The U.S. Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA) has released updated chapters to its Cyber Essentials Toolkits (revised August 17, 2020). CISA, the U.S. risk advisor, is tasked with key responsibilities in relation to defending cyber threats against “.gov” networks while collaborating with federal government partners to build more secure and resilient American infrastructure.

CISA’s Toolkits are a set of modules designed to break down the CISA Cyber Essentials into digestible action items for information technology (IT) teams, information security professionals, and executive leadership. The overall goal of the two-page Toolkits is to improve cyber readiness with respect to the interrelated aspects of organizational cultures. Each chapter includes numerous links to external security-related resources, controls, and FAQs for additional support. While CISA is focused on governmental websites and agencies, the advice and essentials set forth in the Toolkits are helpful starting points and reminders for private organizations of all sizes.

Chapter 1 focuses on being a culture-changing cyber leader; this requires awareness of cybersecurity basics and being able to secure the collective buy-in of the organization’s management teams. According to the guide, essential actions for cybersecurity leaders include:
approaching cyber as a business risk;
determining how much of the organization’s operations are dependent on IT;
leading investment in basic cybersecurity; and
building a network of trusted relationships for access to timely cyber threat information.

The chapter also stresses the need to collaborate with IT staff and others on the development of cybersecurity policies.

Chapter 2 concentrates on the staff and users of an organization, emphasizing that the staff is often the first line of defense, necessitating proper cybersecurity training and reinforcement. Essential actions in relation to staff and users include:

- leveraging basic cybersecurity training and escalation skills;
- developing a culture of awareness to encourage employees to make good choices online (and offline);
- learning about risks like phishing and business email compromise;
- identifying and using available training resources and identifying and encouraging privacy champions; and
- maintaining awareness of current events related to cybersecurity; this requires proactivity and being in tune with the threats that industry peers are facing.

Lastly, Chapter 3 assesses how to protect an organization’s critical assets, applications and systems. This requires ongoing monitoring and vigilance in relation to which devices are connected to an organization’s networks, role-based access controls, and use of current security safeguards. Essential actions for protecting key assets and systems include:

- learning what is on a given organization’s network by inventorying all hardware and software assets and establishing a monitoring strategy for them;
- leveraging automatic updates for all operating systems and third-party software;
- implementing secure configurations for all assets so that physical and virtual assets are protected, and removing unsupported or unauthorized such assets;
- leveraging email, firewall and web browser security settings to prevent attackers from delivering malicious code; and
- creating application integrity and list policies so that only approved software can operate on the organization’s systems.

©2020 Greenberg Traurig, LLP. All rights reserved.