With Cyberattacks on the Rise, White House Releases Cybersecurity Framework

Given the apparent vulnerabilities evidenced by recent cyberattacks to big-box retailers, cybersecurity remains a top priority for both the federal government and private sector. On February 12, the National Institute of Standards and Technology (NIST) published the voluntary *Framework for Improving Critical Infrastructure Cybersecurity*. The framework provides an opportunity for the private sector to engage the federal government on cybersecurity. Numerous sectors, from energy, financial services and telecommunications to health care, insurance and defense, have much to lose and must continue to work with the federal government to mitigate cybersecurity risks.

Although the framework provides voluntary guidelines, it may provide a foundation for mandatory requirements via federal regulations; requirements as a condition of award for acquisitions, and enforcement actions by state attorneys general and the Federal Trade Commission. That said, the private sector must prepare for the possibility of mandatory requirements and to work with the federal government to further develop the framework, especially since many critical issues remain unresolved.

The recent data breach incidents have also led to renewed interest in cybersecurity at the congressional level. Various committees in both the House and Senate have held hearings to examine recent data breach incidents and received testimony from federal agencies and departments, retailers, processing companies and consumer groups. The hearings have emphasized an interest in new technologies, including the EMV chip, tokenization, mobile payments, and tools for online fraud, among others. Additionally, Sens. Leahy (D-VT), Rockefeller (D-WV) and Carper (D-DE) have introduced data security breach notices bills as have several House Republicans.

Lastly, the ongoing events in Ukraine present an interesting juncture on cybersecurity. Specifically, hackers in Ukraine have launched large denial-of-service attacks against both pro-Western and pro-Russian Ukrainian news organizations. While the U.S. contemplates aid and sanctions to help Ukraine maintain its sovereignty against Russia, will it condition or seek to address Ukraine's reputation as a hacker haven?

Both the federal government and private sector must work together to prevent and mitigate data breaches, denial-of-service attacks, and other cybersecurity incidents. Given the prospect of mandatory requirements, the private sector must act now to address its issues and concerns related to cybersecurity. The framework and general congressional interest provide an opportunity for the private sector to engage the federal government prior to the emergence of such requirements. Accordingly, companies must develop and implement comprehensive government relations strategies to address cybersecurity issues in both the near- and long-term.

Manuel Ortiz
Shareholder
mortiz@bhfs.com
T 202.872.5297