Center for Cyber & Homeland Security

THE GEORGE WASHINGTON UNIVERSITY

Trends in Technology and Digital Security

Cybersecurity in the Financial Services Sector

Issue Brief 4 in a Series
Based on Fall 2017 Symposium Proceedings

Panelists
John Carlson - Financial Services Information Sharing and Analysis Center
Adam Palmer - Financial Services Roundtable
Scott Petry - Authentic8

Panel Moderator
Frank J. Cilluffo

Panel Rapporteur
Sharon L. Cardash

This publication is the exclusive work product of the Center for Cyber & Homeland Security. It was made possible thanks to the financial support of Razor's Edge Ventures and Raytheon Company.

RAZOR'S EDGE

Raytheon

Issue Brief Series on Trends in Technology and Digital Security
Cybersecurity in the Financial Services Sector

On September 14, 2017, CCHS convened a Symposium on Trends in Technology and Digital Security. Four panels addressed emerging threats and their implications for security policy, with a focus on digital infrastructure protection and anticipatory analysis. In a series of Issue Briefs, CCHS shares the findings and recommendations that emerged from the Symposium, primarily on a not-for-attribution basis. This fourth Brief in the series addresses Cybersecurity in the Financial Services Sector.

The Ecosystem: A Snapshot

Banks are on the front lines, under cyber-assault daily, since that is where the money is. However, banks are stress-testing and exercising aggressively; and can absorb the intelligence surrounding cyber incidents, since the sector is dedicating significant resources to cybersecurity. When you think about public-private partnerships in the context of cybersecurity, they tend to be long on nouns and short on verbs; but when it comes to the financial services sector, it is the gold standard. Industry groups that seek to foster collaboration within and beyond the financial services sector, for cybersecurity and other purposes, include the "FS-ISAC" and "BITS".

FS-ISAC: Financial Services - Information Sharing and Analysis Center

What is the FS-ISAC and what does it do? The FS-ISAC consists of about 7,000 financial institutions, now in thirty-nine countries, with about 100 staff members located in eight countries. It is one of the primary vehicles for sharing threat and incident information, both for cyber and physical matters. As a result, the FS-ISAC has been very busy with Hurricanes Harvey and Irma, with a lot of work falling on its plate simultaneously. As a vehicle for sharing information and analysis, it should be emphasized that the FS-ISAC is all voluntary. It is not a government agency. It is a 501(c)6 non-profit organization funded by its 7,000 member-firms and sponsors.

In addition to information sharing, the FS-ISAC is also involved in conducting exercises, many of them in conjunction with the U.S. Treasury Department—through a highly successful series, called the Hamilton series—which looks at different types of cyber-attacks in different parts of the industry, to simulate how industry and government would respond to such events. This activity has been immensely helpful, for both the public and private sector, to understand what our vulnerabilities are, and what are some initiatives that we need to fill the gap.

The FS-ISAC has also been responsive to Presidential Executive Orders, including one that designated some of the largest firms as critical infrastructure. In this regard, the FS-ISAC launched a separate subsidiary—the Financial Systemic Analysis and Resilience Center (the FSARC)—that was formed by eight large financial services firms (now up to sixteen), to come together to collaborate much more deeply on information sharing, intelligence, analysis, and also working with law enforcement to respond to a growing threat of cyber

criminals and enterprises. FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cybersecurity threats, through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. government, including the Department of the Treasury, the Department of Homeland Security, and the Federal Bureau of Investigation.

FSARC collaborates with U.S. government partners and plans to expand its operational processes, establish a physical location for the Center, and add additional financial institutions that are eligible to participate. That initiative is now launched, underway, and getting fully staffed up. The FSARC is another way that the FS-ISAC is working in partnership with the U.S. government to understand threats to the sector, particularly on the critical infrastructure side, with a current focus on liquidity risks and wholesale payments.

The FS-ISAC is thus a platform for collaboration, discovery, and mutual support, not only around events (whether cyber or physical); but also for understanding what the vulnerabilities are, how they could impact the industry, and what the industry should do in response to that. As a result of this collaboration, the FS-ISAC also puts out products—best practices papers—and has done a lot of work, in this regard, around ransomware and account takeover attacks.

The FS-ISAC has also done some interesting work around destructive malware. That was one of the early Hamilton exercises, which simulated a SONY Entertainment type-attack, where malware basically destroyed SONY's systems. What was really concerning about that case, from a critical infrastructure protection perspective, was that the attackers destroyed data. For the FS-ISAC, that was a very concerning development, in that FS-ISAC members are highly dependent upon the availability and integrity of data for consumer and investor confidence. One after-action task was the preparation of a best practices paper on actions financial institutions should consider before, during, and after, a destructive malware attack.

Another outcome of a Hamilton exercise was the creation of another subsidiary of the FS-ISAC—called Sheltered Harbor. Sheltered Harbor was established in 2016 to enhance the financial services industry's resilience capability in the event of a major disaster event. Sheltered Harbor is based on standards and the concept of mutual assistance. Should a financial institution be unable to recover from a cyber-attack in a timely fashion, firms that adhere to the Sheltered Harbor standards will enable customers to access their accounts and balances from another financial institution. Sheltered Harbor members access specifications for common data formats, secure storage ("data vaults") and operating processes to store and restore data, and receive a Sheltered Harbor acknowledgement of adherence to the specification. Accordingly, there is a mutual support component, and also an extra layer of consumer protection. The idea is, hopefully, to mitigate market impact, in terms of concerns about the integrity of data across the industry (systemic risk).

The above are examples of what the FS-ISAC is involved in, but it really starts with people coming together voluntarily in a trusted environment, through emails, conference calls, and

the entity's secure portal in which one can post information. Having control over how that information may be used by others is immensely important; hence, the FS-ISAC operates according to what is known as "the traffic light protocol": "Red" means the information is for the member's eyes only. "Amber" means that you can share with others on a need-to-know basis. And "Green" means that you can share with government partners and others.

Finally, the FS-ISAC's intelligence officer has played a very important role, fostering collaboration with law enforcement, and working with other critical infrastructures. The FS-ISAC intelligence officer sees information coming through the voluntary channel; she flags it and then seeks consent from the relevant parties to be able to share that information with government parties, in order to make requests of government agencies to see if there are other pieces of information that they can share and potentially declassify. This process builds trust between the public and private sectors.

BITS: The Technology and Policy Division of the Financial Services Roundtable

The Symposium was joined by Adam Palmer, Vice President of Cybersecurity Risk Management at the BITS division of the Financial Services Roundtable. The Financial Services Roundtable (FSR) consists of roughly the top 100 financial services companies, as determined by market capitalization. FSR is involved in regulatory policy issues, housing policy issues, and cybersecurity matters. The FSR cybersecurity focus group is BITS, which concentrates upon operational cybersecurity issues/risks.

A top BITS priority is regulatory harmonization for cybersecurity. Here the goal is to try to encourage government to harmonize, not duplicate; to align, not layer. BITS also seeks to encourage the regulators and the government to step up their game, to have strong data security for BITS members. BITS also seeks to encourage public-private partnerships, in order to foster collaboration across the government and with BITS member-firms, with the aim of trying to improve policy as it pertains to response during a major incident.

In terms of key programs, the policy group of the regulatory arm of BITS is currently highly focused on the issue of domestic alignment—rather than duplication—in the context of the question: What if all fifty U.S. States were each to develop their own cybersecurity frameworks? (New York, for one, has done so). But, what if each State framework were different? The matter is also an issue at the international level.

BITS seeks to identify best practices, for efficiency, and for other purposes. As an example, BITS is presently hosting joint meetings of its Security group and its Fraud group, looking at the synergy and shared concerns between the two. Despite the existence of overlap, the CISOs and the Fraud (prevention) leaders in organizations are often very siloed. Therefore, BITS is looking at improving this operational structure to foster coordination and faster response.

BITS is also looking at the impact of new technology. Everybody wants technology that is faster, better, operational, scalable, and safe. Here, there are some significant issues concerning the financial services sector, including:

1. Artificial Intelligence. How can you use A.I. to improve and automate overall data governance?

2. Quantum Computing. How close are we to a threat where a quantum computer can defeat encryption?

3. Cloud Computing. While it is not a completely new paradigm (as we have entrusted information to third-party computers externally for a long time), the key is how you implement controls; i.e., how do you effectively monitor your system, and manage those controls that are being enforced?

4. Blockchain. Many financial services firms are considering Blockchain as an authentication tool. It may enhance authentication, and there is much talk about how to implement this distributed ledger technology. And, finally:

5. Active Cyber Defense. How far, from an operational policy standpoint, are you willing to go? What is the role of government and of the private sector? What is allowable from a policy perspective? How far can private entities go to gather intelligence on attackers who are aggressively targeting companies? There is still a feeling that cybersecurity strategy is "4,000 years old", meaning that we are still building a higher wall. As Symposium panelist Adam Palmer explained, BITS members do not just want to be a victim and build a higher wall each year, and then watch the bad guys get together and break through the wall. At some point, companies say: What can I do to empower law enforcement, what can I do to cooperate with the authorities and actively improve my defense? Is there more that I can do to be secure, beyond just improving my defense?

Another important BITS activity is the CEO Council. BITS is working with its CEOs to develop and process responses to major threats. For example, what happens if a major U.S. bank loses all communications with Asia? How does the government provide for mutual assistance, or support in the form of another financial institution stepping in to help? What is the regulatory relief that might be provided to allow this? How would institutions support, in this scenario? The related jurisdictional, policy, and operational issues need to be settled at a high level.

A further concern, at the government agency level, is regulator data security. If there is a data breach and a BITS member has to report that information by disclosing and sharing it with the regulators, are they secure? What does the U.S. government do to secure that data, to protect it? BITS seeks to have an open dialogue about how that data is to be used and protected.

In summary, BITS tries to be proactive, not reactive, to these issues in the financial services sector, keeping in mind that financial services firms are on the front line of cybersecurity. Adam Palmer, the Symposium member from BITS, emphasized the need to focus not only on risks, but on positive solutions.

Taking a Different Tack: Neutralizing the Threat Space with a Remote Browser

Rather than analyzing the threat space more deeply, another Symposium participant detailed a different, less traditional, approach to cybersecurity, pursuant to which the central question is: What if the threat space was irrelevant? To this end, the participant's company builds a one-time use, disposable browser, in the cloud. It allows you to interact with the Web through a full-fidelity interactive display, but no Web code ever reaches your environment. In fact, no IP attribution of your environment is ever exposed to the Internet.

The concept is simple: the browser is built fresh at the start, you use it, and it is destroyed at the end of the session. There is no need to worry about the content coming into your network, if it never touches you. No cookies, trackers, or malicious code ever reaches the end device. All you receive is an encrypted remote display of that session. You do not need to worry about links you may have just clicked. Any malware has no access to local system resources, like the registry or file system; and since that malware executes in a virtual environment and gets destroyed at the end of the session, it cannot persist. By analogy, it is like using rubber gloves when you change the wheel of your car; you do not need to worry about washing your hands, since you have rubber gloves on.

Virtualizing the browser is not an inherently new idea. Citrix and VMware have been doing things like this "forever." Cloud infrastructure is not inherently new either. The cloud has been around for years, and has become commonplace. We have seen ebbs and flows between centralized and decentralized computing capabilities since the dawn of the computer age. The browser is a completely decentralized application. And the ability to manage applications with enterprise policies is not inherently new.

But the participant's company has combined the virtualization and embedded policies within the browser, which has not been done before—a secure remote browser with policies to govern things like access controls, user credentials, data loss prevention policies, and more. When packaged as an integrated solution that allows an organization to deploy a browser that supports specifically their mission—whether it is safe browsing for employees, regulated employees accessing regulated data without violating compliance, or mission analysts conducting open-source intelligence for cybersecurity counter-research—through a spoofable and disposable infrastructure, the solution is highly disruptive.

By contrast, consider the present state of the cybersecurity industry: I.T. is conditioned by the cybersecurity vendor community to buy the latest, greatest, next-generation technology. Every time a new threat emerges, a new set of "next-gen." technologies are marketed, which promises to solve the latest threat. It started with executable blocking and IP blacklisting; then data analytics; now it is machine learning and artificial intelligence.

Yet, if you look at what data is coming into the network and puts it at breach, a large percentage of that data comes from the browser. The browser was designed in the 1980s, at the research consortium CERN, which was what Tim Berners-Lee described as "a safe environment"—for sharing research papers, text-based, internally within the research community. The protocols are brilliant and resilient. But they were not designed with any concept of security or content controls. Basically, a browser makes a connection to a host,

the host bundles up a big blob of data, delivers it down to the browser, and the browser dutifully renders that content.

Since then, however, that environment has exploded dramatically: today, every page view delivers a payload to the browser that contains cookies, trackers, potentially malicious links, redirects, suspect or malicious content like Flash or Javascript. And the cybersecurity industry sells to I.T. more single "drugs" to attack more single "bugs" to try and close that environment. These solutions try to detect the threat after it has reached the network and device. This "one bug, one drug" approach is "a mess"—I.T. is on a never-ending "hamster wheel" of purchasing more technology that works too late—after the malware has breached the network. The participant's company offers an alternative, simpler approach: put the browser in an environment that does not expose your environment—a browser that runs remotely and that you can throw away when you are done.

About Us

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan "think and do" tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues.

Website http://cchs.gwu.edu **Email** cchs@email.gwu.edu **Twitter** @gwcchs