PUBLICATION

Recent Government Cyber Alert and Draft Guide for Financial Institutions: Lessons for All Organizations

November 04, 2015

All organizations, including financial institutions, continue to face significant security threats across their wide ranging IT systems. Such organizations are particularly vulnerable if they cannot track networked devices and software across large geographic areas and diverse tech platforms. The challenges are compounded for organizations attempting to oversee subsidiaries, branches, contractors and other affiliates, in addition to their own employees.

On October 26, 2015, the National Cybersecurity Center of Excellence (NCCoE) issued a draft guide regarding the monitoring and management of IT hardware and software assets. In its guide, *IT Asset Management* (Special Publication 1800-5a), the NCCoE, which is part of the National Institute of Standards and Technology (NIST), illustrates how financial institutions can use commercially available technology to modernize their risk management practices. This guide must be reviewed and understood by financial institutions, as it provides the industry with a tool that should not be ignored. While the guide was directed at financial institutions, all organizations with personally identifiable information (of customers or employees) or who have sensitive trade secret information would be well served by reviewing and adopting key points from the guide.

The guide encourages organizations to build a single system capable of monitoring their entire asset portfolios and explains how organizations can accomplish this goal. The hope is that organizations can achieve lower total cost of IT asset ownership and improved responses to security threats.

The guide is comprehensive and encompasses traditional physical asset tracking, IT asset information, physical security, and vulnerability and compliance information. In particular, the example solution provides organizations the capability to track, manage and report on IT assets throughout their entire life cycle, allowing organizations to improve their security posture through enhanced visibility of assets, identification of vulnerable assets, quicker response to security alerts and the ability to provide detailed system information to auditors. In addition, the guide provides implementers and security engineers with instructions and examples of the required components for installation, configuration and integration. Using this guide, an organization's information security experts should be able to pinpoint the standards-based products that will integrate best with the organization's existing IT tools and infrastructure.

NCCoE is soliciting comments on the draft until January 8, 2016.

This guide is particularly useful in light of the recent *Joint Statement on Cyber Attacks Involving Extortion* that the Federal Financial Institutions Examination Council (FFIEC) issued on behalf of its members. The FFIEC issued the statement to alert financial institutions of the increasing frequency and severity of cyberattacks involving extortion, and specific risk mitigation related to threats associated with such attacks. The FFIEC statement emphasizes the importance of maintaining effective programs to ensure that organizations identify, protect against, detect, respond to, and recover from these types of cyberattacks.

For more information on how this may affect your business or related matters, contact any member of the Firm's Privacy and Information Security Team.