Testimony of

Wm. Douglas Johnson

On behalf of the

American Bankers Association

before the

Subcommittee on Crime and Terrorism

of the

Committee on the Judiciary

United States Senate

Testimony of
Wm. Douglas Johnson
On behalf of the
American Bankers Association
before the
Subcommittee on Crime and Terrorism
of the
Committee on the Judiciary
United States Senate

Wednesday, July 8, 2015

Chairman Graham, Ranking Member Whitehouse, members of the subcommittee, my name is Doug Johnson, senior vice president, payments and cybersecurity policy, of the American Bankers Association (ABA). In that capacity, I currently lead the association's physical and cybersecurity, business continuity and resiliency policy and fraud deterrence efforts on behalf of our membership.

I appreciate the opportunity to be here to represent the ABA and discuss the importance of modernizing our legal framework in the current cyber-crime environment The ABA is the voice of the nation's $15 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $11 trillion in deposits and extend over $8 trillion in loans.

I also have the privilege of serving as vice chairman of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC) and on the board of directors of the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Established in 2002, the FSSCC is the national critical infrastructure protection coordinator for the financial sector, focused on operational risks. Because the FSSCC fits into a larger

network of sector coordinating councils, it is uniquely positioned as the leader within financial services for developing strategies to improve shared critical infrastructure and homeland security.

Established in 1999, the FS-ISAC is the designated operational arm of the FSSCC. The Center supports the protection of the global financial services sector by assisting FSSCC, Treasury as well as regional agencies and entities to identify, prioritize and coordinate the protection of critical financial services, infrastructure service and key resources. The FS-ISAC also facilitates sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, potential protective measures and practices.

As the 114th Congress engages in public debate on the important issue of cybersecurity and cybercrime, we share your concerns regarding the need to modernize our laws to meet the cybercrime challenges our nation faces. The ABA, now through its Center for Payments and Cybersecurity Policy, has historically been very supportive of these collaborative efforts to protect our sector's and nation's cyber infrastructure from private criminal actors and nation state threats. The financial sector is an acknowledged leader in defending against such threats. These efforts are highly mature and increasingly focused on international and cross-sectorial efforts to enhance our collective ability to defend against and respond to cybersecurity attacks that attempt to disrupt or destroy the systems we depend on, compromise personally identifiable information, steal intellectual property, or otherwise conduct criminal acts. We support buttressing our nation's ability to defend against, deter, and prosecute the perpetrators of these acts and will continue to work with Congress and this committee to achieve these goals.

In my testimony I will focus on three main points:

- **The cyber threats we face continue to evolve and become more complex.**
- **Our defenses against these threats continue to mature but challenges remain.**
- **Congress can assist by enhancing the civil and criminal penalties and tools we can use against our attackers.**

I. The Cyber Threats We Face Continue to Evolve and Become more Complex

According to the "Worldwide Threat Assessment of the US Intelligence Community," cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact, and the range of cyber threat actors, methods of attack, targeted systems, and victims are also expanding, highlighting the persistent and ever-changing nature of the threats the private sector faces and will face in the future.[1] Attacks that once were singular in focus, be it a denial of service attack on financial institutions, an attack against merchant point-of-sale devices, or an attempt to destroy or wipe data of an energy company, may now contain a variety of such attack vectors. Such multi-faceted attacks create particular challenges for the victimized company or companies, necessitating the simultaneous maintenance of availability, integrity, and confidentiality of data when formerly a cyber-attack might have impacted only one of these vital data security components.

Attackers of every variety are also becoming increasingly adept at defeating security practices, increasing the velocity with which companies must move to ensure they understand how cyber risks are changing and what mitigating measures are most effective against these risks. It is indeed an arms race. The tools that these perpetrators are using now have the capacity to destroy as well as compromise data, or in the alternative remain on systems for extended periods of time prior to detection.

Another increasing challenge for financial institutions and the private sector generally is the need to digest an increasingly larger volume of cyber threat data. Determining the relevance of a particular piece of threat data, analyzing the magnitude of the threat, evaluating which systems might be impacted, and devising the appropriate course to take to mitigate the threat if necessary has become increasingly difficult.

Who is being attacked is also changing. Prior to 2014, much of the private and public sector cyber security focus was on critical infrastructure and the payments system. Now there is recognition that, given the broader motivations of attackers for conducting a cyber-attack, essentially any company and any sector could be subjected to a significant, highly visible attack.

---

[1] Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, February 26, 2015, available at: http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

The motivations for such attacks are indeed broadening. Nation states are becoming more adept at compromising private and public computer systems for reasons ranging from retribution for perceived wrongs to espionage.

II. Our Defenses against These Threats Continue to Mature but Challenges Remain

The cybercrime threat certainly knows no boundaries. The increased activities of nation states and foreign criminal enterprises attempting to disrupt financial services through denial of service attacks, compromise U.S. customer financial data, or steal U.S. company and governmental trade secrets, point to the challenge we as a nation currently face in reaching overseas to apprehend and prosecute such actors. The overseas sale of the spyware and other tools used to facilitate these crimes is also difficult to prevent. We face vast botnet armies of infected computers, distributed internationally, attempting to use these tools to infect our financial customers' electronic devices, compromise their personal financial information or hijack their internet banking sessions.

The financial services sector's capacity to withstand the direct attack on our critical financial infrastructure as a result of the significant, purportedly nation state-based denial of service attacks demonstrated our sector's capacity to, through the FS-ISAC, act collectively to respond to major attacks and minimize their capacity to cascade through the sector.

Our sector has also initiated civil legal action, in conjunction with the FS-ISAC and Microsoft, to take down botnets responsible for compromising our customer's personal computers in order to extract their financial information. ABA was a declarant in several of the civil suits that successfully seized U.S.-based servers facilitating criminal botnets. These actions also cleansed millions of individual financial customer personal computers that had been infected in order to facilitate botnet traffic.

In April of this year the level of national and international coordination regarding such efforts took an additional step forward in the takedown of the "Beebone" botnet. In this instance, the FBI, the Department of Justice, and the National Cyber Investigative Joint Task Force-International Cyber Crime Coordination Cell (IC4), in coordination with other international law enforcement bodies, coordinated the takedown with the international financial sector. As a result of the court-authorized seizures of over 1000 domains, computers infected with Beebone could no longer report to the criminals responsible for the infection. Instead, infected computers were

redirected to a sinkhole server operated by Europol's European Cybercrime Centre, which is facilitating victim identification and remediation. As was the case with earlier botnet takedowns, as a result of the court-authorized domain seizures, computers infected with Beebone will no longer report to the criminals responsible for the infection. Instead, infected computers will be redirected to a sinkhole server operated by EC3, which will facilitate victim identification and remediation.

We also support recent action by the Administration, through executive order, authorizing the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, to impose sanctions on those individuals and entities that he determines to be responsible for or complicit in malicious cyber-enabled activities that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, economic health, or financial stability of the United States.

In addition to making it clear that sanctions authority will in the future be utilized against those that perpetrate cybercrimes, another important component of the order is the specification of what are considered significant malicious cyber-enabled activities to include:

- Harming or significantly compromising the provision of services by entities in a critical infrastructure sector;
- Significantly disrupting the availability of a computer or network of computers, including through a distributed denial-of-service attack;
- Misappropriating funds or economic resources, trade secrets, personal identifiers, or financial information for commercial or competitive advantage or private financial gain;
- Knowingly receiving or using trade secrets that were stolen by cyber-enabled means for commercial or competitive advantage or private financial gain; or
- Attempting, assisting, or providing material support for any of the harms listed above.

The sanctions executive order sends a strong signal to cybercriminals and foreign entities that America is committed to fighting this increasing threat, and that we share this commitment to working together to help protect our critical infrastructure and the economic security of our country.

III. Congress can assist by Enhancing the Civil and Criminal Penalties and Tools We Can Use Against our Attackers

The fact that attackers are becoming increasingly adept at defeating cybersecurity practices and mitigating measures points to the need for industry and government to develop and deploy enhanced measures on an ongoing basis with greater speed. While the threat detection, information sharing, and incident response capabilities our sector has leave us well positioned to withstand such attacks, we must also increase the potential that our attackers face real consequences for their actions.

Nation states that attack us generally deny attribution, or even if they take credit for the attacks currently do not fear the consequences. While the FBI and the Department of Justice have had increasing success in indicting members of overseas criminal networks and partnering with the private sector to disrupt botnets and other malicious activity, generally the organizations perpetrating these acts are not fearful of attribution, extradition, and prosecution to the degree that it impacts their risk/reward calculation.

While the recent executive order regarding sanctions is also important, it is widely recognized that Congress can also assist by passing legislation to fill important gaps that current law or executive action cannot fill. As such, we support this committee's efforts, as outlined in the recently circulated discussion draft, to propose the "International Cybercrime Prevention Act of 2015," which would:

- Clarify that U.S. economic espionage statutes cover acts committed on behalf of a foreign government;
- Enhance law enforcement tools to prosecute trade secret theft;
- Enhance the ability of trade secret owners to recover damages and keep their trade secrets confidential in court proceedings;
- Ensure our government can prosecute foreign individuals that possess or traffic credit card numbers, regardless of whether that individual is the criminal who stole the numbers in the first place;

- Allow service on foreign defendants outside U.S. jurisdiction. Foreign organizations with no agent or principal place of business within the U.S. should not be immune from service;
- Make the use of surreptitious interception devices a money laundering and RICO predicate and a Computer Fraud and Abuse Act violation;
- Authorize the forfeiture of surreptitious interception devices, proceeds from the sale of spyware, and property used to facilitate these crimes. While current law allows for prosecution of these crimes, cybercrime property and proceeds should not be exempted from forfeiture;
- Attack the use of overseas-controlled botnets by permitting the Department of Justice to seek a civil injunction to prevent ongoing Computer Fraud and Abuse Act (CFAA) violations in cases involving large numbers of victim computers;
- Create a CFAA violation for criminals who knowingly cause damage to a computer that controls critical infrastructure systems; and
- Allow the prosecution of government and corporate insiders that use their access for criminal purposes.

We look forward to working with Congress, this committee, and the Administration as we work to improve the legal and operational tools necessary to deter, detect, apprehend, and prosecute those that are using technology designed to create a more efficient and effective global economy for criminal purposes. We also strongly encourage Congress to act swiftly to enhance our abilities to share critical cybersecurity threat information, as well as to enact a national data security and notification law.