HARBORING DATA

Information Security, Law, and the Corporation

Edited by Andrea M. Matwyshyn

STANFORD LAW BOOKS
An Imprint of Stanford University Press
Stanford, California

2 The Information Vulnerability Landscape

Compromising Positions: Organizational and Hacker Responsibility for Exposed Digital Records

Kris Erickson and Philip N. Howard

DATA COLLECTION, management (or mismanagement), and unwanted disclosures of personal information have become the subjects of public debate. In early 2005 a series of high-profile cases culminating in the loss of more than 140,000 customer credit records by ChoicePoint helped generate significant public interest in the dangers associated with digital records of personal information.[1] Then, in the summer of 2006, the Department of Veterans Affairs admitted that some 26.5 million personal records had been compromised.[2] In 2007 the Chicago Board of Elections was accused of compromising voter files,[3] and the Census Bureau admitted to posting records for over 300 households online.[4]

The threats to information security are varied: for example, search engines increasingly index Web pages that may not be meant for public consumption, and employee use of file-sharing software exposes many different kinds of files to communication networks. Organizations use various levels of passwords and encryption to try to prevent access to data on stolen laptops. Data security is never perfect, and credit card companies, universities, and government agencies cannot perfectly predict security lapses. But the growing number of news stories about compromised personal records reveals a wide range of organizational mismanagement and internal security breaches: lost hard drives and backup tapes, employee theft, and other kinds of administrative errors.

So far, blame has been directed at all parties involved: at the state, for being lackadaisical in regulating organizations that deal with electronic records; at the private sector, for not giving personal privacy and information security enough priority; and finally at the end users themselves, for not taking better care of managing their online identities in order to mitigate the risk of fraud. A significant amount of the information in these records concerns health and credit records, which are often combined to generate a convincing electronic portrait of an individual, thus effectively reconstituting their identity.[5] These stolen identities can also be used to fraudulently deceive government agencies and credit organizations.

The threat of electronic data theft also has serious implications for societies that increasingly rely on the security of data networks to conduct daily life. For example, as more of our political system becomes computerized, there is a stronger possibility that electronic data could contain information about an individual's political beliefs or voting records, which are now both easier to access and highly detailed.[6] Yet most U.S. citizens report being uninterested in learning how to better manage their personal data or in learning about the ways organizations mine for data.[7] However, both policy makers and computer software and hardware companies are, nevertheless, aggressively enrolling individual consumers in the task of securing their own data against loss or theft.

Often at the center of these privacy breaches is the hacker archetype. Using intellectual property law, court challenges, and amicus briefs, corporate and government leaders have reframed the meaning of the term "hacking" from a character working for freedom of access to technology and information to one that is deviant and criminal.[8] However, the actual role of hackers in the computer security sector is considerably more complex. Many hackers not only enjoy technical challenges but are sometimes even enlisted by corporations and governments for their specific skills.[9] Even though the campaign against hackers has successfully cast them as the primary culprits to blame for vulnerability in cyberspace, it is not clear that constructing this target for blame has resulted in more secure personal digital records.

This chapter explores how responsibility for protecting electronic data is currently attributed and examines legislation designed to manage the problem of compromised personal records. In our investigation we compare the aims of legislation with an analysis of reported incidents of data loss for the period of 1980–2007. A discrepancy between legislative responses to electronic data loss and the actual damages incurred reveals that responsibility for maintaining the security of electronic personal records has been misplaced and should be reexamined. We conclude with a brief discussion of the options for public policy oversight.

Legal Evolution—from Regulating Hackers to Regulating Corporations

Scholars often point out that new information technologies consistently present legislators with the challenge of regulating issues for which there are no readily apparent legal precedents. Lawmakers are frequently cast as lagging behind technological innovation, as they struggle to catch up with new forms of behavior enabled by rapidly evolving technology. Traditional legal concepts such as private property and trespass often become problematic when applied in online contexts enabled by information and communication technologies. For example, E. A. Cavazos and D. Morin have argued that the law has struggled to adequately account for the nuances of computer-mediated communication.[10] These tensions become particularly apparent when lawmakers have attempted to regulate behavior across several legal jurisdictions, such as in the case of music piracy and online gambling.[11] Particularly in the context of information security of digital information, legislation has been questionable in its effectiveness as a deterrent. The law first turned to regulating the act of computer intrusion committed by "hackers" and now has turned to regulating the consequences of intrusion and data leakage through data breach notification statutes.

Regulating Computer Intrusion and Hackers

The Computer Fraud and Abuse Act (CFAA) was passed in 1984 in response to growing political and media attention surrounding the dangers of computer crime. The act criminalized exceeding authorized access to private computer systems, making it a felony offense when trespass leads to damages over a certain monetary threshold. The CFAA underwent major revisions in 1986 and 1996, and it was further strengthened by the passage of the USA Patriot Act in 2002. Overall, these revisions have served to make the act more broadly applicable to various kinds of computer crime, while also increasing the punitive response to these offenses.[12]

For example, the revisions in 2002 were tailored to make it easier to surpass the $5,000 felony threshold. The threshold was waived in cases where the computer systems involved are used for national security or law enforcement purposes. In cases not involving national security, the definition of "damage" was broadened to include costs relating to damage assessment and lost revenue during an interruption of service. The $5,000 threshold is also cumulative over multiple machines if more than one system is involved in a single attack.[13] In addition, the maximum sentence for felony computer trespass was raised from five to ten years for first-time convictions, and from ten to twenty years for repeat offenses.[14]

Given the relatively harsh penalties for computer intrusion in comparison with those for other crimes in which victims suffer personal physical harm, it is surprising that the CFAA has not been more effective as a deterrent. The apparent surge in computer-related offenses, including the theft of online personal records, suggests that the punitive nature of this legislation is not having the desired effect.[15] The belief that all hackers are malicious is essentially a myth—many members of the computer hacker subculture do not condone destructive behavior and do not consider their activities to be particularly malicious.[16]

Arguably the most significant threat posed by computer criminals comes not from the core group of white, black, or gray hat hackers but from individuals who use hacker techniques to invade systems for monetary gain.[17] Since knowledge and tools developed by more experienced hackers can easily be obtained on the internet, the capability to penetrate insecure networks has propagated outside of the original hacker community to other groups, ranging from inexperienced teenagers to international crime syndicates.[18] These individuals may feel protected from the law by the relative anonymity of computer-mediated communication, or they may be located in jurisdictions where harsh criminal penalties for computer fraud do not apply.

Regulating Corporate Data Leaks Through Breach Notification Statutes

Although the CFAA aids in the prosecution of criminals who engage in electronic data theft and trespass, individual states have taken additional legal steps to regulate the management of electronic records. In 2003 the state of California introduced a new provision to the Information Practices Act, the "Notice of Security Breach." This addition to the California Civil Code obliges any business or agency that has been the victim of a security breach to notify any parties whose personal information might have been compromised. The California legislation defines "personal information" as an individual's full name, in combination with one of the following types of data:

(1) Social Security number

(2) Driver's license number or California Identification Card number

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

The organization responsible for handling the compromised data must notify potential victims individually, unless the cost of notification exceeds a threshold amount of $250,000, or if the total number of individuals affected is greater than 500,000. In these cases, substitute notification can be made using a combination of email notification and disclosure to major media outlets. Notification must be carried out "in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement [. . .] or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[19] Following in California's footsteps, at least forty additional states had enacted similar legislation by 2007. Unlike the CFAA, however, this legislation does not directly address the issue of network security. It does not formalize standards or rules for information security; nor does it make organizations accountable for poor security practices that make them vulnerable to attack. The legislation punishes businesses only for failing to notify the public, rather than for negligence in securing electronic records. Since adequately securing a computer network from intrusion is an expensive prospect, this legislation essentially lets businesses off the hook by making them liable for damages only when they fail to notify affected individuals that their data have been compromised. Interestingly, by failing to assign responsibility for data loss to those agencies that manage electronic personal information, this legislation serves in part to shift that responsibility to the individual users, since they are the ones who must take steps to protect their identity once notified of a breach.[20]

So far, the legal responses to electronic identity theft in the United States have sought to minimize the direct involvement by the state, instead relying on a partnership between the interests of private firms and the consumers of those services. The two major forms of legislation governing the security of computer records in the United States—the CFAA and the California data breach notification laws—closely resemble offline governmental strategies that seek to place responsibility on individual consumer-citizens while disciplining those who do not adequately protect themselves.[21] Moreover, the hesitation of public agencies in the United States to draft legislation that would directly influence the terrain of data security is consistent with the overall trend of regulatory devolution, a shift that began before the information sector occupied such a primary position in the national economy.

The legislative choices that policymakers in the United States have made to combat the problem of data insecurity have been shaped by the tenet that governments should interfere only minimally with markets. Thus, legislative initiatives have eroded public policy oversight of corporate behavior. In the arena of data security for private information, this erosion has meant deemphasizing the role of government and public policy oversight in data security, encouraging industry self-regulation among the firms benefiting in the retention of personal data, and increasing individual responsibility for managing our personal data.

Analysis of Compromised Electronic Records, 1980–2007

We conducted a search of incidents of electronic data loss reported in major U.S. news media from 1980 to 2007. These included print publications with national circulation, such as the *New York Times*, the *L.A. Times*, and *USA Today*, along with major broadcast news media. Because some news reports contained references to more than one incident, we employed a snowball methodology to expand our analysis by including additional security breaches mentioned in the same article. Duplicate entries were eliminated by comparing news stories on the basis of organizations involved, dates, and other incident details. In instances where papers reported different quantities of lost records, we chose the most conservative report. We also consulted lists of electronic data breaches compiled by third-party computer security advisories, such as the Identity Theft Resource Center (www.idtheftcenter.org) and Attrition.org. Our method yielded 852 incidents, 39 of which were discarded because they involved citizens of other countries. Of the remainder, 813 incidents were successfully cross-checked with LexisNexis and Proquest to ensure accuracy.[22]

Our list of reported incidents is limited to events in which one or more electronic personal records were compromised through negligence or theft. We acknowledge that there are occasions when end users consider their personal information compromised when the data are sold among third parties for marketing purposes without their informed consent. For this study, we look only at incidents of compromised records that are almost certainly illegal or negligent acts. For the purposes of this chapter, we define electronic personal records as data containing privileged information about an individual that cannot be readily obtained through other public means. Rather than become involved in the broader debate about the virtues and dangers of online anonymity, we have chosen to focus only on data that are more sensitive than the information that we regularly volunteer in the course of surfing the Web (such as one's name or

025

internet protocol [IP] address). We define "personal data" to be information that should reasonably be known only to the individual concerned or be held by an organization under the terms of a confidentiality agreement (such as between a patient and a care provider). Electronic personal records therefore could include individuals' personal credit histories, banking information such as credit card numbers or account numbers, medical records, Social Security numbers, and grades earned at school. We focused only on incidents in which compromised personal records were kept for a legitimate purpose by a firm, government agency, or other organization. Consequently, "phishing" or spoofing scams in which victims are deceived into volunteering their own personal information are not included in our analysis. All of the incidents in our analysis deal with data that were maintained in electronic form, although in some cases compromised data were contained on lost or stolen computer hardware.

Between 1980 and 2007, some 1.9 billion records were reported compromised by government agencies, firms, hospitals, universities, and the military. This is the sum of compromised records from 813 incidents in which some estimate of the volume of lost records was offered, though in 61 of these incidents the volume of the security breach was unknown. In a sense, this number of lost records is larger than one might expect because a few landmark incidents account for a large portion of the total number of records compromised. On the other hand, we conservatively recorded the number of records lost in each incident: if a range of the number of compromised records was offered, we recorded the lowest number; if no exact number was reported, we recorded zero compromised records; in news stories where it was reported only that "hundreds" or "thousands" of personal records were compromised, we recorded 100 or 1,000 compromised records. Moreover, the number of confirmed incidents—813 in all—may seem smaller than expected given the twenty-seven-year time frame of our search. Some articles report multiple incidents, and of course many incidents were covered by journalists on multiple occasions. In 2004 the Census Bureau estimated that there were 217 million adults living in the United States. We can conservatively estimate that for every U.S. adult, in the aggregate, nine private records have been compromised. Unfortunately we cannot know how many of these compromised private records have actually been used for identity theft, or how many were sold to marketing companies.

Table 2-1 shows the number of reported incidents and volume of compromised records between 1980 and 2007, along with their distribution by sector.

TABLE 2-1 Reported Incidents and Volume of Compromised Records by Sector, 1980–2007

Time Period			*Commercial*	*Educational*	*Government*	*Medical*	*Military*	*Total*
1980–1989	Records	N	90,000,002	0	0	0	4,190,000	94,190,002
		%	96	0	0	0	4	100
	Incidents	N	3	0	1	0	3	7
		%	43	0	14	0	43	100
1990–1999	Records	N	53,369,339	0	20	3,010	461	53,372,830
		%	100	0	0	0	0	100
	Incidents	N	16	0	1	2	3	22
		%	73	0	5	9	14	100
2000–2007	Records	N	1,764,690,029	9,050,483	74,101,500	5,506,212	999,356	1,854,347,580
		%	95	0	4	0	0	100
	Incidents	N	275	244	173	79	13	784
		%	35	31	22	10	2	100
Total	Records	N	1,908,059,370	9,050,483	74,101,520	5,509,222	5,189,817	2,001,910,412
		%	95	0	4	0	0	100
	Incidents	N	294	244	175	81	19	813
		%	36	30	22	10	2	100

NOTE: A zero value in sectors with no incidents indicates that no records were compromised. A zero value in sectors with incidents indicates that the volume of compromised records was not recorded.

The majority of incidents involved commercial actors; less than a third of the incidents involved colleges, universities, or nonprofit agencies; and the remainder involved government, hospitals, and the military. When the exceptional loss of 1.6 billion personal records by Acxiom Corporation is removed, the commercial sector still accounted for approximately 308 million individual compromised records, four times that of the next-highest contributor, the government sector.[23] The education and nonprofit sector accounted for a small percentage of the overall quantity of lost records, but accounted for 30 percent of all reported incidents, suggesting that educational organizations suffer from a higher rate of computer insecurity than might be anticipated. This could be explained by the fact that colleges and universities maintain large electronic databases on current and past students, staff, faculty, and alumni, and have an organizational culture geared toward information sharing. However, medical organizations—which presumably also maintain large quantities of electronic data—reported a significantly lower number of incidents of data loss. These differences may be the result of strong privacy legislation in the arena of medical information, but comparatively weak privacy legislation in the arena of educational and commercial information.

Although Table 2-1 has aggregated twenty-seven years' worth of incidents, the bulk of the reports occur between 2005 and 2007, after legislation in California, Washington, and other states took effect. There were five times as many incidents in the period between 2005 and 2007 as there were in the previous twenty-five years. Interestingly, the mandatory reporting legislation seems to have exposed educational organizations as a major source of private data leaks. Since 1980, 36 percent of the incidents involved commercial firms, but in the three most recent years, 33 percent of the incidents involved educational organizations. These kinds of organizations may have been the least equipped to protect the data of their students, staff, faculty, and alumni.

For the majority of incidents, the news articles report some information about how the records were compromised. A closer reading of each incident, however, reveals that most involved different combinations of mismanagement, criminal intent, and, occasionally, bad luck. The hacker label was often used, even when the theft was perpetrated by an insider, such as a student or employee. Moreover, company public relations experts often posited that personal records were only "exposed," not compromised, when employees posted private records to a website or lost a laptop and the company could not be sure that anyone had taken specific advantage of the security breach.

TABLE 2-2 Reported Incidents and Volume of Compromised Records by Type of Breach, 1980–2007

Time Period			*Administrative Error*	*Exposed Online*	*Insider Abuse or Theft*	*Missing or Stolen Hardware*	*Stolen-Hacked*	*Unspecified Breach*	*Total*
1980–1989	Records	N	0	0	0	0	90,000,002	4,190,000	94,190,002
		%	0	0	0	0	96	4	100
	Incidents	N	0	0	1	0	3	3	7
		%	0	0	14	0	43	43	100
1990–1999	Records	N	0	3,030	20	20,000	33,430	53,613,350	53,372,830
		%	0	0	0	0	0	100	100
	Incidents	N	0	0	1	1	10	7	22
		%	0	0	5	5	45	32	100
2000–2007	Records	N	35,322,843	5,984,901	11,011,773	53,278,191	1,712,595,473	36,154,399	1,854,347,580
		%	2	0	1	3	92	2	100
	Incidents	N	26	145	34	325	204	50	784
		%	3	18	4	41	26	6	100
Total	Records	N	35,322,843	5,987,931	11,011,793	53,298,191	1,802,628,905	93,660,749	2,001,910,412
		%	2	0	1	3	90	5	100
	Incidents	N	26	148	36	326	217	60	813
		%	3	18	4	40	27	7	100

NOTE: A zero value in a type of breach with no incidents indicates that no records were compromised. A zero value in sectors with incidents indicates that the volume of compromised records was not reported.

Table 2-2 shows that the legislation has also seemed to have the effect of forcing the reporting organizations to reveal more detail about the ways these private records get compromised. In the early reports, most incidents were described as an unspecified breach or as the general result of hacker activity. However, for the period between 2000 and 2007, 27 percent of the incidents were about a breach caused by a hacker, 7 percent of the incidents involved an unspecified breach, and 66 percent of the incidents involved different kinds of organizational culpability. For example, sometimes management accidentally exposed private records online, administrative error resulted in leaked data, or employees were caught using the data for activities not related to the work of the organization. On some occasions, staff simply misplaced backup tapes, while on others, computer equipment such as laptops were stolen.[24]

A single incident, involving 1.6 billion compromised records at the Acxiom Corporation, accounts for a large portion of the volume of records lost in the period 2000–2007.[25] If this event is removed from this period, then 44 percent of the compromised volume and 26 percent of the incidents were related to hackers, 42 percent of the compromised volume and 68 percent of the incidents involved organizational behavior, and 14 percent of the compromised volume and 6 percent of the incidents remain unattributed. If this event is removed from the volume of compromised records for the whole study period—between 1980 and 2007—then 50 percent of the total volume of compromised records was related to hackers, 27 percent of the volume was attributed to the organization, and 23 percent remained unattributed. Removing this event from the total number of incidents for the whole study period does not change the overall allocation of responsibility in major news reports: 66 percent involved organizational management, 27 percent of the incidents involved hackers, and 7 percent remain unattributed. Regardless of how the data are broken down, hackers account at most for half of the incidents or the volume of compromised records.

If we distinguish the reported incidents that clearly identify a hacker from those related to some other form of breach, the organizational role in these privacy violations becomes clear. Figure 2-1 separates the stories in which a hacker was clearly identified as the culprit from those in which the cause of the breach was unspecified, and from those in which the cause of the breach was related to organizational action or inaction. In this latter category, we consider organizational behavior to include four types of security breach: accidental exposure of personal records online, insider abuse or theft, missing

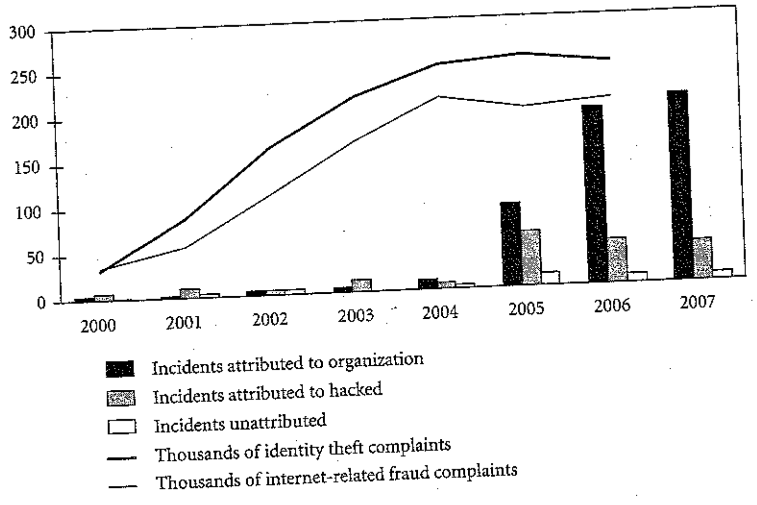

FIGURE 2-1 Incidents of Compromised Personal Records, Identity Theft Complaints, and Internet-Related Fraud Complaints, 2000–2007

SOURCE: Based on authors' calculations of incidents of compromised personal records, 2000–2007. Identity Theft Complaints and Internet-Related Fraud Complaints from the U.S. Federal Trade Commission Consumer Sentinel Project Team, *National and State Trends in Fraud and Identity Theft*, 2000–2003 and 2003–2006.

or stolen hardware, or other administrative error. First, it is notable that as more states required organizations to report compromised digital records, the volume of annual news stories on the topic increased significantly. In fact, there were more reported incidents in the period 2005–2007 than in the previous twenty-five years combined. We found 126 incidents of compromised records between 1980 and 2004, and 687 incidents between 2005 and 2007. Just summing these incidents, when mandatory reporting legislation was in place in many states, we find that 72 percent of the stories concern data that were accidentally placed online or exposed through administrative errors, stolen equipment, or other security breaches such as employee loss of equipment or backup tapes.

Several factors might explain the pattern of increasing incidents and volume of compromised data over time. First, there is the possibility that the results are skewed by the relative growth of new, fresh news stories devoted to this issue and the loss of older stories that disappeared from news archives as time passed. Perhaps there have always been hundreds of incidents every year, but only in recent years has the severity of the problem been reported in the news. If this were the case, we would expect to see a gradually decaying pattern with a greater number of reported cases in 2007 than in 2006, 2005, and so on. However, the dramatic difference in reported incidents between later years and early years suggests that this effect does not adequately explain our observations. A second possibility is that greater media attention or sensationalized reporting in 2005 and 2006 led to a relative over-reporting of incidents, compared with previous years. Literature on media responses to perceived crises or "moral panics" would suggest that a similar effect commonly accompanies issues that are granted a disproportionate amount of public attention, such as the mugging scare in Great Britain in the 1970s or the crackdown on the rave subculture in the 1990s.[26] Although it is unlikely that media outlets have exaggerated the amount of electronic personal record loss, it is possible that in previous years a certain number of events went unreported in the media owing to lack of awareness or interest in the issue of identity theft. A third possibility is that there were more reported incidents of data loss between 2005 and 2007 because organizations are maintaining and losing a larger quantity of electronic data and because a changing legislative environment in many states is obliging organizations to report events publicly that would have gone unreported in previous years. The fourth possibility, and the most plausible one, is that mandatory reporting legislation has exposed both the severity of the problem and the common circumstances of organizational mismanagement.

It is likely that a combination of factors explain our observations. Data breach notification legislation that requires the prompt reporting of lost records in California came into effect in 2003; however, the legislation was not widely adopted and implemented by other states until 2005, which might help to explain the dramatic increase in reported cases. Data breach notification legislation in California, as in many other states, requires notification when a state resident has been a victim of data loss, regardless of where the offending organization resides. Therefore, organizations located in states without data breach notification laws, such as Oregon, are still required to report cases to victims who live in states that have enacted this type of legislation, such as New York. The nature and complexity of many databases means that, in many cases, compromised databases are likely to contain information about residents who are protected by data breach notification legislation, thus increasing the total number of reported cases.

Conclusion

The computer hacker is one of the most vilified figures in the digital era, but are organizations just as responsible as hackers for compromised personal records? To examine the role of organizational behavior in privacy violations, we analyzed 852 incidents of compromised data between 1980 and 2007. In the United States, some 1.9 billion records have been exposed, either through poor management or hacker intrusions: about nine personal digital records for every adult. There were more reported incidents between 2005 and 2007 than in the previous twenty-five years combined, and while businesses have long been the primary organizations hemorrhaging personal records, colleges and universities are increasingly implicated. Mandatory reporting laws have exposed how many incidents and how many records have been lost because of organizational mismanagement, rather than hackers. In the period since these laws came into force, 7 percent of incident reports do not attribute blame, 27 percent blame hackers, and 66 percent blame organizational mismanagement: personally identifiable information accidentally placed online, missing equipment, lost backup tapes, or other administrative errors.

Surveying news reports of incidents of compromised personal records helps expose the diverse situations in which electronic personal records are stolen, lost, or mismanaged. More important, it allows us to separate incidents in which personal records have been compromised by outside hackers from incidents in which breaches were the result of an organizational lapse. Of course, we should expect organizations to perform due diligence and safeguard the digital records holding personal information from attack by malicious intruders. But often organizations are both the unwilling and unwitting victims of a malicious hacker. Through this study of reported incidents of compromised data, we found that two-fifths of the incidents over the past quarter-century involved malicious hackers with criminal intent. Surprisingly, however, the proportion of incident reports involving hackers was smaller than the proportion of incidents involving organizational action or inaction. While 27 percent of the incidents reported clearly identified a hacker as the culprit, 66 percent of the incidents involved missing or stolen hardware, insider abuse or theft, administrative error, or the accidental exposure of data online. The remainder of news stories record too little information about the breach to determine the cause—either organizations or individual hackers might be to blame for some of these incidents.

Figure 2-1 helps put the trend line analyzed in this chapter into the context of identity theft complaints received by the Federal Trade Commission.

In 2006 and 2007, the FTC received roughly 250,000 consumer complaints of identity theft and 200,000 consumer complaints of internet-related fraud annually. Such official consumer reports can serve as an indicator of the outcome of compromised digital records, and it is interesting to note that until 2004 fewer than fifty news stories about compromised digital records were reported each year. Beginning a year later, the rate of such news reports increased dramatically, bringing into view a clearer picture of the ways in which personal electronic records get compromised.

Organizations probably can be blamed for the management practices that result in administrative errors, lost backup tapes, or data exposed online. And even though an organization can be the victim of theft by its employees, we might still expect organizations to develop suitable safeguards designed to ensure the safety of client, customer, or member data. Even using the news media's expansive definition of hacker as a basis for coding stories, we find that a large portion of the security breaches in the United States are due to some form of organizational malfeasance.

One important outcome of the legislation is improved information about the types of security breaches. Many of the news stories between 1980 and 2004 report paltry details, with sources being off the record and vague estimates of the severity of the security breach. Since the enactment of mandatory reporting legislation in many states, most news coverage provides more substantive details. In 2007 only one of the 263 news stories did not make some attribution of responsibility for a security breach.

Legislators at the federal and state level have adopted two main strategies to address the problem of electronic record management. On one hand, they have directly targeted individuals (computer hackers) whose actions potentially threaten the security of private electronic data. The CFAA has been repeatedly strengthened in response to a perception that electronic data theft represents a material and growing concern. However, our data suggest that malicious intrusion by hackers makes up only a portion of all reported cases, while other factors, including poor management practices by organization themselves, contribute more to the problem.

The second strategy employed by regulators might be thought of as an indirect or "disciplinary" strategy. Data breach notification legislation obliges organizations that manage electronic data to report any data loss to the individuals concerned. Companies, wary of both the negative publicity and the financial costs generated by an incident of data loss, are encouraged to adopt more responsible network administration practices. Similarly, end users are urged to weigh both the risk of doing business electronically and the costs associated with taking action once they are notified of a breach. The practice of using a risk/reward calculus to achieve policy objectives through legislation has been termed governing "in the shadow of the law" by some contributors to the critical legal studies and governmentality literature.[27]

One potential problem with this strategy is that the risks and rewards will be unequally distributed among individual, state, and corporate actors. While a large corporation might possess the resources and technical skill necessary to encrypt data, secure networks, and hire external auditors, other organizations in the private or public sector might not find the risk of potential record loss worth the expenditure necessary to secure the data. Governing through this type of market discipline is likely to result in a wide spectrum of responses from differentially situated actors.

There are a number of alternatives open to lawmakers and policy advisers that could materially strengthen the security of electronic personal records in this country. Alternatives include setting stricter standards for information management, levying fines against organizations that violate information security standards, and mandating the encryption of all computerized personal data. However, the introduction of legislation to directly regulate organizations that handle electronic information would certainly be controversial. A wide variety of agencies, companies, and organizations manage personal records on a daily basis. This complexity would hinder the imposition of standardized practices such as encryption protocols. Corporations would probably balk at the prospect of having to pay fines or introduce expensive security measures and accuse the government of heavy-handed interference. Others might argue that the imperatives of free-market capitalism demand that the government refrain from adopting punitive legislation, especially in order to maximize competitiveness. In the incidents studied here, most of the security breaches were at commercial firms and educational organizations, rather than breaches of individuals' security. However, identity theft can have a significant impact on individuals whose identities are stolen; it can also have a significant impact on the reputation of the organization that was compromised.

Although computer hacking has been widely reframed as a criminal activity and is punished increasingly harshly, the legal response has obfuscated the responsibility of commercial, educational, government, medical, and military organizations for data security. The scale and scope of electronic record loss over the past decade would suggest that organizational self-regulation or self-monitoring is failing to keep our personal records secure and that the state has a more direct role to play in protecting personal information. State-level initiatives have helped expose the problem by making it possible to collect better data on the types of security breaches that are occurring, and to make some judgments about who is responsible for them. If public policy can be used to create incentives for organizations to better manage personally identifiable information and punish organizations for mismanagement, such initiatives would probably have to come at the state level. Electronically stored data might very well be weightless, but the organizations that retain personally identifiable information must shoulder more of the heavy burden for keeping such data secure.