NASS
National Association
of Secretaries of State

UPDATED May 5, 2021

ISSUE BRIEFING: Cybersecurity Risk Assessments

The Issue: A growing number of entities are leveraging risk-based methods to build their cybersecurity strategies. For example, the Cybersecurity and Infrastructure Security Agency (CISA), which describes itself as "the nation's risk advisor," uses risk management approaches to support U.S. critical infrastructure security. To take a risk-based approach to cybersecurity, entities conduct assessments to understand their risks and compare them by characteristics like severity and urgency.

Risk assessments empower leaders within an organization to make informed decisions regarding which risks to mitigate, factoring in when and how to leverage limited resources. If an organization understands its own risk posture, it is also better prepared to identify and respond to possible incidents. Risk assessments are also crucial as an organization procures new systems or services. Introducing a new system into an IT environment likely introduces new risk(s) that must be understood in the larger risk context of the organization.

What does a cybersecurity risk assessment entail?

Cybersecurity risk management involves identification, assessment, mitigation, monitoring and governance. Key considerations when beginning a risk assessment include determining the assessment scope and defining what methodologies best fit an organization's needs.

Determining Scope: Entities can conduct risk assessments at multiple levels, ranging from assessing the risk of an entire ecosystem or enterprise to assessing the risk of a specific system. Scoping is a critical step in planning a risk assessment.

Defining Methodology: There are multiple approaches to defining cybersecurity risks. It is important to decide what risks you are assessing and what methodologies best meet an organization's assessment needs prior to an assessment. One way to approach defining risk is determining the risk to the confidentiality, integrity, and availability of data and systems. (See the EI-ISAC Spotlight on the CIA Triad for more on this.) A different approach is to evaluate the potential impacts of risks on the mission of an organization. Methodologies may be quantitative, qualitative or a combination of both.

Where do we start?

All entities have cybersecurity risks. A risk management approach, of which risk assessments are a key step, allows organizations to address risks and reduce their potential impacts in a structured manner on an ongoing basis. The NIST Guide for Conducting Risk Assessments provides detailed guidance for a diverse group of risk management professionals ranging from organizational leaders to those who conduct business functions and those who oversee IT and cybersecurity. While this guidance was written primarily for federal agencies, NIST encourages state, local, and tribal governments, as well as private sector organizations, to consider using it.

NIST describes the process of assessing information security risks using four overarching steps with activities within each step:

1. Prepare for assessment.
    a. Identify the purpose of the assessment.

b. Identify the scope of the assessment.
c. Identify the assumptions and constraints associated with the assessment.
d. Identify the sources of information to be used as inputs to the assessment.
e. Identify the risk model and analytic approaches to be employed.

2. Conduct assessment.
   a. Identify relevant threat sources.
   b. Identify threat events that could be produced by those sources.
   c. Identify vulnerabilities that could be exploited by threat sources through specific threat events and the predisposing conditions that could affect exploitation.
   d. Determine the likelihood that the identified threat sources would initiate specific threat events and the likelihood that the threat events would be successful.
   e. Determine the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation resulting from the exploitation of vulnerabilities by threat sources.
   f. Determine information security risks as a combination of likelihood of threat exploitation of vulnerabilities and the impact of such exploitation.
3. Communicate results.
   a. Share information developed in the execution of the risk assessment to support other risk management activities.
4. Maintain assessment.
   a. Monitor risk factors identified in risk assessments on an ongoing basis and understanding subsequent changes to those factors.
   b. Update the components of risk assessments reflecting the monitoring activities carried out by organizations.

This is one of multiple ways to conceptualize a risk assessment. Several self-service tools tailored specifically to election systems and processes are available at no cost. These tools are designed to help make risk assessments simpler and more robust for election officials to administer.

- CISA/EAC Election Security Risk Profile Tool
- Center for Internet Security (CIS) Election Security Self-Assessments

Here is an example of the findings of a national election cybersecurity risk assessment:

- CISA Election Infrastructure Cyber Risk Assessment

All federal, state, local, tribal and territorial governments can receive CISA Cyber Hygiene Services at no cost. Because elections have been designated as critical infrastructure, certain CISA services are prioritized for election administration entities. See the CISA Election Infrastructure Security Resource Guide for information on no cost services for election administration entities and how to receive them.

For additional questions on this issue, please contact NASS: (202) 624-3524 or lforson@sso.org.