Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

November 6, 2014

Cybersecurity Issues and Challenges

Overview

Information and communications technology (ICT) is ubiquitous and increasingly integral to almost every facet of modern society. ICT devices and components are generally interdependent, and disruption of one may affect many others. Over the past several years, experts and policymakers have expressed increasing concerns about protecting ICT systems from cyberattacks.

The risks associated with any attack depends 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 generally fall into one or more of five categories: *criminals* intent on monetary gain from crimes such as theft or extortion; *spies* intent on stealing classified or proprietary information used by government or private entities; *nation-state warriors* 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? Cybersecurity is in many ways an arms race between attackers and defenders. ICT systems are very complex, and attackers are constantly probing for weaknesses, which can occur at many points. Defenders can often protect against weaknesses, 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, 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 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.

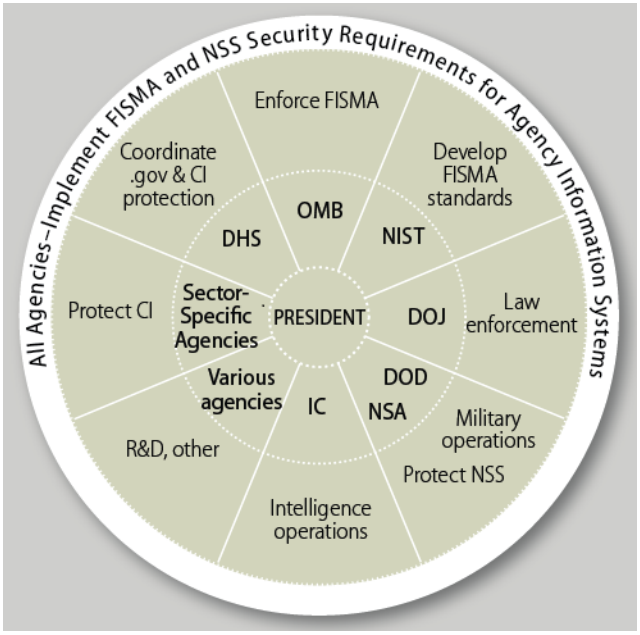
Most cyberattacks have limited impacts, but a successful attack on some components of critical infrastructure (CI)—most of which is held by the private sector—could have significant effects on national security, the economy, and the livelihood and safety of individual citizens. Thus, a rare attack with high impact can pose a much larger risk than a common 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. Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for CI. More than 50 statutes address various aspects of cybersecurity, and new legislation has been debated since the 111th Congress. However, no major cybersecurity bills have been enacted since the Federal Information Security Management Act (FISMA) in 2002.

Figure 1. Federal Agency Roles in Cybersecurity



Source: CRS.

Notes: DHS: Department of Homeland Security; DOD: Department of Defense; DOJ: Department of Justice; 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. DOD is responsible for military cyberdefense and, through NSA, security of NSS, which handle classified information. NSA is also part of the IC. DHS has operational responsibility for protection of civilian systems and is the lead agency for assisting the private sector in protecting CI assets under their control. DOJ is the lead agency for enforcement of relevant laws.

What Does the Cybersecurity Executive Order Do? In February 2013, the White House issued Executive Order 13636 and Presidential Policy Directive 21 to address CI cybersecurity through voluntary public/private sector collaboration and use of existing regulatory authorities. Among other things, the documents expanded an existing DHS information-sharing program and 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 has received generally positive reviews, but it appears too early to determine the extent to which it will improve CI cybersecurity.

Legislative Proposals

Beginning in the 111th Congress, many bills have been introduced that would address cybersecurity issues. Several have passed the House, both in the 112th and 113th Congresses, and one passed the Senate, but none had passed both chambers as of October 2014. The main issues addressed by the bills are

- **Information Sharing**—easing access of the private sector to classified threat information and removing barriers to sharing within the private sector and with the federal government. *Controversies:* Roles of DHS and the IC, impacts on privacy and civil liberties, and risks of misuse by the federal government or the private sector.
- **FISMA Reform**—updating the 2002 law to reflect changes in ICT and the threat landscape. *Controversies:* Role of DHS, OMB, and Commerce, and flexibility of requirements.
- **R&D**—updating agency authorizations and strategic planning requirements. *Controversies:* Agency roles, topics for R&D, and levels of funding.
- **Workforce**—improving the size, skills, and preparation of the federal and private-sector cybersecurity workforce. *Controversies:* Hiring and retention authorities, occupational classification, recruitment priorities, and roles of DHS, NSA, NSF, and NIST.
- **Privately Held CI**—improving protection of private-sector CI from attacks with major impacts. *Controversies:* Roles of DHS and other federal agencies, and regulatory vs. voluntary approach.
- **Data-Breach Notification**—requiring notification to victims and other responses after data breaches involving personal or financial information of individuals. *Controversies:* Federal vs. state roles and what responses should be required.
- **Cybercrime Laws**—updating criminal statutes and law-enforcement authorities relating to cybersecurity. *Controversies:* Adequacy of current penalties and authorities, impacts on privacy and civil liberties.

Long-Term Challenges

The executive-branch actions and proposed legislation 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. Cybersecurity, in contrast, 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, cybersecurity R&D may affect the design of ICT, 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.

For additional selected CRS reports relevant to cybersecurity and a list of experts, see CRS Issues Before Congress: *Cybersecurity* at www.crs.gov.

Eric A. Fischer, efischer@crs.loc.gov, 7-7071

IF00053