Fordham Urban Law Journal

Volume 35 | Number 1 Article 6

2008

Securing Online Transactions: Crime Prevention is the Key

Michael Ena

Securing Online Transactions: Crime Prevention is the Key

Cover Page Footnote
The author would like to thank Professor Alexander H. Southwell for his comments on this work.

SECURING ONLINE TRANSACTIONS: CRIME PREVENTION IS THE KEY

*Michael Ena**

> What we . . . must confront today is an entirely new breed of criminal—one that transcends geographic boundaries or borders with a high degree of stealth and anonymity. We have witnessed the emergence of the professional Cybercriminal, a foe at home and abroad that continuously probes our critical infrastructure for weakness and vulnerability, in order to victimize the American public in a multitude of ways, and profit from our loss.
>
> James M. Sheehan,
> Special Agent in Charge, Criminal Division,
> FBI Los Angeles.[1]

INTRODUCTION

The commercial use of the Internet came as an afterthought. The Internet's original designers aimed to create a communication system resilient in the face of a nuclear attack, not a secure network for business and consumer transactions.[2] A widespread use of commodity operating systems and software products delivering rich functionality but lacking security aggravated the problem.[3] Vi-

* J.D. Candidate, Fordham University School of Law, 2009; M.S., Computer Science, New York University; Ph.D., Physical and Mathematical Science, Moscow University; B.S., M.S., Applied Mathematics and Computer Science, Moscow University; Certified Information Systems Security Professional (CISSP). The author would like to thank Professor Alexander H. Southwell for his comments on this work.

1. Press Release, FBI Los Angeles, Operation Web Snare Leads to Charges in Los Angeles Against High-Tech, Intellectual Property Offenders (Aug. 26, 2004), http://losangeles.fbi.gov/pressrel/2004/websnare082604.htm [hereinafter FBI Press Release].

2. *See, e.g.*, Scott Charney, *The Internet, Law Enforcement and Security*, 662 PLI/PAT 937, 943 (2001).

3. *See, e.g.*, Fred Volgelstein, *Why Hackers Are a Giant Threat to Microsoft's Future*, FORTUNE, Oct. 18, 2004, at 263 (noting that until recently, Microsoft did not write programs with the hacker threat in mind focusing instead on the stability of its Windows operating systems and adding new features to its software); *see also* Larry Greenemeier, *Underground Buzz on New Bots*, INFO.WK., Oct. 9, 2006, at 44 [hereinafter Greenemeier, *Buzz on New Bots*](noting that operating system monoculture facilitates hacker attacks and proliferation of malicious software); Gregg Keizer, *Exploit-for-Sale Hacker Pins Bug on Vista's E-Mail App*, COMPUTERWORLD, Mar. 23, 2007, *available at* http://www.computerworld.com/action/article.do?command=PrintArticleBasic&articleId=901419; Robert McMillan, *New IE7 Bug Could Help Phishers*, IDG NEWS SERVICE, Mar. 14, 2007, *available at* http://www.computerworld.

ruses, worms, and hacker attacks caused tremendous damage and made securing Internet communications and Internet-connected computer systems the primary concern of software vendors and information technology ("IT") professionals.[4] A patchwork of technologies and software products emerged to protect computer systems and to make the Internet suitable for commercial use.[5]

By offering an inexpensive global communication medium, the Internet enabled businesses to provide information and deliver innovative products and services to a much wider audience of consumers around the corner or around the world.[6] For retailers, moving mail order business to the Internet expanded their customer base and reduced their costs.[7] The financial industry, especially global banking and financial services companies, quickly recognized and leveraged the tremendous potential of the Internet.[8] Now any customer with an Internet connection can access bank accounts and execute transactions at practically any time and from any location.[9] The customer can use a broadband connection to the Internet, a dial-up, or a satellite link in some remote place or aboard a ship.

---

com/action/article.do?command=ViewArticleBasic&articleId=9013098&source=NLT_SEC&nlid=38.

4. *See, e.g.*, Peter Coffee, *Security: Next Steps*, EWK., Jan. 8, 2007, at 37.

5. *See, e.g.*, Anne Chen, *Demo: Security Rules*, EWK., Feb. 21, 2005, at 28; *Law Firm Makes Case for eRoom*, EWK., Apr. 2, 2007, at 42 (reporting that DLA Piper USA uses the Documentum eRoom software to provide secure information sharing between its 32,000 attorneys in twenty four countries).

6. *See, e.g.*, *Cambridge Technology Partners Launches Industry's First Global Internet Banking Initiative With Security First Technologies*, BUS. WIRE, Nov. 20, 1996, *available at* http://findarticles.com/p/articles/mi_m0EIN/is_1996_Nov_20/ai_18872833.

7. *See, e.g.*, Martin Michael, *The Next Big Thing: A Bookstore?*, FORTUNE, Dec. 9, 1996, at 168-70 (one of the early reports about the Internet startup company Amazon.com, now one of the leading online retailers).

8. *See, e.g.*, Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 AM. U. L. REV. 967, 969 (1997) (pointing out that the financial industry is interested in leveraging electronic commerce and payment systems to deliver innovative products and services, develop new markets, and lower operational costs); Jerry Jackson, *Check Out Banking Via PC; Home Banking With Personal Computers Is Becoming Common, but It Pays to Know Which Service Offers the Options You Need*, ORLANDO SENTINEL, Oct. 23, 1996, at E1; Martyn Williams, *Citibank Japan Launches Internet Banking Service*, NEWSBYTES, Dec. 22, 1998, *available at* 1998 WLNR 4065946.

9. *See, e.g.*, CitiDirect® Online Banking, http://www.citidirect-online.com (last visited Nov. 17, 2007) (Internet-based corporate banking system offering from Citigroup).

Ensuring the security of online transactions, however, is a challenging task.[10] The global nature of the Internet exposes online businesses to attacks by cybercriminals of all types from all over the world.[11] Financial institutions, merchants, and organizations storing data that criminals can exploit for illicit financial gains are among the primary targets. Therefore, these institutions and actors must ensure that their computer systems can withstand attacks of the most sophisticated and skilled intruders, including organized crime syndicates, terrorist organizations, and foreign government agencies.[12] At the same time, it is critically important for American society to secure online transactions, ensure consumer confidence in conducting business online, and protect Americans from being victimized at an increasing rate.[13]

This Comment illustrates how government regulation, criminal justice, private legal actions, and market forces contribute to the security of online transactions. Further, it argues that government regulation aimed at the prevention of cybercrime should be the primary focus of the efforts to improve online security. Part I explains that malicious hackers are becoming an integral part of organized crime and terrorist organizations. Part II provides an overview of various attack schemes used by cybercriminals.

Part III examines industry efforts intended to prevent cybercrimes through technological solutions and raising awareness of information security issues among business leaders, government officials, and consumers. The discussion continues with an overview of private legal actions where plaintiffs attempted to hold business organizations accountable for failing to secure their personal and financial information.

---

10. *See, e.g.*, Michael Singer, *Feeling Safe Online*, BANK SYSTEMS & TECH., Mar. 2007, at 19 (pointing out technical difficulties in securing online transactions); Sandra Gittlen, *New Attacks Leave Online Transactions Vulnerable Even After Sign-On Authentication*, COMPUTERWORLD, Aug. 28, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9000174.

11. *See, e.g.*, Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003, 1071 (2001).

12. K.C. Jones, *University Unveils Cyber Threat Calculator*, INFO.WK., Jan. 26, 2007, *available at* http://www.informationweek.com/1122/threat.htm (noting that foreign states, especially Russia and China, as well as "individuals, political groups, religious groups and organized crime groups . . . pose ongoing risks and should be considered cyber threats").

13. Sharon Gaudin, *ID Theft Is Exploding in the U.S.*, BANK SYSTEMS & TECH., Mar. 7, 2007, *available at* http://www.banktech.com/showArticle.jhtml?articleID=198002061 (reporting that fifteen million Americans fell victim to identity theft in the past twelve months, a fifty percent increase since 2003).

Part IV addresses the role of the government in improving the security of online transactions. In particular, the discussion shows that many cybercrimes were precipitated by an organization's failure to adhere to basic information security principles. Using financial institutions as an example, Part IV also shows how government regulation can force business organizations to maintain adequate security of their computer systems.

Part V provides a discussion of various approaches to securing online transactions. Ultimately, Part V concludes that government regulation and oversight, the deterrent effect of criminal prosecution, and the right to enforce through private legal action compliance with government-mandated information security standards may be the optimal way to improve the security of online transactions and prevent cybercrime.

I. CYBERCRIME: A GROWING THREAT

A. Hackers as a Part of Organized Crime and Terror Networks

An inherent lack of security in the Internet architecture and relative user anonymity make the Internet an attractive medium for extortion[14] and crimes involving theft of personal information for illicit financial gain.[15] According to a recent IDG News Service report, hackers have joined forces with organized criminal groups to engage in increasingly sophisticated criminal schemes operated exclusively for profit.[16] Although computer crime experts agree that most computer-related crimes go either undetected or unreported,[17] the Internet Crime Complaint Center recently reported

14. *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) (upholding an indictment of a Russian hacker on charges of conspiracy, computer fraud, extortion, and possession of unauthorized access devices for breaking into a financial transaction processing company's computer systems and demanding a payment for his assistance in securing the systems).

15. Press Release, U.S. Dep't of Justice, Hackers from India Indicted for Online Brokerage Intrusion Scheme that Victimized Customers and Brokerage Firms (Mar. 12, 2007), http://www.cybercrime.gov/marimuthuIndict.htm. "A federal grand jury in Omaha, Neb., has indicted three individuals on charges of conspiracy, fraud and aggravated identity theft stemming from a high-tech, international fraud scheme designed to hijack online brokerage accounts for profit." *Id.*

16. Jeremy Kirk & Robert McMillan, *2006: The Year in Security*, IDG NEWS SERVICE, Dec. 7, 2006, *available at* http://www.computerworld.com/action/article.do?command=PrintArticleBasic&articleId=9005743 [hereinafter Kirk & McMillan, *Year in Security*] (noting that in 2006, financially motivated cybercriminals emerged as public enemy No. 1).

17. *See, e.g.*, Charney, *supra* note 2, at 943-44.

that the total annual amount of losses reported in 2006 was $198 million, compared with $183 million in 2005.[18]

Financial institutions are among the primary targets of cybercriminals. According to recent reports, organized crime groups have offered millions of dollars for help in breaking into financial institutions' computer networks.[19] The FBI has confirmed the existence of organized crime structures in parts of the hacking community, particularly in Eastern Europe, that function as criminal enterprises.[20] In such instances, hackers break into computer systems and steal data, while other individuals sell the data for profit to those who exploit the stolen data in order to gain unauthorized access to credit card, bank, and brokerage accounts of unsuspecting victims.[21] According to industry observers, the market for stolen identities has recently reached one billion dollars.[22]

The most alarming development in the area of information systems security is that terrorist organizations now perceive cybercrimes both as a source of financing for their activities[23] and as a new weapon in their arsenal.[24] For example, according to law enforcement organizations, the Irish Republican Army and the terrorists that plotted the foiled bombing of the Los Angeles

18. NATIONAL WHITE COLLAR CRIME CENTER & FEDERAL BUREAU OF INVESTIGATION, INTERNET FRAUD CRIME REPORT 3 (2006), http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf. IC3 is a clearing house for all kinds of cybercrime complaints designed to track the prevalence of Internet fraud in the U.S. and run by the FBI in partnership with the National White Collar Crime Center. IC3 started operation on May 8, 2000. *Id*. at 4.

19. Larry Greenemeier, *A Researcher Passes on the Big Leagues*, INFO. WK., Feb. 12, 2007, at 36 (reporting that a computer security researcher declined an offer from a criminal group that offered to pay him $2.8 million for each financial services company he helped to infiltrate).

20. Larry Greenemeier & J. Nicholas Hoover, *The Hacker Economy*, INFO. WK., Feb. 12, 2007, at 32 [hereinafter Greenemeier & Hoover, *Hacker Economy*].

21. *Id.*

22. *Id.* at 38.

23. *See, e.g.*, Todd M. Hinnen, *The Cyber-Front in the War on Terrorism: Curbing Terrorist Use of the Internet*, 5 COLUM. SCI. & TECH. L. REV. 5, 9 (2004) (noting that terrorists perpetrate online crimes to support their missions). Terrorists use the Internet to raise funds, as a means of communication, for the propaganda of their ideas, and for recruiting new members. Terrorists also plan to use the Internet to attack critical elements on the national infrastructure. *Id.* at 5.

24. *See, e.g.*, Jeremy Kirk, *Russian Expert: Terrorists May Try Cyberattacks*, IDG NEWS SERVICE, Dec. 13, 2006, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9006003; Robert Lazner & Nathan Vardi, *The Next Threat*, FORBES, Sept. 20, 2004, at 70 (discussing the vulnerability of the United States economy to terrorist cyberattacks); Tom Zeller Jr., *On the Open Internet, a Web of Dark Alleys*, N.Y. TIMES, Dec. 20, 2004 at C1 (warning about the danger of cyberterrorism).

International Airport used identity theft to finance their activities.[25] Imam Samudra, the radical Muslim cleric and mastermind of the devastating 2002 Bali bombing attacks that claimed 202 lives, called for fellow Muslim radicals to take jihad into cyberspace and tap into online credit card fraud as a source of funding.[26]

Although some individuals still break into computer systems for fun, bragging rights, or as a prank, they do not pose nearly as much of a threat to the security of online transactions as highly motivated, increasingly sophisticated, well-organized, and well-funded groups of cybercriminals and cyberterrorists.[27]

B. Hacker Tools for Sale

Contrary to popular belief, most of the attacks perpetrated against computer systems do not require a high level of technical sophistication.[28] Many hacking tools, as well as legitimate computer programs that cybercriminals use for malicious purposes are freely available for download on the Internet,[29] while more sophisticated tools are offered for sale.[30] According to a recent study by IBM, attacks will likely increase in 2007 because cybercriminals organize networks dedicated to the production and commercial distribution of increasingly sophisticated malicious software ("malware") that is later used in criminal attacks on computer systems.[31] Additionally, Raimund Genes, the chief technical officer ("CTO") of Trend Micro, a security software vendor, contends that

25. Timothy L. O'Brien, *Gone in 60 Seconds*, N.Y. TIMES, Oct. 24, 2004, at § 3-1.

26. Alan Spires, *An Indonesian's Prison Memoir Takes Holy War into Cyberspace; In Sign of New Threat, Militant Offer Tips on Credit Card Fraud*, WASH. POST, Dec. 14, 2004, at A19.

27. *See, e.g.*, Robert McMillan, *Two Charged with Hacking LA Traffic Lights*, IDG NEWS SERVICE, Jan. 10, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9007751 (reporting that two individuals were charged with illegal computer access for allegedly hacking into the Los Angeles traffic control center and turning off traffic lights at four intersections in August 2006).

28. *See, e.g.*, Stephen E. Henderson & Matthew E. Yarbrough, *Frontiers of Law: The Internet and Cyberspace: Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 11-12 (2002) (noting that a fifteen year-old teenager from Montreal was responsible for crippling several major internet sites in 2000 by launching attacks against them).

29. *See id.* at 12.

30. *See, e.g.*, Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 32 (noting that malicious software, or malware, such as keyloggers, worms, and viruses, has become a valuable commodity in the hacker economy).

31. Paul McDougall, *Organized Malware Factories Threaten Internet Users, Study Says*, INFO.WK., Jan. 30, 2007, *available at* http://www.informationweek.com/shared/printableArticle.jhtml?articleID=197001739.

the revenue generated by the malware industry exceeded the twenty-six billion dollars earned by legitimate computer security vendors in 2005.[32]

The industrial production of malware will make it much more difficult for IT professionals to stay ahead of hackers in securing computer systems.[33] Gunter Ollmann, the director of security strategy at IBM's Security Systems unit, warned that the criminal malware infrastructure allows cybercriminals to target their attacks and build custom malware to be used against specific organizations.[34] This development increases the risk for high-value targets, such as financial institutions, payment processing companies, and big retailers.[35]

"Zero-day exploits" take advantage of newly discovered security vulnerabilities before software vendors issue patches for their affected products and, therefore, are especially valuable for cybercriminals.[36] In 2006, cybercriminals unleashed zero-day attacks on an unprecedented scale, raising serious concerns in the software development and IT industry.[37] But since it is legal to post information on the Internet about unpatched security vulnerabilities in commercial software products, law enforcement can do little to prevent the creation of code, which exploits these vulnerabilities.[38]

The next Section provides a brief overview of attack schemes that cybercriminals use to cripple computer systems and gain unauthorized access to information that may enable them to execute fraudulent transactions.

II. INFORMATION SYSTEMS SECURITY AND CYBERATTACKS

The primary goals of information system security professionals are to ensure the availability of computer systems and the data stored in them for authorized users, as well as to protect the integ-

32. *See, e.g.*, Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 36.

33. *See, e.g.*, Singer, *supra* note 10, at 19 (pointing out that cybercriminals are often better equipped than information security professionals).

34. McDougall, *supra* note 31.

35. Jaikumar Vijayan, *Targeted Attacks Pose New Security Challenge*, COMPUTERWORLD, June 27, 2005, *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,102779,00.html (reporting a massive credit card security breach caused by a targeted attack and pointing out that stopping such attacks is extremely difficult).

36. *See, e.g.*, Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 36 (reporting that last year, zero-day exploits were selling for twenty to thirty thousand dollars each).

37. *See* Kirk & McMillan, *Year in Security*, *supra* note 16.

38. *See* Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 36.

rity and confidentiality of the data.[39] Any attack against a computer system affects at least one of these three major components of information security.[40]

A. Denial-of-service Attacks

Denial-of-service ("DoS") attacks are primarily aimed at disrupting the availability of computer system resources to authorized users, usually, by sending invalid data that causes the server software to crash or by flooding computer systems with invalid requests.[41] The increasing number of unsolicited junk e-mails, known as spam, can also cause a DoS by decreasing or denying availability of e-mail services to authorized users and by clogging their mailboxes with unwanted e-mails, thus interfering with the user's ability to send and receive legitimate e-mail messages.[42] To launch distributed denial-of-service ("DDoS") attacks, cybercriminals, using malware installed on hundreds or even thousands of compromised computer systems, attempt to flood the victim's network with requests and disrupt access to the target Web site or to overload the victim's servers and cause them to crash.[43]

Even more dangerous is a distributed reflective denial-of-service ("DRDoS") attack, where the attacker uses compromised computers to send connection requests to many other computers on the Internet specifying the victim as the originator of the requests.[44] This causes the computers receiving the requests to send replies to the victim's computer multiple times causing the victim's network to be clogged with their replies.[45]

---

39. SUSAN HANSCHE ET AL., OFFICIAL GUIDE TO THE CISSP EXAM 3-8 (2004). The Certified Information Systems Security Professional (CISSP) certification offered by the International Information Systems Security Certification Consortium is a well-respected industry certification credential for information security professionals. *See* International Information Systems Security Certification Consortium, CISSP – The International Gold Standard, www.isc2.org/cgi-bin/content.cgi?category=97 (last visited Nov. 17, 2007).

40. HANSCHE, *supra* note 39, at 3-8.

41. *Id.* at 155. Although DOS can result from natural and man-made disasters, such as hurricanes, earthquakes, blackouts, software glitches, or explosions, this Section is concerned with intentional disruption of computer systems' availability by malicious hackers.

42. *Id.*

43. *Id.* at 155-56.

44. For more information on DRDoS, see Steve Gibson, *DRDoS* (2002), http://www.grc.com/dos/drdos.htm. The technique of replacing the originator's address in network data packets or e-mails sent over the Internet is called spoofing. *Id.*

45. *Id.* Multiple replies result from the design of Internet protocols. If the sender does not receive an acknowledgment that a packet of data sent reached its destination, the sender will retry several times before giving up. Perpetrators of DRDoS

DDoS attacks are not a kids' game anymore; they have become a weapon of choice for cyber-extortionists and unscrupulous businesspeople attempting to bring down competitors' Web sites.[46] The DDoS, and especially DRDoS, attacks are very difficult to investigate because of the difficulty in tracing them back to the attackers.[47] Nevertheless, in Los Angeles in 2004, the FBI executed the first arrests related to a large-scale DDoS attack used for commercial purposes in which two businessmen hired a team of hackers to bring down competitors' Web sites.[48]

B. Spam

In 2004, Microsoft founder and chief software architect Bill Gates predicted that spam would be gone by 2006.[49] Despite his prophecy, spam comprised up to ninety percent of all e-mails in 2006.[50]

IT administrators are constantly struggling to protect their e-mail servers from an ever increasing volume of spam.[51] To bypass e-mail filters, spammers started using images instead of text in their e-mails.[52] To avoid detection, spammers often use compromised computers and unprotected wireless networks to send millions of junk e-mail messages.[53] Although modern anti-spam systems usually filter out around ninety-eight percent of spam e-mails, spam-

---

attacks exploit this protocol design feature for a dual purpose, as an attack amplifier and as an additional layer of stealth. *Id.*

46. *See, e.g.*, FBI Press Release, *supra* note 1; *see also* Timothy L. O'Brien, *The Rise of Digital Thugs*, N.Y. TIMES, Aug. 7, 2005 at § 3-1.

47. *See, e.g.*, Gibson, *supra* note 44.

48. *See* FBI Press Release, *supra* note 1; *see also* Federal Bureau of Investigation, *The Case Of The Hired Hacker: Entrepreneur and Hacker Arrested for Online Sabotage* (2005), http://www.fbi.gov/page2/april05/hiredhacker041805.htm.

49. Kirk & McMillan, *Year in Security*, *supra* note 16.

50. *Id.*

51. *See, e.g.*, Dan Kaplan, *New Flood of Spam*, SC MAG., Mar. 2007, at 16 (reporting a 100% increase in spam volume in October 2006 compared to October 2005 and linking the growth to the increased use of image spam).

52. *Id. See also* Robert McMillan, *"Rock Phish" Blamed for Surge in Attacks*, IDG NEWS SERVICE, Dec. 12, 2006, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9005958&pageNumber=1 [hereinafter McMillan, *Rock Phish*] (reporting increased use of image spam that is much more difficult to identify and intercept); SYMANTEC CORPORATION, SYMANTEC MESSAGING AND WEB SECURITY, A MONTHLY REPORT – FEBRUARY 2007 (2007), http://www.symantec.com/avcenter/reference/Symantec_Spam_Report_-_February_2007.pdf (reporting increase in image spam).

53. FBI Press Release, *supra* note 1 (reporting that a spammer was charged under the CAN SPAM Act, Pub. L. 108-187, 117 Stat. 2699, for using open and unencrypted wireless networks to send bulk e-mails advertising pornographic Web sites).

mers ensure that a large number of their e-mails still reach users' mailboxes by employing automated spam engines to send out a huge volume of e-mails.[54]

Cybercriminals often use spam e-mails in various fraud and identity theft schemes to gain unauthorized access to financial accounts or for large-scale deployment of various types of malware.[55]

C. Phishing

As financial institutions and online merchants make their Web sites more secure, cybercriminals more often resort to relatively low-tech attacks, such as phishing.[56] "Phishing" refers to criminals' creation of e-mails and Web sites, designed to look like e-mails and Web sites of well-respected legitimate businesses, financial institutions, and government agencies—in order to trick Internet users into disclosing their financial account or other sensitive personal information[57]

Although software vendors add anti-phishing features to their products, cybercriminals change their tactics to stay ahead of the game.[58] More sophisticated phishing attacks may attempt to exploit vulnerabilities in a financial institution's or online payment services company's Web site in order to redirect the victim's browser to a malicious Web site while maintaining the appearance that the victim is still connected to a legitimate Web site.[59] Other phishing attacks may involve the use of deception to install spyware on victims' machines in order to steal sensitive personal information.[60] Attackers also started using unique URL's for each phishing e-mail they send to make it more difficult to identify and

54. Jeremy Kirk, *Spam Fight Escalates*, COMPUTERWORLD, Oct. 2, 2006, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=266043 [hereinafter Kirk, *Spam Fight*] (pointing out that attempts to filter out more than 98% of spam will result in some legitimate e-mail messages being filtered out as well).

55. *See infra* Part II.C-E for a detailed discussion.

56. *See* McMillan, *Rock Phish*, *supra* note 52 (reporting that a highly sophisticated group of cybercriminals known as "Rock Phish" targets European and U.S. financial institutions, such as Citibank, ETrade, Barclays, and Deutsche Bank). R

57. U.S. DEP'T OF JUSTICE, SPECIAL REPORT ON "PHISHING" (2004), http://www.usdoj.gov/criminal/fraud/docs/Phishing.pdf.

58. *Id.*

59. *See, e.g.*, Wikipedia, Cross-Site Scripting, http://en.wikipedia.org/wiki/Cross-site_scripting. This type of attack is called cross-site scripting. *Id.*

60. Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 36-37.

block the attack.[61] "Spear phishing" is another type of phishing attack where attackers target a specific group of Internet users, for example employees of a particular financial institution, in an attempt to steal their access credentials.[62] Criminals often use automated phishing tools, spam engines, and botnets in their phishing attacks.[63]

Despite extensive efforts by software vendors to improve the security of their products, phishing is still a serious threat to the security of online transactions.[64] Victims of phishing attacks suffer financial losses, and must spend time and money rebuilding their credit and good name.

D. Zombies and Botnets

Compromised computers with installed malware remotely controlled by cybercriminals are usually referred to as zombies.[65] A botnet is a group of zombies controlled by a particular hacker or criminal group.[66] The owners of zombie computers are not usually aware that their computers have become part of an illicit network and a tool in the hands of cybercriminals.[67]

Botnets have become a very important and extremely dangerous weapon in the cybercriminals' arsenal because of their concentrated power, which criminals can use to perpetrate various malicious acts on the Internet.[68] Botnet attacks are growing in number,

---

61. McMillan, *Rock Phish*, *supra* note 52. This technique allows attackers to avoid protective features in Web browsers and other software based upon blacklisting URLs that belong to known phishing Web sites. *Id.*

62. *See, e.g.*, Timothy L. O'Brien, *Gone Spear Phishin' For a New Breed of Hackers, This Time It's Personal*, N.Y. TIMES, Dec. 4, 2005 at § 3-1; Ellen Messmer, *Fish for New Employees and Get Phished?*, NETWORK WORLD, Mar. 13, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9012978 (reporting phishing attacks targeting company employees).

63. *Id*. *See infra* Part II.D for a discussion of botnets.

64. Robert McMillan, *Microsoft Sees Botnets as Top '07 Net Threat*, IDG NEWS SERVICE, Dec. 27, 2006, *available at* http://www.computerworld.com/action/article.do?command=PrintArticleBasic&articleId=9006818 [hereinafter McMillan, *Botnets Top '07 Threat*]. According to Aron Kornblum, a senior attorney with Microsoft's Internet Safety Enforcement team, Microsoft continues to see phishing as a "serious threat." *Id.*

65. Stephen Labaton, *An Army of Soulless 1's and 0's*, N.Y. TIMES, June 24, 2005, at C1 (warning about the growing danger of zombies).

66. *See, e.g.*, Evan Ratliff, *The Zombie Hunters*, NEW YORKER, Oct. 10, 2005, at 44.

67. Labaton, *supra* note 65, at C1.

68. *Id.* According to Christopher Painter from the U.S. Department of Justice's computer crime and intellectual property section, botnets have become "the Swiss Army knife of computer hacking." *Update*, SC MAG., Apr. 2007, at 14.

sophistication, and power.[69] Microsoft considers botnets to be the top Internet threat of 2007.[70]

To deploy botnet software, hackers typically use automated tools that exploit known security vulnerabilities in popular software products and the complacency of users who fail to install the latest security updates or who visit unsafe Web sites infected by malware.[71] For example, a hacker's robot can scan the Internet in a predefined address range probing each computer it finds for known vulnerabilities, weak passwords susceptible to guessing, or for backdoors opened by malware already present on the computer.[72] Once the robot succeeds in gaining control over vulnerable computers, it will install malware that the robot owners will later use to steal information; for spam and DDoS attacks; or to temporarily store illegal, malicious, or stolen files.[73]

Hackers often deceive users into downloading software to their computers as a part of a seemingly innocent software package, such as a screen saver, game, or some utility program.[74] Sometimes hackers attempt to lure unsuspecting users to visit Web sites that will attempt to install malware on their machines by exploiting Web browser vulnerabilities or inadequate security settings.[75] Since Internet users have become more cautious, hackers have started using compromised legitimate Web sites for the dissemination of malware.[76]

---

69. Thomas Claburn et al., *Beware the Bots*, INFO.WK., Oct. 9, 2006, at 48.

70. McMillan, *Botnets Top '07 Threat*, *supra* note 64.

71. *See, e.g.*, Greenemeier, *Buzz on New Bots*, *supra* note 3, at 44.

72. *Id.*

73. *Id.*; *see also* Claburn et al., *supra* note 69, at 44. There are products, usually implemented as software or a combination of software and hardware components, known as firewalls, that among other functions, can make computer systems "invisible" to other computers on the Internet. This, of course, does not apply to publicly available Web sites that by design should be accessible to all Internet users. There, firewalls protect computer systems from attacks by blocking unwanted and malicious requests according to pre-defined algorithms. *See generally* Thomas DeFelice, *Designing and Implementing Firewalls*, DATA COMMUNICATIONS MANAGEMENT, June 2002.

74. Malware using this delivery mechanism is also known as a Trojan horse or Trojan. *See* HANSCHE, *supra* note 39, at 162. R

75. *See* Roger A. Grimes, *Ever-Evolving Malware is Getting Nastier*, INFOWORLD, June 1, 2007, http://www.infoworld.com/article/07/06/01/22OPsecadvise_1.html (warning about the rising danger of Web site-based malware).

76. *See* Gregg Keizer, *Bank of India Site Hacked, Serves up 22 Exploits*, COMPUTERWORLD, Aug. 31, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9033999&intsrc=hm_list (reporting that a Russian gang of cybercriminals is suspected of breaking into the Bank of India web site and using it to install malware on computers of Internet users that visited the web site).

To deploy malicious code, cybercriminals often use extensive spam campaigns[77] utilizing automated spam engines that leverage the tremendous computing power of botnets to send millions of e-mails within a very short period of time making it practically impossible to trace those spam e-mails back to their true originators.[78] Botnets also enable cybercriminals to perform with ease other operations that require tremendous computing power, such as generating unique images for millions of spam e-mails in order to avoid spam filters or breaking encryption and recovering messages, passwords, or data.[79] This computing power poses a very serious threat to the security of online transactions that rely on encryption for ensuring integrity and confidentiality.

E. Mobile Technology: New Frontiers for Financial Institutions and Cybercriminals

In an attempt to increase their customer base and reduce costs, financial institutions constantly look for new delivery channels for their services.[80] As customers demand faster, more convenient services, financial institutions turn to new technologies to expand their customer relationships to compete with other financial services providers.[81]

Many financial institutions view mobile technology as one of the ways to expand their services in an increasingly mobile society.[82] Several banks announced pilot projects to explore the viability of mobile banking and assess customer interest in this new delivery channel.[83] For example, Bank of America launched a service allowing its customers to transfer money and pay bills on mobile de-

77. Labaton, *supra* note 65, at C1 (reporting on a spam campaign launched by unknown cybercriminals where instead of promised revealing pictures of Jennifer Lopez users downloaded malware onto their computers after clicking on a link provided in the e-mail).

78. *See* Claburn et al., *supra* note 69, at 48.

79. *See id.* Cryptanalysis is the science of breaking encryption schemes. *See, e.g.*, Bruce Schneier, *Self-Study Course in Block Cipher Cryptanalysis*, 24 CRYPTOLOGIA 18, 18-33 (2000).

80. Maria Bruno-Britz, *Mobilizing Retail Payments*, BANK SYS. & TECH., Apr. 2007, at 35-36.

81. *See id.*

82. Jane J. Kim, *Mobile Banking Shifts Into Higher Gear*, WALL ST. J., Feb. 21, 2007, at D1.

83. *See* Bruno-Britz, *supra* note 80, at 36. R

vices while Citibank announced an intent to pilot a real-time person-to-person mobile payment service.[84]

At the same time, the rapid growth of wireless and mobile technologies that are much more difficult to secure than their wired counterparts raises serious security concerns among IT professionals and Internet users.[85] Many consumers doubt the security of mobile banking.[86] Recent research shows that security concerns in the United States will likely delay the adoption of mobile banking.[87] Some industry insiders suggest that mobile banking in the United States is still at least five years away.[88]

There are good reasons for these security concerns. The growing popularity of mobile devices and Internet-enabled cell-phones makes them appealing targets for virus writers, bot creators, and malicious hackers.[89] As mobile devices become more technologically sophisticated and widespread, mobile malware becomes more prevalent and dangerous.[90] Experts predict sharp increases in attacks against mobile devices as more financial institutions roll out mobile banking initiatives.[91] While some types of malware creators concentrate their attention exclusively on mobile devices, others attempt to use mobile devices, more vulnerable than conventional computers, as entry points for the penetration of corporate net-

84. *Id.*; *see also* Press Release, Citigroup Inc., Citi & Obopay to Pilot Innovative Mobile Person-to-Person Payment Service (Feb. 28, 2007), http://www.citigroup.com/citigroup/press/2007/070228a.htm).

85. *See, e.g.*, Dan Nystedt, *Wireless Growth in Asia Leads to Security Woes*, IDG NEWS SERVICE, Dec. 13, 2006, *available at* http://www.computerworld.com/action/article/do?command=ViewArticleBasic&articleID=9005978&source=rss_news50.

86. Nancy Feig, *Everyone's Ready for Mobile Banking, Except Consumers*, BANK SYS. & TECH., Mar. 16, 2007, *available at* http://www.banktech.com/blog/archives/2007/03/everyones_ready.html.

87. *See* Bruno-Britz, *supra* note 80, at 36. **R**

88. *See id.*

89. *See, e.g.*, Greenemeier, *Buzz on New Bots*, *supra* note 3, at 44.

90. Jeremy Kirk, *Security Vendor Detects Aggressive Mobile Worm Variant*, IDG NEWS SERVICE, Aug. 4, 2006, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9002213 (reporting that a "security vendor has detected a new variant of an aggressive Russian mobile worm that uses some alarming new tricks").

91. John Blau, *Experts: 2007 Bodes Ill for Mobile Banking*, IDG NEWS SERVICE, Jan. 22, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9008788&source=NLT_SEC&nlid=38.

works.[92] The more connected our society becomes, the more opportunities there are for cybercriminals to launch their attacks.[93]

The growing sophistication of cybercriminals raised serious concerns in the software industry and among companies conducting business online and led to extensive efforts to improve online security. Businesses and individuals that sustained losses from criminal attacks perpetrated over the Internet filed legal actions against companies whose failure to ensure adequate security of their computer systems precipitated the attacks. The next Section explores these issues in more detail.

III. Industry Response and Private Legal Actions Under State Law

Rising losses from cybercrimes have prompted a wide spectrum of industry responses. Software companies have added new security features to their products, patched newly discovered vulnerabilities, and helped law enforcement agencies to investigate Internet crimes. Security vendors and Internet service providers ("ISPs") now offer new products and services aimed at improving security of online transactions. Financial services companies are continuing their efforts to raise awareness of cybercrimes and online security. Businesses and consumers are bringing legal actions in an attempt to recover their losses.

A. Industry Fights Back

Industry concerns about Internet threats and consumer confidence in conducting business online have led to efforts directed at improving security through technological innovation, development of new security standards,[94] and raising awareness of security issues among business leaders and consumers.[95]

92. Cara Garretson, *Mobile Devices Expose Networks to Security Threats*, Network World, Feb. 23, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&taxonomyName=crm&articleId=9011680&taxonomyId=120&intsrc=kc_feat.

93. *See* Greenemeier, *Buzz on New Bots*, *supra* note 3, at 44.

94. *See, e.g.*, James F. Bauerle, *SPeRS Revisited: Establishing Standards to Assure Enforceable Electronic Financial Transactions*, 122 Banking L.J. 1033, (2005); PCI Security Standards Council, Payment Cards Industry Data Security Standard (Sept. 2006), https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf; Darryl K. Taft, *OASIS Approves New Web Services Security Standards*, eWeek.com, Mar. 27, 2007, *available at* http://www.eweek.com/print_article2/0,1217,a=204078,00.asp.

95. *See, e.g.*, Claburn et al., *supra* note 69, at 50.

IT managers in many companies are more cautious now when it comes to protecting their computer systems.[96] Organizations monitor their employees' use of computer resources to detect abuse and fraud.[97] To handle information security breaches, organizations create incident response teams that include not only IT professionals, but also legal counsel to provide guidance and ensure compliance with applicable laws and regulations.[98]

ISPs have expanded their services to help customers protect their computers from spam, malware, phishing attacks, worms, and viruses.[99] Security vendors have developed new software and hardware products and expanded their services to protect networks from criminal attacks.[100] To help individual Internet users keep their computers safe, some security vendors provide free basic versions of their products for personal use,[101] while software vendors provide free security updates for their products and free malware removal tools.[102]

In an attempt to improve the security of their products and to fight cybercrime, software vendors have joined forces with law enforcement agencies. For example, Microsoft worked with the National Security Agency in securing the Windows operating systems.[103] Microsoft's Internet Safety Enforcement team, now a sixty-five person operation, worked on cases involving worms, vi-

96. *See, e.g.*, Mathias Thurman, *Putting the Brakes on Net Integration*, COMPUTERWORLD, Nov. 27, 2006, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=274042 (an IT manager reporting how cautiously his company proceeded on integrating its computer system after an acquisition).

97. C.J. Kelly, *Looking Into What We Can Look Into*, COMPUTERWORLD, Mar. 5, 2007, *available at* http://www.computerworld.com/action/article.do?command=PrintArticleBasic&articleId=283640.

98. *See, e.g.*, Kevin Mandia, *Dissecting the Damage of Hackers*, LEGAL TIMES, Jan. 29, 2007, at 31.

99. *See, e.g.*, Jim Duffy, *Verizon Business Goes Phishing with New Service*, NETWORK WORLD, Mar. 7, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9012500.

100. *See, e.g.*, Claburn et al., *surpra* note 69, at 50 (discussing new information systems security services and appliances); Kirk, *Spam Fight*, *supra* note 54 (reporting on the latest developments in the arms race between security vendors and spammers).

101. *See, e.g.*, Check Point Software Technologies Ltd., Welcome to ZoneAlarm® Downloads, http://www.zonealarm.com/store/content/company/products/znalm/freeDownload1.jsp (last visited Nov. 17, 2007).

102. *See, e.g.*, Microsoft, Windows Update, http://windowsupdate.microsoft.com (last visited Nov. 17, 2007); Microsoft, Malicious Software Removal Tool, http://www.microsoft.com/security/malwareremove/default.mspx (last visited Nov. 17, 2007).

103. Robert McMillan, *NSA Helped Microsoft Set Security for Vista*, COMPUTERWORLD, Jan. 15, 2007, *available at* http://www.computerworld.com/action/article.do?command=PrintArticleBasic&articleId=279002.

ruses, child pornography, typosquatting,[104] botnets, and helped law enforcement track down international cybercriminals.[105]

Pressured by the financial industry and online payment service providers, software vendors have added anti-phishing features to their products.[106] In order to encourage customers to use their online services, financial institutions are working hard to maintain the security of their Web sites while attempting to educate their customers about phishing and other Internet-related scams.[107] RSA Security, a security software vendor, is planning to extend its phishing Web site take-down service to help financial institutions and online merchants detect dangerous Trojans[108] that steal customer financial information. The software will remove the Trojans and shut down the associated Web sites.[109]

The weakest links in the United States payment system continue to be businesses that accept credit and debit card payments and the consumers themselves.[110] To address these issues, the payment card industry requires merchants to comply with stringent information security standards.[111] The enforcement of these standards, however, is not always adequate. For example, the security breach at the TJX Companies, Inc. ("TJX")[112] last year that compromised the credit card information of millions of customers resulted from the merchant storing credit card data in violation of the Visa Operating Regulations[113] and Payment Cards Industry Data Security

104. Typosquatting is a technique that relies on typographical errors made by Internet users when inputting a Web site address into a Web browser to lead users to a Web site owned by a typosquatter. *See* Wikipedia, Typosquatting, http://en.wikipedia.org/wiki/Typosquatting (last visited Nov. 17, 2007).

105. *See* McMillan, *Botnets Top '07 Threat*, *supra* note 64 (reporting that Microsoft helped law enforcement agencies to track down a cybercriminal gang that operated from Bulgaria).

106. *Id.*

107. *See, e.g.*, Citigroup, Learn About Spoofs, http://www.citibank.com/domain/spoof/learn.htm (last visited Nov. 17, 2007).

108. *See supra* note 74 and accompanying text. R

109. Robert McMillan, *RSA to Offer Trojan Take-Down Service*, IDG NEWS SERVICE, Mar. 15, 2007, *available at* http://www.infoworld.com/article/07/03/15/HNrsatrojantakedown_1.html.

110. *See, e.g.*, Richardson v. DSW, Inc., No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005) (customers sued a merchant for damages sustained as a result of a credit card information theft from the merchant's computer system); *ID Theft Is Exploding in the U.S.*, BANK SYS. & TECH., Mar. 7, 2007, http://www.banktech.com/showArticle.jhtml?articleID=198002061.

111. *See, e.g.*, Visa, Cardholder Information Security Program, http://usa.visa.com/merchants/risk_management/cisp_merchants.html (last visited Nov. 17, 2007).

112. *See* The TJX Companies, Inc., http://www.tjx.com (last visited Nov. 17, 2007).

113. *See, e.g.*, Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 32. Visa Operating Regulations do not permit merchants to store or retain credit or debit card

Standard.[114] To prevent such incidents, IBM and Microsoft are working on technological solutions aimed at securing online purchases of goods and services.[115]

Visa, the world's leading credit card payment company, regularly brings together leaders and decision makers from business, government, and technology organizations to discuss security of electronic payments.[116] To help the private sector and government agencies ensure that their information security staff has an up-to-date knowledge of the best industry practices and procedures, several not-for-profit organizations are offering a number of information security certifications and educational resources.[117]

The next Section discusses the role of industry-wide information security standards and looks at the attempts of private parties to hold businesses that failed to comply with the standards accountable for the resulting losses.

B. Industry Information Security Standards and Private Legal Actions Under State Law

In some instances, financial institutions and private individuals bring legal actions under state law to recover damages from merchants and banks that failed to protect customer data stored in their computer systems from unauthorized access and fraudulent use by cybercriminals. Plaintiffs, however, are unlikely to succeed unless they can show damage suffered as a direct consequence of the defendants' failure to protect the data.

For example, in *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, Banknorth, a financial institution, sued the merchant, B.J.'s Wholesale Club ("B.J.'s"), and Fifth Third Bank, B.J.'s acquiring bank, which processed debit card payments on B.J.'s behalf, for breach of

numbers. *See also* Banknorth, N.A. v. BJ's Wholesale Club, Inc., 394 F. Supp. 2d 283, 284 (D. Me. 2005).

114. PCI SECURITY STANDARDS COUNCIL, PAYMENT CARDS INDUSTRY DATA SECURITY STANDARD (2006), http://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf.

115. *See* Brian Prince, *IBM Shields Online Personal Data*, EWK., Feb. 5, 2007, at 27 (reporting that IBM is working on a new software product that will allow customers to purchase items without revealing their identity).

116. *See* Matt Hines, *Visa Summit Gathers Players in E-Payments Industry*, INFOWORLD, Mar. 7, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9012490.

117. *See, e.g.*, International Information Systems Security Certification Consortium, (ISC) Credential Examinations, http://www.isc2.org/cgi-bin/content.cgi?category=700 (last visited Nov. 17, 2007); ISACA, CISA (Certified Information Systems Auditor), CISM (Certified Information Security Manager), http://www.isaca.org/certification (last visited Nov. 17, 2007).

contract and negligence to recover losses suffered by Banknorth when criminals stole their customers' debit card information stored in B.J.'s computers.[118] The defendants retained customer debit card information in violation of the Visa Operating Regulations and failed to protect it from theft.[119] Banknorth also brought an equitable subrogation claim alleging that since it reimbursed its cardholders for the fraudulent purchases that resulted from defendants' negligence, it should recover from the defendants in place of the cardholders.[120] The defendants moved to dismiss Banknorth's complaint.[121] The court found that each claim involved a factual dispute beyond the scope of the motion to dismiss and denied the plaintiff's motion.[122]

Later, however, on the defendants' motion, the case was transferred to the United States District Court for the Middle District of Pennsylvania where two other cases arising from similar circumstances were already pending.[123] The district court granted the defendants' motion to dismiss for failure to state a claim.[124]

The court held that Banknorth's contract claim failed because it was not a third-party beneficiary of the contracts between the defendants, B.J.'s and Fifth Third Bank, or between B.J.'s and Visa U.S.A.[125] The court also held that the economic loss rule barred Banknorth's negligence claim because Banknorth did not allege any damages and only sought to recover for its economic losses.[126] Banknorth's equitable subrogation claim also failed because the court found that Banknorth paid its customers on its own obligation and not on its customers' obligation from B.J.'s.[127] The court also dismissed all complaints in the other two cases against B.J.'s and Fifth Third Bank on similar grounds holding that there was no legal basis for the relief sought by the plaintiff.[128]

---

118. 394 F. Supp. 2d at 284-85.
119. *Id.*
120. *Id.* at 287.
121. *Id.* at 284.
122. *Id.* at 285-88.
123. Banknorth, N.A. v. BJ's Wholesale Club, Inc., 442 F. Supp. 2d 206, 207-08, 210-16 (M.D. Pa. 2006). The two other pending cases were Sovereign Bank v. BJ's Wholesale Club, Inc., 395 F. Supp. 2d 183 (M.D. Pa. 2005) and Pa. State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317 (M.D. Pa. 2005). *Id.*
124. *Banknorth*, 442 F. Supp. 2d at 208.
125. *Id.* at 210-11.
126. *Id.* at 211-14.
127. *Id.* at 214-16.
128. *See* Pa. State Employees Credit Union v. Fifth Third Bank, Civil No. 1:CV-04-1554, 2006 WL 1724574 (M.D. Pa. June 16, 2006) (dismissing the claim against the bank); Sovereign Bank v. BJ's Wholesale Club, Inc., Civil No. 1:CV-05-1150, 2006 WL

The attempts of individual plaintiffs to institute class action suits against merchants who failed to protect customers' credit card information have not had much success either. In *Richardson v. DSW, Inc.*,[129] and *Hendricks v. DSW Shoe Warehouse, Inc.*,[130] customers attempted to institute class actions against a shoe retailer who failed to protect customers' personal information stored in its computer systems from theft. The customers sought a reimbursement of credit monitoring service fees incurred attempting to protect themselves from identity theft after learning about the security breach.[131] The *Richardson* court, however, rejected all of the plaintiff's recovery theories except for her implied contract claim,[132] while the *Hendricks* court dismissed the whole complaint, distinguishing *Richardson v. DSW, Inc.* and holding that the plaintiff failed to allege cognizable damages.[133]

From the perspective of these cases, it is unlikely that attempts to hold businesses accountable for information security breaches under state law will have a noticeable effect on improving security of online transactions. As the cases discussed in this Section illustrate, although the existence of industry standards, such as the Visa Operating Regulations, provide some reassurance to the consumers, they do not guarantee adequate information security since the enforcement of such standards is not uniform. Moreover, plaintiffs who suffer losses as a result of noncompliance with the standards are often unable to hold the parties responsible for the breach accountable. The next two Sections discuss the role of the federal government in improving online security.

IV. The Role of the Federal Government

A. Criminal Prosecution of Internet-related Offenses Reveals a Lack of Security

Criminal prosecution plays an important role in securing online transactions by holding perpetrators of cybercrimes accountable and deterring future crimes. Since theft laws are perceived to be

1722398 (M.D. Pa. June 16, 2006) (dismissing the claim against the bank); *Banknorth*, 442 F. Supp. 2d 206 (dismissing all claims against the merchant); Sovereign Bank v. BJ's Wholesale Club, Inc., 427 F. Supp. 2d 526 (M.D. Pa. 2006) (dismissing all claims against the merchant); *Pa. State Employees Credit Union*, 398 F. Supp. 2d 317 (dismissing all claims against the merchant).

129. No. 05 C 4599, 2005 WL 2978755 (N.D. Ill. Nov. 3, 2005).

130. 444 F. Supp. 2d 775 (W.D. Mich. 2006).

131. *Id.* at 775.

132. *Richardson*, 2005 WL 2978755 at *20-21.

133. *Hendricks*, 444 F. Supp. 2d at 781.

inadequate for the prosecution of cybercrimes, between 1978 and 1999 all fifty states and the federal government enacted computer misuse statutes.[134] Although the statutes differ in their approaches, they usually contain a basic prohibition against unauthorized access to computer systems, supplemented with additional elements to define specific criminal offenses.[135]

In 1984 Congress enacted the first version of the federal computer misuse statute—the Computer Fraud and Abuse Act ("CFAA").[136] The statute was intended to protect computers used by the federal government and financial institutions.[137] In 1986, Congress amended the CFAA to add protection for "federal interest computers."[138] The 1986 amendments included a replacement of the phrase "federal interest computer" with "protected computer."[139] Since any computer used in interstate commerce or communications became a "protected computer" within the meaning of the statute, the amendments extended the statutory protection to computers owned by state or local government entities and private parties.[140] The statute applies even if all involved computers are located in the same state.[141]

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA Patriot Act"),[142] the Cyber Security Enhancement Act of 2002,[143] and the Computer Software Privacy and Control Act of 2003[144] included further changes to the CFAA. Responding to the growing concerns about cyberterrorism and cybercrimes, the new legislation made it a criminal act to knowingly transmit a computer program, code, or command that results in damage to a protected

134. *See, e.g.*, 18 U.S.C.A. § 1030 (West 2007); ORIN S. KERR, COMPUTER CRIME LAW 27 (2006).

135. KERR, *supra* note 134, at 28.

136. Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, tit. II, § 2102(a), 98 Stat. 2190 (1984).

137. *See id.* The statute made accessing classified information without authorization a felony. It also made unauthorized access to financial records or trespass into a government computer a misdemeanor. S. REP. NO. 99-432, at 3 (1986).

138. *See, e.g.*, Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

139. *See id.* at 1128.

140. *See, e.g.*, Ryan P. Allace et al., *Computer Crimes*, 42 AM. CRIM. L. REV. 223, 229-30 (2005).

141. *See id.* at 230.

142. USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

143. Cyber Security Enhancement Act of 2002, Pub. L. No. 107-296, § 225, 116 Stat. 2135, 2156 (2002).

144. Computer Software Privacy and Control Act, H.R. 4255, 108th Cong. (2003).

computer regardless of whether the access to the protected computer was authorized.[145] The statute also criminalized unauthorized access that damages a protected computer even if the intruder did not intend to cause the damage.[146] In addition, the statute penalized intentional unauthorized access to a protected computer where the intruder obtained information from the protected computer.[147]

The CFAA also provides victims of computer crimes with a limited private cause of action for losses suffered.[148] The plaintiff can bring a civil action either for acts where the defendant intentionally accessed a protected computer and caused losses during any one-year period of at least $5000 or, in more rare cases, where the defendant's acts caused modification or impairment of medical records, physical injury, a threat to public safety, or damaged a government computer system.[149]

To complement the computer crime specific legislation, Congress amended traditional criminal statutes to include crimes that involved computers and included enhanced sentences for crimes committed with the help of computers.[150] For example, the Sentencing Guidelines allow longer sentences for defendants that used special skills—which includes computer skills—in the commission of a crime.[151] As the Ninth Circuit explained in *United States v. Mainard*:

---

145. *See* Allace et al., *supra* note 140, at 231-32.

146. *See id.* at 232.

147. The statute provides:

> (a) Whoever . . .
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
> (B) information from any department or agency of the United States; or
> (C) information from any protected computer if the conduct involved an interstate or foreign communication . . . .

18 U.S.C.A. § 1030(a)(2) (West 2007). This is the most frequently charged section 1030 crime. KERR, *supra* note 134, at 28.

148. 18 U.S.C.A. § 1030(g) (West 2007).

149. 18 U.S.C.A. § 1030(a)(5)(B) (West 2007). In practice, for example in spyware cases, the $5000 threshold often prevents plaintiffs from bringing their civil actions under the CFAA. *See, e.g.*, Michael D. Lane, Note, *Spies Among Us: Can New Legislation Stop Spyware from Bugging Your Computer?*, 17 LOY. CONSUMER L. REV. 283, 293 (2005).

150. *See* Lane, *supra* note 149, at 229; *see also* Katyal, *supra* note 11 (arguing in favor of stricter penalties when computers are used to commit crimes).

151. U.S. SENTENCING GUIDELINES MANUAL § 3B1.3 (2005).

> In a sense, abuse of a special skill is a special kind of abuse of trust. It is a breach of the trust that society reposes in a person when it enables him to acquire and have a skill that other members of society do not possess. . . . When the person turns those skills to evil deeds, a special wrong is perpetrated upon society, just as other abuses of trust perpetrate a special wrong upon their victims.[152]

Law enforcement agencies have successfully apprehended and prosecuted a number of individuals under the CFAA for unauthorized access and misuse of computer systems. For example, in *United States v. Phillips*,[153] a University of Texas student, in violation of the University's acceptable computer use policy, gained unauthorized access to government and private computers and managed to accumulate a large volume of personal and proprietary data, such as credit card and bank account information, birth records, passwords, and Social Security numbers. When the University's Information Security Office learned about the suspicious Internet activities of the student, it issued several warnings but took no meaningful action.[154] Moreover, the University admitted Phillips, then an undergraduate student, to its graduate computer science program.[155] After Philips caused numerous crashes of university computer systems, the University finally contacted the Secret Service.[156] Phillips was convicted in a jury trial on one count of computer fraud under the CFAA[157] and one count of possession of an identification document containing stolen Social Security numbers[158] and was sentenced to five years probation, five hundred hours of community service, and a restitution of $170,056.[159]

Although major financial services companies, which are heavily regulated and audited by the government, generally provide much better security for their computer systems than less regulated businesses, some smaller players in the financial services industry may have insufficient information security controls.[160] For example, in *United States v. Marles*, the defendant, a former employee of a credit card company, gained unauthorized access to his personal

152. 5 F.3d 404, 406 (9th Cir. 1993).
153. 477 F.3d 215, 218 (5th Cir. 2007).
154. *Id.* at 217-18.
155. *Id.* at 217.
156. *Id.* at 218.
157. 18 U.S.C.A. § 1030(a)(5)(A), (B)(i) (West 2007).
158. *Phillips*, 477 F.3d at 218; *see also* 18 U.S.C.A. § 1028(a)(6) (West 2007).
159. *Phillips*, 477 F.3d at 218-19.
160. *See infra* Part IV.B for a discussion of government regulation of information security.

account using the expertise he gained as an employee and fraudulently increased his credit line to be able to transfer balances from his higher interest rate credit cards.[161] The defendant pleaded guilty to computer fraud and was sentenced under the CFAA.[162] Clearly, the credit card company did not have proper access controls in place to prevent former employees from accessing its computer systems.

In *United States v. Willis*, the Tenth Circuit upheld a conviction under the CFAA[163] of a debt collecting agency employee who provided criminals with access credentials to a LexisNexis™ Web site, which enabled the criminals to commit identity theft and credit card fraud.[164] Apparently, the employee was the sole person responsible for creating and revoking LexisNexis™ access privileges of the debt collecting agency employees,[165] a clear violation of basic information security principles.[166]

United States v. Ivanov was a rare case where United States law enforcement successfully apprehended and prosecuted a foreign hacker in the United States under the CFAA for conspiracy, computer fraud, extortion, and possession of unauthorized access devices.[167] The hacker broke into a U.S. financial transaction processing company's computer systems and demanded payment for his assistance in making those systems secure.[168] The company's failure to secure its computer systems made the break-in possible.

Despite these successful prosecutions, many cybercrimes go unpunished because of the immense technical complexities in investigating these crimes and finding their perpetrators.[169] Nevertheless, criminal prosecution of online fraud serves as a deterrent contributing to the security of online transactions. As will be discussed in Part V, crime prosecution together with government regulation

161. 408 F. Supp. 2d 38 (D. Me. 2006).
162. *Id.* at 39.
163. *See* U.S.C.A. § 1030(a)(2)(C), (c)(2)(B)(iii) (West 2007).
164. 476 F.3d 1121, 1123 (10th Cir. 2007).
165. *Id.*
166. One of the basic information security principles is a separation of duties where no employee can single-handedly perform a critical business function. For example, creation of access credentials must require participation of one or more additional employees or supervisors who verify the legitimacy of the action and approve it. *See, e.g.*, David Ferraiolo & Richard Kuhn, *Role-Based Access Controls* (National Institute of Standards and Technology 1995), *available at* http://hissa.nist.gov/rbac/paper/rbac1.html.
167. 175 F. Supp. 2d 367, 369 (D. Conn. 2001).
168. *Id.*
169. *See, e.g.*, Katyal, *supra* note 11, at 1074-75.

and private legal actions constitute an integral element of an effective cybercrime prevention scheme.

B. The Financial Industry as an Example of Government Regulation of Information Security

Extensive government regulation reaches practically all aspects of the financial industry, including information security.[170] Financial institutions are constantly working on improving the security of their online systems in order to ensure compliance with government regulation and make their clients feel safe online.[171]

The Federal Financial Institutions Examination Council ("FFIEC") prescribes uniform principles, standards, and examination procedures to promote consistency in the supervision of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.[172] The FFIEC Information Technology Examination Handbook (the "Handbook") consists of several booklets that cover various aspects of financial institutions' information technology operations.[173] The Handbook provides a framework for the examination of financial institutions' information technology infrastructure by government agencies;[174] and provides guidance to financial institutions in their day-to-day technology operations.[175] The Information Security booklet of the Handbook contains more than a hundred pages addressing all aspects of information security governance, policies, procedures, and their implementation.[176]

FFIEC views information security as an ongoing process, where financial institutions should have proper controls in place to pro-

170. The major legislative acts regulating financial institutions include the Bank Service Company Act, 12 U.S.C. § 1867(c); Bank Protection Act, 12 U.S.C. § 1882; Fair and Accurate Credit Transactions Act, 15 U.S.C. §1681w; Gramm–Leach–Bliley Act, 15 U.S.C. § 6801 and § 6805(b); Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Supervising agencies implement these legislative acts through regulations and guidance letters.

171. *See, e.g.*, Singer, *supra* note 10, at 19.

172. *See* FFIEC Web site, http://www.ffiec.gov (last visited Nov. 17, 2007).

173. FFIEC, INFORMATION TECHNOLOGY EXAMINATION HANDBOOK, http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html (last visited Nov. 17, 2007).

174. *See id.*

175. *See id.*

176. *See* FFIEC, IT EXAMINATION HANDBOOK, INFORMATION SECURITY (2006), http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

vide effective day-to-day management of information security and appropriate responses to changing threats, business conditions, and new technologies.[177] Financial institutions must identify and manage security risks by implementing appropriate countermeasures, testing the implementations, and subsequently monitoring residual risks.[178] With great detail, FFIEC specifies other aspects of information security, such as access controls, including the administration of access rights, user authentication, use of encryption, prevention of malicious code, software development practices, personnel security, including background checks and screening, data security, intrusion detection, security incident response practices, management of outsourced systems, and physical security of the premises.[179]

To strengthen IT compliance, FFIEC prescribes internal audit procedures for financial institutions.[180] In addition, the supervising government agencies conduct regular audits of financial institutions within their sphere of responsibility and, in the case of violations, take appropriate enforcement actions.[181]

This process ensures that financial institutions comply with all applicable laws and regulations, including government-mandated information security standards. While this extensive regulation is necessary to ensure stability and security of the national financial system and to prevent crimes, including online fraud, it is very expensive for both the government and financial institutions.

V. Discussion: A Case for Federal Information Security Legislation

A. Market-based Approach to Information Security

Despite the efforts of the software companies and financial services industry to improve security of online transactions,[182] some observers are skeptical about the industry's ability to do so.[183] They point out that the industry is predominantly concerned about

177. *See id.* at 1.

178. *See id.* at 10-15.

179. *See id.* at 22-95.

180. FFIEC, IT Examination Handbook, Audit (2003), http://www.ffiec.gov/ffiecinfobase/booklets/audit.pdf.

181. For example, Office of the Comptroller of the Currency regulates national banks, federally chartered branches, and agencies of foreign banks. *See* FFIEC, Enforcement Actions and Orders, http://www.ffiec.gov/enforcement.htm (last visited Nov. 17, 2007).

182. *See supra* Part III.A for a discussion of these efforts.

183. *See, e.g.*, Charney, *supra* note 2, at 945.

its bottom line and uses return-on-investment as the main metric that drives business decisions.[184] There are good reasons for this skepticism. For example, in their cost reduction effort, United States corporations, including major financial institutions, increasingly send work abroad together with sensitive personal and financial information about their customers.[185] This inevitably increases the risk of security breaches and identity theft.[186]

Numerous security breaches show that many companies still do not take the security of their computer systems seriously enough. The 2006 theft of 45.6 million credit card numbers and personal information of approximately 451,000 individuals from TJX was the biggest information security breach in history.[187] In March 2007, law enforcement agencies in Florida arrested several individuals suspected to be part of a fraudulent scheme that used credit card information stolen from TJX.[188] According to Mark Pullen, a manager at RSA Security, by 2010 many industries will have to deal with the same security issues that threaten online financial transactions today, and most will not be ready for the challenge.[189]

---

184. *See id.*

185. *See, e.g.*, Stan Gibson, *No Retreat: Continue Outsourcing Despite Global Terror*, EWEEK.COM, July 19, 2006, *available at* http://www.eweek.com/article2/0,1759,1991268,00.asp.

186. *See* Samantha Grant, *"I Just Bought a Flat Screen T.V. in Kolkata?" Application of Laws for International Outsourcing Related Identity Theft*, 11 PGH J. TECH. L. & POL'Y 1, 2-5 (2006).

187. *See* Jaikumar Vijayan, *TJX Data Breach: At 45.6M Card Numbers, It's the Biggest Ever*, COMPUTERWORLD, Mar. 29, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9014782. Recent information indicates that, contrary to the numbers TJX disclosed to the Securities and Exchange Commission in March of 2007, the security breach may have compromised as many as ninety-four million accounts. *See* Jaikumar Vijayan, *Update: TJX Victim Tally Rises to 94M*, COMPUTERWORLD, Oct. 29, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=306333&source=NLT_SEC&nlid=38. The future will show whether the action that a number of financial institutions recently filed against TJX will share the fate of similar suits against B.J.'s. *See* Jaikumar Vijayan, *Scope of TJX data breach doubles: 94M cards now said to be affected*, COMPUTERWORLD, Oct. 24, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9043944&pageNumber=1 (reporting that a number of financial institutions are seeking a class action certification for the lawsuit they filed against TJX in Boston, Massachusetts, seeking compensation for the losses they suffered as a result of the breach); *see also supra* Part III.B for a discussion of suits against B.J.'s in 2005 and 2006.

188. Matt Hines, *Stolen TJX Data Used in Florida Crime Spree*, INFOWORLD, Mar. 21, 2007, *available at* http://www.computerworld.com/action/article.do?command=ViewArticleBasic&articleId=9013942.

189. Michael Crawford, *2010: A Security Odyssey*, COMPUTERWORLD AUSTL., Nov. 16, 2006, *available at* http://www.computerworld.com/action/article.do?command=

From a cost-benefit perspective, it may cost a financial institution or a merchant less to accept, at least to some extent, online fraud as a business risk and to reimburse customers who suffer losses, rather than to implement and maintain a comprehensive information security infrastructure. From a public policy perspective, however, it is desirable to ensure adequate private sector spending on information security in order to reduce identity theft threats from organized crime and terror networks.[190] Ultimately, consumers will have to foot the bill whether businesses spend money paying off cybercriminals, or on improving the security of conducting business online.

Despite the widely publicized efforts of software vendors to improve security of their products,[191] software industry observers reported forty percent more security vulnerabilities in 2006 than in 2005, with the major software companies being the biggest offenders.[192] Some software vendors use what amounts to security defects in their products to force customers to subscribe to their paid update services or to pay for upgrades to newer versions of their products by discontinuing security fixes for the older ones.[193] Other software vendors use security concerns to create new revenue streams by offering new products instead of spending money on improving the security of their existing product offerings.[194]

The growing sophistication of cybercriminal attacks and the apparent inability of the software industry to prevent them because of the inherent conflict of interests between performance-based metrics and solid but inevitably expensive information security programs suggests that technology alone is unable to resolve the current security issues.

The next Section continues this discussion with an overview of the difficulties facing law enforcement agencies charged with investigating cybercrimes and bringing the perpetrators to justice. The discussion suggests that these difficulties significantly diminish the

---

ViewArticleBasic&taxonomyName=Spam__Malware_and_Vulnerabilities&articleId=9005164&taxonomyId=85&intsrc=kc_li_story.

190. *See supra* Part I.A.

191. *See supra* Part III.A for a discussion of these efforts.

192. Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 39 (reporting that in 2006 the number of detected security vulnerabilities in software products reached 7247).

193. *See, e.g.*, Douglas A. Barnes, *Deworming the Internet*, 83 TEX. L. REV. 279, 295-97 (2004).

194. *See, e.g.*, *id.*

deterrent effect of criminal prosecution, especially when criminals launch their attacks from overseas.

B. Criminal Prosecution

Criminal investigations of complex cybercrimes require extensive resources and specialized technical expertise.[195] Industrialized production of increasingly sophisticated malware makes it even more difficult for law enforcement to investigate cybercrimes.[196] To reduce the risk of being caught and to thwart criminal investigations, malware creators developed anti-forensic software designed to remove all traces of the intrusion, thus further complicating investigations.[197]

Moreover, despite a number of successful prosecutions of cybercriminals,[198] law enforcement agencies cannot keep up with the growing cyberthreat because of its transnational nature.[199] Consequently, law enforcement agencies must rely on the cooperation of the private sector and foreign governments in their fight against cybercrime.[200] For example, last year, FBI Cyber Action teams relied on the cooperation of Microsoft and other private and public organizations in tracing the attack of the Zotob malware to a credit card theft ring in Morocco and Turkey.[201] Relying on this assistance, the FBI was able to help local authorities track down and arrest some of the perpetrators.[202]

Although courts have upheld the extraterritorial application of the CFAA,[203] when cybercriminals perpetrate malicious acts in the United States from overseas, law enforcement agencies are often

195. *See, e.g.*, Katyal, *supra* note 11, at 1071-75.

196. *See supra* Part I.B for a discussion of commercialized production and distribution of hacker tools.

197. Kelly Jackson Higgins, *Tools Fight Forensics*, DARK READING, Mar. 19, 2007, http://www.darkreading.com/document.asp?f_src=dr_csi_one&doc_id=119806.

198. *See supra* Part IV.A.

199. *See, e.g.*, Greenemeier & Hoover, *Hacker Economy*, *supra* note 20, at 39.

200. *See, e.g.*, Federal Bureau of Investigation, FBI Cyber Action Teams Traveling the World to Catch Cyber Criminals (Mar. 6, 2006), http://www.fbi.gov/page2/march06/cats030606.htm.

201. *See id.*

202. *Id.*

203. *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001) (noting that Congress intended the CFAA to be applied extraterritorially and upholding the indictment under the CFAA where a Russian hacker broke into computers in the United States while he was physically located in Russia). Some commentators argue against this broad interpretation of the statute. *See, e.g.*, Mark Rasch, *Ashcroft's Global Internet Power-Grab*, BUS. WK., Nov. 26, 2001, *available at* http://www.businessweek.com/technology/content/nov2001/tc20011126_6812.htm.

unable to investigate the perpetrators, apprehend them, and bring them to justice.[204] "The fundamental issue is that we have a law enforcement model that's geographically based, but there's no geography on the Internet," explained Dan Kaminsky, a security expert with DoxPara Research.[205] Since cybercriminals can quickly destroy forensic evidence of their malicious acts, the investigation of cybercrimes requires swift and decisive actions by law enforcement agencies. United States law enforcement, however, may not be able to wiretap criminals overseas or conduct searches, seizures, or arrests without the close and timely cooperation of local authorities.[206] The cooperation of local authorities varies widely from country to country and depends, for example, on the existence of a mutual legal assistance agreement between a particular foreign country and the United States.[207] In the absence of a mutual legal assistance agreement, which makes assistance obligatory, in order to obtain evidence from a foreign country, American law enforcement agencies have to rely on letters rogatory, a judicial procedure enabling one country to request judicial assistance from another on a basis of comity.[208] The U.S. Justice Department warns, however, that this process may take a year or more, and even in urgent cases, will likely take more than a month.[209]

All this undermines the deterrent and retributional effects of federal criminal law with regard to domestic, and especially, foreign cybercriminals. To compensate for this, some academic authors suggest steeper penalties for online crimes.[210] As discussed in the next Section, however, a better approach would be to focus primarily on the prevention of cybercrimes with criminal prosecution, with civil litigation playing an important but secondary role in ensuring online security.

---

204. *See, e.g.*, Katyal, *supra* note 11, at 1074-75.

205. *See* Greenemeier & Hoover, *Hacker Economy, supra* note 20, at 38-39. **R**

206. *See id.* at 39.

207. See for example, Bruce Zagaris, *Uncle Sam Extends Reach for Evidence Worldwide*, 15 CRIM. JUST. 4 (2001), for a detailed discussion of mutual legal assistance agreements.

208. *See id.*

209. *See* KERR, *supra* note 134, at 602 (quoting U.S. DEPT. OF JUST., U.S. ATT'YS MANUAL, CRIMINAL RESOURCE MANUAL § 275 (1997)).

210. *Id.* Other authors are skeptical, however, about the deterrent effect of such proposals. *See, e.g.*, Paul H. Robinson & John M. Darley, *The Role of Deterrence in the Formulation of Criminal Law Rules: At Its Worst When Doing Its Best*, 91 GEO. L.J. 949, 954-55 (2003).

C. The Role of Government Regulation and Private Legal Actions in Enforcing Information Security

The common theme of the criminal and civil cases discussed in Parts III and IV was the systematic failure of businesses, universities, and other organizations to follow sound information security policies and procedures, maintain an adequate level of information security, and protect their computer systems from unauthorized access by insiders, former employees, and malicious hackers located in the United States and abroad.[211] Due diligence in maintaining information system security would have prevented most of these cybercrimes and made fraudulent transactions virtually impossible.

As discussed above, market forces alone will likely be insufficient to ensure adequate security of online transactions.[212] Government-mandated information security standards can help achieve this goal. Extensive government regulation of information security in financial institutions already plays a critical role in ensuring safety of online financial transactions.[213] Government regulation of information security combined with private enforcement of government-mandated information security standards and vigorous prosecution of computer crimes may be the optimal and cost-effective solution for improving the security of online transactions.

1. *Enforcing Information Security Through Private Legal Actions Under Current Law*

The threat of private actions by defrauded individuals and business organizations against negligent businesses and government agencies that failed to protect their confidential information may force organizations to treat information security issues seriously.[214] In such actions, however, plaintiffs face multiple challenges.

Usually the plaintiff has to show damages that resulted from the defendant's failure to provide adequate protection for plaintiff's personal data.[215] Also, in most cases losses from Internet crimes

211. *See, e.g.*, United States v. Zenski, 125 F.3d 845 (2d Cir. 1997) (successful prosecution of criminal group that used a hacker to break into computer systems and steal credit card information for subsequent use in fraudulent transactions); United States v. Petersen, 98 F.3d 502 (9th Cir. 1996) (successful prosecution of a hacker for credit card and other computer-related fraud).

212. *See supra* Part V.A.

213. *See supra* Part IV.B.

214. *See supra* notes 110-113 and accompanying text. R

215. Hendricks v. DSW Shoe Warehouse, Inc., 444 F. Supp. 2d 775 (W.D. Mich. 2006) (dismissing a class action where the plaintiff attempted to recover for the cost of

do not exceed one thousand dollars.[216] Therefore, it is impractical for an individual plaintiff to sue a negligent party that failed to secure plaintiff's personal information unless the plaintiff's damages resulted from a massive security breach and the plaintiff can bring her suit as a class action on behalf of all similarly affected individuals.

Plaintiffs who attempt to bring such class actions, however, face numerous obstacles in pursuing their claims. For example, despite the global nature of the Internet, plaintiffs usually have to bring their class actions under state law, where differences in substantive law and choice of law rules across states may prevent the plaintiffs' attempts to certify their suits as nationwide class actions.[217]

2. *Imposing Tort Liability on the Software Industry*

Some commentators argue that the software industry is mature enough to be held strictly liable in tort for damages caused by defects in its products.[218] The likely response from the computer industry would be to market devices with very limited functionality. This strict liability approach is appropriate for specialized devices, combining both hardware and software components and intended for very specific purposes, such as medical monitoring devices, power plant control systems, or network security appliances. In this case, the imposition of liability on the manufacturers of such devices for injuries and damage caused by their failure is certainly justified by the need to compensate victims and ensure reliability of the device's software and hardware components.

---

credit monitoring and identity theft prevention after the theft of customer information from defendant's computers).

216. NATIONAL WHITE COLLAR CRIME CENTER & FEDERAL BUREAU OF INVESTIGATION, *supra* note 18, at 8 (reporting that the median dollar loss from Internet crimes in 2006 was $724).

217. *See generally* Richard H. Acker, *Choice-Of-Law Questions in Cyberfraud*, 1996 U. CHI. LEGAL F. 437 (1996); *see also* Drooger v. Carlisle Tire & Wheel Co., No. 1:05-CV-73, 2006 WL 1008719, at *22 (W.D. Mich. Apr. 18, 2006) ("[I]f this case were certified as a nationwide class action, the Court would have to try the case under the laws of the 50 states. . . . While not necessarily the death knell to certification, a nationwide class under every state's law would only be permissible were there no conflicts of law."); Michael Ena, Comment, *Choice of Law and Predictability of Decisions in Product Liability Cases*, 34 FORDHAM URB. L.J. 1417 (2007) (pointing out that choice of law rules adopted by a particular state may limit plaintiffs' ability to bring their suits as class actions in that state).

218. Frances E. Zollers et al., *No More Soft Landings for Software: Liability for Defects in an Industry that Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 780-82 (2005).

A strict liability approach, however, is not appropriate for today's general-purpose computers and the software designed to run on them. Imposition of such liability will make software prohibitively costly or significantly reduce the wide variety of features offered by today's software products and impede the flexibility computer owners enjoy in picking and choosing software for their computers. At this time, neither consumers, legislators, nor the software industry itself seem ready for the imposition of across-the-board liability for defects in software products.

3. *Private Actions as a Means of Improving Information Security Practices at Government Agencies*

Attempts to use private actions to improve information security in government agencies did not bring much success either. For example, in *Cobell v. Kempthorne*, beneficiaries of Individual Indian Money trust accounts held by the United States government brought an action under the Administrative Procedure Act[219] and the common law of trusts[220] against the federal government trustee seeking *inter alia* injunctive relief to force the Department of the Interior to disconnect from the network computer systems holding Indian trust data to protect its integrity and confidentiality.[221] Despite the shameful state of information system security at the Department of the Interior,[222] the D.C. Circuit overturned the preliminary injunction granted by the district court due to a lack of an "imminent threat" or "specific reason" to be concerned that the trust data stored in the Department's computers was a target.[223] Unfortunately, the *Cobell* court did not understand that any personal or financial information stored in any computer system connected to the Internet is a target for malicious hackers who are constantly probing computer systems for vulnerabilities in an attempt to gain unauthorized access to information and exploit it for illegal financial gains.

---

219. 5 U.S.C.A. § 706 (West 2007).

220. *See, e.g.*, U.S. v. Mitchell, 463 U.S. 206, 226 (1983) ("It is well established that a trustee is accountable in damages for breaches of trust." (citing RESTATEMENT (SECOND) OF THE LAW OF TRUSTS §§ 205-212 (1959))).

221. 455 F.3d 301 (D.C. Cir. 2006). The plaintiffs relied on the common law of trusts and the Administrative Procedure Act, which allows courts to compel an administrative agency action that is unlawfully or unreasonably withheld. *Id.* at 304.

222. *Id.* at 308-10 (citing numerous vulnerabilities in the Interior's computer systems reported by several information security contractors who conducted penetration tests).

223. *Id.* at 315-17.

4. *Civil Remedies Under the Computer Fraud and Abuse Act*

Overall, given the global nature of the Internet, state civil remedies that vary from state to state cannot serve as a way of enforcing and promoting consistent information security measures aimed at prevention of online fraud.

Federal civil remedies provided by the CFAA, however, are more closely aligned with the cross-jurisdictional nature of the Internet. But in many cases perpetrators of cybercrimes are either judgment proof, impossible to locate, or the total cost of litigation far exceeds the value of the remedy the court provides. For example, in *Tyco International (U.S.) Inc. v. John Does, 1-3*, the plaintiff, an ISP, sued a spammer for overloading the ISP's e-mail servers, alleging trespass to chattels and violation of the CFAA.[224] The ISP sought to enjoin the spammer from accessing its computer systems under the CFAA[225] and to recover damages, attorney's fees, and costs.[226] The court granted the injunction, awarded $10,621 in damages and costs, and denied recovery of attorney's fees.[227] The ISP, however, spent $136,000 just to track down the spammer.[228] As the *Tyco* case shows, the ex post compensatory damages and injunctive relief that the CFAA provides[229] are unlikely to make most of the victims of cybercrimes whole since the perpetrators are usually either judgment proof or very difficult, if not impossible, to locate and bring to justice. Therefore, suggestions to focus legislative effort on the new means used to perpetrate cybercrimes or on the consequences of such crimes rather than the inadequate security measures that made those crimes possible[230] will not yield effective means for combating and prevent cybercrimes.

224. No. 01 Civ.3856(RCC), 2003 WL 23374767, at *1 (S.D.N.Y. Aug. 23, 2003).

225. 18 U.S.C.A. § 1030(g) (West 2007). The statute provides: "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief . . . ." *Id.*

226. *Tyco Int'l (U.S.) Inc.*, 2003 WL 23374767, at *1.

227. *Id.* at *7.

228. *Id.* at *1.

229. 18 U.S.C.A. § 1030(g) (West 2007).

230. *See, e.g.*, Susan W. Brenner, *Law in an Era of Pervasive Technology*, 15 WIDENER L.J. 667, 768-84 (2006) (criticizing the reactive approach of the federal legislature to the emerging technology trends where new legislation focuses on new ways to perpetrate criminal acts and suggesting that instead the legislative efforts should focus on the harm resulting from cybercrimes).

5. *Proposal for Federal Information Security Legislation*

According to recent research, sixty percent of information security incidents between 1980 and 2006 resulted from organizational mismanagement.[231] Moreover, most of the thirty-one percent of breaches attributed to hackers[232] likely resulted from failures of organizations to maintain adequate security of their networks and computer systems. Therefore, businesses and government institutions can eliminate most of the security breaches by adhering to sound information security practices. Given the cross-jurisdictional nature of the Internet, there is a need for federal legislation mandating information security standards for online transactions to ensure consistent implementation and enforcement of information security policies and procedures across the country, including collection, storage, and dissemination of personally identifiable information.[233]

First, ex post remedies are usually inadequate to compensate victims of computer crimes. Therefore, if a particular organization stores personal or financial information in computer systems lacking adequate security and protection from unauthorized access, even before any security breach occurs, the affected individuals should have a right under federal law to seek injunctive relief and force the organization to fix security issues or refrain from collecting and storing sensitive data.

Second, federal law should also provide victims of cybercrimes with a right to hold organizations accountable for the harm caused by cyberattacks launched from their negligently maintained com-

231. Lisa Vaas, *Corporations Bear Brunt of Blame*, EWK., Apr. 2, 2007, at 17. This does not mean that all these incidents resulted in actual damage to the individuals and organizations whose information was compromised. For example, information on lost magnetic media or stolen laptop computers does not necessarily end up in the hands of cybercriminals willing to exploit it.

232. *Id.*

233. Some argue that uniform government-mandated information security standards may be "unworkable." *See, e.g.*, Kenneth M. Siegel, Comment, *Protecting the Most Valuable Corporate Asset: Electronic Data, Identity Theft, Personal Information, and the Role of Data Security in the Information Age*, 111 PENN. ST. L. REV. 779, 821 (2007) ("Even if we ignore the fact that technology changes at a rapid pace, effective data security is very dependent upon each individual company's business, making a one-size-fits-all approach to information security unworkable."). The problem, however, is that it does not make much difference to malicious hackers whether they manage to steal credit card numbers from a major retailer or from a small mom and pop online store. Likewise, it does not make any difference for the customers who suffer losses as a result of the breach. Therefore, any business storing personally identifiable information should adhere to the strict government-mandated uniform information security standards or refrain from retaining such information.

puter systems and networks.[234] Unlike cybercriminals, these defendants are not judgment proof and are relatively easy to locate and identify. Unlike individual Internet users, they have resources and expertise to secure their networks and computer systems.[235] In addition, courts will not have any significant difficulty in asserting personal jurisdiction over such defendants.[236]

Third, federal information security standards should provide a uniform data classification scheme requiring stricter protection for more sensitive information. Organizations, therefore, will have a choice to either retain certain sensitive data and provide an adequate level of protection or refrain from retaining that data and avoid the related expenses. Federal information security standards should require business organizations, universities, and government agencies to establish well-defined information security management policies and procedures; ensure adequate data protection and malware prevention; maintain strict access control; provide training and screening of the personnel; and adhere to sound software development practices.

Fourth, the standards should impose certain technological solutions aimed at improving online security. For example, the standards may mandate that organizations monitor outgoing network traffic and prevent their network users from concealing their identity by altering ("spoofing") the originating address on their e-mails or network packets. Further, the standards should require ISPs to deny their services to customers spoofing their addresses. These measures would make it easier to track down perpetrators of spam and DDoS attacks, thus increasing the deterrence effect of criminal justice. Also, ISPs should be required to ensure the security of their customers' computers and deny Internet access to customers whose computers are missing required security software and updates. One cannot expect that all users will secure their computers unless ISPs ensure compliance.[237]

---

234. *See, e.g.*, Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, *in* THE LAW AND ECONOMICS OF CYBERSECURITY (Mark Grady & Francesco Parisi eds., 2005).

235. *Cf.* Henderson & Yarbrough, *supra* note 28 (arguing for holding negligent computer owners liable for damages caused by computer misuse facilitated by the owners' failure to maintain adequate security of their computers).

236. Robert Louis B. Stevenson, Note, *Plugging the "Phishing" Hole: Legislation Versus Technology*, 2005 DUKE L. & TECH. REV. 6 (2005) (emphasizing difficulty in finding perpetrators of cybercrimes and obtaining personal jurisdiction over them).

237. *But c.f.* Siegel, *supra* note 233, at 821 (implying that users will educate themselves about online threats and secure their computers by installing firewalls, antivirus software, and the latest security patches).

Imposition of liability under federal law for failure to comply with the information security standards would deter negligent behavior and promote uniformity and consistency of information system security across the nation. It is important, however, to carefully implement information security legislation, maintaining a proper balance between ensuring security and preventing excessive liability that may adversely affect the progress of society.[238] New legislation should not open technology companies and businesses, which use new technology to deliver their goods and services, to the expense of unlimited litigation and unpredictable damage awards. Reasonable efforts to comply with federally-mandated information security standards should be sufficient to protect businesses from liability.

It is also important that new legislation does not result in the over-regulation of technologies that can be used to commit crimes, thus preventing victims of computer crimes and investigators from using the same technologies to investigate criminal activity and track down the perpetrators of computer crimes.[239]

CONCLUSION

As discussed in Part V, once a cybercrime is committed, it is highly unlikely that the perpetrators will be held accountable and will compensate the victim for the sustained losses. Investigation and criminal prosecution of cybercrime is difficult, and many crimes go unpunished. At the same time, self-regulation and market forces do not necessarily ensure security of online transactions because of the inherent conflict of interests in the industry.[240] Many computer-related crimes are not even reported because businesses try to avoid bad publicity and the potential loss of customer confidence.[241] Since private legal actions under the current law usually do not result in adequate compensation for cybercrime victims either,[242] crime prevention becomes the key to ensuring the

238. *Cf.* Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 311 (2005) (warning about maintaining a proper balance between loss distribution and limits on liability in tort actions arising from identity theft).

239. Beryl A. Howell, *Real World Problems of Virtual Crime*, 7 YALE J.L. & TECH. 103, 122 (2005) (warning about the dangers that ill-defined legal norms may pose for computer crime victims engaged in a self-help effort to combat computer crime and track down the perpetrators).

240. *See supra* Part V.A.

241. *See supra* Part V.A.

242. *See supra* Part V.C.1

security of online transactions. Therefore, there is a need for comprehensive federal regulation and oversight combined with appropriate legislation extending rights of private parties to enforce government-mandated security standards and demand adequate security from the organizations handling their private information. Government organizations, businesses, and individuals should also have a legal right to recover their losses from organizations whose negligence in maintaining computer systems security precipitated cybercrime regardless of who committed the actual crime.

These measures would improve online security and reduce crime. As a result, law enforcement agencies would be able to investigate and prosecute a higher percentage of cybercrimes, thus increasing the deterrent effect of criminal justice.

As more businesses and government agencies move online, securing online transactions through the prevention of cybercrimes becomes critical both in protecting against fraud, cutting off a substantial source of illegal income for organized crime and terrorist organizations, as well as ensuring further growth of the national economy.