Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 19, 2024

Cybersecurity: A Primer

Introduction

The information technology that Americans use to chat with loved ones and make purchases are the same that can be turned against them to deny access to services, steal their information, or compromise the digital systems they trust.

These tools exist in cyberspace, and the security of that environment is a vast endeavor involving government, the private sector, international partners, and others.

This In Focus provides an overview of cybersecurity for policymaking purposes, describes issues that cybersecurity affects, and discusses potential actions Congress could take.

The Nature of Cybersecurity

The term "cyber" is frequently attached to a variety of security issues, underscoring the fact that issues surrounding the management of cyberspace and its security are immense and complicated.

To highlight how complicated it is, consider that the federal government does not have a single definition of *cyberspace* or *cybersecurity*. The Cyberspace Solarium Commission defined "cyber" as

> Relating to, involving, or characteristic of computers, computer networks, information and communications technology (ICT), virtual systems, or computer-enabled control of physical components.

While this definition may be suitable for a broad discussion about information technology, it does not account for relevant policymaking considerations concerning cybersecurity. Essentially, *cybersecurity* is the security of *cyberspace*.

As an example, consider a single smartphone. An American company may have designed the device, but the device may be built by a different company abroad using material from yet another country. The phone runs on software built by one company but modern operating systems borrow code from other companies and developers. Once a user has the device it will likely be connected to a variety of networks such as a home wireless network, a corporate network, and a cellular network. Each of these networks has its own infrastructure, but also share common internet infrastructure. The user will also install applications that contain code and use infrastructure by yet other myriad companies. Imagining users at the center, one can see large and intricate systems on one side and the other to create these devices and ensure their operation. The entire infrastructure and all those services that are part of *cyberspace* exist to deliver an experience to a user, a human.

Thus, from a policymaking standpoint *cybersecurity* can be considered the security of cyberspace—which includes the devices, infrastructure, data, and users that make it up. To support cybersecurity policymaking, adjacent fields also need consideration. Education, workforce management, investment, entrepreneurship, and research and development are necessary to get a product to market. Developers, law enforcement, intelligence, incident response, and national defense are necessary to respond when something goes awry in cyberspace.

Threats

The nation faces many threats (manmade and not) with an array of capabilities to carry out attacks. Threat actors may directly target the elements of cyberspace (e.g., networks, data, services, and users). However, they may also use these elements to attack industry through cyberspace.

For instance, a hacker operating independently or under a nation-state's instruction may target a hospital system. The hacker may send ransomware to a hospital to extort payment before the hospital can regain access to its files and devices. However, during that attack the hacker may also install a tool on the hospital's network, providing persistent access they will use to steal data, including patient information or other sensitive information. The hacker can then use that information to identify additional targets. In this scenario the hacker has attacked the hospital network, networked medical devices, and patient data.

The Director of National Intelligence (DNI) delivers the Intelligence Community's *Worldwide Threat Assessment* to Congress. In 2024, the DNI highlighted The People's Republic of China, the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea (North Korea), and criminals as the greatest concerns. These actors have demonstrated a growing capability and capacity for attacks against U.S. interests.

China is the most active actor conducting espionage campaigns and also has the capability to disrupt infrastructure. Russia seeks to use disruptions in cyberspace to bolster its military and foreign policy goals. Iran's aggressiveness in using cyber capabilities threatens networks and data. North Korea uses cyberspace to spy, steal, and disrupt. Transnational criminal organizations will continue to conduct phishing, fraud, and ransomware attacks for their own economic gain and under the direction of a nation-state. The more these adversaries engage in cyberattacks, the more their expertise and willingness to use their capabilities grow.

In addition to threat actors, users face threats from inherent vulnerabilities in software. The Log4j vulnerability is one

such example of widely used code that put many internet servers at risk of exposing user data.

Policy Areas

Given that cybersecurity is a large and complex issue area, paring it down to sub-issue areas can help in both understanding problems and crafting solutions. Four areas to consider are information and system security, device security, governance, and international relations.

Information and System Security

Computer scientists characterize security through three attributes:

- *Confidentiality*: that data is only known to authorized parties. A data breach is an example of how confidentiality is compromised, while encryption is a tool used to ensure confidentiality.
- *Integrity*: that data and systems are not altered without authorization. Data manipulation is an example of how integrity is attacked, while data-checking tools, such as hashing, ensure one can verify the integrity of data.
- *Availability*: that data and systems are available to authorized parties when they choose. Ransomware attacks availability; backups are a tool to support data availability.

Related to integrity is the concept of *authentication* or that users can verify data is from a trusted source. The internet was built using technologies that assume the trust of its users, but as the internet has grown into a global network, anonymity and data manipulation have proliferated, complicating the options a user has when determining the validity of online information. Inaccurate identifiers also frustrate companies seeking to verify their users—leading many to adopt zero-trust architectures where users are continuously authenticated.

Device Security

Similar to information security, the security of the system (e.g., the application, servers, routers, appliances, devices) can also be understood through the lenses of confidentiality, integrity, and availability. For an internet-connected device which monitors a building's energy use, the utility and customer will want to ensure data on the device is only accessible to them (confidentiality), the device accurately states how much energy is used (integrity), and the device is always monitoring usage (availability).

Governance

Many different entities are involved in cybersecurity. Government entities with regulatory authority may choose to exercise that authority by scrutinizing an industry's cybersecurity activities. Manufacturers may choose to adopt standards and best practices. Users may be savvy or oblivious to their cybersecurity risk. Network access and services providers may provide products which mitigate cybersecurity risk or transfer that risk to another party, such as to an insurer or to a security company. The interaction between all these parties through agreements, contracts, treaties, or other pacts creates a complex layer of responsibility and accountability for cyberspace. In addition to formal agreements, there are tacit understandings and expectations of each of these parties which continue to evolve as government and industry negotiate their shared responsibility for national cybersecurity.

International Relations

The internet is a global network, where a packet of data originating from one country can move to another at the speed of light. The devices that make up the infrastructure of the internet have a global supply chain. The software those devices require to operate are often created by an international workforce. Policies that one country establishes may have market effects in another.

The Internet-of-Things (IOT) highlights the international nature of cybersecurity. Devices may be built in one country to the standards of another where they will be sold. But, since they connect to the internet, they may become infected with malware from a third country, and be used against users in a fourth—all with little to no user action.

Policy Considerations

In crafting policy to address cybersecurity issues Congress has many options. Below is a list of possible actions Congress may take to strengthen cybersecurity (in alphabetical order).

Assess Resources. Congress may choose to examine an existing authority to determine if adequate investment to carry out Congress's intent has been made and adjust investments in that area to align with current expectations.

Conduct Oversight. Congress has direct oversight over the operations of the federal government, including the security of agencies' information technology and data. Congress may choose to call hearings and solicit testimony to ensure the cybersecurity of the nation, which includes the security of critical infrastructure and consumer data protection.

Develop a Program. Congress may choose to establish a program to address a facet of cybersecurity by authorizing an agency to do such work and appropriating funds for it.

Establish Rights. Congress may choose to establish the conditions for the use of technology, such as legal requirements for data privacy, retention, and use.

Incentivize Behavior. Congress may choose to incentivize the behavior of manufacturers, developers, vendors, or consumers either directly (such as through a grant program) or indirectly (such as by providing liability protections). One way Congress has incentivized behavior is through grant programs allowing underfunded entities (e.g., state and local governments) a steady capital stream.

Regulate Industry. Congress may choose to direct an industry to adopt standards or best practices, or participate in information sharing.

Study the Issue. Congress may choose to spur activity by directing agencies to develop a report or strategy.

Chris Jaikaran, Specialist in Cybersecurity Policy

Disclaimer