VIRGINIA JOURNAL OF LAW & TECHNOLOGY

SPRING 2012 UNIVERSITY OF VIRGINIA VOL. 17, NO. 01

Virtual Crimes, Real Damages Part II: *What Businesses Can Do Today to Protect Themselves from Cybercrime, and What Public-Private Partnerships are Attempting to Achieve for the Nation of Tomorrow*

FERNANDO M. PINGUELO, WAYNE LEE AND BRADFORD W. MULLER[†]

[†] Fernando M. Pinguelo, a Partner at Norris McLaughlin & Marcus, P.A. and Chair of its Cyber Security and Data Protection Group, is a United States-based trial lawyer who devotes his practice to complex business lawsuits with an emphasis on how technology impacts disputes. He has lectured internationally and written dozens of articles on the topic, and appeared on television as a legal commentator on various high-profile cases. He works closely with business owners and executives to develop strategies to manage business and legal issues related to electronic documents. As an adjunct law professor at Seton Hall University School of Law, Mr. Pinguelo developed and teaches a state-of-the-art course on Electronic Discovery (eDiscovery) and how technology impacts lawsuits. The U.S. Fulbright Program designated Mr. Pinguelo a Fulbright Specialist for his work in eDiscovery. Mr. Pinguelo also founded and contributes to the *ABA Journal* award-winning blog, eLessons Learned. To learn more about Mr. Pinguelo, visit www.CyberJurist.com or email him at info@CyberJurist.com. Mr. Pinguelo would like to acknowledge the research efforts of Zach Arbeitel that helped contribute to this article.

Wayne Lee is the Managing Principal of eDiscovery for the investigative response unit at Verizon Business Security Services, a provider of information security services for global businesses. He has more than fourteen years of experience in data security and litigation support. Mr. Lee has combined his extensive experience with leading edge technologies and strict discipline in delivery methodologies to engage eDiscovery legal matters for clients. In the past, he has assisted dozens of clients through large electronically stored information (ESI) projects with multifaceted electronic discovery requirements. Mr. Lee is also a senior forensic examiner, having taken the lead in many high-profile data breach investigations around the world involving fraudulent payment cards, internal corporate security incidents and online security compromises. He has worked closely with the United States Secret Service, the Federal Bureau of Investigation, and the Royal Canadian Mounted Police.

Bradford W. Muller, an Associate at Norris McLaughlin & Marcus, P.A. and member of its Litigation and Internet Law groups, is a graduate of Seton Hall University School of Law, *magna cum laude*, where he was a Comments Editor on the *Seton Hall Law Review*. Prior to his current position, Mr. Muller was a Judicial Law Clerk to the Honorable Anthony J. Parrillo, New Jersey Superior Court, Appellate Division. Mr. Muller has been a panelist at cybercrime-focused events held at The Masters Conference in Washington D.C., the University of Virginia School of Law, and Seton Hall Law; and has authored numerous articles on how technology impacts the law and business.

ABSTRACT

In their first piece, *Virtual Crimes, Real Damages: A Primer on Cybercrime In the United States and Efforts to Combat Cybercriminals*, Pinguelo and Muller offered a straight-forward discussion of the major forms of cybercrimes affecting the government and business community today, along with a review of federal efforts to combat cybercrime and a compilation of federal and state cyber-related statutes and pending legislation. In this follow-up piece, the authors are joined by a distinguished cybersecurity specialist, Wayne Lee, who provides a discussion of measures that businesses can implement immediately to secure their data and improve defenses against a data breach. Pinguelo and Muller also analyze the various public-private partnerships on cyber-defense currently at work in the United States, and explain how those partnerships are helping create a safer cyber-future.

TABLE OF CONTENTS

I. Introduction 76
II. Prevention Measures: A Technology Expert's Take on Cybercriminals, and Key Procedures That Can Be Implemented By Businesses to Improve Their Cybersecurity 80
A. Measures That Businesses Can Immediately Implement to Enhance Their Cybersecurity 82
III. Public-Private Partnerships: Government and Business Working Together for a Safer Future 85
A. Department of Homeland Security's Project 12 86
B. Electronic Crimes Task Forces and Working Groups 86
C. National Cyber-Forensics & Training Alliance (NCFTA) 87
D. InfraGard 88
IV. Conclusion: Moving Forward Together 88

I. INTRODUCTION

"You have learnt something. That always feels at first as if you had lost something."[1] What we as practitioners find most helpful when counseling clients on

[1] GEORGE BERNARD SHAW, MAJOR BARBARA 128 (Penguin Books 1957) (1907). With strong conviction, the character Andrew Undershaft in George Bernard Shaw's *Major Barbara*, affirms: "You have learnt something. That always feels at first as if you had lost something." *Barbara* begins with a look into the Undershaft's family financial troubles. The Undershafts soon turn to their father, Andrew Undershaft, a major leader in arms manufacturing, to resolve their fiscal quandary. His daughter, Barbara, who works with the Salvation Army, objects to her father's successful business because of its propensity to

cybersecurity issues is to address some of the most basic aspects of these concepts in the hopes that once the basics resonate, we can then enhance their understanding with a deeper review of the issues and a comprehensive plan designed to integrate both technological and human resources to create the solution for their business. That was our intent in our article *Virtual Crimes, Real Damages: A Primer on Cybercrime In the United States and Efforts to Combat Cybercriminals*,[2] where we offered a straight-forward discussion of the major forms of cybercrimes affecting the government and business community today, along with a review of federal efforts to combat cybercrime and a compilation of federal and state cyber-related statutes.

In the year that followed the article's publishing, the cyber-world has continued to march forward, becoming ever more dangerous and complex. Whether it be the Federal Trade Commission (FTC) accusing social media giant Facebook of deceiving consumers regarding their privacy protections,[3] or the data breach at South Korea's SK Communications which resulted in the personal information of 35 million Nate and CyWorld social network users being compromised,[4] the rise of "Child Identity Theft,"[5] or the "Anonymous" hacking group successfully disrupting the websites of the U.S. Department of Justice and Federal Bureau of Investigation (FBI),[6] we continue to be bombarded by news about the growing dangers presented by the Internet.[7] Cybercrime has grown so pervasive in the thoughts of Americans that even when cybercrime is not the cause of online troubles, such as when Wikipedia implemented a one day voluntary

engender violence and war, and because of her experiences with and commitment to the Salvation Army's mission. Throughout the play, Major Barbara struggles to come to terms with her father's business as he attempts to win her favor by making a sizeable donation to the Salvation Army. Towards the end of the play, Barbara and the rest of the Undershaft family visit her father's factory and soon recognize the importance of their father's business and that it is not so easy to label it a destroyer of peace.

Often, a result of gaining a new perspective involves an initial misunderstanding. The crisis of feeling that Undershaft's daughter, Major Barbara, experiences can be attributed to her realization that her father is perfectly willing to sell his dynamite for peaceful purposes or for the eradication of injustice even if humanity is unsure of how to properly use it. Despite her initial dislike for her father, Major Barbara by the end of the play acknowledges how vital her father's business is to the survival of their community. *See* John Gassner, *Bernard Shaw and the Making of the Modern Mind*, 23 COLLEGE ENGLISH 517, 517–25 (1962).

[2] 16 VA. J.L. & TECH. 116 (2011).

[3] Cecilia Kang, *Facebook settles privacy complaint, agrees to ask permission for privacy changes*, WASH. POST, BLOG Nov. 29, 2011, http://www.washingtonpost.com/blogs/post-tech/post/facebook-settles-ftc-privacy-complaint-agrees-to-ask-user-permission-when-making-privacy-changes/2011/11/29/gIQAw8k68N_blog.html.

[4] Liam Tung, *Anatomy of a Cunning APT: The SK Communications Breach*, CSO ONLINE, Sept. 29, 2011, http://www.cso.com.au/article/402450/anatomy_cunning_apt_sk_communications_breach.

[5] A recent study found that 10.2 percent of the child participants had been the victims of identity theft, which represents a fifty-one percent higher attack rate than that witnessed in adult participants. RICHARD POWER, CHILD IDENTITY THEFT: NEW EVIDENCE INDICATES THIEVES ARE TARGETING CHILDREN FOR UNUSED SOCIAL SECURITY NUMBERS 9–10 (2011), *available at* http://www.cylab.cmu.edu/files/pdfs/reports/2011/child-identity-theft.pdf.

[6] *Anonymous Strikes Back After Feds Shut Piracy Hub Megaupload*, CNN.COM, Jan. 20, 2012, http://edition.cnn.com/2012/01/19/business/megaupload-shutdown/index.html.

[7] However, the constant tidal wave of technology is, every now and then, placed in check. For example, in a recent opinion, the United States Supreme Court ruled that warrantless "GPS" tracking is unconstitutional. United States v. Jones, 565 U.S. ___, No. 10–1259, 2012 WL 171117 (Jan. 23, 2012).

black-out in protest of pending federal anti-piracy legislation,[8] many people simply assume that hackers are to blame.

In "reply" to our original piece, Professor Jonathan J. Rusch[9] drafted an article titled *Foreground and Background in Cybercrime: A Reply to Pinguelo and Muller*,[10] whereby he expanded upon the discussion presented in *Virtual Crimes*, *Real Damages*, in part by calling for a "global response to cybercrime." The depth and breadth of Professor Rusch's knowledge is evident in his writing, and he adds an important voice to the conversation. However, for the Chief Information Officer and General Counsel advising their Board of Directors as to immediate steps that their company can implement in order to reduce its vulnerability to a cyber attack, there is simply no time to wait for a "global" approach.[11] Business leaders need advice on how to proceed in the current environment—a dangerous world where the cyber-threat continues to grow despite the best efforts of the United States government and private industry.[12]

It is with these pressing concerns in mind that we offer this second piece. We have brought into the discussion Wayne Lee, Managing Principal in eDiscovery and

[8] Sarah McBride & Jasmin Melvin, *Pockets of Internet go dark to protest piracy bills*, REUTERS, Jan. 18, 2012, http://www.reuters.com/article/2012/01/18/us-internet-protest-idUSTRE80H01U20120118. It is also worth noting that the federal anti-piracy legislation that Wikipedia was responding to is, at the least, very troubling:

> Bottom line: This legislation would chill the free flow of expression of ideas on the Internet simply because it creates greater liability and exposure for websites and others . . . While average users may not initially feel the pain, they certainly will in the long run as information exchange reduces due to the threat of exposure to lawsuits and related concerns.

Mark Clayton, *Would SOPA and PIPA Bills 'Break Internet?' Anti-piracy Measure Being Revised*, THE CHRISTIAN SCIENCE MONITOR, Jan. 18, 2012 (quoting co-author Fernando M. Pinguelo), *available at* http://www.csmonitor.com/USA/Politics/2012/0118/Would-SOPA-and-PIPA-bills-break-Internet-Anti-piracy-measure-being-revised.

[9] Professor Rusch is Deputy Chief for Strategy and Policy, Fraud Section, Criminal Division, United States Department of Justice, and also a Lecturer in Law at the University of Virginia Law School, and Adjunct Professor at Georgetown University Law Center.

[10] 16 VA. J.L. & TECH. 361 (2011).

[11] Besides the detriment that cyber attacks can have on a company's bottom-line through expensive recovery costs, loss of valuable information, and bad press, data breaches expose the company to potentially expensive civil lawsuits. *See* Sarah Romanosky, David A. Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation* (Feb. 19, 2012), http://ssrn.com/abstract=1986461. However, the viability of this type of civil suit, where often the damages alleged are "future" in nature, remains a fluid topic. *See* Reilly v. Ceridian Corp., No. 11- 1738, 2011 WL 6144191 (3d Cir. Dec. 12, 2011) (finding that two law firm employees whose financial data was hacked lacked standing to sue the payroll-processing company who plaintiffs alleged allowed the breach, since there was no evidence that the stolen data had been or would be used, and the injuries alleged were too speculative).

[12] *See* Frank Gonnello, Jr., *IAPP Global Privacy Summit – Day 2 Recap*, ELESSONS LEARNED, Mar. 9, 2012 (quoting renowned cyber lawyer Renato Opice Blum who underscores the importance of understanding "'the most recent dilemmas facing privacy and cyber practitioners, [and being] active in this space [so as to] deal with complex issues in an uncertain legal environment.'"), http://ellblog.com/?p=2864.

Investigative Response for Verizon Business.[13] In Part II, Mr. Lee will address specific types of behavioral characteristics of persons and enterprises that commit cybercrime, explore examples of prevention measures necessary to reduce the effects of cybercrime, and provide a practical discussion of best practices that companies of all sizes can implement to bolster their defense against cyber-attack.[14] As Professor Rusch's article illustrates, a single company's attempt at creating a "security culture" within its ranks is not enough to solve the cybercrime problem on a macro-scale. However, for that particular company, following the sage advice of an industry professional such as Mr. Lee can be the difference between its survival and demise.[15]

In Part III, we return to a conversation of what is occurring, at the governmental level, to address the risks to the American economy and national defense posed by cybercrime.[16] However, we shift the focus to public-private partnerships that are in effect

[13] Verizon Business is a well-known player in the cybersecurity industry and has been a part of the remediation teams for several large-scale cyber-attack incidents, including its recent work conducting a forensic review of the attacks against Stratfor, a global intelligence analysis firm whose website was temporarily disabled as hackers stole personal information belonging to thousands of the company's customers. *See, e.g.*, Cassandra Vinograd, *Stratfor back online after cyberhack*, ASSOCIATED PRESS, Jan. 11, 2012, http://www.google.com/hostednews/ap/article/ALeqM5gBn0_Wo99U_glnkcFX_9JnG8MC6Q?docId=6b9114fdea4b4aa3aa6b13fc262d8cb3. Each year, the Verizon RISK Team, in cooperation with the U.S. Secret Service and Dutch High Tech Crime Unit, issues its "Data Breach Investigations Report," which provides a comprehensive study of the past year in data breach news, threat agents, and threat actions. *See* Wade Baker, et. al, Verizon RISK Team, 2011 DATA BREACH INVESTIGATIONS REPORT (2011), *available at* http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf. According to the 2011 report, 2010 was an anomalous year, in that, when studying the combined caseload of Verizon and the U.S. Secret Service, the "all-time lowest amount of data loss occurred in the same year as the all-time highest amount of incidents investigated." *Id.* at 2. Verizon's forthcoming 2012 report will focus attention on the unique cyber challenges posed by "hacktivism," a topic discussed in more detail later in this article. *See also* Mark Clayton, *Bradley Manning: Will the alleged WikiLeaks ally have a compelling defense?* CHRISTIAN SCIENCE MONITOR, Feb. 23, 2012 (quoting co-author Fernando M. Pinguelo: "'This is the first case that highlights the concept of hacktivists, really bringing to light organizations like Anonymous and their drive to expose things for what they are – not money-driven, but ideology-driven.'"), *available at* http://www.csmonitor.com/USA/Justice/2012/0223/Bradley-Manning-Will-the-alleged-WikiLeaks-ally-have-a-compelling-defense.

[14] Indeed, some of the best advice is that which, at first glance, appears obvious, but which many companies fail to implement, such as "basic security measures as simple as performing background checks on employees and limiting their access to highly sensitive information . . . ." Mark Clayton, *Bradley Manning case signals US vulnerability to 'insider' cyberattack*, THE CHRISTIAN SCIENCE MONITOR, Dec. 22, 2011 (quoting co-author Fernando Pinguelo), *available at* http://www.csmonitor.com/USA/2011/1222/Bradley-Manning-case-signals-US-vulnerability-to-insider-cyberattack.

[15] Life and death being an appropriate comparison because, as we all know, "corporations are people, my friend." James Oliphant, *Romney in Iowa: 'Corporations are People' Too*, L.A. TIMES, Aug. 11, 2011, *available at* http://articles.latimes.com/2011/aug/11/news/la-pn-romney-state-fair-20110811. Further, hacking incidents have the potential not only to poison a victim-company's customers against it, but also investors, especially in light of the Securities Exchange Commission's (SEC) recent guidance which now requires that a company's cybersecurity-related risks and costs be disclosed in their SEC filings. U.S. Securities and Exchange Comm'n, Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 Cybersecurity (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[16] The Obama Administration continues to take a proactive approach to cybersecurity issues, as evident by its recent release of a "Bill of Rights" for Internet users. *See* THE WHITE HOUSE, *Consumer Data*

today to systemically improve cyber-defense. Our hope is that these joint efforts between government and business will expedite the creation of a cybercrime-resistant nation and economy.

II. Prevention Measures: A Technology Expert's Take on Cybercriminals, and Key Procedures That Can Be Implemented By Businesses to Improve Their Cybersecurity

Before delving into specific measures that can be employed by a company to better protect itself from a cyber attack, it is useful to first briefly discuss who "cybercriminals" are, as only then can we understand what motivates them. There are generally three categories of individuals who commit, or are accessories to, cybercrimes: persons who have malicious intent, persons who are "morally flexible," and persons who are unwitting patsies.[17] There will always be a population of people who act deliberately and maliciously for financial gain, for ideological reasons (*i.e.*, "hacktivism"), or for bragging rights. In each of these cases, there is a self-serving purpose behind the individual's actions.

Criminal enterprises like the Russian Business Network[18] and others flourish in a target rich environment. These enterprises are highly complex ecosystems where each individual plays a role, such as the programmer who writes malware, a hacker who penetrates a network to steal data, the seller of stolen credit card data, the embosser of counterfeit cards, or persons who use counterfeit cards to purchase goods that will later be converted to currency. This is only a high-level description. An underground black market with strong alliances and intricate operations is rooted deeply within the cybercriminal community. Within this community, a person can easily purchase the newest version of malware, buy specific services such as a Distributed Denial of Service (DDoS) attack[19] to take down a network, or hock his or her own wares and specialties.

Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[17] Excluded from this analysis, of course, are nation-states that are engaging in cyber-spying and cyber-warfare. *See, e.g.*, Siobhan Gorman, *Chinese Hackers Suspected In Long-Term Nortel Breach*, The Wall Street Journal, Feb. 14, 2012, *available at* http://online.wsj.com/article/SB10001424052970203363504577187502201577054.html?mod=djemalertNEWS.

[18] *See* Brian Krebs, *Shadowy Russian Firm Seen as Conduit for Cybercrime*, Wash. Post, Oct. 13, 2007, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461_pf.html.

[19]

> A Denial of Service ("DoS") attack is essentially an effort by an attacking computer to overwhelm the processing power of the victim computer and effectively take it out of commission. A Distributed Denial of Service ("DDoS") attack is a DoS attack that is carried out by several computers acting in concert. Both types of attacks are carried out through Internet connections between the attacker and the victim, and the victim computer is often a server hosting a website.

Jason Gonzalez, *What is a DDoS Attack and How Can You Prevent One?*, Corp. Compliance Insights (Feb. 14, 2011), http://www.corporatecomplianceinsights.com/what-is-a-ddos-attack-and-how-can-you-prevent-one/.

As technology has advanced, cybercriminals have become more sophisticated, leveraging stolen information from a company to perform phishing attacks against their customers, business partners and even competitors. Identity theft in cyberspace is a major concern, especially for corporations, as a well-crafted e-mail from your bank or business partner may actually have been sent by a hacker. Indeed, hackers have stolen customer e-mail lists from companies to be used in targeted phishing attacks.[20]

In some instances, the hacker's motivation moves from a pure financial payout to, perhaps, a political statement. Cybercriminals participate in corporate espionage by targeting intellectual property or proprietary information, then release it to the masses or otherwise use it to damage the company's reputation. This past year, we saw the continued rise of hacker groups involved with international "hacktivism,"[21] often in retaliation to some political discourse.[22] One such group, Anonymous,[23] made headlines for taking down the websites of the Central Intelligence Agency (CIA), the Department of Justice, and Citibank.[24]

On the other hand, malicious insiders, or morally flexible individuals, are not your garden-variety cybercriminal; usually they are an employee who has already been involved with small infractions or minor insubordination at the victim organization. The disgruntled employee, or an employee who leaves for a position at another company, that has a flawed character and low integrity is susceptible to make the wrong choices.

[20] *See, e.g.*, Mike Lennon, *Massive Breach at Epsilon Compromises Customer Lists of Major Brands*, SECURITY WEEK (Apr. 2, 2011), http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands.

[21] "'The thing that distinguishes hacktivism from financially motivated attackers is that they're loud and they preannounce . . . .'" Mathew J. Schwartz, *Anonymous Leaves Clues In Failed Vatican Attack*, INFORMATIONWEEK SECURITY (Feb. 29, 2012) (quoting Amichai Shulman, Chief Technical Officer of Imperva), http://www.informationweek.com/news/security/attacks/232601726?cid=nl_IW_daily_2012-02-29_html&elq=bb8ce690a0b9454aad2c10d394ff5f0f. Although "hacktivism" has moved to the forefront of the media's attention, law enforcement has experienced increased success in locating and arresting key members of hacktivist groups. *See* Kelly Jackson Higgins, *LulzSec Leader Turns Informant As Feds Arrest Key Members Of Hacking Group*, DARKREADING (Mar. 6, 2012), http://www.darkreading.com/database-security/167901020/security/news/232602124/lulzsec-leader-turns-informant-as-feds-arrest-key-members-of-hacking-group.html?cid=nl_DR_daily_2012-03-07_html&elq=8890b02c68c848b982750ee0ee1f6fc8.

[22] *See, e.g.*, Joshua Rhett Miller, *Pennsylvania tear gas maker is latest target for Anonymous hackers*, Feb. 14, 2012, FOXNEWS.COM, http://www.foxnews.com/scitech/2012/02/14/pennsylvania-tear-gas-maker-is-latest-target-for-anonymous-hackers/.

[23] Anonymous' failed attack against the Vatican's website gave experts a rare glimpse into many of the group's advanced hacking techniques. *See* Schwartz, *supra* note 21; *see also* IMPERVA, *Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack* (2012), *available at* http://www.imperva.com/docs/HII_The_Anatomy_of_an_Anonymous_Attack.pdf. The Vatican is an interesting target in that it has now been noted, by the U.S. State Department, as a potential hub for money laundering, listed as one of the sixty-seven countries that are "of concern." U.S. DEP'T OF STATE, BUREAU FOR INTERN. NARCOTICS AND LAW ENFORCEMENT AFFAIRS, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT: MONEY LAUNDERING AND FINANCIAL CRIMES 31 (Mar. 2012), *available at* http://www.state.gov/documents/organization/185866.pdf.

[24] *See, e.g.*, Chloe Albanesius, *Anonymous Takes Down CIA Web Site*, PCMAG.COM (Feb. 10, 2012) http://www.pcmag.com/article2/0,2817,2400140,00.asp; *see also* Reggie Ugwu, *Anonymous Takes Down Citigroup and Citibank Websites*, COMPLEX.COM (Feb. 3, 2012,), http://www.complex.com/tech/2012/02/anonymous-takes-down-citigroup-and-citibank-websites.

Cybercrime is often not as "black and white" as robbing a bank, but more of a thin grey line of deception that results in more subtle crimes. For these individuals, the reasoning may be, "If I can get away with 'borrowing' office supplies, then I should be able to get away with copying company data onto a thumb drive." However, this activity can escalate over time, with each subsequent crime being justified. Fortunately, there are fewer cases of malicious insiders than external perpetrators, but the loss caused by a trusted insider is potentially much greater because of his or her privileges and unfettered access within the organization.

The last category of cybercriminal, or more accurately, an important tool for the cybercriminal, is the unwitting patsy—the "everyday person," which represents the majority of the population. Most of us go about our lives with very limited awareness or understanding of cybersecurity, Internet fraud, or cyber-espionage. Take, for example, the occasional Spam or Phishing e-mail that makes it through a company's firewall and email filter. The employee may, without thinking a second thought, click on the message, thereby causing his or her computer to be hijacked and credentials stolen, and perhaps exposing the company's valuable data. The unwitting patsy is ground zero for a malware infection, and represents the gateway and the initial point of entry for many cybercriminals. "We" are the lowest hanging fruit. "We" are the unwitting patsy.

A. Measures That Businesses Can Immediately Implement to Enhance Their Cybersecurity

As a preface, it is important to note that advance planning is a key prevention measure for any business. In an emergency incident response situation, a well-written and properly socialized incident response plan will be the best method to inform the relevant stakeholders, identify the incident, and contain the security breach. Often times during an emergency situation, well-intentioned administrators make changes that either disrupt the business or jeopardize the integrity of the digital evidence. It is critical that the incident response plan lays out a proper chain of command. [25]

Companies should also perform a mock-incident response training scenario once a year to ensure adoption of the plan and its effectiveness, as a well-oiled machine functions much more efficiently than a rusty one. A mock-incident exercise will also test the viability of the written plan. [26] Finally, companies should work with a team of dedicated IT security experts who are knowledgeable and experienced in dealing with IT security threats and incident response. This can be an internal team or an external partner. It may not always make sense for every organization to have this level of expertise in-house, thus partnering with a reputable company may be the more reasonable solution.

Combined with the above preparations, companies can improve their cybersecurity and response to attacks by taking the following ten measures:

[25] Baker, *supra* note 13 at 67.

[26] *Id.*

1. The most effective way to prevent cybercrime at the workplace is through enhancing employee knowledge. Training that generates awareness of the security threats that may come from email, privileged access, weak passwords and the like is vital. Training should also be provided to all employees on the topics of social engineering, tampering, and fraud, using a top-down approach. [27]

2. Employees should be instructed to create robust passwords on their systems. It is advisable to use a complex alphanumeric password with a minimum length of 7 characters. If possible, the password should include the use of ASCII characters. These passwords can be relatively simple and easy to memorize without losing their effectiveness, such as "eX@mp1e."

3. At a minimum, companies should encrypt their sensitive data with AES encryption.[28] It does not pose as significant of a problem if your company's data is stolen, but the cybercriminals are unable to read it.

4. A business should take all of its sensitive or proprietary information and put it in "the bank." Network Segmentation is an effective method to lock down and secure a part of the network or systems that has the most confidential data. Another benefit of this method is that the cost of securing and locking down a portion of a company's network is far less expensive than doing the same for the entire enterprise. [29]

5. Companies should also perform a quarterly vulnerability scan of the external network and an annual scan of the internal network. This routine maintenance can uncover gaps and holes that may be left on a company's network and systems.

6. Companies would be well-served to practice better management of access at every level: network, system, and user credentials. This includes purging or disabling default accounts, accounts belonging to former employees, and accounts that are no longer used. Further, as the saying goes, "*Quis custodiet ipsos custodes*?" (Who will guard the guards themselves?). Privileged user/system accounts and administrators have rights to all areas of the enterprise. Companies must have in place some type of monitoring or logging system that tracks these administrators and others, especially around areas where sensitive data is stored. This will ultimately provide a detailed record for accountability and may even act as a deterrent. [30]

7. Companies must properly monitor egress network traffic for anomalies or spikes in the netflow data. For example, if a company discovers that its data is being ex-

[27] *See id.*

[28] *See* John Schwartz, *U.S. Selects a New Encryption Technique*, N.Y. TIMES, Oct. 3, 2000, *available at* http://www.nytimes.com/2000/10/03/business/technology-us-selects-a-new-encryption-technique.html. Certain non-U.S. statues mandate explicit security protocols for entry of data, access to data, and transfer of data protected under those provisions. *See* Kenneth N. Rashbaum, Matthew F. Knouff and Dominique Murray, *Admissibility of Non-U.S. Electronic Evidence*, XVIII RICH. J. L. & TECH. 9, 32-33 (2012), http://jolt.richmond.edu/v18i3/article 9.pdf.

[29] *See* Baker, *supra* note 13 at 67.

[30] *See id.* at 65-66.

filtrated out of the enterprise to an IP address in Eastern Europe, and the company has no customers there, then that should set off a few alarms. [31]

8. Businesses should monitor log data because it provides a wealth of information before, during, and after the breach. It is important to log relevant systems and devices properly, as the fingerprints of a hacker are normally found there. Log data is the forensic investigator's crime scene in the form of digital evidence. [32]

9. A company's IT team should keep secure code development in mind, as failure to do so may open the enterprise to an attack on its website or software. Typically when programming or developing code or website content, the only goal is to make sure it is functional. There are various vulnerabilities—stemming from poor code reviews and poor application testing—such as SQL injection,[33] cross-site scripting,[34] and exploitation of session variables. [35] Companies should ensure that secure coding practices are combined with practical web/software application scanning. [36]

10. The easiest way for a hacker to get in is through an "open door." Specifically, this open door may come in the form of insecure remote-access services that are public-Internet-facing and are not locked down. Such an open door could potentially provide a hacker with direct control of a server with access to the company's network.

[31] *Id.* at 66.

[32] *Id.* at 66-67.

[33] SQL Injection occurs "when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data." THE OPEN WEB APPLICATION SEC. PROJECT, OWASP TOP 10 – 2010: THE TEN MOST CRITICAL WEB APPLICATION SECURITY RISKS T10, A1 (2010), *available at* https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

[34] Cross-site scripting "flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation and escaping." This process "allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites." THE OPEN WEB APPLICATION SECURITY PROJECT, TOP TEN 2010-MAIN (2010), *available at* https://www.owasp.org/index.php/Top_10_2010-Main.

[35]

> Attacks on session IDs and resource IDs take advantage of the fact that some software accepts user input without verifying its authenticity. . . . Many server side processes are vulnerable to these attacks because the server to server communications have not been analyzed from a security perspective or the processes "trust" other systems because they are behind a firewall. In a similar way servers that use easy to guess or spoofable schemes for representing digital identity can also be vulnerable. Such systems frequently use schemes without cryptography and digital signatures (or with broken cryptography). Session IDs may be guessed due to insufficient randomness, poor protection (passed in the clear), lack of integrity (unsigned), or improperly [sic] correlation with access control policy enforcement points. Exposed configuration and properties files that contain system passwords, database connection strings, and such may also give an attacker an edge to identify these identifiers. The net result is that spoofing and impersonation is possible leading to an attacker's ability to break authentication, authorization, and audit controls on the system.

G. Hoglund and G. McGraw, *CAPEC-21: Exploitation of Session Variables, Resource IDs and other Trusted Credentials*, CAPEC (Jan. 1, 2007), http://capec.mitre.org/data/definitions/21.html.

[36] Baker, *supra* note 13 at 66.

An "open door" may also be exposed through vulnerabilities in the company's software or through an inexcusably weak password for a system that has been long forgotten. Two-factor authentication is one way to secure remote access services to keep hackers from gaining entry to the corporate network.

Although companies cannot prevent all hacking incidents, these relatively simple measures—combined with diligent employee training, custom technology tools tailored to a business' needs, and thorough incident response planning—can help improve a company's cybersecurity and prepare it to respond effectively to those incidents that do occur.

III. Public-Private Partnerships: Government and Business Working Together for a Safer Future

> *Cybersecurity issues have been addressed piecemeal in varying ways by different government entities at the Federal, State, local, tribal, and territorial level; private companies and industry organizations; and academic institutions. Although these groups have initiated and sustained various levels of collaboration, cyber threat and vulnerability concerns require an even more systematic, integrated approach.*
>
> The President's National Security Telecommunications
> Advisory Committee[37]

Cooperation between private industry and the government can be highly effective in achieving goals that would be much more difficult or costly for the government to handle on its own. It is in this spirit that the federal government has entered into a series of collaborative efforts with private industry and academia in an attempt to further the cause against cybercrime and bolster the nation's defenses in the event of all out cyber-war.[38] A number of those efforts are highlighted below. Encouraging the growth of these partnerships, and the creation of even more robust joint efforts, will be of vital importance in combating the cyber-threat for years to come.

[37] The President's National Security Telecommunications Advisory Committee, Cybersecurity Collaboration Report: Strengthening Government and Private Sector Collaboration Through a Cyber incident Detection, Prevention, Mitigation, and Response Capability 2 (May 21, 2009), *available at* http://www.ncs.gov/nstac/reports/2009/NSTAC%20CCTF%20Report.pdf.

[38] A guiding principle for public-private cooperation was aptly set forth several years ago by one commentator:

> In particular, government and the private sector, with information technology companies in a leading role, should work together to ensure the development of strong criminal laws and the capability to enforce them, to share information that will enhance security, and to support the security education and training of citizens.

Scott Charney, *Combating Cybercrime: A Public-Private Strategy in the Digital Environment* (Mar. 31, 2005), *available at* http://www.nwacc.org/programs/conf05/UNCrimeCongressPaper.doc (written for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2005, Bangkok, Thailand).

A. Department of Homeland Security's Project 12

Led by the Department of Homeland Security (DHS), Project 12 seeks to define the federal government's role for "extending cyber security into critical infrastructure domains" and to find new ways for the federal government and private companies to work cooperatively.[39] According to the National Security Council, DHS and its private-industry partners have "developed a plan of shared action with an aggressive series of milestones and activities" which "addresses security and information assurance efforts across the cyber infrastructure to increase resiliency and operational capabilities throughout the [Critical Infrastructure and Key Resources (CIKR)] sectors."[40] This effort entails "a focus on public-private sharing of information regarding cyber threats and incidents in both government and CIKR."[41] For a deeper study of the joint efforts being undertaken through Project 12, consult the Comprehensive National Cybersecurity Initiative (CNCI) Project 12 Report, titled *Improving Protection of Privately Owned Critical Network Infrastructure through Public-Private Partnerships*.[42]

B. Electronic Crimes Task Forces and Working Groups

The USA PATRIOT Act[43] mandates that the United State Secret Service establish a nationwide network of Electronic Crimes Task Forces (ECTFs), bringing together federal, state and local law enforcement, in addition to prosecutors, private industry and members of academia, with the "common purpose" of "prevention, detection, mitigation and aggressive investigation of attacks on the nation's financial and critical infrastructures."[44] ECTFs have been established in Secret Service offices based across the United States.[45] In addition to assisting in the investigation of cyber-related offenses and in protecting "critical infrastructure," the task forces hold meetings whereby members "share case studies and recent trends in cyber crimes, explore new technologies in the field, establish new relationships and strengthen existing ones, and . . . discuss new methods to advance efforts to protect the nation's critical infrastructure from cyber-attacks," while also providing training seminars for members of law enforcement, prosecutors and private industry personnel.[46]

[39] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-388, CYBERSECURITY: PROGRESS MADE BUT CHALLENGES REMAIN IN DEFINING AND COORDINATING THE COMPREHENSIVE NATIONAL INITIATIVE 19 (Mar. 2010), *available at* http://www.gao.gov/new.items/d10338.pdf.

[40] NAT'L SEC. COUNCIL, THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, *available at* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

[41] *Id.*

[42] THE COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE, PROJECT 12 REPORT: IMPROVING PROTECTION OF PRIVATELY OWNED CRITICAL NETWORK INFRASTRUCTURE THROUGH PUBLIC-PRIVATE PRTNERSHIPS (2008), http://info.publicintelligence.net/NetworkInfrastructurePublicPrivate.pdf.

[43] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, H.R. 3162, 107th Cong. (1st Sess. 2001).

[44] U.S. SECRET SERVICE, *Electronic Crimes Task Forces and Working Groups*, http://www.secretservice.gov/ectf.shtml (last visited Jan. 22, 2012).

[45] *Id.*

[46] U.S. SECRET SERVICE, *New York/New Jersey Electronic Crimes Task Force*, http://www.secretservice.gov/ectf_newyork.shtml (last visited Jan. 22, 2012).

C. National Cyber-Forensics & Training Alliance (NCFTA)

A non-profit corporation, the NCFTA "has established an expansive alliance between subject matter experts (SMEs) in the public and private sectors (more than 500 worldwide) with the goal of addressing complex and often internationally-spawned cyber crimes. These SMEs, from industry, academia and government, each bring specific talents and experiences to the partnership."[47] The NCFTA has formal partnerships or agreements with over forty private organizations and more than fifteen American and international law enforcement or regulatory agencies.[48] The NCFTA "manages the collection and sharing of intelligence with industry partners, appropriate [law enforcement groups], and other cross-sector SMEs," with the objective of developing "real-time intelligence to an actionable level in order to identify and mitigate threats, identify threat actors, and provide intelligence to domestic and international [law enforcement groups] to neutralize the threats."[49] According to the NCFTA, its efforts have resulted in the successful prosecution of over 300 cybercriminals worldwide.[50]

The NCFTA has also taken a major role in the "Digital Phishnet" project, which was created as a joint effort of the NCFTA, federal law enforcement agencies (such as the FBI, Secret Service, the FTC, and the U.S. Postal Inspection Service), five e-commerce and technology companies (such as Microsoft), four large internet service providers (including America Online and Earthlink), and several top U.S. banks.[51] The project, which was created to improve the collection and development of intelligence regarding phishing attacks, [52] has led to the identification of 6,000 "drop accounts,"[53] the creation of more than 600 investigative reports, and the recovery of compromised accounts equaling more than $220 million in prevented economic loss.[54]

[47] NATIONAL CYBER-FORENSICS & TRAINING ALLIANCE, *About the NCFTA*, http://www.ncfta.net/about-ncfta (last visited Jan. 22, 2012).

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Press Release, Federal Bureau of Investigation, An Unprecedented Cyber Partnership "Digital PhishNet" Is Reeling In Cyber Crooks (Jan. 24, 2005), http://www.fbi.gov/news/stories/2005/january/phishnet_012405.

[52] "In a typical 'phishing scheme,' a spam email, which imitates a message from a legitimate author and is designed to steal personal information through malicious software or lure the recipient into sharing such information, is sent to a potential victim." Fernando M. Pinguelo and Bradford W. Muller, *Virtual Crimes, Real Damages: A Primer on Cybercrimes in the United States and Efforts to Combat Cybercriminals*, 16 VA. J.L. & TECH. 116, 129 (2011) (citing Alison Diana, *Phishers Target Social Media, Universities*, INFORMATIONWEEK, Oct. 12, 2010, http://www.informationweek.com/news/security/cybercrime/showArticle.jhtml?articleID=227701164&cid=nl_IW_daily_2010-10-15_html).

[53] "Drop accounts" are "cyber warehouses where criminals store stolen credentials." National Cyber-Forensics & Training Alliance, Digital Phishnet, *available at* http://www.ncfta.net/ncfta-initiatives/digital-phishnet (last visited Jan. 22, 2012).

[54] *Id.*

D. InfraGard

InfraGard represents a collaborative effort between the federal government and private industry with the goal of protecting the nation's critical infrastructure from cyber threats.[55] InfraGard is a FBI program, with members from private industry, academia, state and local law enforcement agencies, and elsewhere, all dedicated to sharing information to prevent hostile acts against the United States.[56] The program has numerous goals, including increasing information sharing between its members and the FBI on issues of counterterrorism, cybercrime, threats to critical infrastructures, etc.; providing members with threat advisories, alerts, and warnings; promoting effective cooperation between members and all levels of government; and providing members with a forum for training and education on counterterrorism, counterintelligence, and cybercrime.[57] InfraGard also offers its members access to a secure website which, among other things, provides information about recent cyber-intrusions and research related to the protection of critical infrastructure.[58]

IV. CONCLUSION: MOVING FORWARD TOGETHER

There is no easy solution to the cyber-threat facing the public and private sectors. Even the most well-prepared, well-funded IT department will not always be able to protect a company from a determined hacker. However, the situation is not hopeless, nor are businesses left to simply wait for the government or international community to effectively respond. Rather, as Mr. Lee's contribution demonstrates, there are relatively simple measures that businesses can immediately implement to better protect their data. Further, concerned companies are encouraged to become involved in one of the many public-private partnerships now at work in the United States. The more proactive the business community becomes in facing the cyber-threat, the closer we move towards a secure Internet.

[55] INFRAGARD, http://www.infragard.net/about.php?mn=1&sm=1-0 (last visited Jan. 22, 2012).
[56] *Id.*
[57] *Id.*
[58] *Id.*