C3 VOLUNTARY PROGRAM

Begin the Conversation: Understand the Threat Environment

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 business.

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 works for 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 a business impact assessment is complete and up to date. Do you know what your critical business functions are? Do your threats have the capabilities to disrupt them? What are your contingency plans and procedures?

Fourth, create or become an active member in an industry or regional information sharing and analysis organization (ISAO) to crowd source security.

Lastly, continuously use what already exists to counter and monitor threats. DHS offers several programs enabling industry to protect and defend critical infrastructure and provide opportunities to share threat intelligence:

- Enhanced Cybersecurity Services (ECS)
- Critical Infrastructure Information Sharing and Collaboration Program (CISCP)

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