The Cyber Crime Wave:
What Bankers Need To Know

A Chris Swecker White Paper

November 2016

Sponsored by: VERAFIN A STEP AHEAD.

The Cyber Crime Wave: What Bankers Need To Know

A Chris Swecker White Paper

Cyber crime and cyber based economic espionage schemes have supplanted traditional bricks and mortar crimes as one of the most significant threats facing government, private industry and law enforcement. Within the private sector the Financial Services industry is arguably the most beleaguered, bearing the brunt of the full range of malicious cyber actors.

These include capable and well-resourced nation-states, such as China or Russia who desire a strategic capability to shut down our financial systems in the event of a conflict with the US; cyber terrorists who believe that attacking the financial system would have as much traumatizing impact on US citizens as a physical attack; and hacktivists, representing such movements as "Anonymous" or other issue driven actors who seek to undermine companies or industries that they do not favor. The most pervasive and imminent risk however is presented by global cyber criminal networks that target financial institutions and their customers inflicting billions of dollars in losses and reputational damage while garnering prodigious sums in illicit profits.

"The most pervasive and imminent risk however is presented by global cyber criminal networks that target financial institutions and their customers inflicting billions of dollars in losses and reputational damage while garnering prodigious sums in illicit profits."

Reliance on the Internet and web based delivery systems has spawned a financial crime industry that spans the globe and is unprecedented in its breadth and scope. E-Commerce has been a game changing benefit to the retail and financial industries and their customers. International criminal enterprises, however, have exploited a host of vulnerabilities inherent in modern day internet based bank products, channels and delivery systems to make cyber crimes the most pressing operational risk facing these industries. Consumers have been inundated with headlines bearing news of the latest data breach such that data protection has become a differentiator driving customer preferences.

Due to the nature of the cyber threats the foundation of an effective cyber risk management strategy transcends technical IT solutions such as firewalls, antivirus, proxy servers, encryption, multifactor authentication etc. First and foremost a culture of security, awareness and threat identification must be instilled from the top down. Most cyber intrusions start with basic social engineering exploits targeting key company employees with spear-phishing emails or luring them to visit infected websites. In fact studies have shown that the most common and successful method utilized by cyber thieves to gain access to the company's IT system is by way of a simple spear-phishing email with an attachment containing malicious code.[1] Recent studies by Intel suggest that 97% of people cannot identify phishing emails.[2] It is critical that every employee from the CEO to bank tellers must be an individual risk

1 Verizon *2016 Data Breach Investigations Report;* McAfee, *Hacking the Human Operating System, http://www.mcafee.com/us/resources/reports/rp-hacking-human-os.pdf*

2 http://securityaffairs.co/wordpress/36922/cyber-crime/study-phishing-emails-response.html

manager as they go about their daily duties. They must be aware and appreciate their role as the first line of defense. Investments in time and resources should be dedicated to education programs geared towards recognition of the latest spear-phishing schemes and how to avoid becoming the weak link that compromises the company's defenses. Finally, the company leadership should be open to collaborating across the financial services industry to gain the initiative from cyber criminals that prey across financial institutions as a deliberate tactic to avoid detection.

"Finally, the company leadership should be open to collaborating across the financial services industry to gain the initiative from cyber criminals that prey across financial institutions as a deliberate tactic to avoid detection."

As part of this distributed risk management strategy all bank employees must also have a mature understanding of the risk actors and their motivations, capabilities and methods. Russian cyber masterminds, many of whom are enabled by current and former intelligence operatives, have recreated in the virtual world the bricks and mortar black market that drove the criminal economies of the former USSR and its satellite states in Eastern Europe.

The dynamics of the cyber crime environment in the dark web is also important. Many compliance and risk professionals, but few rank and file employees, know that the virtual black market provides the forum for virtually all aspects of what has become the most profitable crime model in the world. This is the human face of what Europol describes as "Crime as a Service".[3] In its 2016 Internet Organized Crime Threat Assessment Europol stated: "the mature Crime-as-a-Service model underpinning modern day cybercrime continues to provide tools and services across the entire spectrum of cyber criminality, from entry-level to top-tier players, and any other seekers, including parties with other motivations such as terrorists." [4]

This crime model differs significantly from that employed by traditional criminal enterprises. Rather than concealing the tools, means and methods of facilitating the crimes, a virtual criminal network can operate anonymously from safe haven countries beyond the reach of US law enforcement to globally propagate the cyber crime wave. Cyber crimes, like everything on the internet has become a viral phenomenon as the criminal masterminds market and sell the latest zero day malware, botnets that distribute the malware, skimming devices and hacking tools of every description. Aspiring cyber criminals who wish to bypass the labor and skills associated with establishing their own criminal hacking capabilities can simply purchase stolen payment card data and rent or buy a franchise of money mules to "monetize" the data by cashing out on cloned credit or debit cards. They can buy enough information to take over online bank accounts or acquire stolen identity data and apply for a variety of credit such as mortgages, credit cards etc.

3 See Europol IOCTA 2016 Internet Organized Crime Threat Assessment: www.europol.europa.eu

4 Ibid

All of this activity serves to not only create a "wiki" crime environment but also generates huge volumes of noise in the financial system that blends in with legitimate transactions which effectively hinders the detection of criminal activity. It is almost the perfect crime model. Data is stolen, but unlike the theft of a tangible object, the data is still present in your system, thus delaying both detection and damage mitigation efforts.

Speaking of detection, banks rely on a system of rules, anomaly detection and predictive analysis to detect criminal fraud and money laundering. These singular event detection strategies however, provide minimal context concerning the relationship between fraud actors and their networked activities. Financial crime rings rely on data and process silos inherent within banks and between banks to avoid detection. Sophisticated social network analysis and industry level collaboration must be employed to combat these networks. Operating in a silo within your own company and across the financial services industry as a whole plays directly into the hands of malignant social networks.

Take for example the creator of the notorious Zeus virus. Evgeniy Bogachev is accused of running the Zeus attack network, thought to have infected more than one million computers. Victims were tricked into downloading malware, which then searched specifically for financial information. Like a wine vintner who produces limited reserve appellations for themselves and select distributors, Bogachev saved the most complex and customized viruses including the GameOver Zeus virus and Cryptolocker for his own criminal ring dubbed the "Business Club" who collaborated across the globe.

Bogachev used this more sophisticated malware in Botnets that, unlike the commercially available Zeus version sold to thousands of internet criminals on the dark web, handily evaded commercial antivirus software. Business Club members were strategically placed around Eurasia, working shifts across all 11 Russian time zones that followed the rising sun in a continuous virtual conspiracy fleecing thousands of victims for hundreds of millions in profits.[5] Business Club members included a virtual supply chain of fraud operators including 24/7 tech support technicians, third-party suppliers of ancillary malicious software, as well as those engaged in recruiting "money mules"— unwitting or willing accomplices who could be trained or counted on to help launder stolen funds.

Bogachev innovated two of the most insidious Internet fraud schemes in history, corporate account takeovers and ransomware. In corporate account takeover Internet thieves use a spear-phishing scheme to gain entry into the computer

> *"Aspiring cyber criminals who wish to bypass the labor and skills associated with establishing their own criminal hacking capabilities can simply purchase stolen payment card data and rent or buy a franchise of money mules to "monetize" the data by cashing out on cloned credit or debit cards. They can buy enough information to take over online bank accounts or acquire stolen identity data and apply for a variety of credit such as mortgages, credit cards etc."*

5 Fox-IT surfaced details of the "Business Club", a security firm based in the Netherlands that secretly gained access to a server used by one of the group's members and published many of their communications.

of an unsuspecting small to medium size business executive. Once inside his/her computer Business Club operatives worked laterally to gain control of the employee responsible for company payments. The *coup-de-grace* is delivered when the operatives sign on to the company's online banking site and create fictitious payees. In a matter of minutes they make a series of payments to these new payees, quickly draining the company's operating cash.

In the most feared scam making its rounds on the Internet, Business Club members gain entry to a company system to inject a form of malware called Cryptolocker, which locks up the company's most precious files and systems, demanding ransom to free the files and allow the company to resume operations. While many companies pay the ransom, about 40% of these companies never regain control of their precious data or IT system.[6]

In a sign of the times the FBI has announced an unprecedented three million dollar reward for the arrest of a cyber hacker. Nevertheless Bogachev hides in plain sight in a resort on the Black Sea. It's a stark example of the enabling posture of the governments of countries who host the most prolific thieves in world history and the challenges law enforcement face in attacking the global crime problem. The Russian government has shown no interest in acting on the Interpol "red notice" published on Bogachev or any other indicted Russian hackers.[7]

Ironically, it is not the deep technical aspects of data protection that present the greatest vulnerability, rather it is the human factor associated with both customer and employee behavior that presents the most successful avenues for criminals to breach the bank's defenses. By addressing these behaviors financial institutions can wring a significant amount of risk out of their business models. Banks that fail to address these vulnerabilities will remain the easiest targets.

For example, although Information Security professionals like to play up the sophisticated malware utilized by cyber thieves, simple spear-phishing is the preferred mode of compromise to gain entry into a bank's IT systems to actually install the malware. As the 2016 Europol report stated "While it is true that in some areas cybercriminals demonstrate a high degree of sophistication in the tools, tactics and processes they employ, many forms of attack work because of a lack of digital hygiene, a lack of security by design and a lack of user awareness."[8] This is even true with respect to the most sophisticated of cyber hackers working

> *"Financial crime rings rely on data and process silos inherent within banks and between banks to avoid detection. Sophisticated social network analysis and industry level collaboration must be employed to combat these networks. Operating in a silo within your own company and across the financial services industry as a whole plays directly into the hands of malignant social networks."*

6 Barkly: *Ransomware by the Numbers:* https://blog.barkly.com/ransomware-statistics-2016

7 A Red Notice is a request to locate and provisionally arrest an individual pending extradition. The General Secretariat at the request of a member country issues it or an international tribunal based on a valid national arrest warrant. It is not an international arrest warrant. INTERPOL cannot compel any member country to arrest an individual who is the subject of a Red Notice. Each member country decides for itself what legal value to give a Red Notice within their borders.

8 2016 Europol IOCTA Report: www.europol.europa.eu

on behalf of nation state sponsors such as China, Russia and terrorist countries such as North Korea and Iran. To quote innovator Jim Hansen, CEO of PhishMe, a successful cyber security company that addresses the human vulnerabilities associated with social engineering; "Organizations are always looking for the mythical silver bullet to solve all of their security woes, and security vendors are increasingly pointing to technology as the answer, ignoring the importance of the human element."

Cyber thieves are similar to most bricks and mortar thieves in one respect: they like to prey on the easy targets utilizing the least expensive and least resource intensive means possible. They utilize social engineering in many different ways to exploit human vulnerabilities to steal and monetize data or extort money from firms. Phishing, spear phishing, smishing[9], and other social engineering exploits have become ubiquitous. The criminals vacuum up all available information carelessly placed by their targets on various social media sites such as LinkedIn, Facebook, company websites etc. They will almost always target high profile executives with a well-crafted email that appears to be from a trusted source. This email will contain a link or attachment that inserts malicious data stealing code into the target's device that enables the thief to either harvest the desired data or a device such as a key logger.

Other schemes target call centers to socially engineer changes to a customer's account to enable cyber thieves to access the funds and effect withdrawals, payments or transfers to themselves or their money mule operatives.

The corrupt or sometimes just careless employee can be a financial institution's worst nightmare. Scams such as CEO fraud, account takeovers and ransomware rely on employees posting too much information on social media sites, careless handling of emails and an over reliance on technical defenses to be successful. Company policies ranging from BYOD and remote access policies concerning how employees can use the office network are important considerations.

Consumers are often targeted and need to be educated as well. They are often the targets of mass phishing and smishing[10] schemes. A barrier to raising customer awareness, however, is a general reluctance on the part of financial institutions to discuss even the possibility of fraud to their customers.

One often-overlooked human factor is the critical role of money mules. E-commerce crime schemes are heavily dependent on an "ant army" of co-conspirators who help "monetize" the stolen data such as credit/debit card

"The corrupt or sometimes just careless employee can be a financial institution's worst nightmare. Scams such as CEO fraud, account takeovers and ransomware rely on employees posting too much information on social media sites, careless handling of emails and an over reliance on technical defenses to be successful."

9 Smishing is a phishing exploit sent via a text message to a mobile device.

10 Smishing is using SMS text phishing messages to infiltrate a bank customer's mobile device in order to capture mobile banking information such as userids and passwords.

numbers and PIN/CVV codes, sensitive personally identifying information (PII), and the like. In FBI Operation Trident BreACH the FBI arrested over one hundred mules in one of the most revealing and successful cyber crime investigations to date. Bogachev's Zeus bot was a significant instrumentality of this crime. Zeus is a Trojan that allowed hackers to target small to medium-sized businesses, churches, municipalities, and individuals (corporate account takeover). The Trojan was transmitted to the victim in phishing email. Once installed, the Trojan harvested online banking usernames and passwords, which allowed the criminals to take over the bank accounts and steal funds. Stolen funds were routed to over 3500 mules that, in turn, moved the funds out of the country. A staggering 92 mules were indicted along with five Ukrainian masterminds. An additional dozen mules were indicted in the UK.

Almost all of the mules arrested or charged in this case were young Eastern Europeans who were either planning to travel to, or were already present in, the United States on J-1 student visas.[11] After entering the United States, the organizers provided the recruits fake foreign passports to open accounts at numerous local banks. After those accounts were opened, other actors in the group would transfer money from cybercrime victims into the mule accounts, typically in amounts close to $10,000. The mules would quickly withdraw the money, keep a portion for themselves (usually 8 to 10 percent) and transfer the remaining amount to other participants in the fraud scheme, usually individuals overseas. Some mules were asked to open a large number of bank accounts to help launder stolen funds through "funnel accounts" that consolidated stolen funds before transferring larger amounts to overseas accounts.

The money mules represent a rare Achilles heel for the global crime networks because they provide a physical presence in the US and other victim countries with which the US has cooperation and extradition treaties. In Trident Breach the FBI cooperated with their counterparts in the UK, the Netherlands, Ukraine and dozens of other countries to identify and eventually arrest members of the mule network. Many financial institutions have begun to track money mules and the data associated with them and use social network analysis to identify mule rings. Perhaps the most useful database in existence regarding money mules and their "herders" is the National Cyber Forensic Training Alliance (NCFTA) money mule database.[12] Financial Institutions can access this rich database by participating in the NCFTA, which is a "give data to get data" environment.

> *"Industry collaboration provides an opportunity to become proactive and actually hunt down these criminal actors, particularly the money mules who provide not only a physical presence but an opportunity to link people, addresses, contact details, accounts and the like. Section 314(b) of the USA PATRIOT Act provides a solid legal basis to share data between financial institutions."*

11 Mules also take advantage of the U.S. government's Visa Waiver Program (VWP) which is an international agreement between 38 countries. The U.S. State Department states that it currently allows citizens of participating countries to travel to the United States without a visa for stays of 90 days or less if they meet certain requirements. The VWP permits travel within the United States for purposes of tourism and certain business activities.

12 The NCFTA is a partnership between the FBI, Carnegie Mellon University and private sector companies including financial institutions to combat cyber crime by sharing information. The Cyber Financial (CYFIN) project focuses on cyber crime and cyber actors targeting the financial sector. The NCFTA has been based in Pittsburg since 2002 and has announced that new offices will be opened in Los Angeles and New York during fiscal year 2016.

As part of the "human factor" risk mitigation strategy, bank employees from the teller to the back office fraud detection and investigation specialists should know and be able to recognize mule behavior and tactics.

Industry collaboration provides an opportunity to become proactive and actually hunt down these criminal actors, particularly the money mules who provide not only a physical presence but an opportunity to link people, addresses, contact details, accounts and the like. Section 314(b) of the USA PATRIOT Act provides a solid legal basis to share data between financial institutions.[13] This provision, which includes a "safe harbor" from liability if used properly, is significantly underutilized. Since the greatest losses are inflicted by criminal organizations who collaborate to fleece banks in scams such as those invented and perpetrated by the Russian mastermind Bogachev, it is only logical that financial institutions themselves begin to collaborate to detect the full scope and breadth of their activities. We must begin to out-network the bad guys.

Despite the success law enforcement has achieved in cases such as Operation Trident BreACH, the best opportunity to truly combat cyber crime rings resides within the industry itself. Arrest and prosecution are helpful and desirable but law enforcement is handicapped by the viral and global nature of this crime paradigm. In designing and implementing risk mitigation strategies financial institutions must account for the greatest vulnerability of all: human behavior. An effective cyber defense system must go beyond technical solutions and account for these human vulnerabilities. Bank employees must be fully educated about the various means and methods bad guys utilize to socially engineer their way in to IT systems and gain access to sensitive data.

No bank employee should ever fall for a phishing scheme or be socially engineered to allow bad actors to access customer data and accounts. Bank customers are well aware of the existence of ecommerce scams and schemes and desire more protection. Concise well-delivered customer education campaigns are a vital part of a cyber risk mitigation strategy. Finally, financial institutions should exploit the Achilles heel of the cyber crime networks by using 314(b) of the USA PATRIOT Act to collaborate across the industry to identify money mule rings and choke this vital link in the criminal chain.

"Since the greatest losses are inflicted by criminal organizations who collaborate to fleece banks in scams such as those invented and perpetrated by the Russian mastermind Bogachev, it is only logical that financial institutions themselves begin to collaborate to detect the full scope and breadth of their activities. We must begin to out-network the bad guys."

13 See Swecker Verafin whitepaper entitled *Section 314(b): The Best Hope for Collaboration Between Financial Institutions to Combat the Movement of Illicit Proceeds* for a full discussion of the use of 314(b): http://verafin.com/resource/section-314b/

About the Author

Chris Swecker

Financial Crimes Consultant and Attorney; retired Assistant Director, FBI; and former Global Security Director, Bank of America

Chris Swecker has 30 years of experience in law enforcement, national security, legal, and corporate security/risk management. Swecker served 24 years with the Federal Bureau of Investigation (FBI) before retiring as Assistant Director of the FBI's Criminal Investigative Division. He was responsible for eight FBI divisions including Cyber, Criminal, International Operations, Training, Crisis Management, Operational Technology, Criminal Justice Information and the Law Enforcement Liaison office encompassing more than half of the FBI's total resources. Swecker also served as the FBI's On Scene Commander in Iraq in 2003 where he led a team of FBI Agents conducting counter-intelligence and terrorism investigations.

As head of the FBI's Criminal Division, Swecker led all FBI criminal investigations including public corruption, money laundering, organized crime/drug trafficking and financial crime matters. He was instrumental in the development of the FBI's post 9-11 strategies, leveraging criminal investigative resources to support counter terrorism/intelligence efforts. He led national task forces on corporate fraud, violent gangs, financial crimes, crimes against children, public corruption and organized crime and established the MS-13 National Gang Task Force and the National Gang Intelligence Center. Swecker has extensive experience in organized crime, money laundering and major drug trafficking investigations.

As Corporate Security Director for Bank of America, Swecker led investigations; physical security; international security; employment screening and executive protection. He executed a comprehensive transformation of all aspects of the security organization, emphasizing the use of advanced analytical software, security technology and fusion of open source, government and internal information to drive strategies to prevent fraud, privacy and security events.

Swecker received the prestigious Presidential Rank Award for his service in Iraq and as Special Agent in Charge of the NC Office. He has testified before Congress on topics such as identity theft, crimes against children, mortgage fraud, human trafficking, financial crimes, information privacy and data compromise, crimes on the Internet, drug trafficking and gangs. He has appeared as a guest on numerous media programs including CNN, CNBC, CTV, 60 Minutes, Good Morning America, C-SPAN's Washington Journal and others. He is a frequent public speaker on financial crimes, money laundering and cyber crimes.

About Verafin

Verafin is the leader in cloud-based, cross-institutional Fraud Detection and Anti-Money Laundering (FRAMLx) collaboration software with a customer base of 1500 financial institutions across North America. Its solution uses advanced cross-institutional, behavior-based analytics to help financial institutions stay a step ahead of numerous types of fraud as well as the BSA, USA PATRIOT Act, and FACTA compliance landscape, while allowing them to collaborate cross-institutionally.

Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Illinois Bankers Association, Massachusetts Bankers Association, CUNA Strategic Services, a preferred service provider of the Independent Community Bankers of America, and has industry endorsements in 44 states across the U.S.

Learn more

For more information on this topic, or how Verafin can help your institution stay a step ahead of financial crime, visit www.verafin.com/framlx, email info@verafin.com or call 866.781.8433.

To access Verafin's archive of webinars, white papers, success stories and other materials focusing on BSA/AML compliance and fraud detection topics relevant to financial institutions across the country, check out our online Resource Center at www.verafin.com