C3 VOLUNTARY PROGRAM

Begin the Conversation: Understand the Threat Environment among State, Local, Tribal, and Territorial (SLTT) Governments

Why Does the Threat Environment Matter?

A ***cyber threat*** is an attempt to damage or disrupt a computer network or system. Cyber threats can become a reality if there are ***vulnerabilities*** present within a network, hardware, or software, which allow an attacker to reduce a system's information assurance. Most cybersecurity guidance addresses access control, configurations, and accountability, but businesses cannot determine risk or know where to invest in security until they know the threat landscape facing their organization.

Where to Start

First, understand and prevent common vulnerabilities. Leverage community repositories, such as the National Vulnerability Database (https://nvd.nist.gov/), to ensure that known vulnerabilities are addressed. This requires that some form of asset management exists in your organization.

Second, determine what cyber events your organization monitors. If information technology and incident response activities are outsourced, insist that the service providers supply threat, incident, and activity reports from network traffic in a format that suits your staff. The National Institute of Standards and Technology (NIST) Cybersecurity Framework and special publications (e.g. NIST SP 800-30) provide a common language for understanding, managing, and expressing cyber risk. Industries may also offer specific security guidance, controls, or threat models.

Third, ensure that an impact assessment is complete and up to date. Do you know what your critical organizational functions are? Do the threats facing your organization have the potential to disrupt these critical functions? What are your contingency plans and procedures?

Fourth, create or become an active member in an information sharing and analysis organization (ISAO) and/or the Multi-State Information Sharing & Analysis Center (MS-ISAC) to crowd source security.

Lastly, continuously use what already exists to counter and monitor threats. By becoming a member of the MS-ISAC, SLTT governments gain access to no-cost cyber threat information sharing products and other resources to protect and defend government networks. States can also take advantage of Albert, an intrusion detection monitoring program, at no cost.

About the C³ Voluntary Program

The Critical Infrastructure Cyber Community (C³) Voluntary Program is a public-private partnership led by DHS to help align critical infrastructure owners and operators with existing resources to assist the use of the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

All of these programs, tips, and resources, can be found on the C³ Voluntary Program website: https://www.us-cert.gov/ccubedvp