Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated December 15, 2020

Cybersecurity: A Primer

Introduction

There is a continued increase in both the utility and risk from networked devices. The very tools Americans use to chat with loved ones and make purchases are the same tools which can be turned against them to deny access to services, steal their information, or compromise the digital system they trust.

These tools exist in cyberspace, and the security of that environment is a large 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 that issues surrounding the management of cyberspace and its security are big and complicated.

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 those devices work.

To highlight how complicated it is, consider that the federal government does not have a single definition of *cyberspace* or *cybersecurity*. Recently, 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*.

When users go online they might work with their bank, get their email, conduct business, or get the news by accessing services. But those services don't exist independently. Those services rely on a common infrastructure of servers and switches, miles of cabling, wireless spectrum, and routers. That same infrastructure is used by other services too, such as utilities and shipping to ensure products arrive as intended—or by businesses to develop new products more efficiently and manage their operations. 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 with an array of capabilities and capacities 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 hospital operations material. 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. For the past few years the Director has addressed "cyber" as the first and most significant risk in the assessment. In 2019, the DNI listed threats by the risk they pose, starting with the countries of Russia, China, Iran, and North Korea:

> As the world becomes increasingly interconnected, we expect these actors, and others, to rely more and more on cyber capabilities when seeking to gain

political, economic, and military advantages over the United States and its allies and partners.

This ordering of countries considers the actor's technical capability, willingness to conduct cyber operations, and effectiveness as a threat to national security.

Policy Areas

Given that cybersecurity is a large and complex issue area, separating 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 breached, 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.

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.

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).

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 from non-governmental organizations 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 may choose to incentivize behavior is through the tax code. Congress could adjust the tax code to impose a penalty or provide a benefit (e.g., tax credit) for certain actions an individual or organization makes to improve cybersecurity.

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, Analyst in Cybersecurity Policy

IF10559

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.