

Managing Information and Its Security: The Role of Policymakers, the Private Sector and Consumers

by Orson Swindle and Patrick Ross *

Introduction

The information age is no longer a cliché, as an ever-faster Internet and ever-expanding storage capacity make information the coin of the 21st century realm. Information encourages the flow of capital, empowers consumers with instant credit and immediate access to needed goods, and expands economic output and productivity. The free flow of information is critical to the functioning of the modern economy.

This information flows over data networks to which all of society are connected. The remarkable benefits derived from information technology and use unfortunately are accompanied by significant vulnerabilities. As we become more dependent upon these networks, people with ill intent become more capable of causing us widespread and costly harm. One need but look at the multitudes of information security breaches and the harm done in 2005 to appreciate the nature of the problem. While the harm done is not nearly as dramatic as portrayed in the media, it is significant in terms of actual consumer harm and, perhaps even more so, in driving perceptions of consumers who fear that they are not safe nor in control. In the recently settled ChoicePoint matter by the Federal Trade Commission (FTC), the penalties imposed included \$10 million in civil penalties and \$5 million in consumer redress.¹ By any standard, this represents major harm to consumers. That said, one study drawing on Federal Trade Commission data found most of the costs were borne by business not consumers.²

There has been a balancing act by government, the private sector and consumers in addressing data security from the dawn of the e-commerce era. But, in an age of global terrorism on the macro level and ever-more sophisticated e-mail scams on

* Orson Swindle is a distinguished fellow with The Progress & Freedom Foundation and director of its Securing the Internet project, and serves as Chairman of Information Security Projects for The Center for Information Policy Leadership at Hunton & Williams LLP, and Patrick Ross is senior fellow and vice president for communications and external affairs with The Progress & Freedom Foundation. The authors are grateful to Eileen Goulding for her research assistance. The views expressed here are those of the authors.

¹ See the FTC web site (<http://www.ftc.gov/opa/2006/01/choicepoint.htm>).

² Thomas M. Lenard and Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," Progress on Point 12.12, The Progress & Freedom Foundation, July 2005.

the micro level, the Internet presents a target-rich environment for those who would engage in fraud and deceit.

The market has proven relatively resilient to these threats to date and can be expected to be so into the future. However, the threats continue and have become even more sophisticated. Obviously, there is merit in further examination of the issue, with an eye toward practical and effective solutions.

What was just a few years ago considered immature and prankish harrassment by computer-savvy youngsters is now the realm of organized criminal activity capable of doing serious damage. Furthermore, there can be proper roles for the government to play on behalf of both consumers and the market. If the promise of the global online marketplace is to be fully realized, government and industry must demonstrate to consumers that they are working to build trust and confidence while bolstering networks and systems and punishing those who would cause harm.

The Threat to Consumers

Data security has long been a central focus of financial institutions, and to a certain extent, those engaged in e-commerce and other handlers of personally identifiable data. Recently it has become a much more common concern with the general public as the list of identity and account-based fraud victims grows.

Information security breaches have appeared on the covers of national news magazines, been featured on numerous television news programs, and has consumed thousands upon thousands of column inches in newspapers. Public attention and consumer discontent will usually attract the interest of elected officials. The increased attention can itself be a cause for concern, as irrational anxiety can depress consumer spending, lead to ineffective or even harmful legislation, and stifle economic growth.

The cause, frequency and nature of the actual harm from security breaches and data compromises vary and can often be difficult to accurately quantify. While a recent study found that the vast majority of identity theft victims have become so as the result of offline crimes³, the relatively new scam known as "phishing" has emerged as a legitimate online identity-based crime threat. From July 2004, attempted phishing attacks have increased at an estimated average of 30% per month, although that growth began from a negligible starting point.⁴ Perhaps more alarming than the increase in phishing attempts is the phishing scam success rate, estimated by the Anti-Phishing Working Group at 5% of recipients as compared to a minuscule rate of 0.01% for spam.⁵ While phishing attempts can be sophisticated enough to nearly fool even

³ Javelin Strategy & Research, "2005 Identity Fraud Survey Report," 2005. A summary is available on its web site -- <http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html>.

⁴ See Robert Stevenson, "Plugging the 'Phishing' Hole: Legislation Versus Technology," 2005 Duke Law & Technology Review, p. 2.

⁵ Ibid.

experts in the field⁶, that victimization rate should decrease with greater awareness and sophistication of online consumers stemming from repeated exposure to this scam.

It must be noted, however, that the threat to any given individual consumer may not be as dire as it is sometimes portrayed. A December 2005 study by ID Analytics that looked at breaches of data found that consumers who have their personal identification compromised face little risk of becoming victims of identity theft. Even with the most dangerous digital data breaches, where social security numbers and other sensitive information were targeted, only about 1 in 1,000 victims had their identities stolen.⁷ Of course, if you are the one victim, the assessment changes dramatically!

This is in keeping with other data regarding offline theft. Visa has reported that only 2 percent of compromised cards are used fraudulently.⁸ This could be a very small number indeed if the breach itself is small, although in a massive breach of 10,000,000 compromised accounts that would be 200,000 victims, not an insignificant number, to say the least.

While estimates of damages are debated, the fact that they are significant is undeniable. For example, the damages as a whole, according to the U.S. Treasury Department's Office of Technical Assistance⁹, are in excess of \$100 billion in harm, exceeding the magnitude of illegal drug sales. The Privacy Rights Clearinghouse's "Chronology of Data Breaches"¹⁰ lists approximately 100 publicly reported disclosures of security breaches for 2005 involving personal information of over 50 million citizens. There were numerous causes for the breaches, including lost laptops, disgruntled employees and lost computer tapes. The most troubling breaches involved sophisticated hackers entering poorly protected information systems and networks giving access to sensitive financial accounts information and other information used in identity or account fraud. And, although difficult to measure, significant participation in electronic commerce surely is being forgone by those feeling insecure. The fear associated with ID theft and data breaches is driving people's perception of reality as the recent data suggests.

For example, Gartner Research indicates that 77% of online banking consumers log in less frequently as a result of fears around security, and 4% stopped paying their bills online altogether.¹¹ One-third of shoppers surveyed by Gartner indicated they were

⁶ Clyde Wayne Crews, Jr., "Cybersecurity: Markets or Mandates?" *Monthly Planet*, Competitive Enterprise Institute, November 2004. Crews admits in the column that despite being a longtime student of online security, he was tempted for a moment when he received an email claiming to be from PayPal, as he had just opened up a PayPal account for CEI and suspected this was a verification email. It wasn't.

⁷ "Fears Over Identity Theft Overblown: U.S. Study," Reuters, Dec. 8, 2005. An overview of the ID Analytics study can be found on its web site –

http://www.idanalytics.com/pdf/Breach_Analysis_Overview.pdf .

⁸ Lenard and Rubin, 2005.

⁹ Jon Swartz, "2005 Worst Year for Breaches of Computer Security", *USA Today*, December 29, 2005.

¹⁰ See <http://www.privacyrights.org/ar/ChronDataBreaches.htm> .

¹¹ Riva Richmond, "Internet Breaches, Scams Drive Buyers off the Web, Survey Finds," *Wall St. Journal*, June 23, 2005.

buying less (because of these concerns about exposure of their transactions) than they would otherwise.¹² The FBI estimates \$67 billion in financial damages annually caused by "cyber crime."¹³

An ABC/Washington Post poll taken after several publicized data breaches found seven out of ten US adults fear they will become a victim of identity theft.¹⁴ A recent survey by IBM found that three times as many Americans believe they'll be the victim of an online crime in the next year than an old-fashioned offline crime.¹⁵ They are changing their behavior as a result of their fears, putting e-commerce and the larger economy at risk as a result. Consumer Reports found that 9 out of 10 US Internet users have adjusted their behavior online, with 30 percent reducing their overall Internet use, 25 percent no longer buying items online, and 29 percent of those who are continuing to shop online cutting back on their purchases. A majority of those online said they have stopped giving out personal information on the Internet.¹⁶

The Threat to Society

Shortly after the September 11th attacks, the Bush administration began a comprehensive review of U.S. security, and cybersecurity was a featured part of the effort. Out of that process grew the National Strategy to Secure Cyberspace -- first released in draft form a year after the attacks and updated since. The Strategy was developed with feedback from industry officials and civil society advocates. It recognized the significant role the Internet could play in a terrorist attack, while also acknowledging that about 85% of the nation's critical infrastructure was in private sector hands. Thus, the Administration concluded, private industry bore a large portion of responsibility for security.

During the development of the Strategy and since its release, the private sector has worked closely with the U.S. government on cybersecurity matters. A number of industry coalitions have emerged to promote cybersecurity and cooperation with the federal government¹⁷, and many of these coalitions and their member companies have

¹² Dinesh C. Sharma, "Data Leaks Denting Web Shoppers' Confidence," CNET News.com, June 23, 2005 (http://news.com.com/Data+leaks+denting+Web+shoppers+confidence/2100-1029_3-5759294.html?tag=nl).

¹³ Joris Evers, "Computer Crime Costs \$67 Billion, FBI Says," CNET News.com, Jan. 19, 2006 (http://news.com.com/Computer+crime+costs+67.2+billion,+FBI+says/2100-7349_3-6028946.html).

¹⁴ Jon Cohen, "Poll: Identity Theft Concerns Rise," ABC News, March 17, 2005 (<http://abcnews.go.com/Business/PollVault/story?id=590413&page=1>).

¹⁵ Gregg Keizer, "Cybercrime Feared 3 Times More than Physical Crime," *Information Week*, January 25, 2006 (<http://www.informationweek.com/news/showArticle.jhtml?articleID=177103904>).

¹⁶ "Leap of Faith: Using the Internet Despite the Dangers," Consumer Reports WebWatch, October 26, 2005 (<http://www.consumerwebwatch.org/pdfs/princeton.pdf>).

¹⁷ Among these cybersecurity advocates are trade groups such as the Business Software Alliance, the Computer & Communications Industry Association, the Computing Technology Industry Association, and the Information Technology Association of America; business coalitions such as the Business Roundtable and the U.S. Chamber of Commerce; and newly created industry coalitions such as Americans for a Secure Internet, the Cyber Security Industry Alliance, and the Internet Security Alliance.

encouraged efforts on Capitol Hill and at the White House to increase the issue's prominence at the Department of Homeland Security.¹⁸ There continues to exist disappointment among some in the private sector regarding the Administration's commitment to data security.

Concerns about terrorist threats and the harms caused by inadequate information security can, if not corrected, deter our use of information technology. We must continue to enjoy and develop upon the benefits that global connection brings. However, we must also recognize our vulnerabilities and find solutions to these vulnerabilities. Computers are essential in virtually every aspect of our lives today. They help us control our electric power system, transportation systems, communications, financial systems, medical and emergency service, and even traffic lights. Networked computers give consumers almost unlimited conveniences and choices.

The benefits of these technologies can only be fully realized if users have confidence that their financial accounts and personally identifying information are safely used, that their privacy is respected, and that no harm will come to them. Corporate counsel advising management to not employ and promote privacy practices in order to avoid potential liability for not keeping promises or making mistakes is shortsighted, as are executive decisions not to invest sufficiently in better information security measures because of a perceived low return on investment. The cost of not investing in better security is obviously rising steeply.

The loss of reputation and customers, stock value deterioration, brand degradation and law suits that come with a data security breach argue for a far better and more responsible approach.¹⁹

Ultimately, as common sense tells us, we need universal recognition of the need to respect the privacy of individuals and their personal and sensitive information and to provide sufficient security for that information.

The U.S. government is, as it should be, working to protect its citizens from possible attacks of all kinds, in the physical world and in cyberspace. Obviously, if the private sector owns 85% of the information technology infrastructure, it shares the heavier burden in finding solutions and for a number of good reasons, not the least of which are its revenue streams, its reputation and its investments. The users of information technology are also key players in this effort to protect these valuable assets and capabilities. In other words, everyone has a role to play... and must begin to play it seriously. Above all, these efforts must be undertaken with care so that any

¹⁸ Congress, believing the official in charge of cybersecurity at the Department of Homeland Security was not sufficiently high on the agency's organizational chart, approved legislation creating a position of assistant secretary of cybersecurity. That move was backed by industry, but the spot remains vacant. See Roy Mark, "Cyber Security Group Flunks Washington," *InternetNews.com*, December 13, 2005 (<http://www.internetnews.com/bus-news/article.php/3570596>) and Caron Carlson, "Industry Lobbies Against Cyber-Security Mandates," *eWeek*, September 27, 2005 (<http://www.eweek.com/article2/0,1895,1864361,00.asp>).

¹⁹ Lenard and Rubin, 2005.

steps taken do not jeopardize our connected world and the legitimate flow of information and data which facilitate virtually all that we do at home and abroad.

Proposed Remedies

Consumers have a growing concern about data security. Congress listens to such concerns and is further tempted to respond quickly to address them. Hasty and perhaps emotion-driven action to regulate data security on the Internet would violate an essential consideration when deciding to let government solve any problem: First do no harm.

There are a number of proposed remedies circulating on Capitol Hill, some of which may not meet the above test. Some have been introduced as bills which include new criminal penalties, notification requirements for owners of personal data, and other new mandates and laws. Some have been proposed informally by members of Congress, advocacy groups and others. There are indications Congress could pass legislation as soon as this year, perhaps by combining separate bills.²⁰ However, with multiple committees vying for jurisdiction over the issue, squabbles could also prevent passage of legislation this year.²¹

The US government has not been idle as Congress debates potential legislation, however. The FTC has pursued information security breaches and identity and account-based fraud cases, including a yearlong investigation involving the compromise of sensitive information on an estimated 163,000 consumers. The target in this case was ChoicePoint, a data broker alleged by the FTC to have turned over consumers' sensitive personal information to subscribers whose applications raised obvious "red flags," such as lying about their credentials, using commercial mail drops as business addresses, and using fax machines at public commercial locations to send multiple applications for purportedly separate companies.

As mentioned earlier, the investigation resulted in a recent settlement in which the company agreed to \$10 million in civil penalties and \$5 million for consumer redress. In announcing the settlement, FTC Chairman Deborah Majoras said "[d]ata security is critical to consumers, and protecting it is a priority for the FTC, as it should be to every business in America."²² Meanwhile, the FTC said the rate of increase in identity theft complaints to the agency has decreased compared to 2004 and 2003²³.

There appears to be a general consensus that a solution to information security breaches, disclosure and notices to those affected must include a national approach, driven in part by the fact that almost two dozen states have passed data security laws

²⁰ Caron Carlson, "Teed Up for '06: Data Breaches, Spyware," *eWeek*, Nov. 28, 2005.

²¹ Sarah Lai Stirland, "Enacting a Law on Data Breaches Will be Difficult," *National Journal's Technology Daily*, Jan. 12, 2006.

²² See FTC press release of January 26, 2006 (<http://www.ftc.gov/opa/2006/01/choicepoint.htm>).

²³ Christopher Conkey, "ID Theft Complaints Still Rising, but Rate of Increase Slows," *The Wall Street Journal*, January 26, 2006.

and a slightly smaller number are considering legislation. The reality is that too many different standards beg for preemption. After all, the Internet is global in nature, and reliance on a federal approach of state laboratories in fact hinders e-commerce and imposes de facto standards of the most onerously regulated state across the U.S.²⁴

Thus, it is only natural that consumers and businesses turn to Washington in search of a uniform solution. There is little consensus, however, on what that solution should be. Certainly no significant consensus exists in the private sector that new legislation or regulations are needed. However, US private industry isn't waiting for government action because marketplace realities are already forcing them to respond to new online threats.²⁵

Some believe the need to have trusting customers and the competitive harm that could come from inadequate security will be sufficient motivation to ensure data protection. Others see federal enforcement of existing fraud laws as being sufficient. But remember, this is an international problem in which there is no consensus approach. Still others would extend the effort at gaining consensus beyond the U.S. to a global solution, perhaps beginning with harmonizing our laws with that of the European Union.²⁶

Former top US government security officials have put forward what they see as modest ways the federal government can assist the market. One has backed the use of the SEC filing system to compel companies to demonstrate implementation of sound information security practices. Another urged Congress to use the federal government to shore up an information or cybersecurity insurance market, with the hope that increased liability protection at lower cost will spur both e-commerce and cybersecurity.²⁷

The more one looks, the more one will find proposed solutions, but it is difficult to find quantitative evaluations of the costs and benefits of these solutions.

Conclusion

²⁴ For more on this subject see Peter S. Menell, "Regulating 'Spyware': The Limitations of State 'Laboratories' and the Case for Federal Preemption of State Unfair Competition Laws," *Berkeley Technology Law Journal*, Summer 2005.

²⁵ Brian Krebs, "Companies Forced to Fight Phishing," *Washington Post*, Nov. 19, 2004.

²⁶ Some would like to see the U.S. harmonize its laws with the European Union's E-Commerce Directive, which among other things enlists ISPs to help combat online fraud. The harmonization effort in Congress has been stalled for several years, however, and others, including many ISPs, oppose harmonization. For more on the subject read Michael L. Rustad and Thomas H. Koenig, "Rebooting Cybertort Law," *Washington Law Review*, May 2005.

²⁷ Patrick Ross, "Former NIPC Chief Calls for 'Soft' Cybersecurity Regulation," *Washington Internet Daily*, April 9, 2003. At a hearing before the House Government Reform Technology Subcommittee, former National Infrastructure Protection Center Director Michael Vatis called for governmental assistance in the cybersecurity insurance market, while former White House cybersecurity czar Richard Clarke supported new SEC filing mandates.

Limited government allows Americans to make their own decisions, permitting society to progress and enjoy greater freedom. Given the tremendous personal and economic benefits that flow from private markets, government officials must resist the urge to “do something” to quickly satisfy political needs, and they must always be mindful of the oft-proven laws of unintended consequences of government “solutions.”

All business models and solutions begin with data. This data and the uses of it are distributed the world over, thus are subject to varying legal requirements. If the data cannot flow, the business processes are halted. We have to get this right.

Rational thinking about solutions must prevail, and improvements in information privacy and security must come to be. The legitimate flow of information is critical to all that we do. Privacy is the appropriate use of data, and information security is the protection of it. Currently, there is no global legal infrastructure to assure that those flows continue -- European law could stop it tomorrow.

The US government can play a positive role by diligently working with the private sector and experts to find an acceptable international framework that overcomes, or at least minimizes, impediments created by conflicting laws (just as among our own states). Our government can also help by partnering with the private sector to educate consumers and businesses and by appropriate and rational attempts to minimize criminal behavior. The federal government must make the issues of technology and finding rational approaches to information privacy and security a high priority, and demonstrate commitment with leadership and adequate resources for the task at hand. Lastly, if market forces fail to correct illegal and unacceptable practices, government action seems likely, necessary and inevitable.

The private sector must recognize this truth and be aggressive and effective in self-regulation. Protecting and respecting the privacy of individuals and their sensitive information must become an integral part of the corporate culture, including the CEO and board members. A more holistic approach to managing information must become the standard way of operating, with information privacy and security a standard, high-priority aspect of those processes. Industry and its management processes must move beyond an internal stove pipe mentality and incorporate privacy and security concerns seamlessly into all aspects of management. New and improved technologies can also help, but we must recognize that our foes in this arena are smart and capable of responding to any new technological challenge.

Consumers also have a role to play in building a secure Internet. Each of us must bear some level of responsibility and accountability for our actions. Access to easily understood information, best practices and effective tools from government and industry to help us all be safer in our computing practices abound, and they can help us bear this responsibility and play our proper role. We need to use them!

There is no single or perfect solution to the problem of securing data in an Internet age. However, there are myriad ways of addressing the problem, and each one

impacts multiple constituencies. Future solutions for making the Internet safe and strong must include a commitment to the continued legitimate flow of information that drives today's commerce; an enhanced respect for individual privacy and a commitment to protect sensitive information; and effective means to minimize vulnerabilities to this vital part of our critical national infrastructure and security. If progress is to be made, all interested and affected parties – government, industry, technologists and consumers – must work together toward these common goals.

The Progress & Freedom Foundation is a market-oriented think tank that studies the digital revolution and its implications for public policy. Its mission is to educate policymakers, opinion leaders and the public about issues associated with technological change, based on a philosophy of limited government, free markets and civil liberties. The Foundation disseminates the results of its work through books, studies, seminars, conferences and electronic media of all forms. Established in 1993, it is a private, non-profit, non-partisan organization supported by tax-deductible donations from corporations, foundations and individuals. PFF does not engage in lobbying activities or take positions on legislation. The views expressed here are those of the authors, and do not necessarily represent the views of the Foundation, its Board of Directors, officers or staff.

The Progress & Freedom Foundation ■ 1444 Eye Street, NW ■ Suite 500 ■ Washington, DC 20005
voice: 202/289-8928 ■ fax: 202/289-6079 ■ e-mail: mail@pff.org ■ web: www.pff.org