Taking a Byte Out of Cybercrime

by: Melissa E. Hathaway

Nations and corporations are embracing and quickly adopting information and communications technologies (ICT) to improve services, increase productivity, and decrease costs. Unfortunately, they have not as rapidly addressed the security measures needed to protect their growing enterprises and technological infrastructure. However, in the last few years a new conversation has emerged regarding cybersecurity, which takes on different meanings as it sits within the twin responsibilities of economic progress and national security. Cybersecurity is a means to enable social stability and promote digital democracy; a method by which to govern the Internet; and a process by which to secure critical infrastructure from cybercrime, cyberespionage, cyberterrorism and cyberwar. As nations and corporations recognize their dependence on ICT, policymakers must find the proper balance in protecting their investments without strangling future growth.

This paper provides a brief overview of the cybercrime problem and examines five case studies to demonstrate that, while national and international law enforcement authorities are working together to address cybercrime, with additional tools they could make even more progress going forward. Today's efforts are under-resourced and hampered by outdated laws. Nonetheless, by sharing actionable information and applying novel interpretations of the law, authorities around the globe are finding ways to address the cybersecurity problem. The recommendations that follow the case studies seek to build on the successes and lessons learned.

The Cybercrime Problem

Media headlines throughout 2011 have been rife with high profile cybercrime events, confirming that insecure computers are being infected every day. Criminals have shown that they can harness bits and bytes with precision to deliver spam, cast phishing attacks, facilitate click-fraud, and launch distributed denial of service (DDoS) attacks. The increasing frequency of these events in recent years and the scale of those affected have been alarming.

Some of the recent headlines include:

- <u>Egypt</u>: During the early days of the social uprising that ultimately lead to the ouster of President Hosni Mubarak, the Egyptian telecommunications authority received an order from the security services to shutdown Internet access. Eighty-eight percent of Egyptians lost access to the Internet during this episode.[1] Other states in the region

[1] Christopher Williams. "How Egypt shut down the Internet." The Telegraph. 28 January 2011. [http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html]

(e.g., Libya and Syria) implemented similar measures to try to maintain social stability as the “Arab spring” continued. While the acts of authoritarian regimes fighting for their political lives may seem extreme to many in the Western world, what these episodes demonstrate is that the very interconnectedness that people around the globe enjoy because of improvements in ICT can be swiftly denied, putting freedom of communications at risk.

- NASDAQ: The operator of the NASDAQ stock market said it found "suspicious files" on its United States based computer servers, and determined that hackers could have affected the functionality of one of its Internet-based client applications.[2] Investigators are considering a range of possible motives, including unlawful financial gain, theft of trade secrets and a national-security threat designed to damage the exchange.[3] Even if none of these results were achieved in this particular case, this episode demonstrates the types of risks to which our investment plans and money are exposed.

- Epsilon: Epsilon, one of the world’s largest marketing services firms, sends 40 billion emails annually on behalf of more than 2,500 clients. In March 2011, Epsilon determined that a subset of its clients' customer data were exposed by an unauthorized entry into Epsilon's email system. The information that was obtained was limited to email addresses and/or customer names, and represented approximately two percent of Epsilon’s customers, including Walgreens, Disney Destinations, Best Buy, and Citigroup.[4] Epsilon and law enforcement fear that even months down the road, customers could receive an email impersonating their bank or credit-card issuer that contains poisonous Web links. Once clicked, those links could install malicious code on their computers or try to trick consumers into divulging valuable information, such as credit card information or log-in data to their banks or social media accounts.[5] This episode demonstrates that personal credentials and privacy, which are routinely captured by businesses and marketing firms, remain at risk.

- RSA SecureID: In March 2011, RSA, the security division of EMC, informed its customers of a breach of its corporate network, which likely reduced the effectiveness of its SecureID two factor authentication token. Two months later, on May 21, 2011, these fears were confirmed when a leading U.S. defense contractor, Lockheed Martin, had its internal networks penetrated by hackers using duplicates of RSA's SecureID

[2] Jonathan Spicer. UPDATE 2-Hackers breach Nasdaq's computers. Reuters On line. 5 February 2011. [http://www.reuters.com/article/2011/02/05/nasdaq-hackers-idUSN0514862120110205]

[3] Devlin Barrett. “Hackers Penetrate Nasdaq Computers.” The Wall Street Journal. 5 February 2011. [http://online.wsj.com/article/SB10001424052748704709304576124502351634690.html]

[4] Epsilon. Public Statement by Epsilon. 1 April 2011.

[5] Ki Mae Heussner. Epsilon Email Breach: What You Should Know. ABC News Online. 4 April 2011. [http://abcnews.go.com/Technology/epsilon-email-breach/story?id=13291589]

tokens.[6] After this breach and several others resulting from the SecureID issue, RSA Security announced that it would replace tokens, upon customer request.[7] This episode demonstrated that even the most trusted, authenticated Internet transactions are at risk.

- Sony: Sony's PlayStation network was taken down on April 20, 2011. A forensics team investigated the scope of the breach and by May 2, 2011, it was reported that the breach affected an estimated 100 million people and spread to Sony's Online Entertainment division. In an effort to expose Sony's underlying vulnerabilities to a breach, the hacker group LulzSec released names, birth dates, addresses, emails, passwords, etc. of Sony's customers.[8] By the end of May 2011, Sony had spent $171 million closing the vulnerabilities on its network and informing its customers of their exposure.[9] This episode serves as an important reminder of the need to educate children of all ages about the risks attendant with providing personal information when participating in online gaming.

- Citigroup. In early June 2011, computer hackers breached Citigroup's network and accessed the names, account numbers and contact data of hundreds of thousands of bankcard holders in North America.[10] This may be the largest breach of a financial institution to date, arming criminals with victims' data. Like the NASDAQ episode, this breach is further evidence of the vulnerability of our financial system to cybercrime.

- Stuxnet. The Stuxnet worm that was used to shut down -- at least temporarily -- Iran's nuclear program, has been widely analyzed around the world. It targets control system vulnerabilities and its source code has been traded on the black market. Security officials worry that this worm, or others like it, will be used again to attack other critical infrastructures that rely on computers and have the same security flaws.[11] This episode demonstrates that hackers can use bits and bytes to attack critical infrastructure targets.

[6] Jeffrey Carr. "An Open Source Analysis Of The Lockheed Martin Network Breach." Digital Dao Blog. 31 May 2011. [http://jeffreycarr.blogspot.com/2011/05/open-source-analysis-of-lockheed-martin.html]

[7] http://www.wired.com/threatlevel/2011/06/rsa-replaces-securid-tokens/

[8] Andy Bloxham. "Sony hack: private details of million people posted online." The Telegraph. 3 June 2011. [http://www.telegraph.co.uk/technology/news/8553979/Sony-hack-private-details-of-million-people-posted-online.html]

[9] Robert Westervelt. "Sony breach timeline shows missteps." Security Bytes online. [http://itknowledgeexchange.techtarget.com/security-bytes/sony-breach-timeline-shows-missteps-says-security-firm/] 31 May 2011.

[10] Maria Aspan. "Regulators pressure banks after Citi data breach." Reuters. 9 June 2011. [http://news.yahoo.com/s/nm/20110609/bs_nm/us_citi]

[11] Stewart Meagher. "Stuxnet worm hits the black market." THINQ. 25 November 2010. [http://www.thinq.co.uk/2010/11/25/stuxnet-worm-hits-black-market/]

A recent report from the online payment company PayPal classifies the above examples into two categories: (1) those that exploit the security flaw in the computer and (2) those that exploit the user through social engineering (where user action is required).[12] While the news stories are alarming by themselves, the exponential growth of new malware being created is also notable. According to Cisco's Global Threat Report First Quarter 2011, web exploits are on the rise -- having increased 46% in the first quarter of 201 -- highlighting more than 105 thousand unique payloads or malware.[13]

In the wake of these breaches in cybersecurity, it is important to consider both how and why countries have allowed themselves to become so vulnerable. As discussed below, there are several reasons. First, our laws have not kept pace with rapid technology improvements and adoption. Second, many countries have underinvested in law enforcement capacity and most law enforcement establishments are unable to manage the volume of incidents as a result. Third, it appears that prosecutorial decisions for regular crime and cybercrime have different thresholds, thus compounding the situation. An example put forth by PayPal[14] and confirmed at a recent Seton Hall Cybersecurity Law conference[15] hypothesized that if a person steals a smart phone worth $500 and is identified and caught, he will likely be prosecuted. However, if an individual steals $20,000 of smart phones on-line and is identified and caught, it is questionable whether he or she will be arrested and prosecuted.

Dealing with cybercrime is not easy. Novel approaches are usually required to address incidents in this area. The following five case studies provide insights into unique uses of the law and partnerships that take a "byte" out of cybercrime. The cases range from local to global cooperation and demonstrate that private and public sectors and law enforcement officials around the globe are committed to ensuring safety and freedom from online threats. But the case studies also show the limitations that restrict the ability of law enforcement to stem the tide of this threat, and suggest solutions that policy makers should consider.

Multi-State Information Sharing and Analysis Center (MS-ISAC) vs. QAKBOT[16]

[12] Michael Barrett, Andy Steingruebl, and Bill Smith. PayPal Combatting Cybercrime: Principles, Policies, and Programs. April 2011.

[13] Cisco Systems Inc. Cisco Global Threat Report First Quarter 2011. April 2011.

[14] Michael Barrett, Andy Steingruebl, and Bill Smith. PayPal Combatting Cybercrime: Principles, Policies, and Programs. April 2011. Page 12.

[15] Seton Hall Law School Conference: Cybersecurity Law and Policy: Changing Paradigms and New Challenges, held in Newark, NJ. 8 June 2011.

[16] Interview with Will Pelgrin of MS-ISAC. 17 May 2011.

The MS-ISAC's Cyber Threat Intelligence Coordinating Group, which operates as a division of the Center for Internet Security, a nont-for-profit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, facilitates the development of situation awareness and identifies inter-relationships between physical and cyber security activities. It features numerous representatives from law enforcement organizations at the federal, state and local levels in the United States. These include: the Federal Bureau of Investigation (FBI), United States Secret Service (USSS), Department of Homeland Security (DHS), State Homeland Security Advisors, State Fusion Centers, the Department of Defense (DoD), the National Guard, New York State Office of Cybersecurity and representatives from the New York State Police. Although relatively new, this group already has been incredibly successful in breaking down the traditional barriers for true information sharing, taking raw intelligence on threats and making it actionable information.

For example, in April 2010 the FBI provided the MS-ISAC with a forensics image of a system that was part of a financial fraud investigation involving a local college. In conjunction with the New York State Office of Cybersecurity, the MS-ISAC analyzed the system for signs of malware. The resulting analysis revealed the system was infected with a multi-component worm/trojan malware called QAKBOT. QAKBOT made its initial appearance in May 2009 and is known to spread through network shares. It downloads additional malware, opens a "back door" on compromised computers allowing for remote access and logs keystrokes, all with the ultimate goal of stealing confidential information. The malware also contains root-kit functionality to allow it to hide its presence.

By analyzing the network traffic, the MS-ISAC was able to identify infected servers as well as highjacked usernames and passwords. With permission of the college, MS-ISAC shared these findings with the FBI and all of the other members of the MS-ISAC. Through this investigation and partnership with the FBI, the MS-ISAC was able to identify and notify 17 state governments infected with this malware. One of the notified states confirmed having approximately 4700 infected systems.

From one college to 50 states, this example of local-to-local learning identified tens of thousands of infected computers. In partnership and by sharing actionable information, MS-ISAC was able to disable the theft of credentials and denied the further invasion of privacy. In the wake of the Epsilon and Sony PlayStation breaches, where our personal information of thousands of consumers was exposed, it is likely that the MS-ISAC and its partners will face and hopefully tackle more crime rings aimed at exploiting the seams between local and national law enforcement efforts.

Microsoft vs. The Rustock Botnet

At its peak performance, the Rustock botnet sent out more than 44 billion spam messages a day including "fake Microsoft lottery scams and offers for fake-and potentially dangerous--prescription drugs."[17] According to Symantec, the security software firm, Rustock constituted the largest source of spam in the world with approximately 50% market share. Spam can be a money making business because those who send it get paid for every email address they send to.

Microsoft decided that the Rustock botnet, the largest generator of spam in the world, was causing an Internet nuisance because it was damaging Microsoft products as well as its reputation. Accordingly, Microsoft turned to the courts to address the issue. On March 16, 2011, U.S. Marshals accompanied employees of Microsoft's digital crimes unit into Internet hosting facilities in five U.S. cities.[18] Using a federal court order, they seized the command-and-control servers that were responsible for manipulating an estimated one million computers worldwide.

Microsoft was not alone in its efforts to take down the Rustock infrastructure. The effort required collaboration between "industry, academic researchers, law enforcement agencies and governments worldwide."[19] Microsoft worked with pharmaceutical company Pfizer, the network security provider FireEye Malware Intelligence Labs and security experts at the University of Washington, each of whom attested in court to the dangers posed by Rustock and the impact on the Internet community. Additionally, Microsoft also worked with the Dutch High Tech Crime Unit within the Netherlands Police Agency to help dismantle part of the command structure for the botnet operating outside of the United States. Microsoft also worked with China's Computer Emergency Response Team (CN-CERT) to block registrations of domains in China, a pro-active approach aimed at preventing the stand-up of future command and control servers.

However, Microsoft did not stop there. The Microsoft digital crimes unit continued to work with global Internet Service Providers (ISPs) and CERTs around the world to remediate the infections. As of early June 2011, nearly sixty days after the initial take down of the servers, Microsoft's international efforts had cleaned up approximately 60% of the infected infrastructure.[20]

[17] Richard Boscovich. "Taking Down Botnets: Microsoft and the Rustock Botnet." Microsoft Blog. 18 March 2011. [http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/02/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx]

[18] Bruce Sterling. Microsoft versus Rustock Botnet. Wired Magazine (online). 28 March 2011. [http://www.wired.come/beyond_the_behond/2011/03/microsoft-versus-rustock-botnet/]

[19] Bruce Sterling. Microsoft versus Rustock Botnet. Wired Magazine (online). 28 March 2011. [http://www.wired.come/beyond_the_behond/2011/03/microsoft-versus-rustock-botnet/]

[20] Interview with Jeff Williams, Microsoft Malware Protection Center. 14 June 2011, at the 23rd Annual FIRST Conference, Vienna, Austria.

Microsoft used the power of the law combined with its global network and presence and demonstrated that a multinational corporation can lead by example. Their efforts relied on multi-party private-public collaboration using legal and technical measures to arrange a coordinated takedown of cybercrime followed by a coordinated clean up of the infection.

FBI vs. The Coreflood Botnet

The Coreflood botnet was designed to record the keystrokes and Internet browsing activity of victims. It collected banking credentials and passwords intended for use by criminals to direct fraudulent wire transfers and rob victim's bank accounts. In a seminal case, U.S. District Judge Vanessa Bryant determined that "allowing Coreflood to continue running on the infected computers will cause a continuing and substantial injury to owners and users of the infected computers, exposing them to a loss of privacy and an increased risk of further computer intrusions."[21]

To target the Coreflood botnet, the FBI obtained multiple criminal seizure warrants to deactivate the existing Coreflood command and control servers. Simultaneously, a temporary restraining order was obtained, directing the defendants to stop engaging in fraud. The order also authorized the U.S. Marshals Service, with the assistance of the FBI, to operate and respond with "stop" commands to infected computers as a substitute command and control server. This approach provided the FBI with time to identify and notify as many of the 2.4 million infected victims as possible of the fraudulent activity and their role in the scheme. By holding the botnet static, anti-virus vendors were able to develop solutions for detecting and removing the Coreflood virus before a new variant was released. These activities collectively, reduced the botnet by approximately 80% domestically and 45% internationally.

The Executive Assistant Director of the FBI's Criminal, Cyber, Response and Services Branch, Shawn Henry, stated that "these actions to mitigate the threat posed by the Coreflood botnet are the first of their kind in the United States and reflect our commitment to being creative and proactive in making the Internet more secure."[22] The joint operation to take down Coreflood involved information sharing between the U.S. Marshals Service and the FBI's regional offices located in New Haven, Connecticut; Dallas, Texas; Richmond, Virginia; Atlanta, Georgia; Cincinnati, Ohio; Phoenix, Arizona; Los Angeles, California; and Newark, New Jersey. It also benefited from international participation by the Estonian National Police. This unique cooperative effort across state lines and international borders used a legal framework that may pave the way for future botnet mitigations by the FBI.

[21] Kim Zetter. "U.S. Wins Court Order to Seize Control of 'Coreflood' Botnet, send kill Signal." Wired Magazine Online. 13 April 2011. [http://www.wired.com/threatlevel/author/kimzetter/]

[22] Federal Bureau of Investigation Press Release, 12 April 2011.

The National Cyber Forensic and Training Alliance (NCFTA) vs. Pump and Dump Scam

NCFTA is a non-profit corporation with a mission of facilitating collaboration between private industry, academia, and law enforcement to identify, mitigate and neutralize complex cyber related threats. In addition to its state and local law enforcement and industry representatives, it enjoys international representation from Canada, Australia, England, India, Germany, the Netherlands, Ukraine, and Lithuania. It provides streamlined and timely exchange of intelligence (cyber threat data) to corporations.

In 2006, NCFTA began an exchange of information on pump-and-dump scams that were pillaging some investment brokerages. These scams involved using compromised account credentials to artificially inflate the price of a stock by purchasing or influencing the purchase of large quantities of a stock and selling that stock at an artificially inflated high price. NCFTA served as the focal point for sharing actionable information related to malware, botnets being utilized, commodities that were being targeted, and other technical information surrounding the criminal behavior. The NCFTA partnered with the FBI, Federal Trade Commission (FTC) and the Securities and Exchange Commission (SEC) to quickly share information related to this fraud trend.

In February 2009, federal agents executed six search warrants at five locations throughout the United States. Ultimately, the FBI found that initial loss estimates were low; as further warrants were executed, the government found that criminals had manipulated or attempted to manipulate approximately 290 stock symbols resulting in millions more in estimated losses. As a direct result of this collaborative effort, five people pled guilty to mail fraud, wire fraud, and CAN-SPAM Act violations for running an international stock spamming operation that forwarded billions of illegal e-mail advertisements to inflate Chinese 'penny' stocks; then reaped substantial profits by trading away these same stocks while others bought them at inflated prices.[23]

In the wake of the NASDAQ breach, the NCFTA may be called upon again to focus efforts to ensure that NASDAQ doesn't experience fraudulent activity. NCFTA's focus on the black market infrastructure that supports cyber threats and crimes, including botnets, hosting companies, malware, money laundering, and shipment/money mule recruitment takes on even more importance as the private sector is suffering more and more breaches that harvest personal credentials and passwords to gain access to financial institutions.

INTERPOL and ICANN, Partnering for Internet Security.

[23] Interview with Ron Plesco, CEO of the National Cyber Forensic and Training Alliance. 5 June 2011.

The International Criminal Police Organization (INTERPOL) performs a significant amount of behind-the-scenes work and facilitates law enforcement cooperation in cyber matters by leveraging its worldwide network of law enforcement officials, agencies, partners, and technology. With 188 member countries, INTERPOL is the second largest intergovernmental organization after the United Nations. On internet security matters, INTERPOL is partnering with the Internet Corporation for Assigned Names and Numbers (ICANN), the non-profit corporation responsible for the global coordination of domain names and Internet protocol addresses.

These two politically neutral, global entities are partnering to enhance common means for preventing and addressing Internet crime. Secretary General Noble recently noted, “the Internet has no borders, and neither do the criminals who exploit it. As the Internet's role in society continues to increase in scope and importance, it is vital for INTERPOL to help create bridges between the international law enforcement community it represents and ICANN in order to advance Internet security practices for the benefit to all.”[24] For example, a secure worldwide communications network, known as I 24/7, that enables INTERPOL’s members to access each other’s national databases to facilitate law enforcement information sharing, is one such bridge that can be used to establish situation awareness and information sharing on particular Internet issues (e.g., hijacking border-gateway protocols or exploitation of the Domain Name System (DNS) registries).

This network could be further enhanced by INTERPOL’s initiative to merge the domains of cyber security, digital forensics, cybercrime investigations and information security into one global cybersecurity focused function. As INTERPOL joins ICANN’s Governmental Advisory Committee as an observer -- coupled with its active membership of the information security committee of the International Standards Organization (ISO), where it helps drive global cybersecurity standards for the law enforcement community -- INTERPOL may be able to enhance local law enforcement efforts and drive down the time from incident detection to interdiction and prosecution. While there are not yet any published reports of joint operations from these organizations, this international partnership demonstrates INTERPOL and ICANN’s commitment to leverage their collective access and global reach to amplify their common goals--to improve the safety and stability of the Internet of the future.

Proposals to Take More “Bytes” Out of Cybercrime

All of these case studies serve to remind us of the importance of cooperation in cyberspace. Individually, law enforcement agencies will never be able to defeat the clever tactics and agile criminal infrastructures behind the episodes described above.

[24] Press Release / Communiqué de Presse - INTERPOL and ICANN advance cooperation on Internet security. 23 May 2011.

Each example shows that by sharing actionable information across borders and across jurisdictions, and using novel approaches and applications of the law, progress can be made in reducing cybercrime. These few examples can be the blue-print for local entities and global institutions to follow. Individual states must recognize that success against international cybercrime will be achieved only if they are willing to commit more to the law enforcement communities and update the laws governing cyberspace and cybercrime. .

If the United States is going to invest in the capabilities and changes required to make a difference in the coming years, following are some of the steps that policy makers should consider taking to better position law enforcement to continuing taking "bytes" out of cybercrime:

1. **Update the Law**. Modern day criminals are using the legal system's speed, or lack thereof, to their advantage. Fraudulent and criminal activities are happening at unprecedented rates and the legal system cannot keep up with the volume. The Electronic Communications and Privacy Act (ECPA) does not provide adequate guidance, flexibility, or privacy protections for the national security community charged with protecting the nation and its critical infrastructure from cyber exploitation or attack. There are different legal standards for access to the data, some requiring subpoena, warrant, or national security letter. These need to be streamlined in such a way to allow for the speed of pursuit of cyber criminals. The Stored Communications Act (SCA) maintains a distinction between stored and transit data that may no longer be relevant given the new technology environment and convergence of managed security service providers with the infrastructure as a service provider (e.g., secure data center hosts). Because courts are increasingly denying government requests for retrospective geo-location data without a warrant (citing the SCA), statutory amendments must include the authority for the national security community to access this information. This will be particularly important as more and more data is stored in the "cloud" by third party providers. Finally, the Computer Fraud and Abuse Act (CFAA) should also be updated to specify that hacking is illegal, regardless of domain, and that the scope of the damage done determines the severity of the penalties, not the location, path taken or victim. IStiffer penalties against cyber criminals should be the first step of a deterrence strategy.

2. **Increase Capacity for Law Enforcement**. Policy makers need to build more capacity within federal law enforcement activities and prioritize cybercrime, counter-intelligence and intellectual property theft as the top initiatives. The FBI is the lead agency responsible for the National Cyber Investigative Joint Task Force (NCIJTF). It is responsible for correlating incidents and connecting the dots of criminal and counter-intelligence activities.

    a. The FBI and NCIJTF need technology modernization for data correlation and domestic threat correlation and better communications infrastructure to tip/queue systems and inform state and local officials. The FBI should consider establishing a complimentary task force located in Silicon Valley focused on the cyber espionage and theft of intellectual property from ICT (hardware and software) companies.

b. The Coreflood botnet example demonstrates that the FBI can realize important successes by embedding personnel with other law enforcement entities to enable swift cross-jurisdictional and country investigations. Currently, the FBI has personnel located in Colombia, the Netherlands, Estonia, Romania, and Ukraine. The FBI should resource and deploy more personnel in a broader representation of countries and -- at the very least -- station personnel in Russia and China. Having cyber-trained personnel in multiple countries noted as havens for cybercrime may lead to quicker takedowns. Having cyber-trained agents in multi-lateral organizations of INTERPOL and EUROPOL, and domestically in the Internet Cyber Complaint Center, will lead to broader situation awareness and unique channels of information sharing.

c. Finally, government needs to increase the private sector's awareness about threats to its cyber infrastructure. A training program that educates corporate leadership on how to mitigate the risk of being a high value target -- including providing them with briefings about the threat to their industry using specific case studies -- may go a long way to reducing the number of incidents and loss of confidential information.

3. **Fortify the NCFTA**. The NCFTA is reliant upon industry partnerships and industry rotational assignments. And while NCFTA is focused on the crimes against industry, it may need to turn to the broader law enforcement community to find incentives to stabilize the rotation of industry experts in and out of the center. Industry may also benefit from championing the establishment of a complimentary NCFTA activity on the West Coast. ICT companies are facing cyber espionage and theft of intellectual property just as the financial services sector is facing cybercrime and theft of money. A second facility that focuses on the specific issues of Silicon Valley may help cross-correlate common exploitation paths and help the ICT industry as a whole develop a stronger defensive posture.

4. **Use and Enforce the Authorities of FTC**. The FTC has the unique ability to investigate and prosecute firms that do not adequately secure consumer information. The FTC's enforcement authority stems from Section 5 of the FTC Act, which declares unlawful all "unfair or deceptive acts or practices in or affecting commerce."[25] Given the number of breaches that have occurred in 2011 alone, the FTC has the opportunity to enforce its authorities and bring actions against companies for failing to safeguard consumer data.

[25] 15 U.S.C. § 45(a).

5. **Inform the Courts of the Threat**. The Department of Justice and the FBI have the responsibility to inform judges and other legal officials of the threat posed to society delivered via information communications technology and the Internet. Furthermore, judges and other officials would benefit from technical training regarding the ease of technology exploitation coupled with anonymity of the attacker. This enhanced focus on awareness-raising and technical training may lead to broader application of administrative warrants, faster pursuit of online criminals, and equal thresholds imposed for online and physical crimes that are similar in kind.

The cybercrime problem will not solve itself. The litany of headlines announcing episode after episode of breaches, hacks and exploitations will continue unless local, national and international law enforcement authorities are provided the means and tools to work together to tackle the problem. The case studies summarized in this paper provide insight into how cooperation among law enforcement authorities can achieve targeted successes. The recommendations to update laws, increase resources, expand industry partnerships and apply all available authorities to build upon the successes described in these case studies are necessary to take the effort to the next level, where law enforcement can take more “bytes” out of cybercrime.