Executive management]. The IRT is led by [_____] or his or her designee.
    b. Declare an incident
    c. Establish, maintain, and update written IRT protocols or incident response plans
    d. Identify roles and responsibilities for IRT standing members
    e. Request or designate ad hoc members for particular events as needed
    f. [request cooperation / establish event response priorities which may supersede daily business responsibilities or require attention outside normal business hours]

2) **IRT Standing Members.** The standing members include named individuals or representatives.

3) **Ad hoc Members or Subject Matter Experts.** Ad hoc members or Subject Matter Experts may be designated as ad hoc resources by the IRT Lead.

Source *
https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.3-3 Texas Team Models and Selection*

7.3 IRT Membership by Roles

The following table contains contact information for current IRT members. Please note that, in some cases, a member listed below may have designated another agency employee to represent him or her. Also, while the IRT generally is composed of standing members, under certain circumstances the formation of an ad hoc group may be necessary.

Standing IRT Membership Contact Information - *Confidential*

Standing Members	Name	Phone	Email	After-hours contact
IRT Lead				
[Chief Information Officer or designee]				
[Chief Information Security Officer or designee]				
[Information Resources Manager or designee]				
[Internal Audit]				
[Office of Inspector General]				
[Other]				
[Other]				
[Other]				
Legal Counsel to the IRT – to avoid losing attorney-client privilege, *do not list legal as a member*				

Ad Hoc IRT Members

Ad hoc Members	Name	Phone	Email	After-hours contact
[Relevant business area, department, division]				
[Communications]				
[External Relations]				
[Open Records]				
[Third parties, e.g., contractor]				
[Department of Information Resources designee]				

Source *
https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.3-4 Texas Team Models and Selection *

7.6 IRT State Government Contact Information

IRT State Government Contact Information

Entity	Contact	Division/Location	Email/Office Telephone
Office of the Governor			
Lieutenant Governor			
Speaker of the House			
State of TX Office of the Chief Information Security Officer			
State Cybersecurity Coordinator			
[Agency Board or Commission Chair]			
[Agency Oversight Senate Committee Chair]			
[Agency Oversight House Committee Chair]			

Source*

https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Table 4.2 Handling an Incident

Assessment Category	Well Done	Adequate	Minimal	No Discussion	Total
Preparation	3	5	2	0	10
Detection and Analysis	4	4	2	0	10
Containment Eradication and Recovery	3	5	2	0	10
Post – Incident Activity	3	6	1	0	10
Incident Handling Checklist	1	6	3	0	10

Eight of the ten states (See Table 4.2) were rated as "*well done*" or "*adequate*" for "Preparation, "Detection and Analysis" and "Containment Eradication and Recovery." "Post-Incident Activity" was the strongest, with nine of the ten states rated as "*well done*" or "*adequate*". Incident Handling Checklist was the weakest with seven of the ten states rated as "*well done*" or "*adequate."*

For example, as Illustration 4.4 shows, Connecticut was rated "*well done*" on "Preparation." Connecticut is creating a robust cyber literacy program to educate grade-school children and government employees. Illustrations 4.5 and 4.6 show that California was rated "*well done*" in "Detection and Analysis" and in "Containment, Eradication, and Recovery." California's plan includes personal problem-solving techniques for detecting and analyzing cyber incidents, and external resources such as outside agencies provide help and advice. California's plan also provides guidance on developing short- and long-term strategies for containing a breach and eliminating the root cause. Illustration 4.7 shows that Texas was rated "*well done*" on "Post-Incident Activity." Texas's plan provides lessons on techniques such as follow-up reporting, data collection, restoring systems, and root cause analysis. Illustration 4.8 shows that Maryland was rated "*well done"* on "Incident Handling Checklist." Maryland's checklist identifies key events that must happen in each phase of the response to an incident.

Illustration 4.4-1 Connecticut Preparation *

Municipal Government

Goals

Each Connecticut municipality needs to make cybersecurity awareness and cybersecurity defense top priorities, relevant to its distinct character. Our goal is for municipal governments to create serious, effective cybersecurity programs to protect citizens and municipal governments and to help make Connecticut a national leader in cybersecurity defense. We seek to have municipalities become active participants in the state culture of cybersecurity responsibility and hygiene and to create effective, local programs to enhance statewide security. Recognizing the value of shared experiences, templates and suggested municipal guidelines should be available and crafted to fit the needs of each distinct municipality. Simultaneously, appropriate local solutions may be most effective and affordable if managed within a regional context in cooperation with state law enforcement and management authorities.

Executive Awareness and Leadership

The critical first step is leadership. The top elected municipal official, the governing board and the head administrative officer all need to recognize the primacy of Connecticut's cybersecurity challenges and advocate for cybersecurity awareness and defense, underscoring the fact that effective cyber defense involves all citizens and is not simply a matter of information technology or management.

A key municipal responsibility should be determination of the adequacy of technical and management defense systems. Recognizing that cyber penetration is possible from any point of municipal communication or operation, both cultural and practice hygiene need to extend throughout local government.

Leadership applies to regional and association cooperation as well. To share lessons learned and best practices, Connecticut municipalities should have the benefit of cybersecurity expertise and practices from the Connecticut Conference of Municipalities (CCM), the Connecticut Interlocal Risk Management Agency (CIRMA), the Council of Small Towns (COST), Connecticut's nine Councils of Government (COGs) and the DEMHS Regional Emergency Planning Teams. These organizations should play leading roles in advancing action plans and supporting municipal cybersecurity defense and response.

Cyber Literacy

The use of shared education programs, adopted appropriately for local use, can help bring municipal employees up to appropriate levels of cyber literacy. All current and future municipal employees need to receive basic education in cybersecurity awareness. Some functions will require customized

Source *
https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en

Illustration 4.4-2 Connecticut Preparation

training. Risk reports to municipal governing authorities should have descriptions of education programs including annual or refresher programs and assessments regarding the extent to which municipal employees have completed them.

Key to building a more secure cybersecurity environment for Connecticut's future is creation of effective education programs in K-12 curricula designed to promote safe computing concepts and practices.

Preparation

Connecticut's towns and cities need to prepare for and rehearse responses to the disruptive effects of a cyber incident or attack ranging in severity from a ransom demand or compromise of personal information such as tax and medical information to the effects of prolonged absence of public utilities. Some specific steps can start the preparation process:

1. Assessment of the steps necessary to prevent a ransom attack and plans to manage an attack should one occur;
2. Plans to protect municipal tax and other sensitive citizen information and to communicate with victims and manage response should there be compromise. Larger cities would benefit from conducting data inventory and classification, while smaller municipalities could survey exposure by completing a data security plan, sometimes called a "written information security plan," or "WISP."
3. Confrontation of the reality that cyber exposure requires both financial and personnel resources while all Connecticut cities and towns face difficult budget constraints. Municipalities have to decide how to reduce risk to acceptable levels, how to reach cost-effective decisions and share regional solutions and whether to purchase cyber insurance. Sharing of common best practices can produce enhanced collective defense, including up-to-date patching, multi-factor authentication, frequent renewal of appropriately complex passwords and assignment of greater levels of personnel for the most critical functions.
4. Definition of municipal cyber crimes and plans to manage them. Decisions regarding municipal, regional and state police protection and investigation capabilities in the event of a cyber crime, and if municipal police are not able to respond, plans regarding guidance to municipal citizens;
5. Recognition that the consequences of a prolonged absence of public utility services would present unprecedented strains on local communities and require expansion of existing severe weather/mutual aid scenarios. Connecticut municipalities need to prepare for the consequences of long outages. Challenges could include heating or cooling shelters, requirement for extended first-responder duty, food, water and medicine shortages and public order disruptions;

Source *
https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en

Illustration 4.4-3 Connecticut Preparation

6. Recognition that a cyber incident could bring public anxiety and panic. Unusual communication demands and channels, such as social media, need to be foreseen and planned; and
7. Awareness of how municipal governments will execute their Cyber Incident Response Plans as part of their Local Emergency Operations Plans and awareness of municipal roles in the State Cyber Disruption Response Plan.

Source *
https://portal.ct.gov/-/media/DAS/BEST/Security-Services/CT-Cybersecurity-Action-Plan-Final.pdf?la=en

Illustration 4.5-1 California Detection and Analysis *

2 Detection

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

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

- **External Agency IDS/IPS.** Provides near real-time threat detection based upon rulesets developed according to an entity's cybersecurity strategy.
- **External Agency Notification.** Phone calls, email, text, postal mail and voice notification are some of the many methods of communication to consider.
- **Open Source**. Information gathered from publicly available sources as news web sites, government web sites, books, and periodicals.

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

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

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

1) Authentication: The system administrator could simply review the Security Information and Event Management (SIEM) logs to understand the account in question and reason for error and advise the ISO
2) Data Handling: The administrator can review SIEM and Active Directory logs to understand the nature of the requests – this could simply be the case of user rights management issues or it could lead to an investigation
3) Data Exfiltration: The system administrator may immediately cease all applicable activities related to the incident in question, secure their workstation or area and contact the appropriate ISO or their representative to begin preserving the information or evidence of questionable activities. Do not turn off power to the device in order to allow cybersecurity personnel to conduct forensics.
4) System Availability: The administrator may review SIEM logs to understand the activity in question and prepare to restore services from a backup and actively review firewall logs

Source * https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.5-2 California Detection and Analysis *

5) Physical: Coordinate with the ISO and the facility infrastructure team to understand the nature of the event and understand how to implement secondary power and possibly provide security personnel to protect the physical perimeter and sensitive areas
6) Other: Disable the user account, take a screenshot and turn in, unplug the computer from the network, actively log authentication and access actions, etc.

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

3 Analysis

The investigation of the incident should include an Event Threat and Impact Analysis in order to categorize the impact of the event on the organization. Once the event's impact level is understood it may be appropriate to escalate the incident response and contact other entities.

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

3.1 Impact Analysis

3.1.1 Functional Impact

Incidents may affect the confidentiality, integrity, and availability of the organization's information.

Category	Definition
None	No effect to the organization's ability to provide all services to all users.
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency.
Medium	Organization has lost the ability to provide a critical service to a subset of system users.
High	Organization is no longer able to provide some critical services to any users.

Table 2 - Examples of Functional Impact Categories

Source *
https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.5-3 California Detection and Analysis *

3.1.2 Information Impact

Incidents may affect the confidentiality, integrity, and availability of the organization's information.

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

Table 3 - Possible Information Impact Categories

3.1.3 Recoverability

The size of the incident and the type of resources it affects will determine the amount of time and resources that must be spent on recovering from that incident.

Category	Definition
Regular	Time to recovery is predictable with existing resources
Supplemented	Time to recovery is predictable with additional resources
Extended	Time to recovery is unpredictable; additional resources and outside help are needed
Not recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated/leaked and posted publicly); launch investigation.

Table 4 - Recoverability Effort Categories

3.2 Types of Threat

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

3.3 Physical Considerations

Any incident involving or affecting physical systems or critical infrastructure mandates the participation of the applicable Critical Infrastructure Protection (CIP) team(s). Incidents involving physical infrastructures have additional considerations in addition to the typical cyber related attacks. Now CIP centric organizations have to consider more than simply network protection principles; they must also take into consideration the acquisition and replacement of systems on the network.

Source *
https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.5-4 California Detection and Analysis *

The Federal Energy Regulatory Commission (FERC) Order 829 mandated additional controls addressing cyber security supply chain risk management for ICS hardware, software and computing services associated with Bulk Electric Systems (BES).

3.3.1 North American Electric Reliability Corporation (NERC) Standards

The North American Electric Reliability Corporation (NERC) created implementation guidance CIP-013-01 to assist with Supply Chain Risk Management. There are many other NERC sponsored standards that may also apply and warrant heavy consideration.

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization		Subject to Enforcement
CIP-003-6	Cyber Security - Security Management Controls	Related Information	Subject to Enforcement
CIP-004-6	Cyber Security - Personnel & Training	Related Information	Subject to Enforcement
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)	Related Information	Subject to Enforcement
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems	Related Information	Subject to Enforcement
CIP-007-6	Cyber Security - System Security Management	Related Information	Subject to Enforcement
CIP-008-5	Cyber Security - Incident Reporting and Response Planning	Related Information	Subject to Enforcement
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems	Related Information	Subject to Enforcement
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments	Related Information	Subject to Enforcement
CIP-011-2	Cyber Security - Information Protection	Related Information	Subject to Enforcement
CIP-014-2	Physical Security	Related Information	Subject to Enforcement

Table 5 – Sample NERC Standards

Source * https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.6 California Containment Eradication and Recovery *

4 Containment

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

The containment plans are usually based on the findings of the security team's investigation of the incident. Often times, the plan relies on limited information gathered during the preliminary detection.

ISO and recovery teams must ensure they don't fall into this stove piped, single source technique of information analysis. Information is acquired from multiple sources based on the attack vector.

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

5 Eradication

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

6 Recovery

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

6.1 Data Recovery

The key to an effective data recovery strategy begins with a well planned and executed backup strategy. A back-up strategy may vary from company to company based on the data type, location, sensitivity, availability requirements, and / or data owners. Other variables may come into play such as location of the backup media or the SOW with an external data recovery vendor. Prior to any data restoration activities, the data owners should confirm with the data custodians of all the previous and current locations of any live or backup data.

6.2 Service Recovery

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

6.3 Site Recovery

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

Source * https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.7 Texas Post-Incident Activity *

SECTION 6

Post-Incident Checklist

The Computer Security Incident Handling Guide (NIST 800-61) provides advisement on event analysis activities. Per section 3.4.1 (Lessons Learned) and section 3.4.2 (Using Collected Incident Data) relevant factors for post-incident and root cause analysis include:

1) **Learning and improving.** Incident Response Teams should hold "lessons learned" meetings with all involved parties after a major incident, and periodically after lesser incidents as resources permit to improve security measures and incident handling processes. Questions to be answered in these meetings include:
    a. Exactly what happened, and at what times?
    b. How well did staff and management perform? Were documented procedures followed? Were procedures adequate?
    c. What information was needed sooner?
    d. Were any steps or actions taken that might have inhibited the recovery?
    e. What would/should staff and management do differently the next time a similar incident occurs?
    f. How could information sharing with other organizations have been improved?
    g. What corrective actions can prevent similar incidents in the future?
    h. What precursors or indicators should be watched for in the future to detect similar incidents?
    i. What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

2) **Follow-up reporting.** An important post-incident activity is creating a follow-up report for each incident. Report considerations include:
    a. Creating a formal event chronology (including time-stamped information from systems);
    b. Compiling a monetary estimate of the amount of damage the incident caused;
    c. Retaining follow-up reports as specified in retention policies.

3) **Data collected.** Organizations collect data that is actionable and decide what incident data to collect based on reporting requirements and perceived value of data collected. Information of value includes number of incidents handled and relative ranking for event types and remediation efforts, and amount of labor and time elapsed for and between each phase of the event.

4) **Root Cause Analysis.** Organizations performing root cause analysis should focus on relevant objective assessment activities including:
    a. Reviewing of logs, forms, reports, and other incident documentation;
    b. Identifying recorded precursors and indicators;
    c. Determining if the incident caused damage before it was detected;
    d. Determining if the actual cause of the incident was identified;
    e. Determining if the incident is a recurrence of a previous incident;
    f. Calculating the estimated monetary damage from the incident;
    g. Measuring the difference between initial impact assessment and the final impact assessment; and
    h. Identifying measures, if any, that could have prevented the incident.

Source *
https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template%202018.pdf

Illustration 4.8 Maryland Incident Handling Checklist *

Appendix E: Sample Incident Handling Checklist and Forensics Guidelines

Action	Done
Detection and Analysis	
Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
Identify which resources have been affected and forecast which resources will be affected	
Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery	
Acquire, preserve, secure, and document evidence	
Contain the incident	
Eradicate the incident	
Identify and mitigate all vulnerabilities that were exploited	
Remove malicious code, inappropriate materials, and other components	
Recover from the incident	
Return affected systems to an operationally ready state	
Confirm that the affected systems are functioning normally	
If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity	
Create a follow-up report	
Hold a lessons learned meeting	

Refer to the corresponding tables within NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for specific incident category guidance.
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

Incident Response and Forensics Guidelines

Preserving forensic data is an essential aspect of any incident response plan. The forensic data acquired during the overall incident response process is critical to containing the current intrusion and improving security to defend against a similar future attack. The following guidelines are provided to assist agencies in the retention of essential forensic data.

Keep detailed notes of all observations, including dates/times, mitigation steps taken/not taken, device logging enabled/disabled, and machine names for suspected compromised equipment. More information is generally better than less information.

When possible, capture live system data (i.e., current network connections and open processes) prior to disconnecting a compromised machine from the network.

Capture a forensic image of the system memory prior to powering down the system.

Source * https://doit.maryland.gov/Publications/DoITSecurityPolicy.pdf

Table 4.3 Coordination and Information Sharing

Assessment Category	Well Done	Adequate	Minimal	No Discussion	Total
Coordination	3	6	1	0	10
Information Sharing Techniques	3	6	1	0	10
Granular Information Sharing	3	6	1	0	10

Nine of the ten states were rated "*well done*" or "*adequate*" in "Coordination and Information Sharing". These results were stronger than for "Incident Response Team Structure" because in that case, there were no plans and no discussion. A good example is California's plan, shown in Illustration 4.9. Their contact roster has building addresses and direct phone numbers for each agency.

`

Illustration 4.9-1 California Coordination and Information Sharing *

Appendix D – Federal Contacts

Resource	Services	Contact Information
Federal Bureau of Investigation	Cyber squads in each field office investigate high-tech crimes, including computer intrusions and theft of personal information.	California Field Offices **Sacramento:** 2001 Freedom Way Roseville, CA 95678 **Phone:** (916) 746-7000 **San Francisco:** 450 Golden Gate Avenue, 13th Floor San Francisco, CA 94102-9523 sanfrancisco.fbi.gov **Phone:** (415) 553-7400 **Los Angeles:** 11000 Wilshire Boulevard Suite 1700 Los Angeles, CA 90024 losangeles.fbi.gov **Phone:** (310) 477-6565 **San Diego:** 10385 Vista Sorrento Parkway San Diego, CA 92121 sandiego.fbi.gov Phone: (858) 320-1800
Federal Emergency Management Agency (FEMA)	Provides disaster response and recovery assistance.	1-800-621-FEMA (3362)
National Cyber Security Division (NCSD), US Dept. of Homeland Security	Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.	Response coordination: (202) 282-8000
CERT Coordination Center (CERT/CC)	Federally-funded CERT provide technical advice to federal, state, and local agencies on responses to security compromises.	CERT 24-hour hotline: (412) 268-7090 forensics@cert.org
US Secret Service	Investigates financial crimes, including identity theft.	**Sacramento Field Office:** 501 I Street, #12100 Sacramento, CA, 95814-2322 **Phone:** (916) 325-5481 **San Jose Field Office:** 28 0 S First Street, #1111 San Jose, CA, 95113 **Phone:** (408) 535-5288 **Fresno Field Office:** 52 00 North Palm Avenue, #207 Fresno, CA, 93704 **Phone:** (559) 487-5204
US Treasury Inspector General for Tax	Works with agencies to ensure that all appropriate actions are taken with regard to Federal Tax Information.	TIGTA Field Division, Dallas: (972) 308-1400

Source *
https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Illustration 4.9-2 California Coordination and Information Sharing *

Administration (TIGTA) and Office of Safeguards		
Federal Trade Commission (FTC)	Regulates consumer business practices.	http://www.ftc.gov Detecting identity theft: http://www.ftc.gov/idtheft
National Institute of Standards and Technology (NIST), US Dept. of Commerce	Advances US measurement science, standards, and technology, including accelerating the development of and deployment of standards and systems that are reliable, usable, interoperable, and secure. Assigned certain information security responsibility under the Federal Information Security Management Act of 2002 (FISMA, 44 USC § 3541, *et seq.*). NIST has published over 200 information security documents on information security standards, guidelines, and other resources necessary to support the federal government.	Main office: (301) 975-NIST inquiries@NIST.gov http://www.nist.gov/index.html Publications: http://csrc.nist.gov/publications/
Office for Civil Rights (OCR), US Dept. of Health and Human Services	Oversees federal civil rights and health information privacy, security, and breach notice by HIPAA.	http://www.hhs.gov/ocr/office/index.html
US Postal Service Inspector Service	The law enforcement arm of the US Postal Service, which investigates crimes that may adversely affect or fraudulently use the US Mail, the postal system, or postal employees.	https://postalinspectors.uspis.gov

Source *
https://www.caloes.ca.gov/LawEnforcementSite/Documents/CaliforniaJoint%20Cyber%20Incident%20Response%20Guide.pdf

Summary of Results:

This chapter provided the results of the content analysis of states' incident response plans. These plans incorporated a good portion of the NIST framework, but much room for improvement remains. The next chapter provides some recommendations and conclusions based on these results.

Chapter V: Conclusion

Chapter Purpose

The purpose of this chapter is to review and summarize the finding from the research presented in this study. The results from the previous chapter will be discussed and the purpose behind the study and make recommendations.

Research Summary

The study analyzes ten states' incident response plans. The first chapter introduced the study and the purpose. Chapter two provided the background history of cybersecurity, threats to organizations, and scholarly literature on incident response plan. Chapter three provided the conceptual framework for the study. Chapter four provided the results from the ten states that was analyzed. Lastly, chapter five concludes the study by summarizing the findings of chapter four and offering recommendation.

Findings

The content analysis shows that more work is needed to strengthen states' incident response plans. The plans are very generic and have a diversity of names, and the states' governors are heavily involved in the plans. But many states lack a chief information officer and a chief security officer, and their IT teams are limited in manpower, which makes it difficult for them to respond in a timely matter. With limited manpower, it is imperative that IT teams be highly proficient in their duties. The governors have given these agencies the freedom to tailor policies, plans, and team models according to their manpower. Regarding incident handling and coordination, most plans cited the NIST framework and tailor it to their own organizations. Overall the state of Texas had the best incident response plan.

Recommendations

Incident Response Team Structure

The content analysis shows that most states lacked a CIO and CSO. A cyber incident response plan must be spearhead by a subject-matter expert. CIOs and CSOs brings a wealth of knowledge, software-development skills, leadership, strategic planning, and project management skills that can prevent organizations from depending on limited manpower and relying too heavily on technology-monitoring devices to track activity on the network.

The incident response policies, plans and procedures, and team models are still very generic. Policies should set the roles of teams and be tailored to specific government agencies. The key elements of a policy are the mission statement and purpose, organizational structure, and reporting requirements. A good incident response plan contains clear, concise procedures that are easy to follow and include all the steps necessary in the event of a cyber incident. The lack of a concrete policy, plans, and procedures leads to confusion and overcomplication and slows down the reporting of incidents.

Handling an Incident

Preparation is the most important phase of incident response. If you fail to plan, then you plan to fail. The state plans were reactive than proactive. In the preparation phase, it is imperative for states to set priorities, get buy-in from leadership and team members, and identify what a cyber breach looks like for that organization. It is also important to determine which team is responsible for what in each phase of the incident, such as containment, eradication, and post-incident events, and to ensure that team members have all the tools necessary to handle an incident, such as a jump bag. Key items to include in jump bags are a laptop with forensic software, contact information for law enforcement, a notebook, a checklist, and flow charts.

Checklists and flow charts are easy to use and effective and provide standards and benchmarks for people to meet. A good checklist and flow chart allow people to be more productive and comfortable about managing multiple tasks.

State plans should also incorporate cyber literacy and training programs for employees. The primary objective of cyber literacy is to build on shared knowledge and skills. At the end of the day, people are your greatest assets, but they can also be your biggest liability. An organization is only as good as its weakest link. Cyber literacy is designed to change peoples' behaviors and reinforce the proper safeguarding of data.

Coordination and Information Sharing

State plans must include good information-sharing practices and identify the personnel who will release information to law enforcement, the media, legal teams, and forensics teams by establishing release agreements. These agreements outline the "5 Ws": who, when, what, why, and how. There should also be a contact roster and a flow charts of afterhours for agencies that need to be contacted in the event of a cyber breach. The key personnel to include on the roster are the CIO, legal team, media team, and law enforcement. There must also be drafted emails with talking points to assist in communicating with outside agencies. Once these plans and agreements have been established, the plan must be rehearsed and updated and become a part of the organization's annual training

Additional Recommendation

Because of the constant changes in technology, there is no one solution to fix all cyber-attacks. No organization is immune to cyber-attacks, and an established incident response plan can prevent damage to systems, reputations, finances, productivity, and critical information. States should look at a militaristic model in cyber security to push out standardization across

platforms. Think tanks such as the MITRE Corporation work with Homeland Security to build and deploy active cyber threats in real time across the Department of Defense. But Homeland Security needs to also work with a system of architecture teams who will create a standardized, extensible model that can be deployed across all states, regardless of human intervention. As cyber threats from China and Russia continue to evolve, it is imperative to standardize platforms and ensure that they can all be synchronized for a unified security framework. The findings in this paper do not extend into defensive and offensive cyber security to analyze types of attacks and how they are dealt with. But at a minimum, states must ensure that their defensive postures align with those of the Departments of Homeland Security and Defense.

Lines of efforts generated by Homeland Security should provide technologies states can use to meet operational policies. Defensive tools such as Shodan allow organizations with constraints to scan all their web-facing protocols to ensure that standards are met on equipment and applications. The migration of organizations toward network less environments on the cloud will allow for standardization to be spread across them more rapidly. Products such as Elastic Load Balancing on Amazon EC2 servers allow organizations to host applications and networks at multiple sites to avoid downtime and service interruptions. Moving away from a hardware model and toward a software-defined environment allows for the best practices and policies to be written as rules within the environment.

Conclusion

This chapter provided findings of the content analysis of state incident response plans and provided recommendations based on this. The results indicate that much work remains to be done to strengthen state plans. Having an CIO in place will ensure that government agencies focus on the right tasks and put the right internal controls in place. Governance, risk, and compliance must be every organization’s number-one priority. A well-developed plan will have

forcing functions that include a risk assessment to ensure that the organization is on the right path.

Key Terms

Acceptable Use Policy (AUP)	An AUP is list of rules you must follow in order to use a website or Internet service. It is similar to a software license agreement (SLA), but is used specifically for Internet services. (Tech Terms, n.d)
Data Breach	The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. (DHS, 2014)
Data Loss	The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party. (DHS,2014)
Encryption	The process of transforming plaintext into ciphertext. Converting data into a form that cannot be easily understood by unauthorized people (DHS, 2014)
Malware	Software that compromises the operation of a system by performing an unauthorized function or process. (DHS, 2014)
Penetration Testing	An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system. (DHS, 2014)
Phishing	A digital form of social engineering to deceive individuals into providing sensitive information. (DHS, 2014)
Social Engineering	Refers to tricking people into divulging personal information or other confidential data. It is an umbrella term that includes phishing, pharming, and other types of manipulation. (Tech, Terms, n.d)
Virtual Private Network (VPN)	A virtual private network is "tunneled" through a wide area network WAN such as the Internet. (Tech, Terms, n.d)
Vulnerability	A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. (DHS, 2014)

Bibliography

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. *ICIS 2006 Proceedings*, 94.

Babbie, E.R. (2010). The practice of social research 12th Edition. Belmont, CA: Wadsworth, Cengage Learning.

Böhme, R. (2016). *The economics of information security and privacy*. Berlin: Springer Berlin.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–48.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

Cichonski, P., Grance, T., Millar, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.* United States Department of Commerce. Retrieved from https://nvlpubs .nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Connell, G. (n.d.). 5 benefits of having a proactive incident response plan. Retrieved from http://info.garlandheart.com/blog/5-benefits-of-having-a-proactive-incident-response-plan

Deere, S. (2018, Aug. 02). Confidential report: Atlanta's cyber attack could cost taxpayers $17 million. *Atlanta Journal-Constitution*. Retrieved from http://www.ajc.com/news/ confidential-report-atlanta-cyber-attack-could-hit-million /GAljmndAF3EQdVWlMcXS0K/

Dhillon, G. (2015). What to do before and after a cybersecurity breach. Retrieved from

https://www.american.edu/kogod/research/cybergov/upload/what-to-do.pdf

Department of Homeland Security. (2014). A glossary of common cybersecurity terminology. National Initiative for Cybersecurity Careers and Studies. Retrieved from http://niccs.us-cert.gov/glossary#letter_c

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review*, *45*(1), 67–87.

Eccles, R. G., Newquist, S. C., & Schatz, R. (2007). Reputation and its risks. *Harvard Business Review*, *85*(2), 104.

Eckert, C. (2017). Corporate reputation and reputation risk: Definition and measurement from a (risk) management perspective. *Journal of Risk Finance*, *18*(2), 145–58.

Fidler, B. (2017). Cybersecurity governance: A prehistory and its implications. *Digital Policy, Regulation and Governance*, *19*(6), 449–65.

Fombrun, C. J. (2012). The building blocks of corporate reputation: Definitions, antecedents, consequences. In M. L. Barnett & T. G. Pollock (Eds.), *The Oxford Handbook of Corporate Reputation* (pp. 94–113). Oxford, UK: Oxford University Press.

Gelinas, R. R. (2010). Cyberdeterrence and the problem of attribution.

Grance, T., Kent, K., & Kim, B. (2004). *Computer security incident handling guide: Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: National Institute of Standards and Technology.

Gawande, A. (2009*). The checklist manifesto: How to get things right.* Gurgaon, India: Penguin Random House.

Haizler, O. (2017). The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking.

Hütter, A., & Riedl, R. (2017). *Chief information officer role effectiveness: Literature review and implications for research and practice.* Cham, Switzerland: Springer Nature.

Kamar, H. (2017). *What is cybersecurity.* Rosen Publishing Group.

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology and Information Management*, *26*(2), 23–47.

Kelly, B. (2016, March 01). 7 Steps to Cyberattack Containment and Eradication. Retrieved from https://blog.rackspace.com/cyberattack-containment-eradication

Killcrece, G. (2003). *State of the practice of computer security incident response teams (CSIRTs).* Pittsburgh, PA: Carnegie Mellon University Software Engineering Institute.

Lawry, R., Waddell, D., & Singh, M. (2007, June). Roles, responsibilities and futures of chief information officers (CIOs) in the public sector. In *Proceedings of European and Mediterranean Conference on Information Systems (EMCIS)* (pp. 24–26).

Mansfield-Devine, S. (2016). Ransomware: Taking businesses hostage. *Network Security*, *2016*(10), 8–17.

Newman, L. H. (2018). The Bleak State of Federal Government Cybersecurity. Retrieved from https://www.wired.com/story/federal-government-cybersecurity-bleak/

Shields, Patricia and Rangarajan, Nandhini. (2013). A Playbook for Research Methods. Stillwater OK: News Forums Press, Inc.

Shields, P. M., & Tajalli, H. (2006). Intermediate theory: The missing link in successful student scholarship. *Journal of public affairs education*, *12*(3), 313-334.

Shields, P., & Whetsell, T. (2017). Public administration methodology: A pragmatic perspective. Eds. Raadshelders, J. and Stillman, R. *Foundations of Public Administration*. (75-92) New York: Melvin and Leigh.

Small Towns Confront Big Cyber-Risks [. (n.d.). Retrieved from https://www.govtech.com/security/GT-OctoberNovember-2017-Small-Towns-Confront-Big-Cyber-Risks.html

Spidalieri, F. (2015). State of the States on Cybersecurity. Retrieved from https://pellcenter.org/eight-states-lead-the-rest-in-cybersecurity/

Tech Terms Computer Dictionary. (n.d.). Retrieved from https://techterms.com/

White House. (2015). Executive order: Promoting private sector cybersecurity information sharing. (n.d.). Retrieved from https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

Wright, Craig, (2011). SANS Institute InfoSec Reading Room: Incident Handler's Handbook. Retrieved from https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

Zhao, J. J., & Zhao, S. Y. (2010). Opportunities and threats: A security assessment of state e-government websites. *Government Information Quarterly*, *27*(1), 49-56.