**Cybersecurity – Cyber Threat Assessment**

**Getting Started**

Cybersecurity is no longer a “want to have” – it is a MUST have. Cybersecurity is one of the biggest vulnerabilities public safety faces. When you look at the NIST Framework and other cybersecurity guidance many organizations feel overwhelmed and do not know where to start, so they simply do not! The general advice is to pick one thing (i.e.; employee education, two factor authentication, and a regular schedule for patches) and start implementing! One-step at a time. Many national organizations provide frameworks and guidance on how to minimize this risk:

**From the NIST Cybersecurity Framework: Step 4: Conduct a Risk Assessment**. This assessment could be guided by the organization’s overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

**National Emergency Communications Plan Goal 6: Cybersecurity:**Strengthen the cybersecurity posture of the Emergency Communications Ecosystem

Objective 6.1: Develop and maintain cybersecurity risk management

Public safety organizations, at a minimum, implement the National Institute of Standards and Technology Cybersecurity Framework

**SAFECOM Grant Guidance Priority 2: Planning and Procedures:**Support statewide emergency communications and preparedness planning efforts through allocation of funding to the following planning activities: Develop and perform risk, resiliency, and vulnerability assessments (e.g., cyber, threat and hazard identification and risk assessment [THIRA])

State and UASI grant funds have a specific (minimum) set aside starting this year: “ … (SHSGP and UASI grantees) required to dedicate a minimum of 20 percent of awards to address four priority areas: cybersecurity (5 percent)” (plus soft targets and crowded places, intelligence and information sharing, emerging threats).

< <https://www.dhs.gov/news/2020/06/30/dhs-announces-grant-allocations-fiscal-year-2020-preparedness-grants> >

**What is a Cyber Threat Assessment?**

A Cyber Threat Assessment is a specialized version of a Risk Assessment. Agencies and Organizations should be taking a close look at their computer systems, remote access services and cloud based accounts. “From exposing weaknesses in systems to issues with compliance, a cybersecurity threat assessment enables organizations to uncover hidden vulnerabilities in people, processes and technology – before a malicious actor can exploit them.”1

Whether an agency prepares their own Cyber Threat Assessment, or if a professional contract is put in place, this document provides information to consider in plan development.

Most Cyber Threat Assessments address the following six steps:

#1 – Characterize EACH of your data systems (what kind of data, who uses it, vendor, retention policy, where does the data come from and where does it go, where is it stored, where and how is it backed-up), pre-determine the data recovery process

#2 – Identify threats and exploits (i.e. unauthorized access, data exposure, and disruption of service)

#3 – Determine risk impact (impacts if the threat was exercised: High, Medium, or Low)

#4 – Analyze the environment (identify threat prevention, detection, mitigation)

#5 – Determine a likelihood rating (how likely is a given exploit)

#6 – Calculate your risk rating

Impact (if exploited) \* Likelihood (of exploit) = Risk Rating

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

CISA – Cybersecurity Infrastructure Security Agency is an agency within the Department of Homeland Security.

CISA has assigned Field Cybersecurity Advisors to help with cyber activities.

<https://www.cisa.gov/cybersecurity> outlines the CISA cybersecurity program. Email: cyberadvisor@hq.dhs.gov

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 Chad.Adams@cisa.dhs.gov

281-714-1259 202-380-6024

**Note:** A growing trend is to have Cybersecurity Insurance; a Cyber Threat Assessment and a Cybersecurity Incident Response Plan will likely be required to purchase coverage.

**National Reference Material Websites:**

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

NIST Guide for Conducting Risk Assessments: <https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>

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

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

CISA Emergency Services Sector Cybersecurity Framework Implementation Guidance: <https://www.cisa.gov/sites/default/files/publications/Emergency_Services_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf>

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>

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.

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>

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

Cybersecurity Assessment Self-Evaluation Tool: (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>

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

**Referenced Sites on Cybersecurity Risk Assessments:**

1 <https://www.optiv.com/security-threat-assessment>

<https://www.tylercybersecurity.com/blog/6-steps-to-a-cybersecurity-risk-assessment>

<https://www.upguard.com/blog/cyber-security-risk-assessment>

<https://www.thesslstore.com/blog/cyber-risk-assessment/> (most detailed and tied to NIST Framework)

<https://www.colocationamerica.com/blog/cybersecurity-risk-assessments>



Karla Jurrens, Texas Deputy SWIC