The Heritage Foundation

LEGAL MEMORANDUM

No. 283 | MARCH 24, 2021

EDWIN MEESE III CENTER FOR LEGAL & JUDICIAL STUDIES

Additional Liability Protections Are Needed Against Cyberthreats

Brian Finch

KEY TAKEAWAYS

Cyberthreats continued to grow during 2020, necessitating additional measures to stem the trend.

Incentives exist in federal law to increase private cybersecurity measures, but they are in need of fine-tuning in order to ensure improved cybersecurity.

The Cybersecurity Information Sharing Act and the SAFETY Act should be amended so that their incentives more directly apply to cybersecurity tools and services.

With good reason, the COVID-19 pandemic dominated most policy-related discussions in 2020. Cybersecurity returned to the forefront at the end of the year, however, with news of the "SolarWinds" cyberattack on U.S. government agencies and private companies. Allegedly carried out by Russian intelligence agents, the SolarWinds attack used a corrupted software update to penetrate some of the federal government's systems, including sensitive components of the Departments of Homeland Security, Treasury, Energy, and various other agencies.[1]

Federal agencies were not the only attack victims. Further investigation uncovered SolarWinds-related attacks on state and local governments, as well as on private companies. As evidenced by the fact that for the first time a death was specifically attributed to a cyberattack, it appears that the risks posed by hackers have reached a new level of severity.

With no reprieve from cyberattacks in sight, private companies in particular will be compelled to continue heavy investments in cybersecurity measures. They continue to do so, however, under a cloud of uncertainty that accompanies the knowledge that every decision and dollar spent may be endlessly questioned by others, including by civil litigants.

Such uncertainty can easily lead to decreased cybersecurity. Companies, for instance, may delay responding to cyber threat intelligence due to worries that the "wrong" decision could expose them to expensive post-attack litigation. Cybersecurity innovation can also be thwarted as companies elect to keep proven (but aging) cybersecurity systems rather than innovative (but untested) security systems and services.

Existing Legislation

There are two existing laws, however, that, with minor adjustments, could materially incentivize companies to undertake increased cybersecurity. One is the Cybersecurity Information Sharing Act (CISA),[2] which encourages the sharing of threat information with the U.S. government. The second is the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, or the SAFETY Act.[3] Both laws encourage wider deployment of cybersecurity measures, but as discussed below, legislative amendments are necessary in order to unlock their full potential.

Cybersecurity Information Sharing Act

The relatively free flow of cyber threat intelligence between entities, whether public or private, is a critical component of cybersecurity. The recent SolarWinds attack proved that definitively, as a victim of the attack in the private sector was the one to alert federal authorities about the ongoing attack and its general characteristics.

Government officials have for some time recognized the value of cyber threat information-sharing and have taken steps to encourage just that. Thus far, the most concrete step they have taken is the Cybersecurity Information Sharing Act. The CISA law, passed as part of the 2016 omnibus spending bill and codified at 6 U.S.C. §§ 1501 et seq., authorized the Department of Homeland Security (DHS) to "encourage robust sharing of useful cybersecurity information among all types of entities—private, Federal, state, local, territorial, and tribal."[4]

Under 6 U.S.C. § 1501(a), the Departments of Homeland Security, Defense, Commerce, Energy, Treasury, and Justice, along with the Director of

National Intelligence and the Attorney General are authorized to develop and implement procedures that allow for the "timely sharing of classified cyber threat indicators and defensive measures" within the federal government as well as to non-federal entities.

Cyber Threat Indicators. Section 1501(6) defines "cyber threat indicators" as:

> [I]nformation that is necessary to describe or identify—
>
> (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
>
> (B) a method of defeating a security control or exploitation of a security vulnerability;
>
> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
>
> (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
>
> (E) malicious cyber command and control;
>
> (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
>
> (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
>
> (H) any combination thereof.

Defensive Measures. Section 1501(7) in turn defines "defensive measures" as follows:

> (A) In general
>
> Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.
>
> (B) Exclusion
>
> The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

> (i) the private entity operating the measure; or
>
> (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

Offensive Measures. Note that the definition of defensive measures is explicitly written to exclude so-called offensive cyber measures. The reason for that exclusion was that neither Congress nor the executive branch was ready to endorse, much less promote, the use of "hacking back" cyber tools by private-sector entities.

Non-Federal Entities. Section 1503(c) of the CISA specifically authorizes non-federal entities (meaning private entities, state and local government agencies, and even local governments performing utility services) to share the aforementioned cyber threat indicators (CTIs) and/or defensive measures (DMs) amongst themselves or with the federal government.

The law adds some limitations on the information-sharing process, including that the information shared must have a "cybersecurity purpose," which is defined as having the "purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability."[5]

Liability Protections. Non-federal entities are incentivized to share information under the CISA through the availability of specific liability protections under § 1505(b), which provides:

> No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure under section 1503(c) of this title.

The statute goes on to qualify the scope of those liability protections by adding that in order to qualify for them, the party who shared or received the third-party threat information must do so in a manner consistent with DHS requirements. Those requirements include:

- The information shared must meet the aforementioned DHS definitions of a cyber threat indicator or a defensive measure;

- The sharing must have been for a cybersecurity purpose;

- Personal information must have been reviewed for and, if identified, removed;

- The information must have been protected through security controls to protect against unauthorized access to or acquisition of it; and

- All other lawful restrictions placed on the sharing or use of such must have been followed.

The DHS, in its CISA guidance, notes that the liability protections for information-sharing apply only to shared cyber threat indicators and/or defensive measures.

The liability protections offered by the CISA are particularly helpful for companies that would otherwise be concerned that the mere act of sharing cyber threat information (whether an "indicator" or "defensive measure") could lead to liability. The liability protections are also useful in mitigating any concerns that sensitive or personal information accidentally contained in any shared data as part of any security program could lead to liability claims.

The statute as currently written falls short, however, in two key areas: first, in addressing emerging concerns related to physical supply chain considerations, and second, with respect to actions taken as a result of receiving threat intelligence.

Corrupted Devices. The first priority for improving the CISA is amending its language so that it explicitly encompasses the threats posed by devices that have been tampered with and/or technologies with intentional, built-in flaws that are hard to detect, not simply compromised and/or malicious software. Sharing warnings about those systems with built-in threats would seem tailor-made for the CISA. Indeed, as currently written, the CISA applies to cyberattacks conducted through tampered/corrupted software, akin to the breach methodology used in the SolarWinds attack. However, it is unclear— possibly even doubtful—that corrupted devices would fall under the category of either cyber threat indicators or defensive measures.

Such threats are well-known, however, particularly in the form of compromised network routers or surveillance cameras that feature built-in spyware.[6] Worries about those threats are so great that, for instance, Congress has ordered the Defense Department to ban the use of specific types of network communications devices and surveillance cameras within either the facilities of Defense Department contractors or the Pentagon itself.[7] As a result, a gap in liability protections exists in the statute that could make companies think twice when discovering tampered equipment that could pose a security threat.

In order to remove any such doubt and ensure that companies can freely share information about cyberthreats in any form, the CISA should be amended to explicitly cover threats posed by tampered/corrupted devices. Indeed, a thorough review of the categories of technical information, policies, and procedures covered by the definitions of CTIs or DMs should be conducted.

Such a review is more than warranted given the breadth and apparent severity of the SolarWinds cyberattack. Again, at the time of this writing, that attack appears to have been conducted via a compromised software update. That attack methodology, whether conducted via software or hardware, is one that has been of significant concern for some time, therefore it makes sense to ensure that such information can be shared as widely as possible.

Clarifying Liability Protections. A more significant and perhaps even more meaningful change to the CISA would be to clarify that its liability protections also apply to actions taken after receipt of shared threat information. Interestingly, § 1505(c)(1)(b) of the CISA states that it does not create "a duty to warn or act based on the receipt of a cyber threat indicator or defensive measure."

This section gives companies protection for not acting upon received cyber threat intelligence, which is warranted, given that companies receive an overwhelming amount of threat information. Indeed, many companies have turned to automated systems in order to process the daily influx of threat information that they receive.

Yet the CISA does not provide protections for companies that choose to act upon received threat intelligence. That is a curious disconnect, as the law could unintentionally be seen as encouraging companies to not act on the threat information that they receive (as there is no duty to so). On the other hand, if they do act—a process that could involve significant time pressure if a threat is imminent—companies could be subject to an avalanche of claims alleging that but for its faulty response to the threat information, the cyberattack in question would not have succeeded.

In such cases, holding companies liable for receiving (but allegedly improperly acting on) shared threat information represents a wholly unnecessary disincentive to information sharing. Companies may elect to reduce their reliance on information-sharing in order to avoid allegations that they ignored warnings about known threats regardless of how or when they were provided.

Congress should resolve this concern by amending the CISA to grant recipients the presumption that—absent a showing of willful misconduct

or fraud—any cybersecurity measures they affirmatively undertook based upon the shared cyber threat indicators or defensive measures were reasonable and appropriate. Such a change would then give private companies an even greater incentive to both receive *and* act upon shared cyber threat intelligence.

The SAFETY Act. After the terrorist attacks of 9/11, fears about tort litigation arising out of new security measures nearly stymied the emerging security market. Vendors of security products and services were concerned that they could be held accountable for damages resulting from terrorist attacks based on claims of "negligent" or "unreasonable" provision of security. These concerns became so prevalent that some vendors indicated that they might abstain from participation in the homeland security enterprise.

Congress and the George W. Bush Administration, in response to such fears, drafted and passed a liability management statute known as the SAFETY Act.[8] The SAFETY Act provides tort liability protections to entities that create, deploy, or otherwise use security technologies, policies, procedures, or services. As DHS noted in its preamble to the SAFETY Act Final Rule, the SAFETY Act was created by Congress for use as "a critical tool in expanding the creation, proliferation and use of anti-terrorism technologies."[9]

SAFETY Act protections are obtained by filing an application with DHS, which reviews the application to determine whether the product or service is effective in combatting "terrorist" threats. Pursuant to 6 CFR § 25.4(a), any product or service (referred to as "Qualified Anti-Terrorism Technology") that is "designed, developed, modified, provided or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause" is eligible for protections under the SAFETY Act.

Assuming the application is approved, the awardee will then either have a cap on tort damages awarded against it or have claims dismissed in their entirety when the DHS Secretary declares that the triggering event is an "act of terrorism."

Terrorism Definition. As defined in both the SAFETY Act statute and Final Rule, an act of terrorism is defined as follows:

The term "Act of Terrorism" means any act determined to have met the following requirements or such other requirements as defined and specified by the Secretary:

> (1) Is unlawful;
>
> (2) Causes harm, including financial harm, to a person, property, or entity, in the United States, or in the case of a domestic United States

> air carrier or a United States-flag vessel (or a vessel based principally in the United States on which United States income tax is paid and whose insurance coverage is subject to regulation in the United States), in or outside the United States; and
>
> (3) Uses or attempts to use instrumentalities, weapons or other methods designed or intended to cause mass destruction, injury or other loss to citizens or institutions of the United States.[10]

Cyberattacks as Terrorism. Since its inception, the SAFETY Act has been interpreted by many to apply to cybersecurity services and technologies—a position supported by the fact that the DHS has granted SAFETY Act awards to multiple such cybersecurity products and services. However, because the trigger for invoking the law is that an "act of terrorism" has occurred, some potential applicants have expressed concern that the SAFETY Act does not apply to cyberattacks, particularly those unconnected to terrorist attacks. That reluctance has only grown in the past few years, causing a number of potential SAFETY Act cybersecurity applicants to refrain from pursuing the law's protections.

The source of that concern stems from the specific language used in the acts of terrorism definition. That statute uses the term "terrorism," which colloquially involves acts of violence or sabotage motivated by political or religious-based grievances. However, in the case of the SAFETY Act, the act of terrorism definition makes no reference to motivation or intent with regard to the terrorist act. Instead, the only triggers needed are that it was an unlawful, intentional act that caused some sort of harm to American persons, property, or economic interests.

Understanding that, it should be apparent that a triggering "act of terrorism" can include cyberattacks unconnected to what would be commonly defined as a "terrorist group." Given the absence of language specifically excluding such a requirement, there continue to be questions as to whether the SAFETY Act can be triggered by a cyberattack without a clear connection to a terrorist group or group operating with a terrorist-like intent.

The most direct way to address that shortcoming would be to amend the language of the SAFETY Act so that it explicitly applies to cyberattacks that have no explicit or implicit connection to terrorist groups. By doing so, the purpose of the SAFETY Act—protecting Americans from malicious attacks with significant physical or economic consequences—will be more fully implemented.

Several sections of the SAFETY Act should be modified in order to end any questions about the applicability of laws to all forms of cyberattacks.

Eligibility. First, in the definitions section of the SAFETY Act, the law defines the product or service eligible for SAFETY Act protections to be a "qualified antiterrorism technology."[11] Such qualified technologies mean "any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, that is designated as such by the Secretary."[12]

While it would seem that the language referring to "information technology" would be enough to explicitly cover cybersecurity technologies and services, that has not proven to be the case. Language should thus be inserted into that section so that the law refers to both an "antiterrorism technology" as well as "cybersecurity technology." Additionally, as discussed below, language should be inserted making clear that cybersecurity incidents separate from "acts of terrorism" would trigger the law's protections.

Cyberattack Protections. Second, the SAFETY Act law should be amended so that it is clear that the protections of the law apply when there has been a "cyberattack" as opposed to an "act of terrorism." The definition of an "act of terrorism," as noted above, is found in § 444(2) of the SAFETY Act.

Critical to note here is that nothing in § 444 (or anywhere else in the SAFETY Act statute) requires that "act of terrorism" have a defined "terrorist" intent or a connection to a "terrorist group." Moreover, nothing indicates that the sole purpose of the protective technologies or services be anti-terrorism in nature. Thus, amending the law to say that its liability protections can be used when there has been either an "act of terrorism" *or* a "cyberattack" would efficiently and smartly allow for its greater use.

As the past few years have demonstrated, terrorist attacks are still (thankfully) rare—but cyberattacks continue nonstop and are highly damaging. The federal government should be doing everything it can to encourage widespread deployment of effective cybersecurity services and technologies, and one way it can do so is by allowing cybersecurity vendors to attach liability protections to their proven systems. With a few amendments, the SAFETY Act will be the perfect vehicle for that.

Conclusion

Battling cyberthreats will require constantly evolving tools and techniques. As part of that, the incentives offered to continually ensure widespread use of effective—if not yet totally proven—cybersecurity tools

must also continually be updated. Accordingly, Congress and the President must work together to ensure that existing incentive programs are used in a manner that promotes good cybersecurity. Amending laws like the CISA and the SAFETY Act so that they encourage private companies to take proactive measures against cyberattacks (without undue fear of costly lawsuits that needlessly question their cyber hygiene) will go far in establishing useful barriers against cyberattacks.

Brian Finch is Visiting Legal Fellow in the Edwin Meese III Center for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation.

Endnotes

1. Kevin Poulsen, Robert McMillan, and Dustin Volz, "SolarWinds Hack Victims: From Tech Companies to Hospital and University," *Wall Street Journal*, December 21, 2020, https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402 (accessed January 2, 2021).
2. 6 U.S. Code §§ 1501 et. seq.
3. 6 U.S. Code §§ 441–444.
4. Cybersecurity and Infrastructure Security Agency, "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance," https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance (accessed March 12, 2021).
5. 6 U.S. Code § 1501(4).
6. Robert Mayer, "Public–Private Initiatives to Secure the Supply Chain," testimony before the Committee on Homeland Security, U.S. House of Representatives, October 16, 2019, https://homeland.house.gov/imo/media/doc/Testimony%20-Mayer.pdf (accessed December 22, 2020).
7. John S. McCain National Defense Authorization Act for Fiscal Year 2019, § 889(a)(1)(B), Public Law No. 115–232.
8. *Federal Register*, Vol. 71, No. 110 (June 8, 2006), pp. 33147–33168.
9. Ibid.
10. See 6 U.S. Code § 444, and 6 Code of Federal Regulations § 25.2 (2006).
11. 6 U.S. Code § 444(1).
12. Ibid.