Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated March 23, 2015

Cybersecurity

Overview

Information and communications technology (ICT) has evolved greatly over the last half-century. ICT devices and components now form a highly interdependent system of networks, infrastructure, and resident data—known as *cyberspace*—that has become ubiquitous and increasingly integral to almost every facet of modern society. Experts and policymakers are increasingly concerned about *cybersecurity*—protecting cyberspace from attack by criminals and other adversaries.

The risks associated with any attack depend on three factors: *threats* (who is attacking), *vulnerabilities* (how they are attacking), and *impacts* (what the attack does).

What are the threats? People who perform cyberattacks include *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing information used by government or private entities; *nation-state warriors* who develop capabilities and undertake cyberattacks to support strategic objectives; *"hacktivists"* who perform cyberattacks for nonmonetary reasons; and *terrorists* who engage in cyberattacks as a form of non-state or state-sponsored warfare.

What are the vulnerabilities? Cybersecurity is an arms race between attackers and defenders. Attackers are constantly probing ICT systems for weaknesses. Defenders can often protect against them, but three are particularly challenging: inadvertent or intentional acts by *insiders* with access to a system; *supply chain* vulnerabilities, which can permit the insertion of malicious software or hardware during the acquisition process; and previously unknown, or *zero-day*, vulnerabilities with no established fix.

What are the impacts? A successful attack can compromise the confidentiality, integrity, and availability of an ICT system and the information it handles. *Cybertheft* or *cyberespionage* can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit. *Denial-of-service* attacks can slow or prevent legitimate users from accessing a system. *Botnet* malware can give an attacker command of a system for use in cyberattacks on other systems. Attacks on *industrial control systems* can result in the destruction of the equipment they control, such as generators, pumps, and centrifuges.

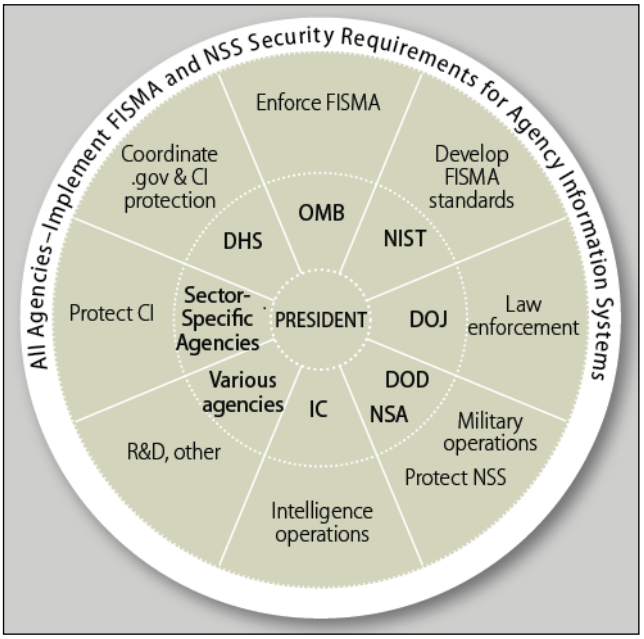
Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which are held by the private sector, such as the electric grid and major financial institutions—could have significant effects on national security, the economy, and the livelihood and safety of individuals. A rare successful attack with high impact can pose a larger risk than a common successful attack with low impact.

Reducing the risks from cyberattacks usually involves (1) removing the threat source, e.g., by closing down botnets or reducing incentives for cybercriminals; (2) addressing vulnerabilities by hardening ICT assets, e.g., by patching software and training employees; and (3) lessening impacts by mitigating damage and restoring functions, e.g., by having back-up resources available for continuity of operations in response to an attack.

Federal Role

The federal role in cybersecurity involves both securing federal systems and assisting in protecting nonfederal cyberspace. All federal agencies are responsible for protecting their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity, and additional legislation has been proposed.

Figure 1. Federal Agency Roles in Cybersecurity



Source: CRS.

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; FISMA: the Federal Information Security Management Act; IC: Intelligence Community; NIST: National Institute of Standards and Technology; NSA: National Security Agency; NSS: National Security Systems; OMB: Office of Management and Budget; R&D: Research and development.

Figure 1 is a simplified schematic diagram of major agency responsibilities in cybersecurity. In general, NIST develops

FISMA standards that apply to federal civilian ICT, and OMB is responsible for overseeing their implementation. DHS has operational responsibility for protection of federal civilian systems and is the lead agency coordinating federal efforts assisting the private sector in protecting CI assets under their control. DOJ is the lead agency for enforcement of relevant laws.

DOD, which accounts for more than 70% of all federal spending on cybersecurity, is responsible for military cyberspace operations, defense support of civil authorities when requested, and, through NSA, security of NSS. NSA is also part of the IC. The director of the NSA also leads the U.S. Cyber Command, whose main mission areas are defending the DOD information networks, providing support to combatant commanders for execution of their global missions, and strengthening the nation's ability to withstand and respond to cyberattack. DOD has the authority to conduct cyberspace activities in support of military operations pursuant to a congressionally authorized use of force outside of the United States, or to defend against a cyberattack on a DOD asset.

What does the cybersecurity framework do? In February 2013, the White House issued Executive Order 13636 to address CI cybersecurity. Among other things, the order required NIST to lead public/private development of a Cybersecurity Framework of standards and best practices for protecting CI. Released in February 2014, the Framework received positive reviews, but it appears too early to determine the extent to which it will improve CI cybersecurity.

Legislative Issues

Since the 111th Congress, more than 200 bills have been introduced that would address cybersecurity issues. Five were enacted at the end of the 113th Congress. They addressed

- **FISMA Reform**—updating the act to reflect changes in ICT and the threat landscape.
- **Workforce**—improving the size, skills, and preparation of the DHS cybersecurity workforce.
- **R&D**—updating agency authorizations and strategic planning requirements.
- **Program Authorization**—providing specific statutory authorization for ongoing activities of NIST (relating to the Framework, education, and awareness); the National Science Foundation (Scholarship-for-Service program); and DHS (the National Cybersecurity and Communications Integration Center [NCCIC]).

In the 114th Congress, debate has centered on three issues:

- **Information Sharing**—easing access of the private sector to threat information and removing barriers to sharing within the private sector and with the federal government. *Controversies:* Roles of DHS, DOD, and the IC; impacts on privacy and civil liberties; risks of misuse by the federal government or the private sector; effects of proposed liability protections.
- **Data-Breach Notification**—requiring protective measures and notification to customers and other parties after data breaches involving personal or financial information of individuals. *Controversies:* Federal vs. state roles; what protections and responses should be required.
- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity. *Controversies:* Adequacy of current penalties and authorities; federal vs. state roles; clarifying scope of current criminal liability, including impacts on civil liberties.

Long-Term Challenges

Current proposals are largely designed to address near-term needs in cybersecurity. However, those needs exist in the context of more difficult long-term challenges relating to design, incentives, consensus, and environment (DICE):

Design: Experts often say that effective security needs to be an integral part of ICT design. Yet, developers have traditionally focused more on features than security, for economic reasons. Also, many future security needs cannot be predicted, posing a difficult challenge for designers.

Incentives: The structure of economic incentives for cybersecurity has been called distorted or even perverse. Cybercrime is regarded as cheap, profitable, and comparatively safe for the criminals. In contrast, cybersecurity can be expensive, is by its nature imperfect, and the economic returns on investments are often unsure.

Consensus: Cybersecurity means different things to different stakeholders, with little common agreement on meaning, implementation, and risks. Substantial cultural impediments to consensus also exist, not only between sectors but within sectors and even within organizations.

Environment: Cyberspace has been called the fastest evolving technology space in human history, both in scale and properties. New and emerging properties and applications—especially social media, mobile computing, big data, cloud computing, and the Internet of things—further complicate the evolving threat environment, but they can also pose potential opportunities for improving cybersecurity, for example through the economies of scale provided by cloud computing and big data analytics.

Legislation and executive actions could have significant impacts on those challenges. For example, R&D may affect ICT design, cybercrime penalties may influence the structure of incentives, the Framework may improve consensus about cybersecurity, and federal initiatives in cloud computing and other new components of cyberspace may help shape the evolution of cybersecurity. See also CRS Issues Before Congress: *Cybersecurity* at www.crs.gov.

Eric A. Fischer, Senior Specialist in Science and Technology
Catherine A. Theohary, Specialist in National Security Policy and Information Operations

IF10159

Disclaimer