Guide to Getting Started with a Cybersecurity Risk Assessment

What is a Cyber Risk Assessment?

Cybersecurity (cyber) risk assessments assist public safety organizations in understanding the cyber risks to their operations (e.g., mission, functions, critical service, image, reputation), organizational assets, and individuals.[1] To strengthen operational and cyber resiliency, SAFECOM has developed this guide to assist public safety communications systems operators, owners, and managers understand the steps of a cyber risk assessment. Included with this guide are customizable reference tables (pages two, three, and four) to help organizations identify and document personnel and resources involved with each step of the assessment. While example entities and organizations are provided, customization is advised.[2]

By conducting cyber risk assessments, public safety organizations may experience a multitude of benefits, such as meeting operational and mission needs, improving overall resiliency and cyber posture, and meeting cyber insurance coverage requirements. It is recommended that organizations conduct cyber risk assessments regularly, based on their operational needs, to assess their security posture. By conducting the assessments, organizations establish a baseline of cybersecurity measurements, and such baselines could be referenced to or compared against future results to further improve overall cyber posture and resiliency and demonstrate progress. These assessments could be conducted with internal resources or with external assistance. For instance, organizations may conduct a review of vulnerabilities based on internal logging and audits of their internet-facing networks.

RISK TERMINOLOGY

THREAT: A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, assets, individuals, other organizations, or society

VULNERABILITIES: A characteristic or specific weakness that renders an organization or asset open to exploitation by a given threat

LIKELIHOOD: Refers to the probability that a risk scenario could occur

RISK: The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences

Additionally, organizations may also use external guides or services that provide different perspectives and highlight potential vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA) provides cyber tools and cyber services that are available at no cost and without commitment to sharing outcomes, such as the Cyber Security Evaluation Tool (CSET®).[3] CISA's other offerings, such as the Cybersecurity Advisors, are available to federal, state, local, tribal, and territorial governments, critical infrastructure owners/operators, and private sector entities to help

[1] CISA, "QSMO Services – Risk Assessment," last accessed October 28, 2021. https://www.cisa.gov/qsmo-services-risk-assessment

[2] SAFECOM recommends the guide be used in conjunction with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), which provides a holistic perspective of the core steps to a cyber risk assessment, and the Public Safety Communications and Cyber Resiliency Toolkit, which provides resources for evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats. This document follows the Identify Function of the risk assessment process identified in the NIST CSF.

[3] For example, CISA's Cyber Resiliency Resources for Public Safety Fact Sheet highlights resources such as the Cyber Security Evaluation Tool (CSET®) and others provided by the federal government, industry, and trade associations. The Fact Sheet assists public safety organizations in determining their network cybersecurity and resiliency capabilities and identifying ways to improve their ability to defend against cyber incidents.

detect and remediate weaknesses in a network or system. They serve as cyber subject matter experts who specialize in risk assessments. In addition, CISA Emergency Communications Coordinators facilitate contact within CISA to assist organizations in addressing complex public safety communications challenges.

While this guide provides an example of a cyber risk assessment structure, it is not a comprehensive list of all available resources and methods. Different approaches may be recommended to mitigate specific incidents (e.g., ransomware attack, denial of service attack, network/database breach), and other assessments may result in greater awareness of vulnerabilities. Each assessment step is accompanied by relevant references to assist with the process. *Please note, this list is not exhaustive and does not imply an endorsement for organizations or their products.*

Public safety organizations are encouraged to visit the resources found in the Appendix A *Helpful Resources by Risk Assessment Step* and Appendix B *Training and Educational Resources* for more information about each step and best practices for developing a cyber risk assessment. Visit cisa.gov/publication/communications-resiliency for additional public safety-focused resiliency resources.

What are the Steps of a Cyber Risk Assessment?

STEP ONE: Identify and Document Network Asset Vulnerabilities[4]

Characterizing or inventorying network components and infrastructure, including hardware, software, interfaces, and vendor access and services will help determine possible threats. For example, consider internal and external cyber processes, internal and external interfaces (check for default passwords), pre-determine data recovery processes, and review access for each system. This process can also help in understanding where breaches may come from within the system.

Table 1: Sample Customizable Table to Identify and Document Network Asset Vulnerabilities

Hardware/Software, Vendor, Internal/External Interfaces, Access, Date of Last Update
Example: Hardware/Software: Email Platform Vendor: Network System Provider Internal/External: Both Interfaces: Connects across machines and as broadly as the Internet Access: All personnel Date of Last Update: Update performed 07/2021; version 12 Response Time/Footprint: within x hours
Organization/Entity/Component: Contact Information: Date last reviewed/accessed (if applicable): Response time/Footprint:
Organization/Entity/Component: Contact Information: Date last reviewed/accessed (if applicable): Response time/Footprint:

STEP TWO: Identify and Use Sources of Cyber Threat Intelligence[5]

Some common threats include, but are not limited to, unauthorized access to secure information, the misuse of data by an authorized user, and weaknesses in organizational security controls.

Table 2: Sample Customizable Table to Identify and Document Cyber Threat Intelligence Sources

Cyber Threat/Vulnerability Information Sources
National Example: National Cyber Awareness System (also known as United States Computer Emergency Readiness Team [US-CERT] alerts) Website: us-cert.cisa.gov/ncas/alerts
National Example: the CISA Known Exploitable Vulnerabilities Catalog Website: cisa.gov/known-exploited-vulnerabilities-catalog
National Example: InfraGard Website: infragard.org/
State Example: Florida Intelligence Fusion Center Contact Information: FloridaFusionCenter@fdle.state.fl.us | (850) 410-7645
Local Example: National Capital Region Threat Intelligence Consortium Contact Information: NTIC@dc.gov | (202) 727-6161
Other Example: Multi-State Information Sharing and Analysis Center Contact Information: soc@msisac.org | (866) 787-4722
Organization/Entity/Component: Role/Responsibility: Contact Information: email | phone | website

[4] NIST. "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 2018. https://doi.org/10.6028/nist.cswp.04162018. 26.

[5] Ibid.

STEP THREE: Identify and Document Internal and External Threats[6]

Threats are not exclusively external to organizations, as internal sources can greatly affect cyber posture as well. Because threat sources can come from inside an organization, it is essential to identify and document internal processes and records (e.g., administrative privileges on a network or hardware, activity logs of those granted access, reliance on a managed service provider or a supply chain software vendor's tools). Individuals, either accidentally or with malicious intent, can impact a network. By identifying and documenting both internal and external threats and vulnerabilities, organizations can help anticipate a breach in the systems and plan accordingly. For instance, the establishment and continuous maintenance of a cyber incident response plan are advised. They can also develop training and exercise programs to maximize cyber awareness and promote continual improvement.

Some common indicators of a cyber breach include:

- Web server log entries that show the usage of a vulnerability scanner
- A threat from a group stating that a cyberattack is imminent (ransomware)
- Unusual user activity
- Unexpected user account lockouts
- Alerts from malware/antivirus software
- Unusual deviation from typical network traffic flows
- Configuration changes that cannot be tracked to known updates

STEP FOUR: Identify Potential Mission Impacts[7]

Information and communications technology are integral for the daily operations and functionality of critical infrastructure. Should these be exploited, the consequences can affect all users of that technology or service and can also affect systems beyond an organization's control. This assessment will consider impacts to all system dependencies and shared resources should a cyber incident occur. This step is crucial in the containment of a cyber breach across shared resources and can be a useful guide when formulating a response plan.

Table 3: Sample Customizable Table to Identify and Document Dependencies and Shared Resources

Dependencies and Shared Resources
Example: Jurisdictional Partners or Agencies on a Shared Network Contact Information: example@example.gov | (XXX) XXX-XXXX Role/Responsibility: spectrum sharing Response time/Footprint: within x hours
Example: County or State Office of Information Technology Contact Information: example@example.gov | (XXX) XXX-XXXX Role/Responsibility: active monitoring of municipal networks Response time/Footprint: within x hours
Example: Telecommunications Provider Contact Information: example@example.net | (XXX) XXX-XXXX Role/Responsibility: 24/7 uninterrupted service Response time/Footprint: within x hours
Name of third-party, non-agency infrastructure and services owner: Contact Information: email | phone | website Role/Responsibility: Response time/Footprint:

[6] Ibid, 27.

[7] Ibid.

STEP FIVE: Use Threats, Vulnerabilities, Likelihoods, and Impacts to Determine Risk[8]

Risk is a guide when formulating an incident response plan, however, it is not the final state of an organization's cyber posture. Note that a cyber risk assessment is not a meant to be conducted just once. Instead, the assessment is intended as an ongoing determination of an organization's cyber measures and should continually be refined as new technologies and methods become available and are adopted.

There are several things to consider when quantifying risk levels, including:

- What assumptions qualify the measurements of "high," "medium," and "low?"
- Are terms such as "risk" and "threat" defined precisely and consistently?
- What assets/devices/systems are at risk in the high-risk scenario?

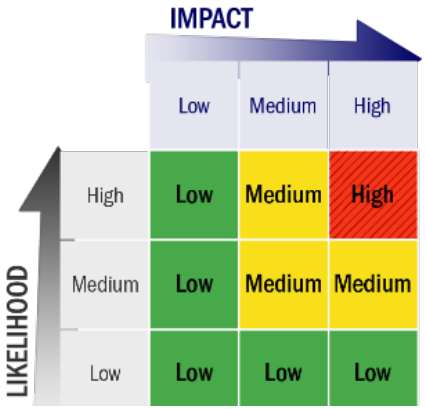

Figure 1: Example Risk Matrix

- What are the cyber threats posed to those assets/devices/systems? (Refer to Steps 1 and3)
- What controls are in place at each tier to mitigate the extent of cyber breaches?
- What level of readiness has IT personnel achieved to respond to a cyber incident?

[8] Ibid.

STEP SIX: Identify and Prioritize Risk Responses[9]

A key aspect of risk-based decision-making for authorizing officials is understanding their information systems' security and privacy posture and common controls available for those systems. A crucial factor in a cyber risk assessment is knowing what responses are available to counter the different cyber threats. Maintaining and updating a list of identified personnel and groups with their contact information is vital to expedite the response time after a cyber incident.

Table 4: Sample Customizable Table to Identify and Document Response, Investigative, and Recovery Resources

Potential Response, Investigative, and Recovery Resources
Example: Texas Department of Information Services Contact Information: datacenterservices@dir.texas.gov | (855) 275-3471
Example: CISA Central Contact Information: Central@cisa.gov | cisa.gov/central
Example: CISA Cybersecurity Advisors (by region) Contact Information: cisa.gov/cisa-regions
Example: US-CERT Contact Information: us-cert.cisa.gov/report | (888) 282-0870
Example: Federal Bureau of Investigation (FBI) Field Offices Contact Information: fbi.gov/contact-us/field-offices
Example: Statewide Interoperability Coordinator (SWIC) Contact Information: example@example.gov | (555) 555-5555
Name of organization/entity Contact Information: email | phone | website

[9] Ibid.

Appendix A: Helpful Resources by Risk Assessment Step

RISK ASSESSMENT STEP ONE: Identify and Document Network Asset Vulnerabilities

- Cybersecurity and Infrastructure Security Agency (CISA) Interoperable Communications Technical Assistance Program (ICTAP) – The ICTAP serves all 56 states and territories and provides direct support to state, local, and tribal emergency responders and government officials through the development and delivery of training, tools, and onsite assistance to advance public safety interoperable communications capabilities.
- CISA Public Safety Cyber Resiliency Assessment Tools Factsheet – This factsheet provides an overview of 22 cybersecurity evaluations available from CISA and other public safety partners. The factsheet helps partners evaluate the scope, requirements, cost structure, and outcomes of assessments as well as aids in the selection of assessments that best align with the organization's unique needs.
- CISA Cyber Security Evaluation Tool (CSET®) – This desktop application guides asset owners and operators through a systematic process of evaluating operational technology and information technology. After completing the evaluation, organizations will receive reports that present the assessment results in both a summarized and detailed manner. Organizations will be able to manipulate and filter content to analyze findings with varying degrees of granularity.
- National Institute of Standards and Technology (NIST) Cybersecurity Framework – This framework provides critical infrastructure owners and operators with standards, guidelines, and best practices to manage cybersecurity risk. This document is not limited to critical infrastructure owners and can be used by any organization looking to improve its cybersecurity and resiliency. The NIST Cybersecurity Framework maps cybersecurity functions to six references, including: *NIST 800-53 Rev. 5*, *International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013*, *Control Objectives for Information and Related Technologies 5 Framework*, *Center for Internet Security Critical Security Controls (CIS CSC)*, *International Society of Automation (ISA) 62443-2-1:2009*, and *ISA 62443-3-3:2013*.
- NIST Guide for Conducting Risk Assessments – This publication provides guidance on conducting risk assessments of federal information systems and organizations. Regular and ongoing risk assessments are intended to give organizational leaders a status of their security measures.

RISK ASSESSMENT STEP TWO: Identify and Use Sources of Cyber Threat Intelligence

- CISA National Cyber Awareness System (US-CERT Alerts) – This no-cost, subscription-based service provides real-time reports on cyber incidents, security issues, vulnerabilities, and exploits. The service also posts regular announcements on topics and issues of interest to the cybersecurity community.
- CISA Resources for State, Local, Tribal, and Territorial Governments – Compiled and regularly updated, this website provides resources to help identify, protect, detect, and respond to cyber threats and incidents for state and local entities. The website also hosts a list of geographically specific resources by state.
- Federal Bureau of Investigation Internet Crime Complaint Center Industry Alerts – This no-cost, subscription-based service posts regular cyber threat reports of breaches that have occurred and are suspected. Provided in each report are a description of the threat, good indicators, and recommended mitigation techniques.

- The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) – MS-ISAC® is a nonprofit organization that produces best practices for securing IT systems and data. The linked webpage displays recommended actions for data security. MS-ISAC® also provides regular updates to its members on cyber vulnerabilities and threats.
- SAFECOM Publications – SAFECOM is tasked with improving designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across federal, state, local, tribal, and territorial governments, as well as international borders. Threat notices are posted on the SAFECOM website to improve cybersecurity posture.

RISK ASSESSMENT STEP THREE: Identify and Document Internal and External Threats

- CISA Public Safety Communications and Cyber Resiliency Toolkit – Developed by CISA for public safety users, this interactive toolkit provides resources by process and function across a network to help improve cyber resiliency. Users can navigate between topics and find linked resources with brief descriptions.

RISK ASSESSMENT STEP FOUR: Identify Potential Mission Impacts

- CISA *Stop. Think. Connect.* Toolkit – Based on the premise that cybercriminals do not discriminate in their targeting, this toolkit provides valuable materials for different audiences to increase understanding of cybersecurity and best practices for securing information.

RISK ASSESSMENT STEP FIVE: Use Threats, Vulnerabilities, Likelihoods, and Impacts to Determine Risk

- CISA Emergency Services Sector – Part of CISA's National Risk Management Center, this website provides industry-specific resources, plans, and training for the Emergency Services Sector. The webpage includes resources such as sector-specific plans, Crisis Event Response and Recovery Access, and other decision-making resources.
- CISA FY2021 Technical Assistance/Statewide Communications Interoperability Plan Guide – This guide provides cyber assessment and cyber awareness services available through CISA's ICTAP
- NIST Risk Management Framework – This resource outlines the Risk Management Framework, which provides a disciplined, structured, and flexible process for managing security and privacy risk. This publication promotes risk management and ongoing information system and common control authorization through continuous monitoring processes.

RISK ASSESSMENT STEP SIX: Identify and Prioritize Risk Responses

- CISA Statewide Interoperability Coordinator (SWIC) Contact List – This list identifies SWICs and their contact information. The list is organized by ten regions, with all fifty-six states and territories represented.
- CISA Emergency Services Sector Cyber Security Framework Implementation Guidance – Designed to be used in conjunction with the NIST Cybersecurity Framework, this guide can help organizations improve their ability to prevent, detect, and respond to cyberattacks. Based on the NIST Cybersecurity Framework recommendations, this guide highlights best practices implementation.
- Public Safety Communications Dependencies on Non-Agency Infrastructure and Services – Developed by SAFECOM and NCSWIC, this white paper provides high-level insights for systems administrators, public administration decision-makers, and other stakeholders involved in public safety communications planning or implementation.

Appendix B: Training and Educational Resources

- CISA Cybersecurity Training and Exercises – Developed by CISA, this website features different training exercises, and upcoming events focused on training those wanting to improve their cybersecurity posture. Webinars and external training sources can be found, as well as contact information for those wishing to learn more about the training process.
- Federal Virtual Training Environment (FedVTE) – This portal provides federal, state, local, tribal, and territorial government employees, federal contractors, and U.S. military veterans free online cybersecurity training. Public content is available for those who do not fall into these categories, but it is recommended that new users register for full access to online training courses.
- National Initiative for Cybersecurity Education – Due to the ever-increasing cyber-attack threat, training and resources to help public safety officials protect their systems and networks have become readily available. Updated regularly, this resource provides a list of free and low-cost learning content that public safety officials can leverage to increase security and resiliency in their communications and network systems.
- The Multi-State Information Sharing and Analysis Center® (MS-ISAC®) – MS-ISAC® aims to improve the overall cybersecurity posture of U.S. states, local, tribal, and territorial government organizations through coordination, collaboration, cooperation, and increased communication. As a part of MS-ISAC®, members can access an array of training and educational resources, including cybersecurity table-top exercise templates, regular webinars examining critical and timely cybersecurity issues, and the MS-ISAC® Toolkit.