CRS INSIGHT

Cybersecurity: Homeland Security Issues for the 116th Congress

March 29, 2019 (IN11088)

|

Related Author

- Chris Jaikaran

|

Chris Jaikaran, Analyst in Cybersecurity Policy (cjaikaran@crs.loc.gov, 7-0750)

Introduction

For policymaking purposes, *cybersecurity* can be considered the security of *cyberspace*. Taking this broad view allows policymakers to examine discrete elements of cybersecurity and determine which parts to address through the legislative process. Cyberspace, itself, includes the infrastructure necessary for the internet to work (e.g., wires, modems, and servers), the services used via the Internet (e.g., web applications and websites), the devices on the network (e.g., computers and Internet-of-Things devices), and the users of those devices. Cybersecurity involves many interrelated issues, such as education; workforce management; research and development; intelligence; law enforcement; and defense.

Recent congressional activity and Member statements suggest that five specific cybersecurity topics with an intersection to homeland security may arise during the 116th Congress. This Insight first discusses the importance of risk management for cybersecurity, then introduces each of those topics: Information Sharing, Critical Infrastructure Protection and Cybersecurity, Cyber Supply Chain Risk Management, Federal Agency Oversight, and Data Protection and Privacy.

Risk Management

When computer scientists refer to cybersecurity, they are generally not talking about security as an absolute and achievable state of safety. Rather, they refer to cybersecurity as a process of risk management. Risk can be managed in four ways: it can be avoided, transferred, controlled, and accepted. To know the appropriate course of action, an organization must first understand which risks they face. Risks can be understood as the *threats* an organization faces, the *vulnerabilities* they have to their systems, and the *consequences* or impacts of a successful attack against them. Risks can be managed against systems, networks, and data. In managing those risks, managers employ an *information security* model to understand risk areas and tools to address risks. Policymakers could choose to examine these risk management factors holistically, or to consider specific elements and ways to address specific risk factors.

Policy Areas

Information Sharing

Policymakers could choose to examine information sharing as a tool that may strengthen an organization's cybersecurity. The need to maintain current awareness of the relationships between technologies and attacks is a reason that information sharing is frequently included in the cybersecurity discussion. Through information sharing, one party seeks to bolster the knowledge of its partners. Information may provide opportunities for organizations to learn from one another, reduce their vulnerability to hacking, and quickly adapt to changing conditions. Successful information sharing occurs when an organization receives information, has the capability to process it, knows how to use it, and makes a change to its practices to better secure itself. However, the advantage to sharing information is only realized when the result is a valuable change in behavior because of the information shared. Some organizations may miss critical information, lack the expertise to understand it, lack the resources to take action, or otherwise not change their behavior.

Critical Infrastructure Protection and Cybersecurity

The National Infrastructure Protection Plan directs the owners and operators of facilities under the nation's 16 critical infrastructure sectors and the sector-governing bodies to consider cybersecurity risks to their sectors. However, their ability to understand risk and to provide resources to manage risk for their sectors varies. In an effort to bolster cybersecurity risk management, policymakers could choose to direct federal agencies to provide assistance to a sector or sectors; to engage in rulemaking; or to otherwise incentivize cybersecurity activities (e.g., expediting security clearances or prioritizing federal contracting opportunities).

To assist a sector, some agencies have specific programs designed to provide information, technical assistance, or capabilities for critical infrastructure. DHS can provide assistance to all sectors. The National Institute of Standards and Technology (NIST) has published a cybersecurity framework to assist those responsible for critical infrastructure.

Cyber Supply Chain Risk Management

Recent news articles and government reports have focused attention on cyber supply chain issues. Managing risks associated with a global and complex product supply chain for information technology (IT) is known as *cyber supply chain risk management* (C-SCRM). C-SCRM refers to addressing both the risks that foreign adversaries may introduce to products and unintentional risks, such as poor quality control and vendor management. Policymakers could choose to pursue legislative options to clarify agency responsibilities relative to C-SCRM, such as increasing awareness, providing oversight, prohibiting certain companies from supplying components or services, or requiring an entity to evaluate products for cyber supply chain risks.

Federal Agency Oversight

Federal agencies collect, process, store, and transmit sensitive information such as personally identifiable information and national security information. Agencies rely on IT to use this information and requested over $17 billion in cybersecurity funding for FY2020. Yet, the Government Accountability Office (GAO) bi-annually highlights that agencies face various challenges in IT management. This is despite existing statutes, guidance, and resources agencies have to assist in managing their IT. Congress could choose to pursue investigations, hearings, or legislation to improve oversight of the government's overall IT program(s), or could focus on an individual agency's cybersecurity efforts. In pursuing this oversight, Congress may review agency spending on IT and cybersecurity, and follow up on GAO and Inspector General (IG) recommendations related to improving agency IT management.

Data Security and Privacy

The Equifax breach and multiple Facebook incidents have highlighted data security and privacy issues. While these concepts may be interrelated, and certain technologies, like encryption, can help achieve both, for policymaking and operational purposes they are distinct. Data security refers to strategies to keep out unauthorized users, while privacy refers to using data regardless of where it is stored or who accessed it. In keeping with the concept of risk management, it is important to consider "from what" one is seeking to secure their data or seek to keep it private when designing policies or strategies for security and privacy. Policymakers could choose to pursue comprehensive (such as the General Data Protection Regulation) or sectoral (such as the Health Insurance Portability and Accountability Act, HIPAA, standards) approaches to data security and privacy. In the past, the federal government has addressed these issues

sectorally. But recent state and federal discussions have focused on more comprehensive approaches.