UNIVERSITY *of* PENNSYLVANIA
JOURNAL *of* LAW & PUBLIC AFFAIRS

Vol. 1 July 2016 No. 1

AN INITIAL, BUT POSITIVE, STEP IN THE REALM OF CYBERSECURITY

Saxby Chambliss

AN INITIAL, BUT POSITIVE, STEP IN THE REALM OF CYBERSECURITY

Saxby Chambliss[*]

ABSTRACT

On December 18, 2015, the President signed the Consolidated Appropriations Act, 2016 (Omnibus) into law. Title I of Division N of the Omnibus contains the Cybersecurity Information Sharing Act of 2015 (CISA). This Article presents insights on the interpretation, intended operation, and significance of CISA from the perspective of a key architect of this important piece of national security legislation.

I. INTRODUCTION

A. Understanding the Cyber Threat

Cyber attacks are not a new phenomenon. For years, government and private sector experts have warned of growing threats, the massive theft of intellectual property to cyber espionage, and billions of dollars being lost by the U.S. economy. The former head of the National Security Agency (NSA) called cyber espionage the "greatest transfer of wealth in history."[1] With the annual cost of cybercrime and cyber espionage to the world economy estimated at more than $375 billion,[2] the "rise of the sophisticated cyber criminal is the fastest growing security threat to organizations and individuals."[3]

Cyber attacks are now commonplace enough that, in 2014, James Comey, the Director of the Federal Bureau of Investigation (FBI), testified before Congress that "[t]here're two kinds of big companies in the United States: those who have been hacked by the Chinese and those who don't yet

---

*Saxby Chambliss is Partner at DLA Piper; former U.S. Senator (2003-2015); and former United States Representative (1995-2003).

[1] Gen. Keith B. Alexander, Dir., Nat'l Sec. Agency, Remarks at American Enterprise Institute (July 9, 2012), https://www.aei.org/events/cybersecurity-and-american-power/.

[2] CTR. FOR STRATEGIC & INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME 6 (June 2014), http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf.

[3] Jeffrey S. Price & Justin D. Wear, *Claims Made and Insurance Coverage Available for Losses Arising out of or Related to Electronic Data,* 51:1 TORT TRIAL & INS. PRAC. L.J. 51, 52 (2015).

know they've been hacked by the Chinese."[4] Consider the high-profile attacks in recent years against restaurants, banks, health insurance companies, social media, retailers, and the Internal Revenue Service and the Office of Personnel Management. Each attack reminds us that cyber incidents can happen against anyone, anywhere, at any time.

Today, law enforcement learns of a large-scale data breach "close to every two to three days"—a notable change from the two to three weeks of years past.[5] There is no single answer for this sharp increase. Certainly, the same technological advances that facilitate communication, enhance productivity, and improve our quality of life have created more opportunities for malicious actors and inadvertent cybersecurity compromises. Even as many organizations look to fortify their computer networks and information systems, not all are prepared.[6] Organizations-including the government-naturally weigh potential risks against the costs and benefits of enhanced security. Some are "soft targets," providing smart and tech-savvy malicious actors with multiple avenues for exploitation. Adding to the complexity, some victims may be reluctant to publicize incidents;[7] this, in turn, can create a false sense of security for consumers, employees, or others. Then there are the threat actors themselves-nation states, organized crime, individual hackers-actively exploiting vulnerabilities for malicious purposes.

Compounding all of this is the fact that data is everywhere. Financial, healthcare, corporate, and government information are now favorite targets of malicious actors.[8] Moreover, ransomware, data manipulation, and even hacks of the personal emails of high-ranking government officials are on the

---

[4] *Sen. Patrick J. Leahy Holds a Hearing on FBI Oversight: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2014) (testimony of James B. Comey, Director of the Federal Bureau of Investigation).

[5] Elise Viebeck, *FBI: Data Breaches 'Increasing Substantially,'* THE HILL (May 14, 2015, 03:01 PM), http://thehill.com/policy/cybersecurity/242110-fbi-official-data-breaches-increasing-substantially (quoting remarks by James Trainor).

[6] *See* PONEMON INST., THE CYBER RESILIENT ORGANIZATION: LEARNING TO THRIVE AGAINST THREATS 2 (Sept. 2015), https://cdn2.hubspot.net/hubfs/427640/RS_Content/Reports/The_Cyber_Resilient_Enterprise_Ponemon_Report.pdf (noting that over 60% of respondents say that their organization either does not have a cybersecurity incident response plan or has only an "ad hoc" plan).

[7] Jacob J. Lew, Sec'y, U.S. Dep't of the Treasury, Remarks at Delivering Alpha Conference Hosted by CNBC and Institutional Investor (July 16, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl2570.aspx.

[8] *See, e.g.*, SYMANTEC, 2015 INTERNET SECURITY THREAT REPORT VOL. 20 (Apr. 2015), https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-securityt hreat-report-volume-20-2015-social_v2.pdf (broadly examining the threats faced across industries).

rise.[9] But stealing data is just one motivation for cyber attacks. Consider the attacks on Sony and the Las Vegas Sands Corporation. Believed to be attributable to hostile foreign governments,[10] these attacks not only caused substantial financial loss but inflicted permanent damage on the victims' computer networks. These attacks are deeply disturbing from a national security standpoint. We know foreign governments seek the intellectual property of American companies, but we are not accustomed to such blatant, malicious, and destructive attacks on our companies for political reasons.

The severity of cyber attacks may also be exacerbated by our own delays in detecting incidents. For example, in 2008, Heartland Payment Systems was breached resulting in the ultimate exposure of the personal information of 130 million people; yet, no one discovered the intrusion until 2009.[11] In its *2015 M-Trends Report*, Mandiant placed the "median number of days that threat groups were present on a victim's network before detection" at 205 days, with the longest presence at 2,982 days.[12] We simply cannot defeat or prevent a threat if we lack the capacity or the will to know it exists.

B. Why Information Sharing Matters

Against this evolving threat, the costs associated with cyber attacks are escalating.[13] There is also the well-placed concern about the "Brand" of a victim company. As a result, cybersecurity is becoming a key topic in

---

[9] *Global Cybersecurity Threats: Hearing Before the H. Select Comm. on Intelligence*, 114th Cong. (2015) (statement of James Clapper, Director of National Intelligence) ("I believe the next push of the envelope is going to be the manipulation or the deletion of data which would of course compromise its integrity.").

[10] Emily Flitter & Mark Hosenball, *FBI Says Sony Hackers "Got Sloppy," Posted from North Korea Addresses,* REUTERS (Jan. 7, 2015), http://www.reuters.com/article/us-northkorea-cyberattack-usa-fbi-idUSKBN0KG1V220150107.

[11] Rachel King, *Lessons from the Data Breach at Heartland,* BLOOMBERG BUSINESS (July 6, 2009), http://www.bloomberg.com/news/articles/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice.

[12] MANDIANT, M-TRENDS 2015: A VIEW FROM THE FRONT LINES 3 (2015), https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

[13] According to a 2015 study released by IBM and the Ponemon Institute, the average cost per record stolen in a breach in the United States is $217, with a total average cost per incident of $6.5 million. PONEMON INST., 2015 COST OF DATA BREACH STUDY: GLOBAL ANALYSIS (May 2015), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03053WWEN&attachment=SEW03053WWEN.PDF.

American boardrooms,[14] and has captured the attention of federal and state regulators and class action lawyers. Many organizations and the government are searching for solutions, including insurance, compliance programs, data policies, incident response plans, and improved security. While no silver bullet will prevent all cyber attacks, one legislative measure took on new urgency in recent years.

It may seem intuitive that companies should be able to share cyber threat information with each other, learning about the threats each faces. Companies not adequately investing in cybersecurity could benefit from understanding the threats being inflicted upon their competitors, partners, or affiliates. Companies that are investing in cybersecurity may not only be role models for others, but as threats change, can more appropriately tailor their own security investments.

It may also seem natural for private entities to share insight with the federal government, enabling law enforcement and intelligence agencies to enhance their understanding of cyber threats by linking this insight with classified or other sensitive information. This analysis can, in turn, be shared with the private sector, equipping them to better detect and prevent malicious activity.[15]

Yet, until just a few months ago, significant legal restrictions undermined the ability of private entities to effectively counter new and challenging threats by sharing cyber threat information. From antitrust laws that could be interpreted to prevent such private collaboration, to freedom of information laws that could leave proprietary information shared with the government vulnerable to disclosure, our laws simply discouraged these simple exchanges of information. Nor did our laws provide companies with liability protection from potential lawsuits, a void made more obvious by the years of litigation faced by telecommunications companies following the disclosure of the post-9/11 Terrorist Surveillance Program. In spite of these significant risks, some private entities voluntarily took part over the years in cyber task forces and various information sharing relationships. However, it eventually became apparent that such participation was unlikely to increase without legislation granting clear sharing authorities and better legal safeguards.

---

[14] *See* NYSE GOVERNANCE SERVICES, A 2015 SURVEY: CYBERSECURITY IN THE BOARDROOM (2015), https://www.nyse.com/publicdocs/VERACODE_Survey_Report.pdf.

[15] Joseph Lawler, *Fallout Coming from JP Morgan Hack Attack,* WASH. EXAMINER (Oct. 14, 2014), http://www.washingtonexaminer.com/fallout-coming-from-jpmorgan-hack-attack/article/2554755 ("We need help and [need to continue] working together with the government . . . The government knows more than we do.") (quoting JPMorgan CEO Jamie Dimon).

C. Where is the Federal Government?

During the lengthy congressional debate about information sharing legislation, the federal government, especially the NSA, faced criticism following the leaks of classified information by Edward Snowden. This criticism impacted the cyber debate as NSA became a favorite target for conjecture and unfounded accusations, leading some to oppose any effort to give them direct access to cyber threat information. It is possible that a bill that simply addressed private-to-private sharing or significantly reduced the role of the NSA and other non-civilian agencies might have been enacted much sooner. But given the vital role that our law enforcement, military, and intelligence agencies share in countering this threat-a threat that originates from nation states, terrorists, organized crime, and lone hackers alike-passing such a limited bill would have been counterproductive.

Throughout most of this debate, I served both as a Member and the Vice Chairman of the Senate Select Committee on Intelligence (SSCI), and as a Member of the Senate Armed Services Committee. I saw firsthand the extraordinary cyber assets, capabilities, and knowledge of the U.S. Government, especially the NSA, which has been blessed with solid leadership and highly trained professionals. Other Intelligence Community agencies, including the Central Intelligence Agency, the Defense Intelligence Agency, and intelligence elements at the FBI and Department of Homeland Security (DHS) play key roles in collecting, developing, and analyzing cyber intelligence. These agencies are very good at what they do. The FBI's law enforcement capabilities and interactions with the private sector are vital, as are the efforts of the Secret Service. Our challenge, then, as policy makers, was to find a process by which all relevant federal agencies could work together as seamlessly as possible to protect the nation against the daily barrage of cyber attacks.

II. PRIOR LEGISLATIVE EFFORTS

As the cyber threat increased, the SSCI and other committees of jurisdiction considered legislative and oversight measures that would improve the government's cybersecurity posture and encourage better coordination and communication among private sector entities and by and with the federal government. While Congress passed some discrete cyber provisions, no bill provided the comprehensive liability protections and flexibility needed to effectively change the status quo. In 2012, however, two bills garnered the attention of the Senate.

A. Lieberman/Collins Bill

From the beginning, the Lieberman/Collins bill was problematic. In spite of the good intentions of its lead sponsors, including Senator Feinstein, there were just too many drawbacks. The bill included everything from DHS mandates and the potential for more regulation to more government programs and an Internet "kill switch." Amid valid questions about DHS's capabilities, there was considerable reluctance to give DHS even more authority. The bill also would have sidelined the NSA and FBI in the sharing of cyber threat information. Further, the complexity of the bill's information sharing provisions and insufficient liability protections might have discouraged, rather than encouraged, broader collaboration. In short, many, including businesses on the front lines of cyber attacks, opposed the bill because it lacked the necessary options, flexibility, and liability protections. For these and other reasons, the bill was ultimately defeated in the Senate during the final months of 2012.

B. Secure It

The competing bill in the Senate, known as SECURE IT, had broad support from the business community. I was a co-author of this bill, specifically the information sharing provisions, along with Minority Leader McConnell, Senator McCain, Senator Burr, and other Ranking Members. Privacy groups, however, opposed the bill because of its strong liability protections and authorities for sharing information with government agencies such as the FBI and NSA. Ultimately, the Majority Leader refused to give the bill its own floor time for debate.

C. Origins of the Cybersecurity Information Sharing Act

Although no bill was enacted in 2012, it was clear that cybersecurity, particularly the sharing of threat and intrusion information, was critical to our national security. Senator Feinstein, as the Chairman of the SSCI, and I, as the Vice Chairman, resolved to overcome our differences and find a path forward. Agreeing that neither her information sharing provisions in the Lieberman/Collins bill nor mine in SECURE IT would gamer enough votes in the Senate, we committed to finding common ground. The Committee subsequently held dozens of meetings, hearings, and briefings with government and private sector representatives and privacy advocates.

In August 2014, the final version of our agreed-upon bill, the Cybersecurity Information Sharing Act (CISA), was voted out of the SSCI by a 14-3 margin, a remarkable result considering the divided

atmosphere in the Senate at the time. Unfortunately, the Majority Leader would not bring the bill to the floor for debate and disposition so the 2014 version of CISA died when Congress adjourned.

III. A POSITIVE STEP: CISA 2015

When the 114th Congress convened in 2015, Senator Burr and Senator Feinstein- as the respective Chairman and Vice Chairman of the SSCI, revived CISA. The Committee again held meetings, hearings, and briefings with stakeholders. Senators Burr and Feinstein negotiated with the White House and other Senators to make bipartisan changes to the bill. The result: CISA passed the Senate by an overwhelming bipartisan vote of 74-21; negotiations were held with counterparts in the U.S. House; and congressional leadership, in particular Majority Leader McConnell, attached CISA to the Consolidated Appropriations Act of 2016 and sent it to the President for signature in December 2015. Senators Burr and Feinstein deserve tremendous credit for their leadership in getting this much-needed and long-overdue bill enacted into law.

A. The Purpose of CISA

In order to understand the importance of CISA, it is first necessary to understand what it is not. CISA is not a surveillance bill. It provides no additional authority regarding government surveillance or intrusions by private entities. Rather, it is entirely voluntary, imposing no coercion, penalty, or other liability if a private entity decides not to share information. CISA's core purpose has always been to encourage *voluntary* sharing of information while providing vital liability and antitrust protections and protecting personal information from exposure.

B. Definitions

In my experience, definitions are the heart of national security legislation. CISA is no exception and its carefully defined key terms include "appropriate Federal entities;" "cybersecurity purpose;" "cybersecurity threat;" "cyber threat indicator;" "defensive measure;" and "private entity." Some of CISA's definitions were drawn from SECURE IT, some from Lieberman-Collins, and others were the product of lengthy negotiations with privacy and business groups. Other terms, such as "personal information" and "real-time" were not defined; however, there was consensus to give them their ordinary meanings. Importantly, CISA intentionally avoided the "near-real-time" construct of some other bills, emphasizing instead that all of the

defined federal agencies must be on the same playing field, receiving and sharing information with each other in real-time, without administrative or bureaucratic delays.

C. Authorizations

At the center of CISA is the authority for private entities to identify threats and develop or use protective measures. CISA confirms that private entities may operate defensive measures on, and monitor, their own information systems or those of consenting customers or suppliers for cybersecurity purposes. As described below, private entities may also share with and receive from private and governmental entities cyber threat indicators and defensive measures. In developing the authorities and methods for private sector sharing, CISA carefully considered privacy concerns while mindful of how threats are detected and analyzed. Private entities that choose to avail themselves of CISA's authorities must comply with lawful restrictions, implement security controls to protect against unauthorized access, and take steps to remove known personal information not directly related to a cybersecurity threat.

D. Methods of Sharing

CISA covers the full spectrum of cyber information sharing: it allows private entities to share cyber threat indicators and defensive measures with each other and the Federal government, and facilitates the government's sharing of such information with private entities. In short, it establishes a solid playing field for effectively preventing and mitigating cyber threats.

In response to privacy concerns, CISA does specify the avenues through which, and the reasons why, the private sector may directly share information with the federal government: (1) reporting crimes, such as data breaches; (2) engaging in existing or future information sharing relationships; (3) conducting meetings, phone conversations, and other non-electronic format discussions; and (4) engaging in real-time automated sharing through the DHS portal. Of note, this construct, which was the subject of considerable debate, creates legal inconsistencies. For example, sharing information by phone directly with an FBI agent will provide liability protection, but sending the same information via email to the same agent offers no protection. It remains to be seen how the courts will view this discrepancy, or whether Congress will act to improve this construct.

E. Liability Protection

CISA is not a free pass and does not incentivize unlawful conduct. Absent full compliance with the clear terms of the Act, there is no liability protection. CISA does offer incentives to encourage broader sharing, including antitrust and Freedom of Information Act exemptions, protection for proprietary information and trade secrets, and regulatory limits.

F. Privacy Measures

CISA was designed to protect privacy interests and includes numerous privacy protections, such as:

- The definition of "cyber threat indicator" limits the information that can be shared.
- Private entities can only monitor their networks, or the networks of others with specific written consent, for cybersecurity purposes.
- Personal information not directly related to a cybersecurity threat must be removed before sharing.
- All information received by the government must be handled under established procedures and privacy protections.
- Most electronic sharing of cyber threat information with the Federal government must be through a DHS civilian portal.
- The government may only use information it receives for specified purposes[16]

G. Congressional Oversight

As with other national security legislation, Congress maintains current insight into CISA's implementation. The Executive branch must submit three separate reports to Congress, including an interagency inspectors general report and an independent report from the Comptroller General of the United States on the removal of personal information from cyber threat indicators.

But these reports are not the beginning and end of congressional oversight. Congress is reviewing the interim guidelines and procedures required by CISA, which were submitted to Congress on February 16, 2016. Also, congressional committees will no doubt hold many hearings and

[16] Given the current threat environment, this limitation may need to be re-examined.

briefings to understand the current threat environment and risks to the private sector and government, how CISA's authorities are impacting the nation's overall state of preparedness, and whether additional legislative measures are needed.

IV. MOVING FORWARD

With the enactment of CISA, private entities and the government may now benefit from mutual exchanges of information, in essence combining forces to prevent and mitigate cyber attacks. While a good beginning, there is more to do, here at home and abroad. On the domestic front, Congress must direct its attention to passing a federal data breach notification bill that clearly and effectively preempts state law, while resisting the temptation to impose onerous standards or regulations on American businesses. Currently, companies must comply with any one or all of 47 different state notification laws. A single, federal notification framework will allow private entities to focus their resources and attention on mitigating and preventing incidents, rather than navigating multiple legal requirements.

Throughout the world, terrorists and nation states are seeking new ways to use cyber threats to spread fear and destruction. If we are to defeat these efforts, we must find some consensus among our allies and other nations on the basics of cybersecurity, such as what constitutes a cyber attack or an "act of war" in the realm of cyber space. With CISA, America has shown its leadership and commitment to improving the playing field. Now is the time for us to extend our leadership and work towards a more secure cyber world.