**Cybersecurity – Cybersecurity Incidence Response Plan**

**Getting Started**

Your agency has done all the right things, Cybersecurity Threat Assessments, end user training but the bad actors have succeeded and you find yourself a victim of a cyber-attack. Now what do you do?

You follow your Cybersecurity Incidence Response Plan!

An effective response plan needs to guide company personnel at all levels in managing a potential data breach in a way that supports rapid and thoughtful response activities. Guidance for Cybersecurity Incident Response Plans are provided in these documents:

The 2019 National Emergency Communications Plan (NECP) Goal 2: Planning and Procedures: Objective 2.3: Incorporate risk management strategies to protect against and mitigate disruptions to mission-critical communications

Success Indicator:

*Public safety organizations that use information technology have a cybersecurity incident response plan in place*

<https://www.cisa.gov/publication/2019-national-emergency-communications-plan>

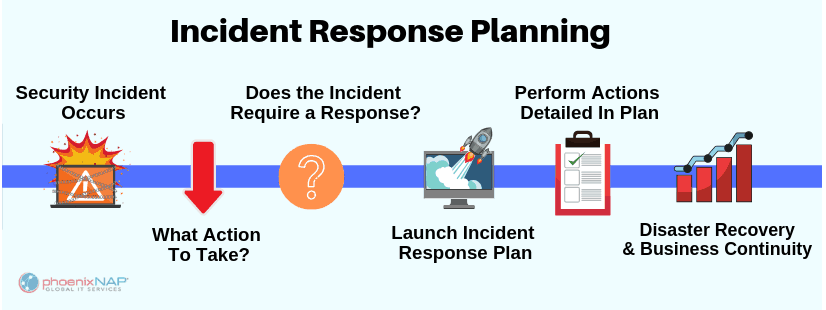
The Texas Statewide Interoperable Communications Plan (SCIP) has an initiative for agencies to prepare a Cybersecurity Incident Action Plan:

Goal 2. Planning and Procedures

Initiative 2.5 Agencies develop a cybersecurity incident response plan

<https://www.dps.texas.gov/IOD/interop/index.htm>

An Incident Response Plan has 6 phases that need to be addressed-- but don’t develop the incident response plan in a vacuum. Include all levels of the organization. Don’t forget that priorities for response can be derived from your Cybersecurity Threat Assessment. This document is a collection of several published articles and guidance documents noted in the reference section.



(image from phoenixNAP)

**Phase 1: Prepare**

This phase will take the most work, it’s not easy! Whether an agency prepares their own Incident Action Plan, or if a professional contract is put in place, this document provides information to consider in plan development. Before beginning formal planning, ECC, PSAP/9-1-1, LMR managers should discuss cyber threats with their agency ‘s or department’s senior  managers, their servicing IT departments, IT vendors, and with  budget officials to ensure planning is understood at various management levels, especially as regards the issue of ransom demands. These policy discussions can help define and qualify responsibilities (especially vendors’ contractual responsibilities for cyber security) before having to deal with an attack.

**1:** **Assemble an internal response team**: Team will guide the actions following a breach of substantial protected information. Team will advise top management of breach and response developments. These need to be decision makers (not necessarily C-Level); Risk Manager, Legal Counsel, PIO, IT Manager, HR Manager (potential PII, PHI exposure), Operations Managers

**2. Differentiate breaches**: Plan should have enough flexibility to establish an appropriate response dependent on the type and severity of the breach. Develop communications protocols dependent on the type of breach. Levels of response can be derived from your Cybersecurity Threat Assessment.

**3: Develop agency incident response training**: Theresponse team, and agency personnel should be trained in how to identify and recognize when a data breach has occurred, and what to do.

**4: Develop a communications plan**: Develop procedures to notify proper outside agencies (in Texas notify DIR), vendors that provide services on your network and law enforcement. Develop procedures to communicate internally as a team if networks are compromised.

**5: Develop evidence preservation plan**: Start an Incident Log, have computer forensics safely copy emails and other communications. Keep list of witnesses.

**6: Identify external data security resources**: When a breach happens is not the time to identify and contract the experts that can lead your recovery. Consider the following specialized resources: Legal Counsel, computer forensics, insurance brokers who specialize in cybersecurity policies

**7. Create an action item checklist**: Prioritized list of action items to be completed immediately after the breach has been identified. Time is critical, hesitation can be damaging. Checklist should at a minimum include:

* Start an incident Log: Date and time breach is discovered, and record all actions taken
* Finalizing and activating both internal and outside response teams and pre-determined plans (communications, evidence preservation) based on the type of breach
* Establish secure perimeter around equipment, taking potentially compromised equipment off line
* Conduct interviews of those with critical knowledge of events
* Computer forensic personnel onsite: make secure copy of affected systems
* Determine actions needed for the next several days

**8. Track legal obligations**: Identify any legal reporting obligations that must be met under state or federal law. Plan should track all data security related notification deadlines, and contract security provisions with vendors

**9. Financial Obligations**: Determine how to track all time and costs to mitigate the breach. Work with financial office to determine insurance coverage, contact information and limitations.

**10. Review, exercise and update the plan regularly:** Conduct (at least) annual review and make any necessary updates. Verify service provider arrangements are current. Conduct regular tabletop exercises to test the plan.

**Phase 2: Identify**

Identification or detection of a data breach looks for deviations from normal operations and activities.

Some of the most common indicators of compromise that should be monitored are:

* Unusual volume or repetition of disk or network activity, especially in normally low activity time frames
* Activity on unusual network ports
* Unexpected software or processes such as network scanners, or credential gathering programs
* Configuration changes that can’t be tracked back to a known update, especially with antivirus protection software
* Unusual user activity
* Unexpected user account lockouts
* Repeated system or application crashes – system running slow or glitchy
* Alerts from malware/antivirus protection systems
* Abnormal behavior during browsing – popups, redirects
* Reports from contacts receiving unusual messages from the organization/agency
* Message from attacker – Ransomware

**Phase 3: Contain**

When a breach has been detected, the normal reaction is to fix it NOW. This is when an agencies’ training kicks in – FOLLOW YOUR INCIDENT RESPONSE PLAN and training! Evidence can be inadvertently destroyed if you don’t follow the proper steps. Follow the advice and direction of your computer forensic team.

Remember:

DON’T panic

DON’T make hasty decisions

DON’T wipe and re-install your systems (yet)

**If you suspect you have fallen victim to a ransomware attack:**

1. Unplug the network cable (but leave the machine on for forensic data)
2. Disable WiFi and Bluetooth
3. Notify your IT department, Financial department and vendor(s)
4. Take a photo of the ransomware message
5. Report the Attack to the State Security Operations Center 888-839-6762 and DIR Cybersecurity Incident Response Team Hotline 877-347-2476
6. Report the Attack to the FBI Internet Crime Complaint Center (IC3) www.ic3.gov
7. Contact your local FBI Field Office

Dallas: 972-559-5000

El Paso: 915-832-5000

Houston: 713-693-5000

San Antonio: 210-225-6741

**Phase 4: Eradicate**

The vulnerability that led to the breach needs to be eliminated. This can be agency policies, procedures, or a technology solution. All traces of malware should be securely removed, and systems should be patched and updated.

If this activity is outside the scope of an agencies’ IT department, additional subject matter experts may be needed and should be noted in the Incident Response Plan.

**Phase 5: Recover**

Once ALL traces of the breach have been eliminated, systems are patched, updated and tested, THEN the compromised system can be reintroduced. (This can take weeks or even months)

**Phase 6: Review**

It is critical that an after-action meeting and report are developed. Learn what worked or didn’t work from the Incident Response Plan and make any necessary adjustments.

**Here are a few thing you can do to get started:**

CISA has assigned Field Cybersecurity Advisors to help with cyber activities. Email: [cyberadvisor@hq.dhs.gov](mailto:cyberadvisor@hq.dhs.gov)

<https://www.cisa.gov/cybersecurity> outlines the CISA cybersecurity program.

Texas Contacts:

George Reeves, Cyber Security Advisor (CSA) Chad Adams, Cyber Security Advisor (CSA)

CISA Region VI – South Texas CISA Region VI – North Texas

[George.Reeves@cisa.dhs.gov](mailto:George.Reeves@cisa.dhs.gov) [Chad.Adams@cisa.dhs.gov](mailto:Chad.Adams@cisa.dhs.gov)

281-714-1259 202-380-6024

**National Reference Material Websites:**

NIST Cybersecurity Framework: <https://www.cisa.gov/publication/cisa-cyber-essentials>

CISA Cyber Essentials Framework: <https://www.cisa.gov/publication/cisa-cyber-essentials>

CISA In depth toolkits on Cyber Essentials: <https://www.cisa.gov/publication/cyber-essentials-toolkits>

CISA Ransomware Guide: https://www.cisa.gov/sites/default/files/publications/CISA\_MS-ISAC\_Ransomware%20Guide\_S508C.pdf



**Available Tools:**

Texas Ransomware Posters: <https://www.dps.texas.gov/IOD/interop/swicDocuments.htm>

Texas DIR Incident Response Template: <https://pubext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Incident%20Response%20Template.pdf>

Texas Information Sharing & Analysis Organization: forum to share information regarding cybersecurity threats, best practices, and remediation strategies <https://dir.texas.gov/View-About-DIR/Information-Security/Pages/Content.aspx?id=169>

MS-ISAC – Multi-State Information Sharing and Analysis Center is a collaborative group whose mission is to improve the overall cybersecurity posture of state, local, tribal and territorial governments. <https://www.cisecurity.org/ms-isac/>

Registration: <https://learn.cisecurity.org/ms-isac-registration>

CISA toolkits geared toward end-users: <https://www.cisa.gov/stopthinkconnect-toolkit>

Cybersecurity end-user training options: Here are sites that offer free guidance on training for staff to protect your cybersecurity:

<https://gcatoolkit.org/smallbusiness/#toolboxes>

<https://cyberreadinessinstitute.org>

DIR Training Program: DIR has developed a certified training, [Cybersecurity Awareness Training](https://www.youtube.com/watch?v=ofRl5VSSgNk&feature=youtu.be). This video is being offered free of charge, to anyone who needs to meet the training requirements of HB 3834.

FedVTE - free on-line cybersecurity training: (veterans and government agencies) [fedvte.usalearning.gov](http://fedvte.usalearning.gov/)

Example courses:

Don't Wake Up to a Ransomware Attack - 1 Hour

Cyber Security Overview for Managers - 6 Hours

**CISA Tools:**

**CISA Resource page:** <https://www.us-cert.gov/resources>

**Cybersecurity Self-Evaluation Tool Assessment** (no charge)

* Provide detailed, effective and repeatable methodology for assessing control systems security encompassing the organization’s infrastructure, policies and procedures
* Self-Administered / <https://ics-cert.us-cert.gov>

**Vulnerability Scanning** – Contact a CISA Cyber Advisor to sign up for this service (no charge)

**Referenced Documents:**

These guidelines are generally summarized from the white paper located here, read the paper for more details:

<https://www.securitymetrics.com/blog/6-phases-incident-response-plan>

and the following articles:

<https://digitalguardian.com/blog/incident-response-plan>

<https://phoenixnap.com/blog/cyber-security-incident-response-plan>

<https://securityintelligence.com/dont-dwell-on-it-how-to-detect-a-breach-on-your-network-more-efficiently/>

<https://www.computerweekly.com/news/252487147/Five-signs-youre-about-to-get-hit-with-ransomware>



Karla Jurrens, Texas Deputy SWIC