Cybersecurity Collaboration

Routes to Stronger Defenses

■ by **Jonathan Cedarbaum**, Partner, WilmerHale and
Sean Reilly, SVP & Associate General Counsel, The Clearing House

As an industry, the financial sector outpaces other economic sectors in cybersecurity preparedness. Despite these efforts, however, cyber criminals still target bank networks, their executives, key employees with escalated privileges, and third parties with important connections to financial institutions. Criminals too often have ready access to sophisticated technology, enjoy the ability to organize and collaborate, benefit from a steady pipeline of talent, and generate enormous streams of illicit revenue with little chance of being caught. This "business model" needs to be disrupted. Foundational to the required change is improving collaboration between financial institutions and the United States government.

A vast and increasingly lucrative network of criminal organizations offers an array of cyber criminal services for hire. The network centers in Russia and many of its neighbors in eastern Europe, but extends into China, the Middle East, and virtually every corner of the globe. These organizations compete like other businesses, but they also collaborate, share ideas, and, like many other tech-based enterprises, innovate rapidly to develop new products and services. Malicious actors targeting financial institutions include: cyber criminals motivated by money, terrorist organizations with varied agendas, so-called "hacktivist" groups with political agendas, and even nation states bent on obtaining intellectual property or accomplishing a foreign policy objective. Banks must constantly adapt to the evolving threat environment, improving their agility, enhancing their capabilities and taking action on information shared by our partners in government.

In response to these growing threats, financial institutions have dramatically increased their own investments in cybersecurity defensive measures. But truly effective cybersecurity will require further improvements by banks, increased efforts by the federal government to defend the financial sector against threats often originating overseas, and, above all, much more effective collaboration between the private sector and the government. As President Obama noted during the recent White House Cybersecurity Summit held at Stanford University, "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as true partners." The private sector, the President acknowledged, "doesn't always have the capabilities needed during a cyber attack, the situational awareness, or the ability to warn other companies in real time, or the capacity to coordinate a response across companies and sectors. So we're going to have to be smart and efficient and focus on what each sector does best, and then do it together."

Yet legal, policy, and organizational impediments continue to hamper the ability of both financial institutions and the government to engage in the sort of effective cybersecurity efforts the president called for. This article examines a number of those impediments and offers some suggestions about how they can be reduced or overcome.

For example, many financial institutions have excellent information security programs in place, but many still need to improve their data security "hygiene." There is no shortage of guides to cybersecurity health – perhaps most notably the federal cybersecurity standards issued

by the *National Institute of Standards and Technology* (*NIST*) in February 2014, known as the Cybersecurity Framework Version 1.0 – but really putting these guides into practice remains the key.

The government, too, needs to do more. Attacks on the financial sector are often intended as attacks on the United States. As the sophistication of cyber threat actors increases and more and more attacks emanate from abroad, the government needs to take a more active role in defending against and responding to these attacks. If that requires new legal authorities, we should candidly discuss what they should be.

Most crucially, financial firms and the government need to improve their collaboration. They need to improve their information-sharing practices with respect to cyber threats and responses. The Financial Sector Information Sharing and Analysis Center plays a critical role in the effort to make actionable cybersecurity intelligence available to financial firms. But much more still needs to be done.

Evolving Threats, Improved Internal Bank Defenses

Consider the evolving threat landscape …

Do you think of "blitzkrieg" as a type of warfare pioneered at the outset of World War II? Of course, it was that. But it is also the name international law enforcement authorities have given to a mass financial fraud campaign planned by a leading Russian cybercriminal who goes by the name of vorvZakone ("thief in law").[1]

Do you think of "high rollers" as casino gamblers with deep pockets? Operation High Roller was another "highly sophisticated, global financial services fraud," designed specifically "to siphon large amounts from high balance accounts," sometimes more than $100,000 at a time.[2]

These examples reflect what one of the leaders of the Secret Service's cyber operations branch has called the "marked increase in the quality, quantity, and complexity of cyber crimes targeting private industry and critical infrastructure."[3]

Leaders of the Secret Service's cyber operations have also noted that "the increasing level of collaboration among cyber-criminals allows them to compartmentalize their operations, greatly increasing the sophistication of their criminal endeavors and allowing for the development of expert specialization."[4] As a result, "[i]llicit cyber crime marketplaces [that] allow criminals to buy, sell and trade malicious software, access to sensitive networks, spamming services, [and] hacking services" have grown at an alarming rate.[5] Some of the more popular sites "boast…membership of approximately 80,000 users."[6] Many of these markets for "fraud-as-a-service" exist in the open internet, though behind password or other walls designed to allow access only to trusted users.[7] Others exist in the so-called "deep web," made up of "darknets," online domains that use various techniques to remain outside the reach of search engines, thus "guarantee[ing] anonymous and untraceable access to Web content and anonymity for a site."[8]

These illicit markets have physical bases around the world, but the most important groups are found

1 Ryan Sherstobitoff, McAfee Labs, Analyzing Project Blitzkrieg, A Credible Threat (2013).

2 Dave Marcus and Ryan Sherstobitoff, McAfee Labs and Guardian Analytics, Dissecting Operation High Roller 3 (2012).

3 Statement of William Noonan, Deputy Special Agent in Charge, U.S. Secret Service, Criminal Investigative Division, Cyber Operations Branch, Before the Subcommittee on Financial Institutions and Consumer Credit of the House Committee on Financial Services 2 (Mar. 5, 2014). See also W. Gragido, Blackhatonomics: An Inside Look at the Economics of Cybercrime (2012)

4 Noonan Statement at 2.

5 *Id*.

6 *Id*.

7 For descriptions of some of the most popular "trojans," i.e., malware designed to infiltrate networks via downloads and steal information, used against the financial industry and their evolution, see EMC, The Current State of Cybercrime 2013, at 3-5 (2013); Symantec, The State of Financial Trojans Version 1.02 (2013).

8 Vincenzo Ciancaglini, Marco Balduzi, Max Goncharov, and Robert McCardle, Trend Micro, Deepweb and Cyber Crime: It's Not All About TOR 3 (2013).

in Russia. So extensive is the Russian cyber criminal industry that security researchers have uncovered extensive menus of goods and services offered, with fairly precise price ranges identified and competition like a mature technology market segment in the United States.[9] "The most popular wares include different kinds of malware, Winlockers, Trojans, spammers, brute-forcing applications, crypters, and DDoS bots."[10] By one estimate, the Russian cybercrime industry, dominated by eight to twelve major criminal organizations, has revenues of roughly $2 billion per year, at least 40 percent of which comes from online banking fraud.[11]

Russia and its neighbors are hardly alone. China's internet presence is the largest in the world, and China has a large and rapidly growing market for cyber criminal goods and services, particularly for those focused on mobile devices.[12] Russia and its peripheries may be the leading incubator of cyber fraud activities, but China may be the biggest source of the broader array of malicious cyber activities overall.[13]

In total, the threats to banks in cyberspace have become more sophisticated, frequent, and costly. By one estimate, the annualized cost of cyber crime to the financial sector has more than doubled in the last five years.[14]

The annual threat assessment by the Director of the Office of National Intelligence puts cybersecurity number one on the list of threats to U.S. security.

With all the focus on sophisticated cyber-threat actors, banks can lose sight of the crucial role of improved cybersecurity hygiene, that is, day-to-day data security risk management practices that can make a difference between an attack succeeding or failing. Some of the recent headline-worthy data breaches may have used points of entry that were accessible due to simple failings, such as inadequate training of employees or inadequate attention to the many routine vendors that may be given access to a company's network. Among the hygiene measures banks should focus on are:

- Training both IT and non-IT personnel regularly and with a more hands-on approach
- Mapping points of entry carefully and reducing those network access points
- Prioritzing types of data and methods of defense within systems, not simply guarding the perimeter

9 Max Goncharov, Trend Micro, Russian Underground 101 (2012). See also Group I-B, State and Trends of the "Russian" Digital Crime Market 2011 (2012) (with profiles of some of the leading figures), and Group I-B, Threat Intelligence Report 2012-2013 (2013).

10 *Id*. at 7.

11 Group I-B, State and Trends of the "Russian" Digital Crime Market 2011, at 5-6; Group I-B, Threat Intelligence Report 2012-2013, chs. 2 and 3. The Russian cyber criminal industry has become so well-developed that it has become a subject of study by sociologists and criminologists. See Thomas J. Holt and Eric Lampke, Exploring Stolen Data Markets Online: Products and Market Forces, 14 Global Crime 155-74 (2013); Thomas J. Holt, Examining the Forces Shaping Cybercrime Markets Online, 31 Social Science Computer Review 165-77 (2013); Marti Motoyama et al., An Analysis of Underground Forums, IMC'11, 71-79 (2011); Frank Wehinger, The Dark Net: Self-Regulation Dynamics of Illegal Online Markets for Identities and Related Services, 2011 European Intelligence and Security Informatics Conference; Bill Chu et al., Examining the Creation, Distribution and Function of Malware On-Line, report prepared for the U.S. Department of Justice (2010); Jason Franklin et al., An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants, CCS '07 (2007).

12 Lion Gu, Trend Micro, The Mobile Cybercriminal Underground in China (2014); Lion Gu, Trend Micro, Beyond Online Gaming Cybercrime: Revisiting the Chinese Underground Market (2013); Zhuge Jianwei, Gu Liang, and Duan Haixin, Investigating China's Online Underground Economy (2012).

13 See, e.g., J.P. Morgan, Cybercrime: This Means War 2 (2013).

14 Deloitte, Transforming Cybersecurity for the Financial Sector (2014).

- Putting in place processes to oversee vendor and other third-party relationships throughout the relationship lifecycle, not merely at their outset

Financial institutions have more than a decade of experience under the data security and privacy requirements established by the Gramm-Leach-Bliley Act and its implementing regulations. The best practices set out in the NIST Cybersecurity Framework Version 1.0 in many respects match those earlier requirements, though they provide more detailed and up-to-date recommendations.[15] The framework appears to go beyond existing requirements and regulatory expectations in a few areas by urging greater attention to:

- Efforts to recover from cybersecurity incidents, particularly the ability to maintain adequate capacity for ensuring the availability of data and systems
- Interrelations among companies in the financial sector and other critical infrastructure sectors
- Aggregating and correlating cybersecurity data from multiple sources
- Monitoring the physical environment, personnel activity, external service providers, mobile code, and unauthorized personnel, connections, devices, and software), not just IT systems
- Continuous and rapid adaptation of information security practices in light of rapidly changing technology, business, and threat environments

Banks should be using the Framework to test and hone the effectiveness of their information security programs, both internally and in their dealings with vendors.[16] The Cybersecurity and Critical Infrastructure Committee established by the FFIEC in late 2013 is expected to issue updated data security guidance soon.

More Vigorous Government Action

While banks do much of the work of cyber defense themselves; they cannot go it alone. The government needs to more as well. The recently released annual threat assessment by the Director of the Office of National Intelligence puts cybersecurity number one on the list of threats to U.S. security.[17] Because so much of the critical infrastructure in the U.S. is in private hands, much of the threat to U.S. security stems from possible attacks on private targets, including the financial system. The government therefore needs to take a more active role in leading the response to these threats.

One threat that illustrates the point is botnets. "Botnet" is short for robot network. Botnets are networks of computers infected with sophisticated malware that enables them to be controlled remotely and used, whether individually or in combination, for various malicious ends. Often containing tens or hundreds of thousands of computers, sophisticated botnets can be used to launch distributed denial of service attacks that can cripple a company's network. A number of major U.S. banks saw

15 The Framework Version 1.0 is available here: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. For an initial analysis, go to http://www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=10737423378. For a description of how the Framework fits into the larger list of cybersecurity initiatives undertaken in response to President Obama's February 2013 Executive Order on Critical Infrastructure Cybersecurity, see Cedarbaum and Schloss, Implementation of the Cybersecurity Executive Order and Presidential Policy Directive, Privacy and Security Law Reporter (Apr. 22, 2013), available at http://www.wilmerhale.com/uploadedFiles/WilmerHale_Shared_Content/Files/PDFs/cedarbaum-schloss-EOPPD-implementation.pdf.

16 See Office of the Comptroller of the Currency, Third Party Relationships: Risk Management Guidance, OCC Bulletin 2013-29 (Oct. 30, 2013), available at http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html; Consumer Financial Protection Bureau, Service Providers, CFPB Bulletin 2012-03 (Apr. 13, 2012), available at http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf; Letter from Roger Cole, Acting Director, Board of Governors of the Federal Reserve System to the Officer in Charge of Supervision, Appropriate Supervisory Staff at Each Federal Reserve Bank, and Banking Organizations Supervised by the Federal Reserve, FFIEC Information Security Booklet, SR 06-12 (July 28, 2006), available at http://www.federalreserve.gov/boarddocs/srletters/2006/SR0612.htm.

17 Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record of James R. Clapper, Director of National Intelligence, before the Senate Select Committee on Intelligence (Jan. 29, 2014) available at http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

this kind of attack in the fall of 2012 by groups linked to the government of Iran. Botnets can also be used to steal financial credentials, as was the case with Game Over Zeus botnet, which the FBI believes was used to steal more than $100 million dollars from hundreds of financial institutions around the globe.

Both the U.S. government and some companies have gone to the court to seek orders enabling them to disable the servers used to power botnets. The Justice Department has also used some of its criminal authorities, such as the prohibitions on bank fraud and wire fraud, as bases for court orders designed to take down botnets. Although a number of these actions have achieved success, government agencies have been reluctant to leverage this tool. That may be partly due to uncertainty about the legal basis, but it also seems to stem from an overarching cyber strategy that focuses less on combating specific attacks and more on collecting information to identify the ultimate masterminds behind an attack. Government agencies should shift their cyber strategy to one that more closely resembles their strategy for old-fashioned bank robberies, which would give greater attention to preventing ... robberies, or quickly disrupting them when they are in progress.

A small step in this direction is included in the package of legislative proposals offered by the Obama Administration, which contains a proposal designed to improve the situation for government actions. It would amend the federal criminal code to make clear that violations of the principal federal anti-hacking statute, the Computer Fraud and Abuse Act, can serve as the premise for injunctive orders as long as at least 100 computers were affected in a one-year period. The proposal is designed to ease efforts by government agencies to "disrupt or shut down botnets" and combat attacks against bank networks.

Increased action by the U.S. government in other areas is also particularly important. The recent proposal by Chinese government to require all banks in China to reveal source code in the IT products they use provides a powerful current example.

On Dec. 26, 2014, the Chinese Banking Regulatory Commission (CBRC) issued draft regulations setting out detailed security standards that IT products purchased by banks must meet in order to be considered "secure and controllable" for use by financial institutions in China. The draft regulations would apply to 68 categories of tech products, including servers, wireless routers, and ATMs. Source code powering operating systems, database software, and middleware must be registered with the CBRC to be considered "secure and controllable," while only wireless routers that have approved encryption or virtual private networking (VPN) certificates may receive the designation. The draft regulations also specify what percentage of new purchases in each product category in 2015 must be considered "secure and controllable." Every new PC purchased this year, must carry the designation.

Government agencies should shift their cyber strategy to one that more closely resembles their strategy for old fashioned bank robberies, which prioritizes combating robberies before or when they occur.

The biggest concern arising from the regulations is that they could be used to provide the Chinese government with a backdoor into bank networks. Having the source code provides a roadmap for hacking the "secure and controllable" devices. In the worst case, those devices will have back doors for nefarious activities already embedded in them and in such a way that could result in the activities being undetectable by banks.

The regulations would initially focus on types of hardware and software where domestic suppliers already have a strong market position compared with their foreign rivals. On Jan. 28 2015, more than a dozen U.S. business groups sent a letter to senior Chinese officials protesting the draft regulations and seeking dialogue to have them

reconsidered. Noting that these draft regulations targeting the financial sector follow a similar effort aimed at the telecom sector, the letter states: "Sovereign interest in a secure and development-friendly cyber economy is best served, in any country, by policies that encourage competition and customer choice, both of which necessitate openness to nonindigenous technologies, as well as close collaboration between industry and government in formal and informal public-private partnerships and other mechanisms."

U.S. officials have also criticized the regulations. U.S. Trade Representative Michael Froman said in a Feb. 27, 2015 statement that the regulations "go directly against a series of China's bilateral and multilateral trade commitments." The rules, he pointed out, "would require technology transfer and use of domestic Chinese intellectual property as a pre-condition for market access – both of which China has committed not to do." Froman pointed out that the rules are designed to protect and favor Chinese companies at the expense of foreign competitors, not to protect bank security, as advertised. "The administration is aggressively working to have China walk back from these troubling regulations," he said in the statement.

Information-Sharing and Collaboration Obstacles

If banks and the government each need to do more on their own, the most important area for improved cybersecurity is more effective collaboration between financial institutions and the government. Information-sharing provides the clearest example where improved collaboration can make an enormous difference.

The sharing of cyber threat information both within the private sector and between the private sector and the government is crucial for several reasons:

- It enables more comprehensive, faster understanding of the threat environment, which is important for companies in developing defensive strategies and diagnoses following a breach
- The government's national security and law enforcement resources have extensive international awareness, which banks may lack; this can be particularly important because foreign governments are involved in many cyber attacks and the biggest cyber-crime organizations are based overseas
- Because critical infrastructure is mostly in the private sector, the government needs information from the private sector in order to build up its understanding of the cyber threat environment and provide effective assistance

The rapid growth of a number of venues for information-sharing, most notably the Financial Services Information Sharing and Analysis Center (FS-ISAC), reflects both the private sector's and the government's recognition of the importance of cybersecurity information-sharing.

Yet, as Leo Taddeo, the special agent in charge of the FBI's cyber and special operations division, acknowledged at a recent conference, financial institutions often have concerns that constrain their willingness to share information. Firms worry about liability risk, regulatory exposure, and reputational harm. They fear the information will be improperly disclosed or used for other purposes.

These concerns should not be overstated. Information-sharing efforts are increasing at an incredibly rapid pace. But those efforts could be made even more effective if certain remaining obstacles were removed. A few examples illustrate the point:

The Right to Financial Privacy Act strictly limits the ability of financial institutions to share customer records with the government absent a subpoena or other process and notification to affected customers.[18] This can hinder information sharing by financial institutions with the FBI, the Secret Service, and other law enforcement agencies in the midst of an attack when, for example, government tools could be used to analyze a bank's systems to identity

18 *See* 12 U.S.C. § 3414.

and/or neutralize the attack. A grand jury subpoena may be used as a vehicle to permit such an analysis of a bank's systems, but securing a subpoena may cause delay when time is of the essence in the heat of an attack.

The Freedom of Information Act (FOIA) makes information shared with the government presumptively subject to public disclosure. Some shared information may be protected by an existing FOIA exemption. For example, the exception for "trade secrets and commercial or financial information" or for "records or information compiled for law enforcement purposes" may apply,[19] but each of these exceptions has specific requirements and only applies when relatively narrow circumstances are present. In order to be confident that information shared with the government for cybersecurity purposes is protected, a bank would have to engage in a specific FOIA analysis of each piece of shared information before sharing. Given the operational need to share information with the government rapidly in cybersecurity investigations, it is impractical to require that banks to conduct this in-depth prior analysis.

Under the Department of Homeland Security's Protected Critical Infrastructure Information program, financial institutions can share information with the federal government and receive certain protections, including protection against FOIA disclosure, loss of trade secret status, and privilege waiver.[20] In order to be protected, however, the information must be shared with the government through DHS (or a handful of other authorized agencies, which don't include critical agencies such as FBI, Secret Service and Treasury), and the information must be "accompanied by an express written statement" that makes rapid sharing, especially of digital information, difficult.[21]

One of the three main components of the cybersecurity legislative package announced by President Obama in January and the executive order he signed at the Stanford Cybersecurity Summit are designed to encourage more effective and extensive cybersecurity information-sharing, in part by addressing the private sector concerns noted above. They represent important efforts to improve cybersecurity information-sharing.

The Obama Administration's legislative proposal would provide both federal legal authorization that would preempt inconsistent state laws and liability protection for the sharing of cyber threat information. Those are very important steps in the right direction. But the proposal would appear to be limited in certain ways.

For instance, its protections would apply only to the sharing of "cyber threat indicators," which would be defined to require the sharing company to have made "reasonable efforts . . . to remove information that can be used to identify specific persons reasonably believed to be unrelated to cyber threat." The exact scope of information that "can be used to identify" individuals is not defined.

Also, authorization to share cyber threat information with the government "notwithstanding any other provision of law" would be given only for information shared with the National Cybersecurity and Communications Integration Center, a component of DHS, which in turn will be required to share the information with other agencies, including law enforcement and intelligence agencies. Authorization to share information directly with other federal agencies, including law enforcement agencies "for investigative purposes," would be given only "consistent with [the agency's] lawful authorities." Thus, it is not clear, for example, that the proposal would remedy the RFPA issue described above.

Despite the limitations of this proposal, and the inherent legal and regulatory complexities of cyber threat information-sharing, moving forward on this front is imperative to financial stability and national security. The challenge for banks and government is staying nimble within a law- and regulation-abiding world, as the cyber thieves and other adversaries collude outside those boundaries. ■

19 5 U.S.C. §§ 552(b)(4), 552(b)(7).

20 6 U.S.C. § 133(a)(1).

21 *Id.* § 133(a).