Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated January 10, 2017

Cybersecurity Issues and Challenges

Overview

Information and communications technology (ICT) is ubiquitous and continually evolving. It is increasingly integral to modern society. ICT devices and components form a highly interdependent system of networks, infrastructure, and resident data known as *cyberspace*.

The process of protecting cyberspace from attacks by criminals and other adversaries is called *cybersecurity*. The risks associated with any such attack depend on three factors: *threats* (who is attacking), *vulnerabilities* (what weaknesses they are attacking), and *impacts* (how the attack affects the victims).

What are the threats? People who perform cyberattacks generally fall into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* involved in espionage—stealing classified or proprietary information used by government or private entities; *nation-state adversaries* who develop capabilities and undertake cyberattacks in support of a country's 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? Attackers and defenders are engaged in a cybersecurity arms race. Attackers constantly probe 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 development or acquisition; 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, the information it handles, and things to which it is connected. *Cybertheft* or *cyberespionage* can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. *Denial-of-service* attacks can slow or prevent legitimate users from accessing a system. *Botnet* malware can give an attacker command of a network of "zombie" computers or devices 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.

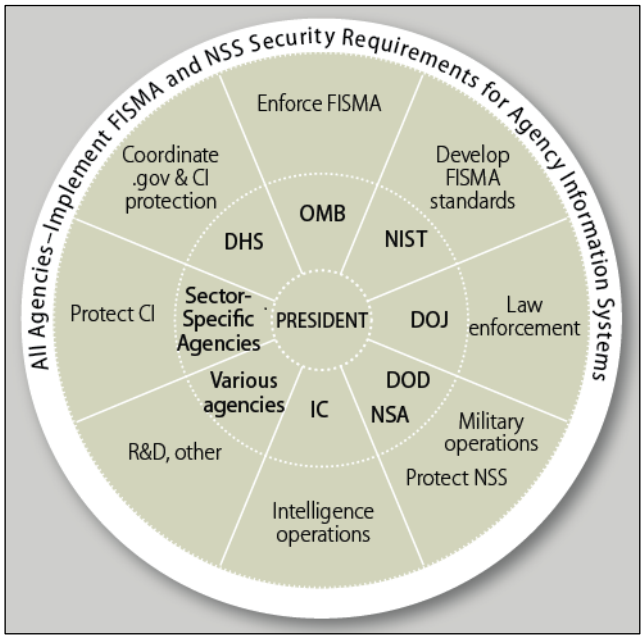
Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare successful 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 systems. 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 several new laws were enacted in the 113th and 114th Congresses.

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 Modernization 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 protecting federal civilian systems and is the lead agency coordinating federal efforts to help private entities protect CI assets under their control. DOJ is the lead agency for enforcement of relevant laws. DOD is responsible for military cyberspace operations, defensive support of civil authorities when requested, and, through NSA, security of NSS. NSA is also part of the IC. One continuing area of controversy with respect to agency missions is what role DOD should play in the protection of civilian ICT.

Legislative Actions

Since the 111th Congress, more than 200 bills have been introduced that would address cybersecurity issues. Several were enacted in the 113th and 114th Congresses. Among the issues they addressed are the following:

- **Federal Information Systems**—updating FISMA to reflect changes in the ICT environment and giving DHS additional authorities to protect federal systems.
- **Information Sharing**—facilitating public- and private-sector sharing of information on cyberthreats and defensive measures and permitting private-sector entities to monitor and operate defenses on their information systems.
- **Program Authorization**—providing specific statutory authorization for ongoing activities of NIST (relating to a framework for CI cybersecurity, education, and awareness); the National Science Foundation (Scholarship-for-Service program); and DHS (the National Cybersecurity and Communications Integration Center [NCCIC] and the intrusion-protection system known as EINSTEIN).
- **R&D**—updating agency authorizations and strategic planning requirements.
- **Workforce**—improving the size, skills, and preparation of the DHS cybersecurity workforce and requiring an employment-code structure for federal cybersecurity personnel.

The Obama Administration also took several actions relating to the above issues and on others, notably in response to attacks believed to have involved nation-state adversaries. That administration also proposed a revolving fund for modernizing federal ICT and established a commission on improving cybersecurity. That and other task forces have made recommendations for Congress and the incoming administration, including the following:

- Improve international cybersecurity strategies and build stronger international agreements.
- Expand deterrence and take a more assertive approach against cybercrime, including measures to raise the costs of cyberattack.
- Improve the usability and affordability of cybersecurity in products and services for consumers and businesses.
- Enact federal legislation on data-breach notification and take other steps to protect data and privacy.
- Address vulnerabilities posed by the Internet of Things (IoT)—the rapidly growing global network of devices connected in cyberspace.
- Streamline, clarify, and strengthen the organization of the federal government with respect to cybersecurity, and strengthen the capabilities of key agencies.
- Strengthen and build on public-private partnerships to improve cybersecurity.
- Clarify the role of active defense and research on vulnerabilities by the private sector.

Long-Term Challenges

The legislation and executive-branch actions discussed above are largely designed to address several well-established near-term needs in cybersecurity: preventing cyber-based disasters and espionage, reducing impacts of successful attacks, improving inter- and intrasector collaboration, clarifying federal agency roles and responsibilities, and fighting cybercrime. 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 IoT—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, cybersecurity R&D may affect the design of ICT, cybercrime penalties may influence the structure of incentives, the NIST cybersecurity 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 Report R43831, *Cybersecurity Issues and Challenges: In Brief*.

Eric A. Fischer,

IF10001

Disclaimer