Insurance Information Institute

INFORMATION SECURITY AND LIABILITY

Is Your Company Prepared for a Data Breach?

March 2006

Claire Wilkinson
Vice President—Global Issues
Insurance Information Institute
110 William Street
New York, NY 10038
Tel: (212) 346-5509
Fax: (212) 732-1916
clairew@iii.org www.iii.org

Introduction

A wide range of electronic systems are in use today that store data and information of a sensitive nature. Businesses of every shape and size increasingly rely on the Internet to sell their products, to service their customers, and to run their internal operations. At the same time, digital devices such as cell phones, MP3 players, PDAs, and laptops have become the essential accessories of modern-day living. These devices interface with the Internet in ever-evolving ways, increasing the ease and speed with which information can be transmitted, downloaded and stored.

As businesses increasingly depend on electronic data and computer networks to conduct their daily operations, growing pools of personal and financial information are being transferred and stored online. This can leave corporations exposed to potentially enormous liability, if and when a breach in data security occurs. A civil complaint filed by New York Attorney General Eliot Spitzer in March 2006 against Washington D.C.-based Web site operator Gratis Internet alleging deceptive business practices, is the latest example of the growing avenues of legal liability that companies face.[1] The suit alleges that Gratis violated its own privacy policies by collecting and selling personal information on more than 7 million users, during a period of three and a half years. Gratis has denied the allegations. The trend of businesses to outsource their IT or business process services also has substantial liability consequences as vendors, both in the United States and increasingly offshore, may not exercise the same degree of care in protecting client data as the original company.

The increasing use of online tools such as blogs and instant messaging is another source of potential liability. The Department of Homeland Security and the National Cyber Security Alliance (NCSA) predict that 2006 will see an increase in Internet attacks targeting instant-messaging networks and handheld devices.[2] The recent Blackberry patent dispute is a good example of how dependent society has become on electronic forms of communication.[3] Two out of every five Americans now have broadband access at home, and in August 2005, the percentage of active U.S. Internet users connecting online via broadband from home reached an all-time high of 61 percent, according to Nielsen/NetRatings. U.S. Census Bureau data shows that in 2003 some 55 percent of U.S. households had Internet access, compared with just 26 percent in 1998 *(Fig. 1)*.[4]

[1] The suit was filed March 23, 2006 in the State Supreme Court of New York. It alleges that Gratis sold personal information obtained from millions of consumers to three independent e-mail marketers despite a strict promise of confidentiality.
[2] Department of Homeland Security and NCSA 2006 Emerging Internet Threat List.
[3] The dispute was settled in March 2006, when Research in Motion Ltd. settled with NTP Inc. for $612.5 million, in full and final settlement of all claims.
[4] *Statistical Abstract of the United States: 2006*, U.S. Census Bureau.

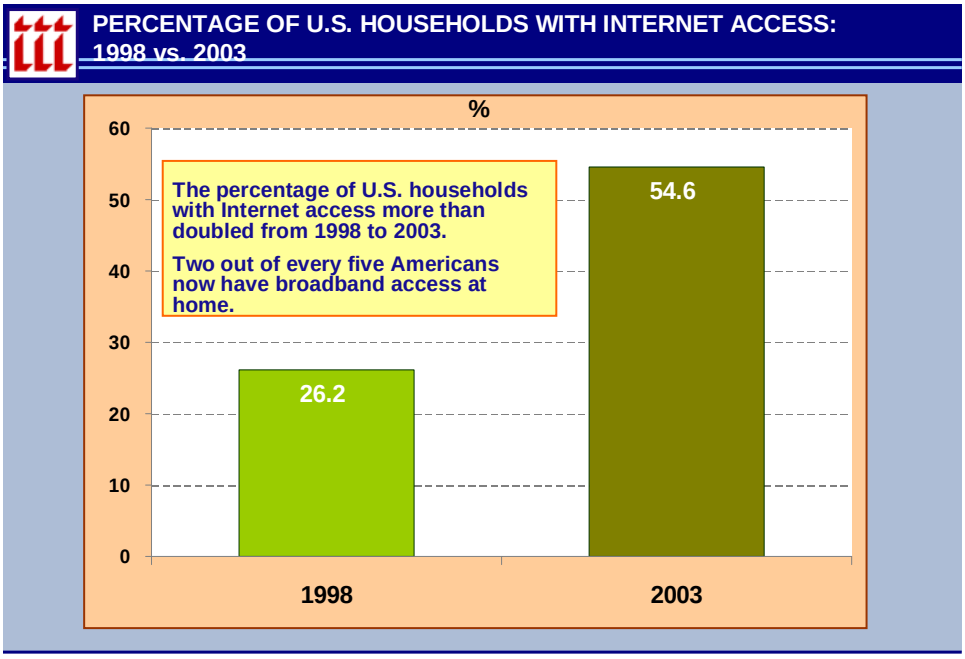


Fig. 1

Source: U.S. Census Bureau, Statistical Abstract of the United States: 2006; Nielsen/NetRatings.

In February 2005, in what is widely regarded as a watershed event, Atlanta-based data aggregator ChoicePoint announced a data breach that compromised the personal information of some 162,000 consumers across the United States. Thieves posed as small business customers and then opened phony ChoicePoint accounts, thus gaining access to consumers' personal information, including names, addresses and social security numbers. As a result of the breach, in March 2005 ChoicePoint said that it would stop selling personal information about consumers to small businesses. In January 2006 ChoicePoint reached an agreement with the Federal Trade Commission (FTC) to pay $15 million to settle charges involving violations of consumer privacy. Under the terms of the agreement, ChoicePoint will pay the federal government a $10 million penalty and $5 million to compensate approximately 800 consumers whom the FTC identified as victims of identity theft. The penalty set a new record for fines assessed by the federal agency. ChoicePoint also agreed to change the way it screens customers, to implement new procedures for handling information, and to get independent security audits every other year until 2026. The incident has prompted intense debate about disclosure requirements at the federal and state level following such data breaches (see later section on regulation).

In this environment, steps to protect the privacy of customers and employees are a critical part of doing business in the electronic world. While traditional insurance policies typically have not handled these emerging risks, in recent years limited coverage under traditional policies has become available and specialist cyber insurance products have been developed to help businesses protect their bottom line. A 2006 corporate risk survey by Swiss Re found that computer-based risks are the number one concern among executives worldwide *(Fig. 2)*.[5]

[5] Swiss Re Corporate Risk Survey: A Global Perspective, Produced for Swiss Re by StrategyOne, March 2006

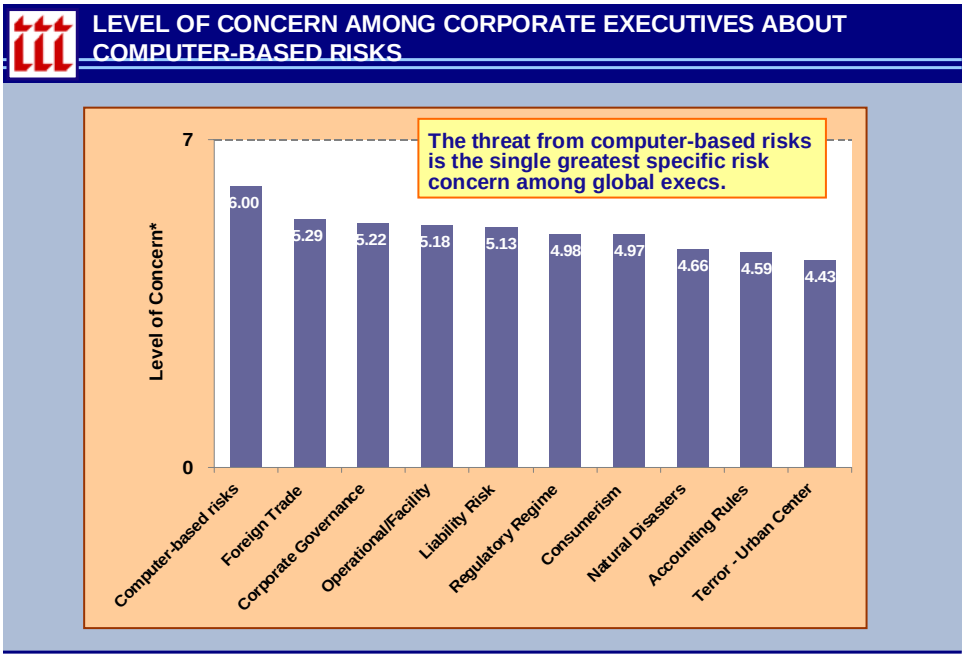


Fig. 2

Source: Swiss Re Corporate Risk Survey: A Global Perspective, March 2006.

***Based on a 0 to 10 scale where 0 is not at all concerned and 10 is extremely concerned.**

According to the survey's findings, senior executives in both the manufacturing and financial sectors rate computer-based risks as their primary concern. Yet growth of the cyber insurance market has been relatively slow in the face of the increasing level of risk. Current estimates suggest that only 25 percent of businesses buy cyber insurance. The cost of coverage may be a factor, while certain businesses may underestimate the risk. This may be due in part to the network security measures being implemented by many businesses up-front. The logic of this approach is that it makes more sense to invest in security to prevent attacks from occurring, than in insurance to cover costs afterward. This strategy also avoids the negative public relations and regulatory consequences associated with breaches.

Structure of Report

This report begins with an overview of the nature of the threats facing businesses from cyber liabilities today, and what the financial impact of such liabilities can be. This is followed by an analysis of the potential avenues of legal liability being pursued against companies that have experienced data breaches. The report then examines the regulatory environment and how recent legislation such as the Gramm-Leach-Bliley Act (GLB) in 1999, the Sarbanes-Oxley Act of 2002 and California's Security Breach Information Act (SB 1386) of 2003, are increasing potential legal liabilities in this area. Following a discussion of the evolving range of cyber insurance products that are available to respond to such risks, the report concludes with the latest information on identity theft trends.

The Nature of the Threat

Frequent media reports on information security and privacy breaches underscore that the threat is growing and potentially unlimited. According to the Privacy Rights Clearinghouse, from February 2005 to date an estimated 100-plus security breaches have occurred, affecting

more than 52 million individuals nationwide. The ID Theft Resource Center puts the number of U.S. data incidents even higher, at more than 152 in 2005 affecting more than 57.7 million individuals *(Fig. 3) (See Appendix 1)*. Further, the breaches are not limited to any one area of business, with corporations, educational institutions, financial institutions, healthcare organizations, as well as state and federal government systems all becoming targets.

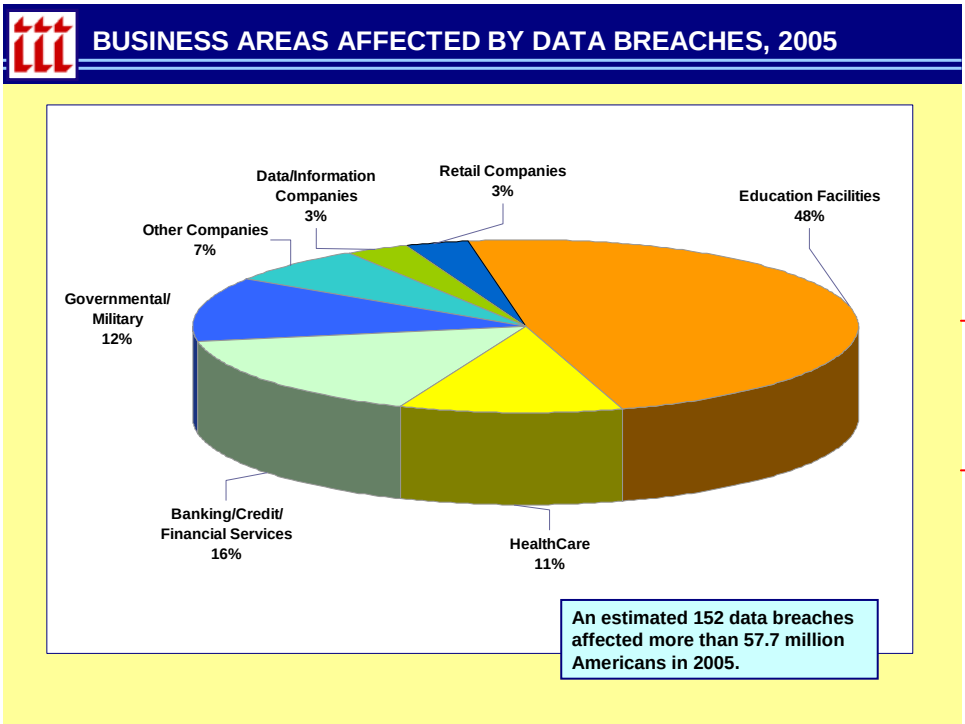


Fig. 3

Source: ID Theft Resource Center, as of 2/21/06

Of the 152 incidents disclosed in 2005, there were breaches at:

- 73 education facilities
- 24 banking/credit/financial service companies
- 18 government/military organizations
- 17 healthcare facilities/companies
- 5 data/information companies
- 5 retail companies
- 10 other types of companies

The actual number of breaches is much higher than published figures suggest. Despite increased pressure to disclose breaches, many corporations are still motivated to conceal them, fearing bad press, lawsuits or copycat attacks *(Fig. 4)*.

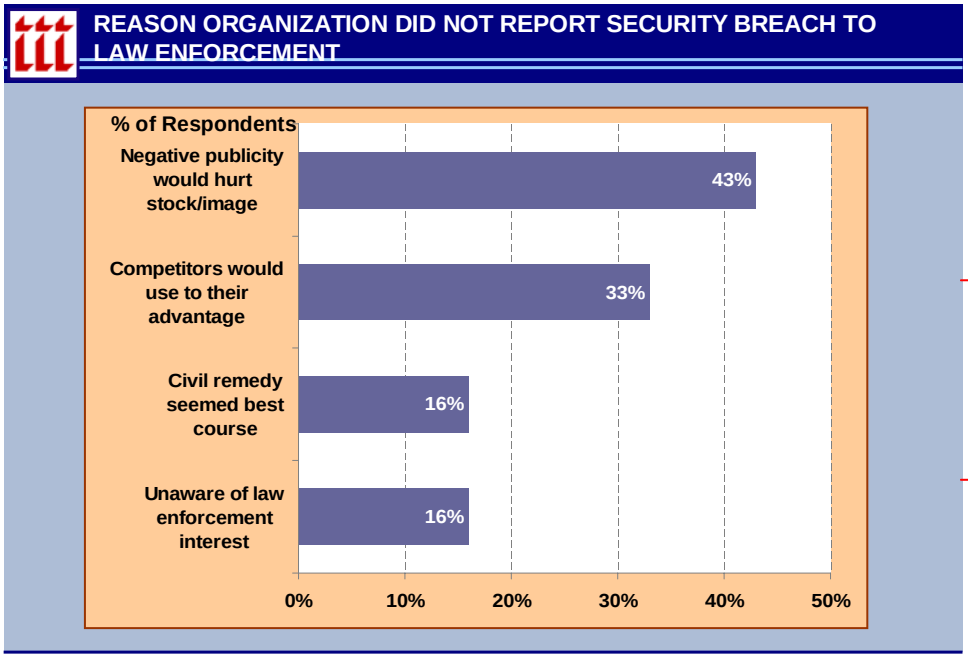


Fig. 4

Source: CSI/FBI 2005 Computer Crime and Security Survey, Computer Security Security Institute.

Some government agencies may refuse to disclose breaches for security reasons. It is also likely that many organizations suffer stealth breaches and never become aware of the breach or its consequences. Today, every entity or organization that has a computer system or network is at risk of being subjected to computer attacks, employee misuse, or loss or theft of information.[6]

The 2005 E-Crime Watch Survey of security and law enforcement executives found that 68 percent of the 819 survey respondents reported at least one e-crime or intrusion committed against their organization in 2004, and 88 percent anticipated an increase in e-crime during 2005 *(Fig. 5)*.

[6] Information Management—New Threats, New Liabilities, Brad Gow, Robert Hammesfahr, Margaret Reetz, Beth Stroup and Cozen O'Conner.

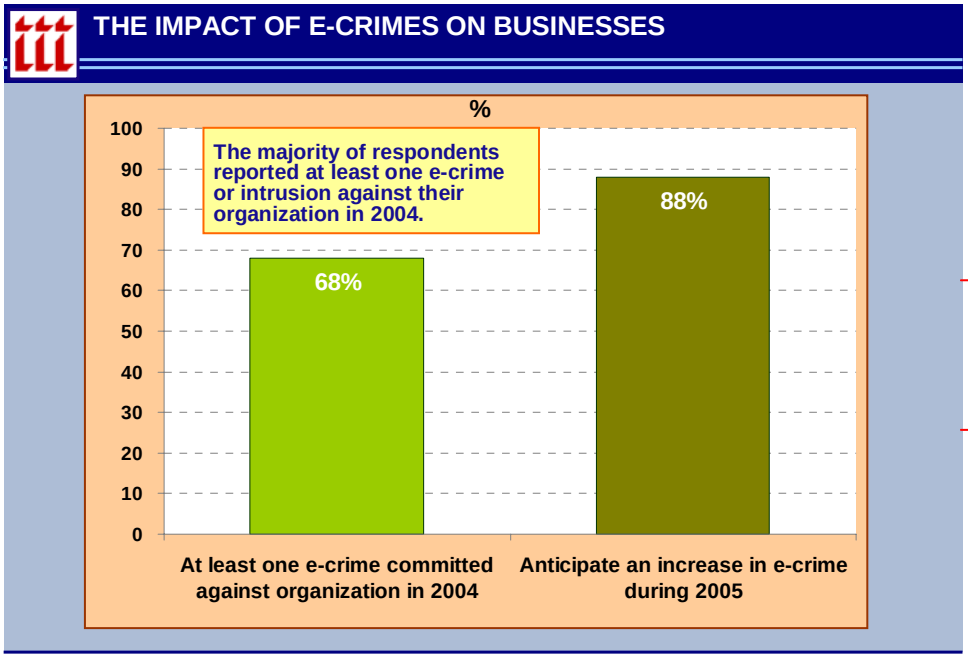


Fig. 5

Source: 2005 E-Crime Watch Survey, CSO Magazine.

When asked what e-crimes were committed against their organizations in 2004, respondents cited virus or other malicious code as most prevalent (82 percent), with spyware (61 percent), phishing (57 percent) and illegal generation of spam email (48 percent) falling close behind *(Fig. 6)*. Phishing, a form of online identity theft whereby emails and Web sites masquerading as official businesses are created and used to deceive Internet users into disclosing their personal data, showed the largest single percent increase of an e-crime year over year, jumping from 31 percent in the 2004 survey to 57 percent in the 2005 survey.

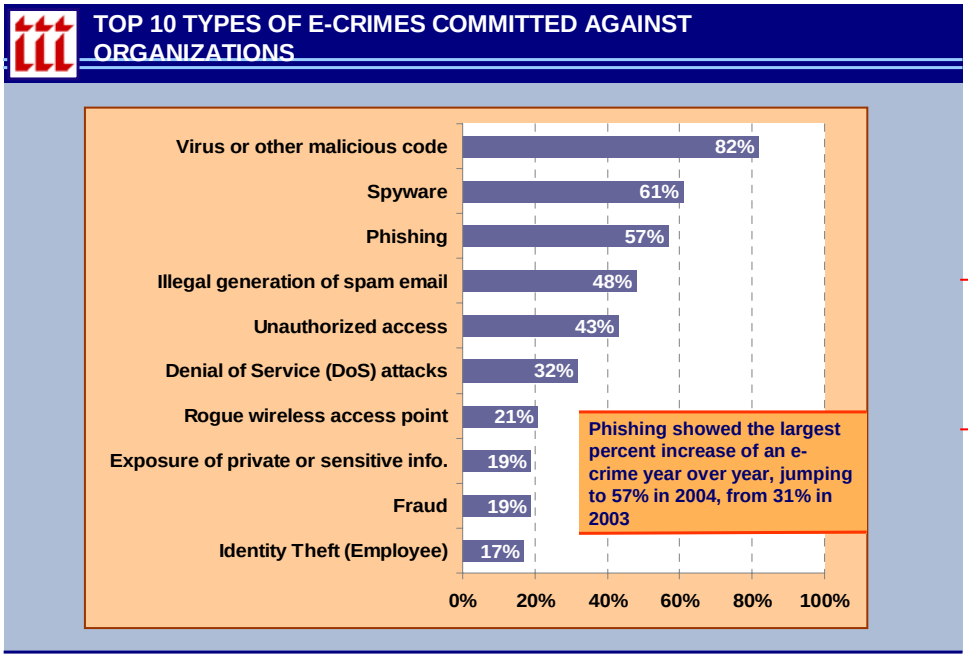


Fig. 6

Source: 2005 E-Crime Watch Survey, CSO Magazine.

The respondents most frequently identified hackers, followed by current employees and foreign entities, as the greatest cyber security threat to their organization *(Fig. 7)*.

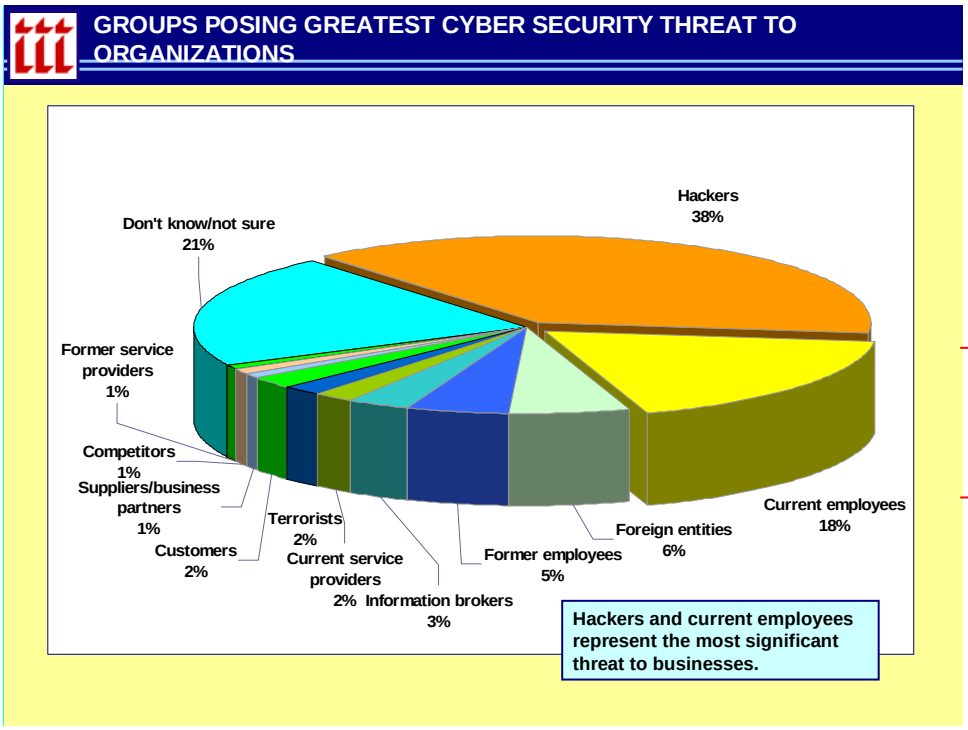


Fig. 7

Source: 2005 E-Crime Watch Survey, CSO Magazine.

Concerns have also been growing about cyber attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering and acts of war. For example, IBM predicts a surge in criminal-driven cyber attacks in 2006.[7] According to IBM, the high profile arrests of cyber criminals in the U.S. and around the world in 2005 indicates a trend toward individuals linked to organized crime and motivated to make money. With software and networks becoming more secure, IBM anticipates a fundamental shift in cyber crime from pervasive global outbreaks to smaller attacks targeted at specific organizations for extortion purposes. It also expects that many criminals may target the most vulnerable access point within a company or organization—its personnel—to execute such an attack. Attacks could also become part of the arsenal of weapons wielded by radical religious or political groups. In February 2006, worldwide protests throughout the Muslim world following publication by a Danish newspaper of cartoons depicting the prophet Mohammed were accompanied by attacks on the Web sites of many Danish businesses.

The growth in cyber crimes could have significant implications for insurers, particularly given the uncertain climate surrounding the long-term management and financing of terrorism risk in the U.S. A Government Accountability Office (GAO) report notes that while increasing computer interconnectivity offers many benefits, it also poses significant risks to the nation's computer systems and to the critical operations and infrastructures they support.[8] The report cites growing concern among U.S. authorities about the prospect of combined physical and cyber attacks that could have devastating consequences. "As larger amounts of money are

[7] IBM 2005 Global Business Security Index Report, January 2006.
[8] Critical Infrastructure Protection: Dept. of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, Government Accountability Office (GAO), May 2005.

transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests," GAO states.

The unknown nature of many cyber attacks is another area of rising concern. Security executives frequently appear to have trouble identifying who is attacking them, where the attack is coming from and how it is being executed. A worldwide study by CIO and PricewaterhouseCoopers reveals that information security executives often don't know about the damage the incidents cause or how they have been attacked.[9] The number of respondents reporting damages as "unknown" jumped to 47 percent in 2005, up from 40 percent in 2003 *(Fig. 8)*.

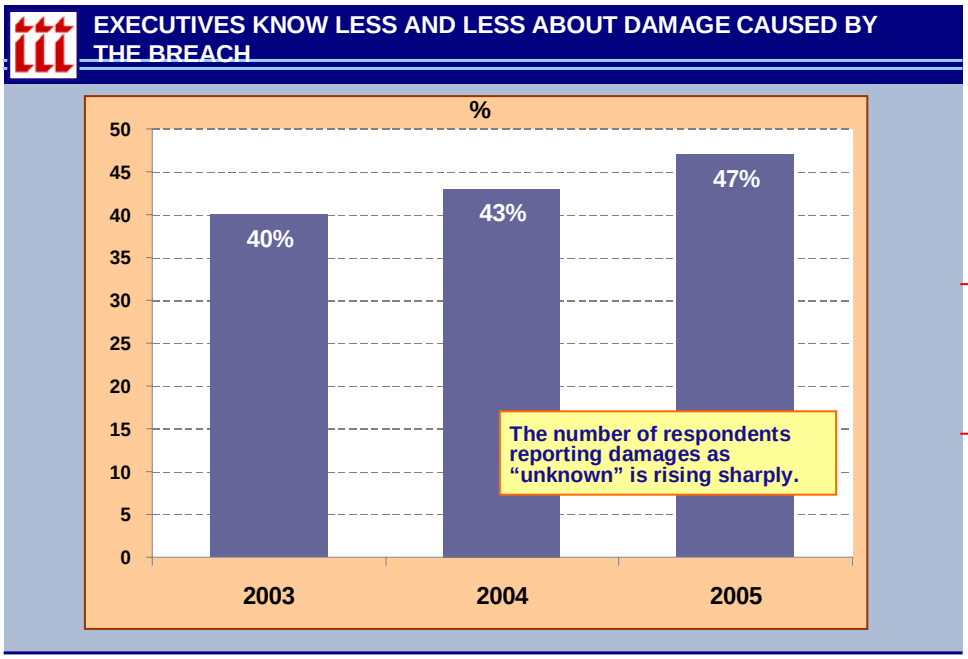


Fig. 8

Source: The Global State of Information Security 2005, CIO and PricewaterhouseCoopers.

In survey responses, "unknown" was the second most prevalent attack type, the fourth most common attack method and the third highest attack source *(Fig. 9)*.

[9] The Global State of Information Security 2005, CIO and PricewaterhouseCoopers, September 15, 2005.

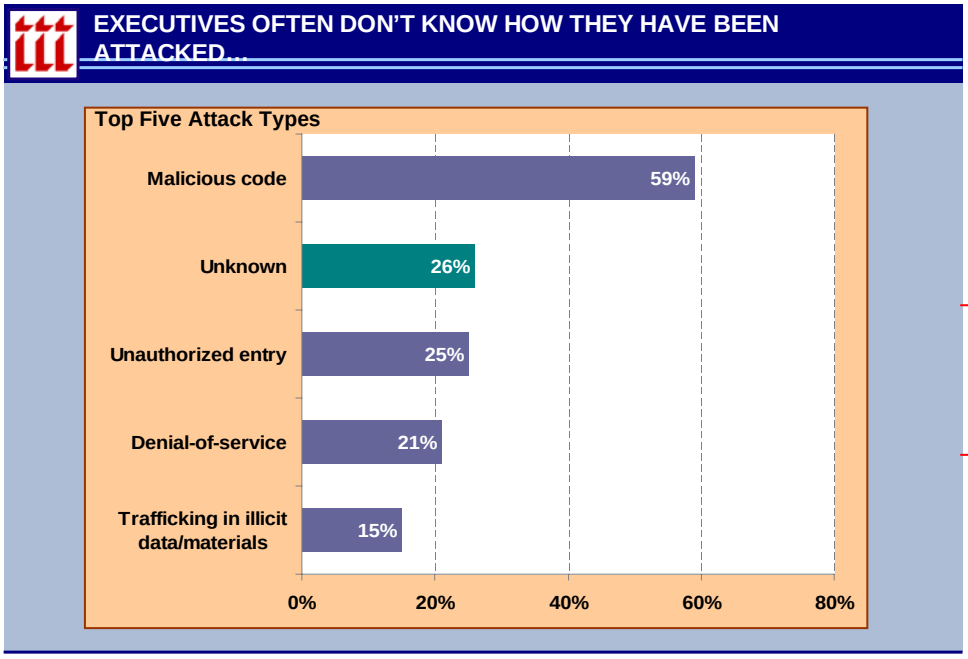


Fig. 9

Source: The Global State of Information Security 2005, CIO and PricewaterhouseCoopers.

In addition, when asked how their organization learned of the attacks, only 21 percent cited data or material damage, behind firewalls and intrusion detection system (IDS) logs, as well as colleague alerts. This indicates that information security professionals most often react, learning of attacks after the damage is done, and frequently are unable to figure out what it was, where it came from or who did it, according to the findings.

The Enemy Within

While much of the focus to date has been on external threats such as viruses, recent research suggests that the more damaging threats are those that stem from within an organization. Breaches due to internal attacks appear to be on the rise. More than double the number of respondents to a Deloitte survey reported attacks from an internal source in 2005 than in 2004 (35 percent in 2005, compared with 14 percent in 2004) *(Fig. 10)*.[10] The number of organizations experiencing internal attacks is also higher than the number reporting external attacks (26 percent in 2005).

[10] 2005 Global Security Survey, Deloitte, June 2005.

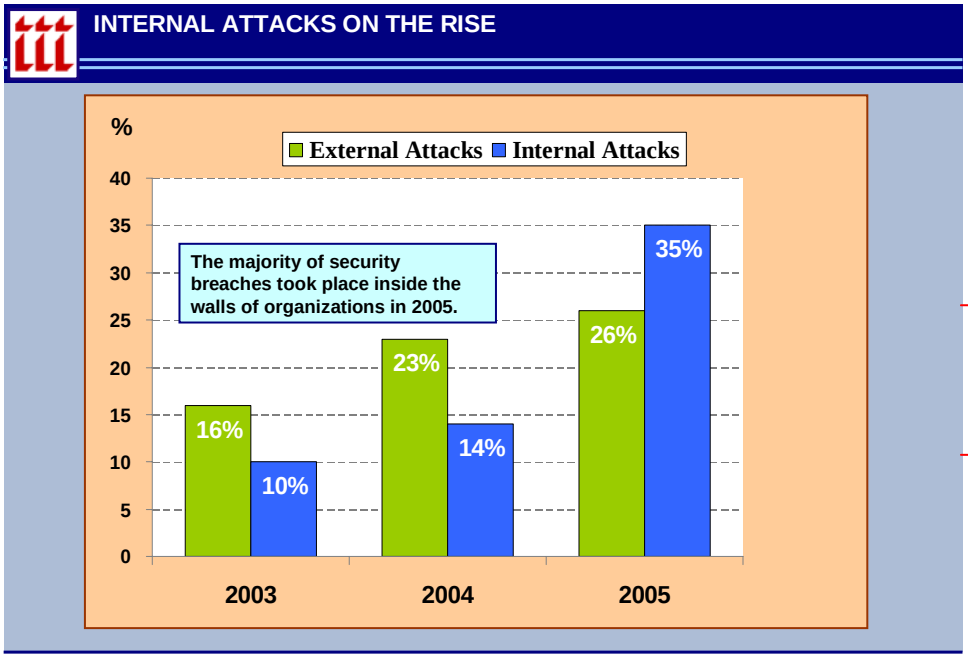


Fig. 10

Source: Deloitte, 2005 Global Security Survey.

Similarly, IBM identifies insider attacks as a trend to watch in 2006. It suggests that as software becomes more secure, computer users will continue to be the weak link for companies and other entities. Criminals will focus their efforts on convincing end users to execute the attack instead of wasting time on lengthy software vulnerability discovery. Globalization, employee layoffs, mergers and acquisitions all present challenges for businesses attempting to educate users against these threats, it states.[11]

Financial Impact on Corporations Suffering Data Breaches

Organizations are increasingly vulnerable to substantial economic loss from cyber security attacks. In the case of an information security breach, financial institutions in particular, can be exposed to significant financial and reputational loss. Customers may decide to sever their relationships with these corporations and government agencies may impose fines and burdensome regulation. A 2005 national survey of nearly 10,000 adults who experienced personal data security breaches found that nearly 20 percent said they had terminated their relationship with the companies that maintained their data, while 40 percent said they were thinking about it *(Fig. 11)*. Furthermore, 5 percent of those surveyed said they had hired lawyers upon learning that their personal information may have been compromised.[12]

[11] IBM 2005 Global Business Security Index Report, January 2006.
[12] National Survey on Data Security Breach Notification, September 2005, Ponemon Institute, sponsored by White & Case.

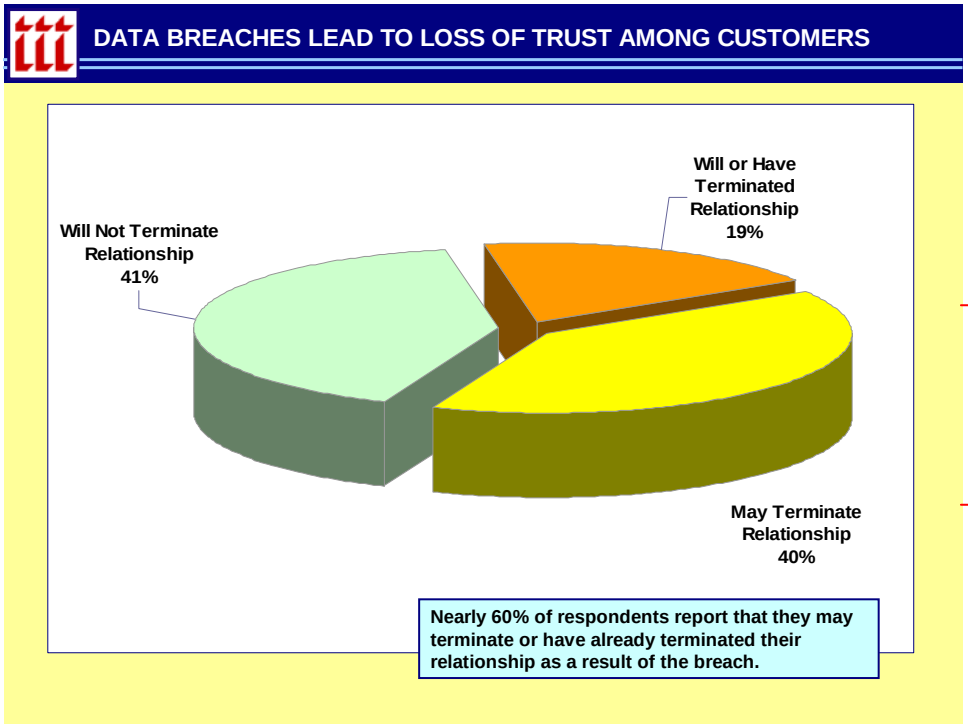


Fig. 11

Source: National Survey on Data Security Breach Notification, Sept. 2005, Ponemon Institute, sponsored by White & Case.

To date a number of companies have recorded reserve charges related to data security breaches, and as the number of data breaches grows, these charges likely will increase. For example, for the year ended December 31, 2005, ChoicePoint recorded pre-tax charges totaling $27.3 million ($20.7 million net of taxes) for the FTC settlement as well as specific legal expenses and other professional fees related to its data breach. Warehouse buying club BJ's Wholesale Club and shoe retailer DSW, both of which reached settlements with the FTC in 2005, have also recorded substantial reserve charges for costs related to data breaches.

As of October 29, 2005, DSW estimated its potential exposure to losses related to the theft in a range of $6.5 million to $9.5 million. It took a charge of $6.5 million in the first quarter of 2005 and said that the reserve amount could increase or decrease as the situation develops. Similarly, BJ's Wholesale Club recorded a pre-tax charge of $3 million in the first quarter of 2005 in relation to its breach, following charges totaling $7 million in 2004. As of October 29, 2005, BJ's said its reserve balance was $4.1 million, representing its best estimate of the remaining costs and expenses related to the matter at that time.

Although varying estimates of financial losses from cyber attacks have been reported over the last several years, the tendency of corporations not to report cyber-crime incidents may mean that actual losses are considerably higher. As much as 80 percent of all cyber-crime activity goes unreported, according to the 2005 CSI/FBI Computer Crime and Security Survey. Clearly, there is the potential for significant financial loss in the future, as illustrated by the following examples:

- The Computer Economics 2005 Malware Report puts the worldwide financial impact of malicious code attacks at $14.2 billion in 2005 *(Fig. 12)*. While this was down from $17.5 billion in 2004, the report points out that the nature of malicious code attacks is changing from overt general threats to more focused, covert attacks targeting specific companies or business sectors.

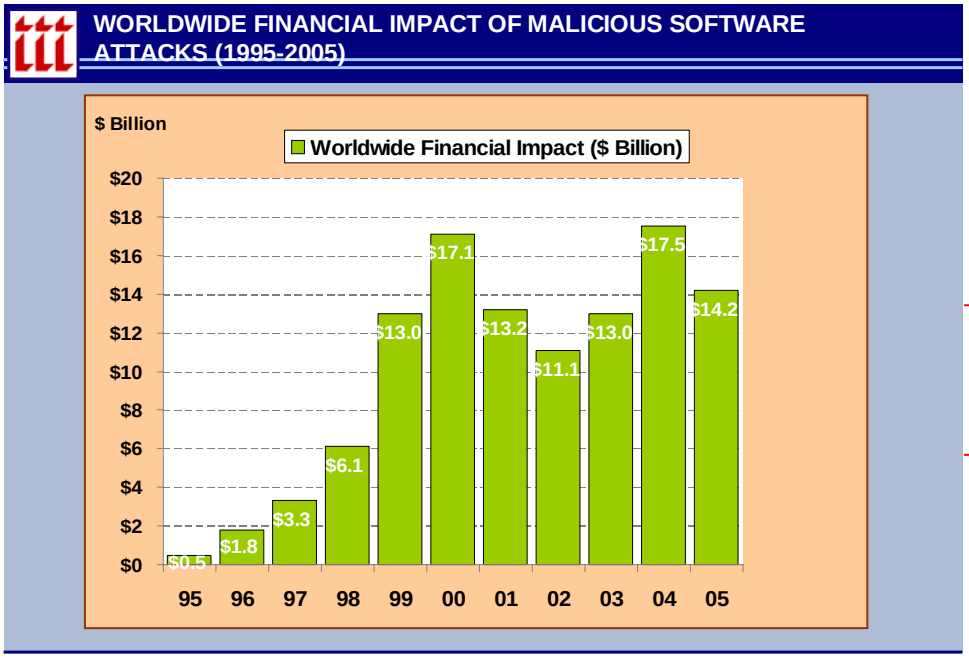


Fig. 12

Source: 2005 Malware Report, Computer Economics.

This means that the economic impact is rising for organizations or industry sectors that are specific targets of attacks. An analysis of the costs shows that "labor"—the expense associated with analyzing, repairing, and cleansing of operating systems, applications, databases, networks, and machines—was the most cost-intensive category in 2005. By comparison, the 2004 study ranked "loss of business revenue" as the most costly category. This shift in ranking may reflect the fact that more focused attacks result in infections that may require a greater manual effort to eradicate. Further, as the nature of attacks becomes more targeted, organizations may be less willing to disclose such incidents, leading to an under-reporting of the category of "loss of business revenue".

- Respondents to the 2005 E-Crime Watch Survey report an average loss of $506,670 per organization due to e-crimes and a sum total loss of $150 million. More than half of respondents (53 percent) expected monetary losses to increase or remain the same during the remainder of 2005 *(Fig. 13)*.

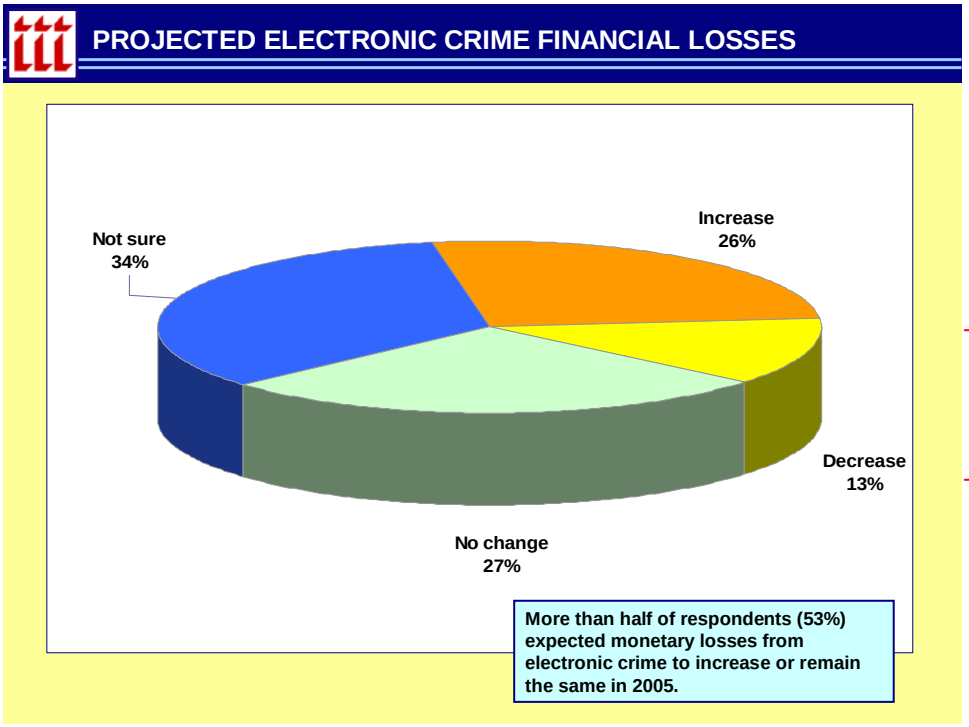


Fig. 13

Source: 2005 E-Crime Watch Survey, CSO Magazine.

The financial loss figures were not comparable to the previous year's survey due to a change in question format. Of those who experienced e-crimes, more than half of respondents (55 percent) reported operational losses, 28 percent stated financial losses and 12 percent declared harm to reputation as a result.

- The 2005 CSI/FBI computer crime and security survey reports a decline in the total dollar amount of financial losses resulting from cyber crime. Total losses for 2005 were $130.1 million for the 639 respondents that were willing and able to estimate losses—down from the $141.5 million losses for the 269 equivalent respondents in 2004. Given that the total number of respondents has increased significantly, the survey shows a dramatic decrease in average total losses per respondent (there were 700 responses in 2005, up from 494 responses in 2004). Losses per respondent dropped to $203,606 from $526,010—a 61 percent decline. However, unauthorized access and theft of proprietary information showed significant increases in average loss per respondent. Unauthorized access accounted for an average loss per respondent of $303,234 in 2005, up from $51,545 in 2004, while theft of proprietary information accounted for an average loss per respondent of $355,552 in 2005, up from $168,529 in 2004. According to the survey, virus attacks continue as the source of the greatest financial losses, and can be attributed to the increased awareness of, and improved technology to cope with some threat types, such as viruses *(Fig. 14)*.

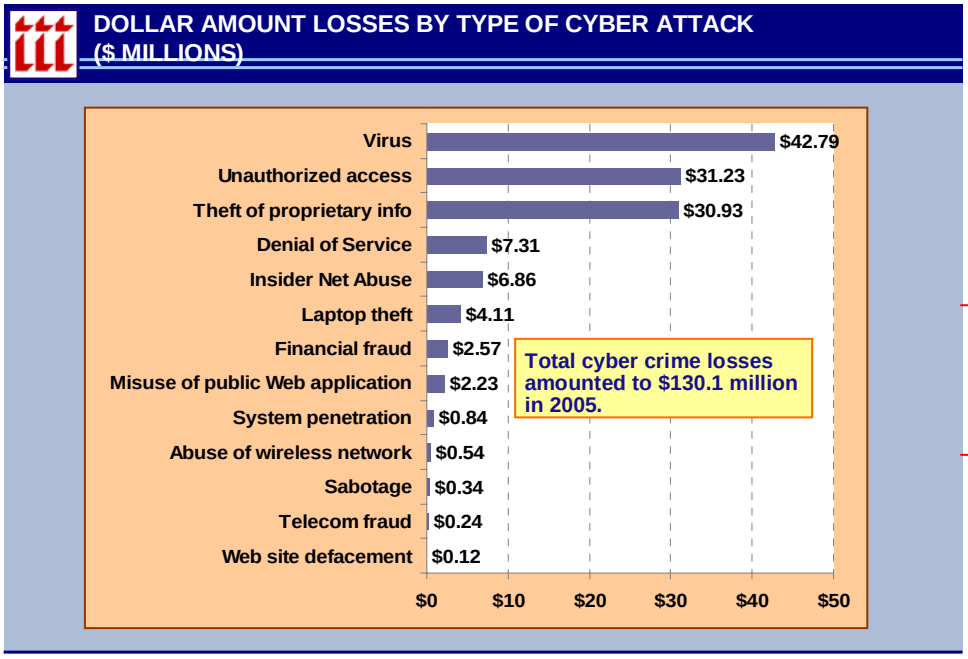


Fig. 14

Source: 2005 CSI/FBI Computer Crime and Security Survey (639 respondents).

Data Breach-Related Litigation

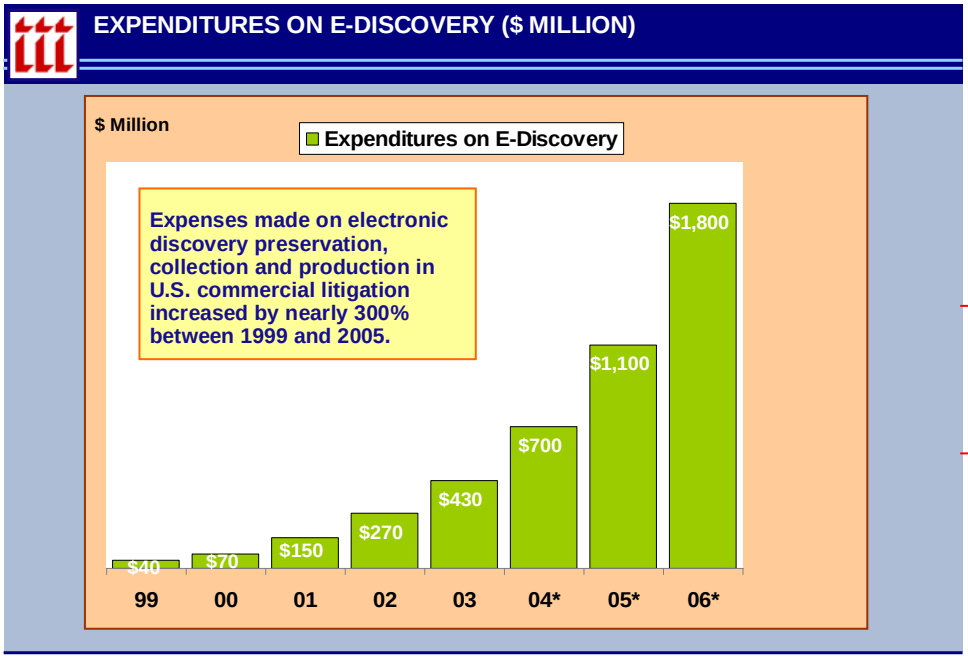
Various theories of legal liability are being tested by attorneys in an attempt to hold corporations liable for breaches in information security. Current cases involve the high profile 2005 data breaches that occurred at ChoicePoint, CardSystems Solutions, LexisNexis and DSW. These cases are seeking monetary, statutory and punitive damages, even though the identity thieves have not necessarily used the personal information in question, nor caused the owners actual financial harm.

The various theories of legal liability being pursued include:

- **Negligence**—company exercised insufficient care, caution and/or control of personal data (e.g., company maintained inadequate firewalls protecting its data systems; failed to conduct background checks of workers who later misused customers' personal information). Liability for negligence may also extend to subcontractors and contract workers.
- **Fraud**—company could be held liable for unauthorized use of personal information by others to commit fraud (e.g., identity thief misuses an existing customer's data to open a new account, or obtain a loan).
- **Misrepresentation**—company knowingly made claims about security of personal information of clients/customers that proved to be inaccurate or false (e.g., validity of company notices and advertising about information practices are in question or deceptive).
- **Personal injury—**company's database of customer personal information fell into wrong hands leading to invasion of privacy (see below), and causing the victim financial harm.

- **Invasion of privacy and misappropriation**—company holding personal information records failed to maintain appropriate controls to properly safeguard customer information.
- **Failure to warn**—company is subject to breach of security, potentially exposing the personal financial records of thousands of clients/customers, and fails to disclose risk or notify them as required under state regulations.
- **Breach of warranty/contract—**company failed to uphold a promise of security in the storage or transfer of data.
- **Vicarious liability—**company could be held liable for any damages incurred by business partners or its customers to whom it has sold data.
- **Securities litigation—**data vendor suffers drop in stock price after disclosure of breach, leading to accusations by shareholders that management failed to exercise appropriate responsibility.
- **Government sanction—**company can face fines/penalties and potentially criminal charges in the event of data breaches. This is likely to emerge as significant issue as more states adopt legislation designed to penalize companies in the event of data breaches.

Companies are also increasingly concerned about litigation arising from electronic discovery. Research suggests e-discovery is the number one litigation-related burden for companies with revenues in excess of $100 million. Over 80 percent of the U.S. companies surveyed now have records retention policies and 75 percent have litigation hold policies. Further, expenses made on electronic discovery preservation, collection and production in U.S. commercial litigation increased by nearly 300 percent between 1999 and 2005 *(Fig. 15)*.



*Projections

Fig. 15

Source: Socha-Gelbmann Electronic Discovery Survey; National Law Journal 8/2/04.

ChoicePoint and Other Data Breach-Related Litigation

A lawsuit was filed against ChoicePoint just days after disclosure of its security breach in February 2005. There are two key areas of litigation in the ChoicePoint case. Firstly, a securities suit filed by shareholders of ChoicePoint has alleged devaluation in the stock price due to the security breach. Class action lawsuits are also being brought in several states for privacy issues, ID theft and violations of various state and federal regulations. The exact outcome of the lawsuits remains to be seen.

On December 12, 2005, in Los Angeles, U.S. district court judge Mariana Pfaelzer questioned whether there was enough evidence to support a group of lawsuits brought against ChoicePoint. Judge Pfaelzer said that there was no evidence that any of the plaintiffs actually had their identities stolen. The judge characterized the evidence as being no more than a letter sent by ChoicePoint stating that the plaintiffs were among a group that might have had their information compromised. However, the plaintiff's attorney stated that merely furnishing personal data to the alleged identity theft ring was sufficient to trigger damages of up to $1,000 per plaintiff under federal consumer protection law. A written ruling in the case is expected to follow.

To date a number of data breach-related lawsuits have been filed against other companies. A few examples follow:

- In July 2005 a class action lawsuit was filed in California Superior Court in San Francisco against credit-card transaction processing firm CardSystems Solutions Inc. after a data breach of debit and credit card accounts potentially compromised the personal information of up to 40 million consumers. The lawsuit alleged that CardSystems, in addition to Visa and MasterCard, violated state law by failing to protect the data and promptly notify customers of the breach.
- In June 2005 Ohio Attorney General Jim Petro filed suit in Franklin County Common Pleas Court, asking the court to order shoe retailer DSW Inc. to individually notify around 700,000 customers affected by its March 2005 security breach. The suit was filed despite the fact that the state's consumer protection laws did not require disclosure.

Litigation based upon the fear of identity theft appears to be another avenue of potential recourse, as the following case illustrates:

- In February 2005, a New York State Supreme Court ruled that an existing tenant is not automatically required to give a landlord his/her Social Security number (SSN). The suit was filed by the tenant after she received a notice from her landlord demanding her SSN and date of birth as a condition for renewing her rent-stabilized lease. The tenant feared disclosure of her SSN might make her subject to identity theft and filed suit alleging that the landlord's request for her SSN constituted a violation of New York's consumer protection statute. The court ruled that "the weight of authority favors treating a Social Security number as private and confidential information." Also, to the extent that the landlord made receiving the tenant's private information a condition of renewing the lease, the court found that the landlord's actions were "clearly deceptive." The case was expected to proceed to trial.

Ultimately it is still too early to know how these types of cases may develop in future, but regardless of how or if liability is determined, the costs associated with legal defense, customer notification and lost business can be significant.[13]

Regulatory Developments

Recent federal legislation and regulations such as the Gramm-Leach-Bliley Act (GLB) and the Health Insurance Portability and Accountability Act (HIPAA) have required businesses to take appropriate measures in the areas of privacy and network security. The Sarbanes-Oxley Act also increased the financial reporting and disclosure requirements of publicly held companies. At the state level, California's Security Breach Information Act (SB 1386), set a precedent in the area of disclosure.

A number of states are expected to follow with legislation related to security breaches and security freezes. State security freeze laws enable consumers to stop identity thieves from getting credit in their names by locking or freezing access to their credit report and credit score. Congress is also considering several bills in which security breach notices would be mandated nationwide. These legislative and regulatory developments are expected to substantially increase potential legal liabilities in this area in future, increasing the need and demand for insurance coverage. A brief outline of the key pieces of legislation and their impact follows.

Gramm-Leach-Bliley (GLB)

The Gramm-Leach-Bliley (GLB) Financial Services Modernization Act of 1999 permitted affiliations between banks, securities firms and insurance companies, and introduced a number of key provisions related to customer privacy. Under GLB, financial institutions are required to disclose to customers their privacy policy for nonpublic information. Nonpublic information can be defined as personally identifiable information collected from, or about, consumers, or resulting from a transaction with consumers. Financial institutions are barred from disclosing customer account numbers or access codes to unaffiliated third parties for marketing purposes, with certain narrow exceptions. Other customer information may be shared with third parties, but customers must be informed and have the right to bar such sharing. Any attempt to gain private customer information by fraud or deception is made a federal crime. GLB is enforced by the U.S. Federal Trade Commission (FTC) and various federal bank/financial regulatory agencies as well as state insurance regulators.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability of Act of 1996 (HIPAA) established new standards for ensuring the security and privacy of individuals' medical information. The act requires healthcare organizations to protect the "individually identifiable health information" of patients and enrollees. "Individually identifiable health information" means any information, including demographic information collected from an individual, and any specific information that identifies, or could reasonably be believed to identify, an individual. The act also guarantees the rights of individuals to have more control over

[13] Kevin Kalinich, "RMs Focusing on Data Breaches," National Underwriter, January 23, 2006.

such information. The HIPAA is enforced by U.S. Department of Health and Human Services and the U.S. Department of Justice.

California's Security Breach Information Act (SB 1386)

California's Security Breach Information Act (SB 1386), which became effective July 1, 2003, was a landmark law that has had far-reaching implications at the state level. Essentially, it requires an agency, person or business that conducts business in California and owns or licenses computerized data that includes "personal information" to disclose any breach of security to any resident whose unencrypted data has been, or is believed to have been, acquired by an unauthorized person. "Personal information" means an individual's first name or first initial and last name in combination with one or more of the following data elements: a drivers license number, social security number or account, credit or debit card number.

More than 20 states now have security breach laws in place, similar to California's law. For example, Washington's SB-6043 was signed into law July 23, 2005, and also requires that consumers in the state be notified when their personal data is compromised. Similarly, New York signed the Information Security Breach and Notification Act (A04254) into law on August 10, 2005 *(See Appendix II)*.

Sarbanes-Oxley Act

The Sarbanes-Oxley Act of 2002 introduced significant changes to financial practice and corporate governance regulation. The act established an independent accounting oversight board to oversee the audit of public companies and more stringent auditor independence requirements. Specifically, it increased the financial reporting requirements of publicly held companies to their shareholders. Annual and quarterly reports must be certified by the principal executive and financial officers of a company. Public companies must also demonstrate due diligence in the disclosure of financial information. The act also introduced provisions designed to eliminate conflicts of interest and criminal penalties for fraudulent financial reporting.

While it does not deal with breach of data per se, the Sarbanes-Oxley Act requires greater reporting and disclosure of data, as well as assurances about data accuracy, with very stringent fines and penalties backing it up. Sarbanes-Oxley is enforced principally by the Department of Labor (DoL) and the Securities and Exchange Commission (SEC), as well as other federal regulatory agencies.

Other Federal Privacy Developments

A number of laws, such as the Fair Credit Reporting Act (FCRA), affect aspects of consumer information-related services, but no federal law comprehensively regulates information brokers or consumer data. However, the ChoicePoint incident and other data breaches have led to calls for Congress to enact tougher privacy laws, and to perhaps broaden the scope of the FCRA to govern information brokers as well as credit reporting agencies.

Several bills are under consideration. For example, H.R. 1080 the "Information Protection and Security Act", and H.R. 1078 the "Social Security Number Protection Act" would require information brokers such as ChoicePoint to comply with new fair information practice rules with the aim of better protecting the privacy and security of

individuals' personally identifiable information. The acts would also subject information brokers to federal regulation by the Federal Trade Commission (FTC).

Insurance Implications

Traditionally, standard property and commercial general liability (CGL) insurance policies have not dealt adequately with the risks of a cyber attack or network security failure. Viruses, hackers and electronic data breaches were not considered a threat when these policies were originally developed. While in the past there have been uncertainties as to which, if any, cyber risks are covered under traditional business policies, these policies have since been clarified to either exclude or add limited coverage for electronic data and other network security risks.

For example, the CGL policy defines property damage as "physical injury to tangible property," and therefore excludes electronic data on the basis that it is not "tangible property." The typical electronic data exclusion in the CGL policy is as follows:

> *Damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.*
>
> *As used in this exclusion, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CD-ROMS, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment.*

However, amendments to the exclusion have since added some limited coverage under the CGL policy. For example, ISO has introduced an endorsement (the Electronic Data Liability endorsement) that extends liability coverage for loss of electronic data if it results from physical injury to tangible property, i.e. if a computer is destroyed by a fire and the data is lost, there would be coverage. In 2004, ISO also introduced a new Electronic Data Liability form that expands the EDL endorsement by providing coverage whether the loss of electronic data results from physical injury to tangible property, *or any other means*. This new form is not designed for policyholders who provide computer products or services, however. It also excludes coverage for liability losses arising from the theft or unauthorized use of data.

While coverage for data breaches may not exist under traditional commercial general liability policies, it is easy to foresee a situation in which enterprising trial lawyers may attempt to hold a company and its directors and officers potentially liable for failure to maintain appropriate controls and regulatory compliance programs following a data breach. This could have implications for liability insurers in the areas of directors' and officers' (D&O), fiduciary, and errors and omissions (E&O) coverage. Businesses could also face litigation from state attorney generals and a variety of state and federal government agencies.

The limitations of traditional liability policies, however, suggest that in general, coverage for these exposures is today largely the domain of specialized cyber-risk coverages, which is the subject of the next section.

Cyber Insurance

Despite the increasing cyber threats facing businesses and the growing number of specialist insurance coverages available, evidence suggests that take-up of these insurance products remains slow. According to the 2005 CSI/FBI Computer Crime and Security Survey, only 25 percent of respondents indicated that their organizations used external insurance to help manage cyber security risks, about on a par with the previous year's reported use *(Fig. 16)*.

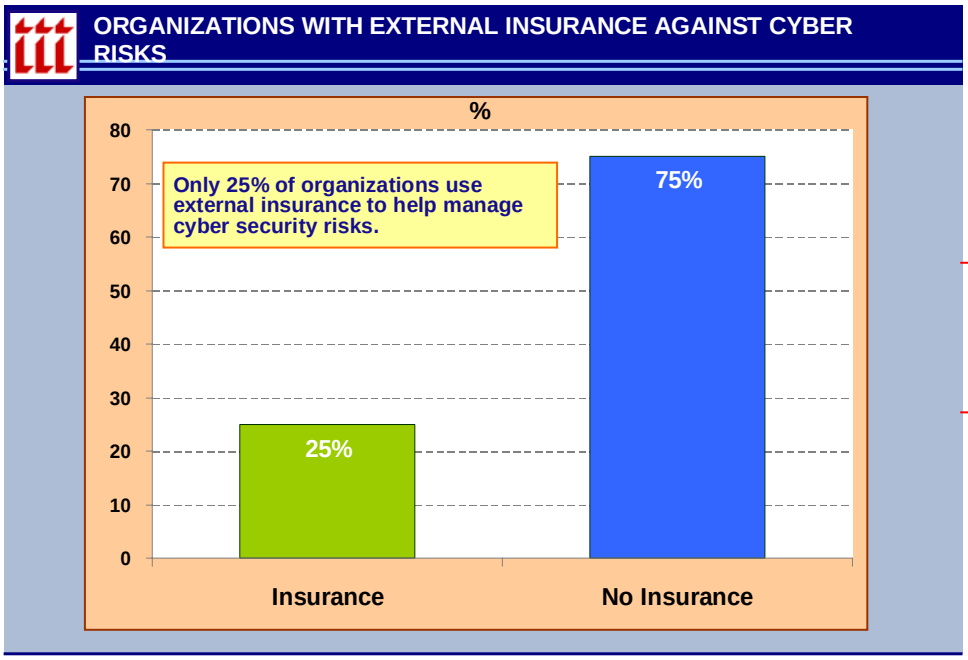


Fig. 16

Source: CSI/FBI 2005 Computer Crime and Security Survey.

This indicates that cyber insurance is not yet gaining momentum, although as the survey notes, many believe that this situation will change over time.

Reasons for the slow take-up of insurance may be due partly to network security measures being implemented by many businesses up-front. The high cost of cyber coverage may be another factor. According to findings from a Swiss Re Corporate Risk Survey, technical solutions appear to be the main mitigation strategy among global executives. In the U.S., for example, only one out of 10 executives reports using insurance as a mitigation strategy.[14] Firewalls, anti-virus software, intrusion detection systems, passwords and biometrics are just some of the computer security measures being used by corporations *(Fig. 17)*.

[14] Swiss Re Corporate Risk Survey: A Global Perspective, Produced for Swiss Re by StrategyOne, March 2006.

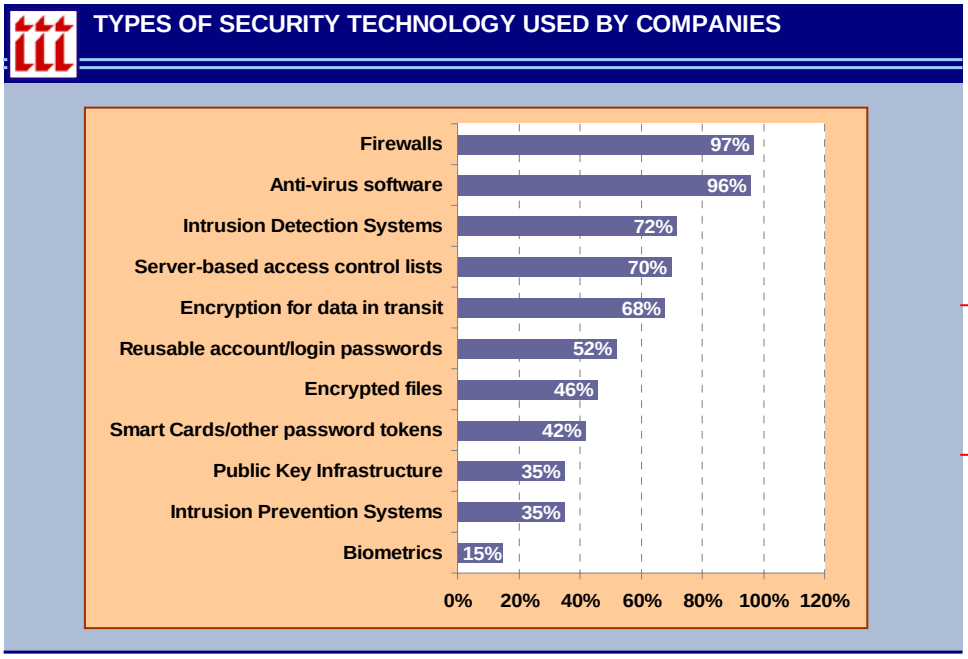


Fig. 17

Source: CSI/FBI 2005 Computer Crime and Security Survey.

A Deloitte survey reveals that new legislation, regulations and lawsuits have led to increasing investment in IT security spending. The survey notes that the majority of security budgets (43 percent) increased by up to 5 percent in 2005, while some 19 percent of respondents indicate an increase of greater than 20 percent over 2004. The greatest investments in security were in the following areas: security tools (64 percent), process improvement (29 percent), consulting (28 percent) and employee awareness and training (15 percent) *(Fig. 18)*.[15]

[15] 2005 Global Security Survey, Deloitte, June 2005.

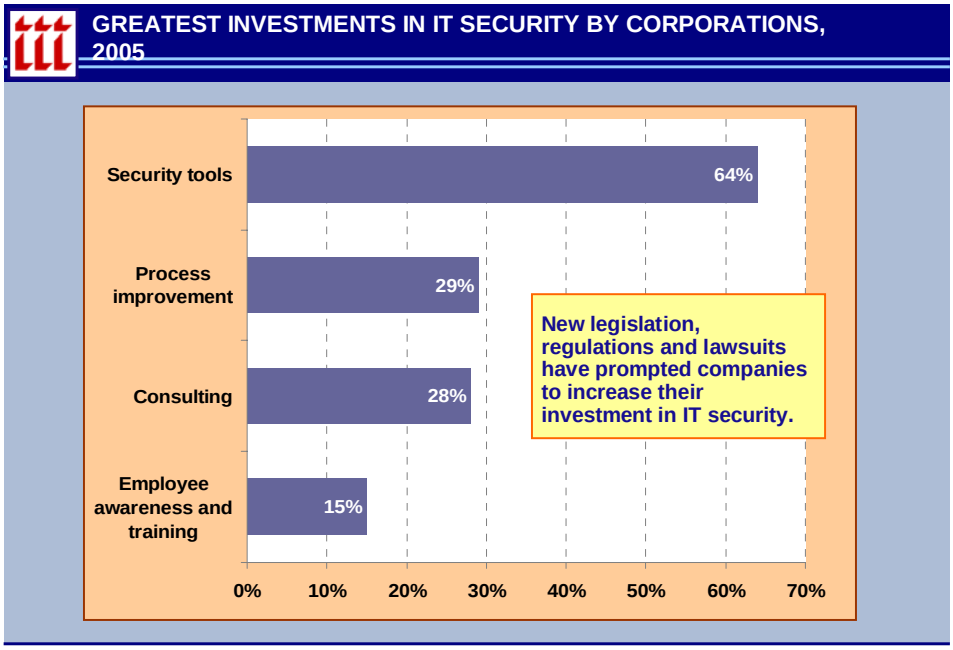


Fig. 18

Source: 2005 Global Security Survey, Deloitte, June 2005.

Yet, a 2005 worldwide study conducted by PricewaterhouseCoopers and CIO Magazine indicates a lack of focus and strategy among corporate executives in the area of information security.[16] While security spending is on the rise, just 37 percent of respondents reported that they had an information security plan in place at their firm, and only 24 percent report they expect to develop one in the coming year. The number of organizations with a security plan rises to 62 percent when the organization employs a chief information security office (CISO) or chief security officer (CSO). Some 40 percent of this year's respondents report that their companies employ a CISO or CSO, up from 31 percent in 2004. The results were based on the responses of more than 8,200 information security executives from 63 countries and represented a broad range of industries including financial services/banking.

Each cyber insurance policy is tailored to the specific needs of a company, including the technology being used and the level of risk involved. Both first- and third-party coverages are available, including:

- **Loss/Corruption of Data**—covers damage to or destruction of valuable information assets as a result of viruses, malicious code and Trojan horses (an apparently harmless program that is actually malicious or destructive and destroys data or breaks the security of a system).
- **Business Interruption**—covers loss of business income as a result of an attack on a company's network that limits the ability to conduct business, such as a denial-of-service computer attack. Coverage also includes extra expense, forensic expenses and dependent business interruption.
- **Liability—**covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company as a result of:

[16] The Global State of Information Security 2005, PricewaterhouseCoopers and CIO Magazine, September 2005.

- Breach of privacy due to theft of data (such as credit card, financial or health-related data),
- Transmission of a computer virus or other liabilities resulting from a computer attack which causes financial loss to third parties,
- Failure of security which causes network systems to be unavailable to third parties,
- Rendering of Internet Professional Services, and;
- Allegations of copyright of trademark infringement, libel, slander, defamation or other "media" activities on the company's Web site.

- **Cyber Extortion**—covers the investigation and settlement of an extortion threat against a company's network, including the cost of hiring a security firm to track down and negotiate with blackmailers.
- **Public Relations—**covers those public relations costs associated with a cyber attack and restoring of public confidence.
- **Criminal Rewards**—covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of the cyber criminal who attacked the company's computer systems.
- **Cyber Terrorism**—covers those terrorist acts covered by the Terrorism Risk Insurance Act (TRIA) and, in some cases, may be further extended to terrorist acts beyond those contemplated in the act.
- **Identity Theft**—provides reimbursement for expenses such as phone bills, lost wages, notary and certified mailing costs and sometimes attorney fees with the prior consent of the insurer. Some companies also offer resolution or restoration services that guide insureds through the process of recovering their identity, such as access to an identity theft call center in the event of stolen customer or employee personal information.

Depending on the policy, coverage can apply to both internally and externally launched attacks as well as to viruses that are specifically targeted against the insured or widely distributed across the Internet. Premiums can range from a few thousand dollars for coverage for small businesses (less than $10 million in revenue) to several hundred thousand dollars for major corporations needing comprehensive coverage. Retentions start at about $10,000 and may exceed $1 million for a Fortune 500 corporation.

Expanding Security and Privacy Liability Coverage

In response to the rising liabilities that companies face from data breaches, a number of insurers are expanding their security and privacy liability coverage. Whereas previous coverage typically would have covered only the release of information due to a failure of computer security, these evolving products also cover the company's failure to protect or wrongful disclosure of private or confidential information by the company, its employees or another third party. For example, a number of policies extend coverage for breach of privacy or security issues caused by the insured's vendors or other business partners. Premiums depend on the size of the company and its risk profile, but can range from several thousand

dollars for smaller companies to $25,000 or more for major corporations, for around $1 million in coverage.

Cyber insurers are also in the process of developing products that would cover a company's cost to comply with state notification laws. Given the increasing burden on companies to comply with state disclosure laws, and the rising costs associated with this compliance, growing interest in these products is expected.

Identity Theft Trends

The Federal Bureau of Investigation (FBI) reports that identity theft is the fastest growing crime in the U.S. It is also the number one consumer complaint received by the Federal Trade Commission (FTC), accounting for 37 percent of all fraud complaints, and in the past five years has claimed 27.3 million victims *(Fig. 19)*.

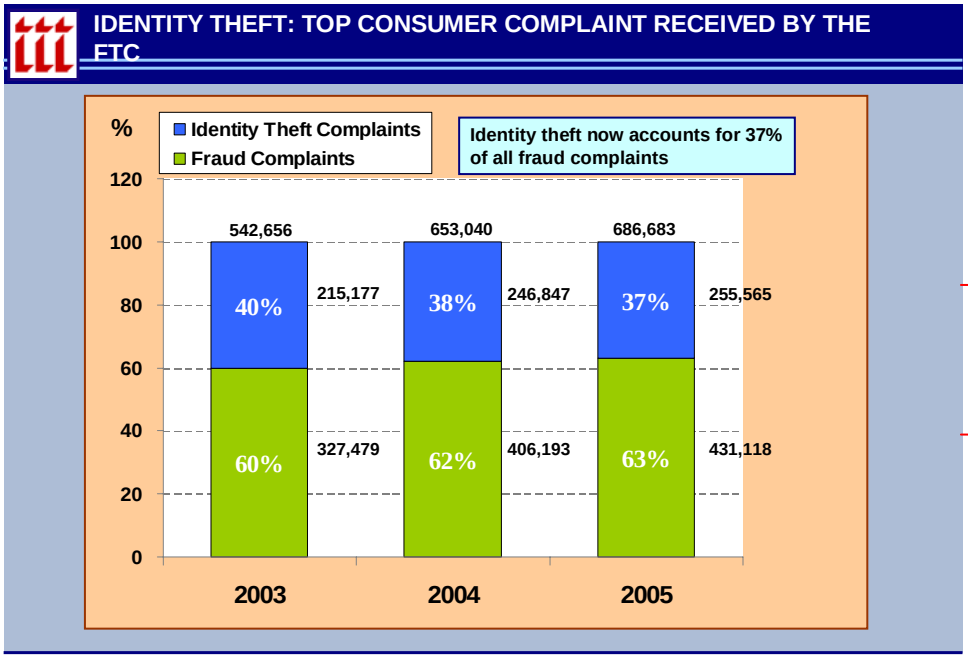


Fig. 19

Source: FTC Consumer Fraud and ID Theft Complaint Data, January 2006.

The most common identity theft complaints to the FTC involve credit card fraud, bank fraud and loan fraud. Financial services institutions are prime targets because they hold their customers money and store large quantities of personal data. Credit card transactions, magazine subscriptions, telephone numbers, real estate records, automobile registrations, consumer surveys, warranty registrations, credit reports, and Web sites are all sources of personal information which can be misused by identity thieves.

The latest available data reveals that while the number of identity theft complaints is slowing, the cost of those losses is increasing. Some 255,565 identity theft complaints were reported last year, according to the FTC, just 3.5 percent higher than the previous year.

This compared with a 15 percent increase in 2004, and a 33 percent increase in 2003. Similarly, a report from Javelin Strategy and Research and the Better Business Bureau found that around 8.9 million people, or 4 percent of U.S. adults, learned that their personal data had been stolen and used to commit fraud in 2005, down from 9.3 million identity theft cases in 2004. However, the average fraud amount per victim increased to $6,383 in 2005, up from $5,885 in 2004, for a total cost of $56.6 billion. The survey findings also showed that businesses absorbed 93 percent of the financial damage, or just under $6,000 per victim.

Researchers attribute the slowdown in identity theft cases to heightened awareness and better fraud-fighting measures. Many banks and credit-card companies are utilizing technologies that assign identity scores to new applications and fraud scores to suspicious transactions. These models operate in a similar way to credit scores, by attempting to determine that new and existing customers are authentic. The FTC reports that credit card fraud (26 percent) continues to be the most common form of reported identity theft followed by phone or utilities fraud (18 percent), bank fraud (17 percent) and employment fraud (12 percent) *(Fig. 20)*.

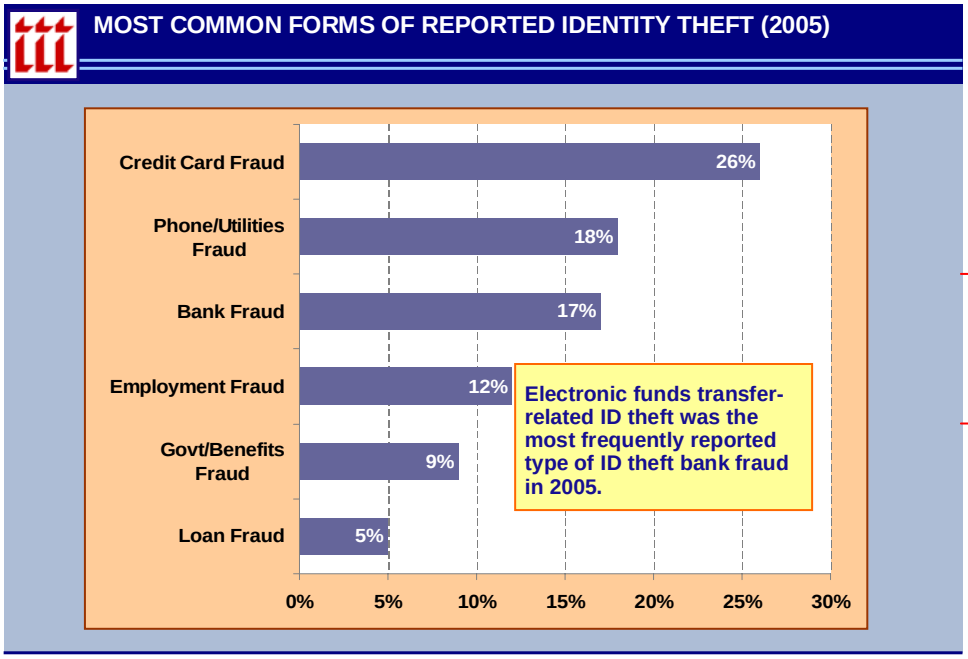


Fig. 20

Source: FTC Consumer Fraud and ID Theft Complaint Data, January 2006.

However, complaints about credit card fraud declined by 1.3 percent to 67,228 in 2005, from 68,113 in 2004. Other significant categories of identity theft reported by victims were government documents/benefits fraud (9 percent) and loan fraud (5 percent). Electronic fund transfer related identity theft was the most frequently reported type of identity theft bank fraud during calendar year 2005.

Many insurers now offer identity theft coverage as part of their homeowners insurance policies. Others sell it as a standalone policy or as an endorsement to a homeowners or renters insurance policy. On average, these policies cost between $25 and $50 for $15,000 to $25,000 worth of coverage. Identity theft insurance provides reimbursement for expenses such as phone bills, lost wages, notary and certified mailing costs and sometimes attorney

fees with the prior consent of the insurer. Some companies also offer resolution or restoration services that guide insureds through the process of recovering their identity.

Conclusion

Media reports on data breaches continue with alarming regularity, striking fear into the hearts of individuals and businesses alike. Whether addresses, social security numbers or personal financial information, these data breaches are the letter or phone call that nobody wants to receive. In an environment of ever-changing and emerging technology, the need to secure privacy along with innovation and efficiency is a difficult balance to strike. Recent high profile data breach incidents have prompted a number of lawsuits, highlighting the growing liability that businesses face in this area. Legislative and regulatory developments are also increasing the burden on companies to ensure that the information provided to them by their clients and customers is properly safeguarded online. This emerging issue has the ability to affect a broad range of sectors, including financial, educational, and government organizations. Looking ahead, insurance has a key role to play as companies and individuals look to better manage and reduce their potential financial losses from cyber attacks.

Appendix I: 2005 Disclosures of U.S. Data Incidents

Date	Entity	Affected
1/03/05	**George Mason University**	30,000
	Officials discover that hackers had accessed private information and Social Security numbers on students and staff.	
1/06/05	**University of Kansas**	1,400
	Administrators send letters to individuals whose personal information, including Social Security numbers, passport numbers, countries of origin, and birthdates, might have been compromised when a hacker accessed a server in November 2004.	
1/05	**Christus St. Joseph Hospital, Houston Texas**	16,000
	Published reports on 4/26 said the hospital had sent letters to 16,000 patients saying their medical records and SSNs may have been compromised due to the theft of a computer in a January burglary.	
1/05	**Kaiser Permanente**	140
	Health care company in March begins notifying patients that a disgruntled former employee had posted confidential information about them on the Internet; U.S. Office of Civil Rights had discovered the breach in January.	
1/18/05	**University of California at San Diego**	3,500
	Officials reveal a mid-November breach may have compromised names and SSNs of students and alumni.	
1/20/05	**University of Northern Colorado**	30,000
	University announces the apparent theft of a computer hard drive containing names, addresses, SSNs, bank account numbers, dates of birth and pay schedules for students and staff members and potentially their beneficiaries.	
1/25/05	**Science Applications International (SAIC)**	Unknown/Not disclosed
	Desktop computers were stolen from the offices of SAIC, a research and engineering company, compromising personal information of current and past stockholders.	
1/26/05	**GMAC Financial Services**	200,000
	News report says company begins “quietly” notifying customers on March 12 that personal data (names, addresses, dates of birth, SSNs, credit scores, marital status and gender) may have been compromised in the theft of two laptop computers from an employee’s car at a regional office near Atlanta.	
1/27/05	**Purdue University**	1,200
	An unknown person or group accessed a computer in the College of Liberal Arts' Theatre Division containing names and SSNs of faculty, staff, students, alumni and business affiliates.	
2/05	**University of California, San Francisco**	7,000
	University acknowledges in March that hackers breached a server used by its accounting and personnel departments in February, exposing names and SSNs of students, faculty and staff members.	
2/2/05	**Indiana University**	Unknown/Not disclosed
	Officials reveal that the F.B.I. and campus police are investigating a computer security breach that left employees' personal information vulnerable. It is unknown how many have been affected.	
2/10/05	**North Carolina Division of Motor Vehicles**	3.8 million
	North Carolina DMV confirms on May 24 it is investigating a state contract worker who downloaded the addresses of more than 3.8 million people from a DMV database. The State Bureau of Investigation said it believes it stopped the employee before driver’s license numbers, SSNs and other information could be compromised.	
2/14/05	**ChoicePoint**	157,000
	Makes notifications stemming from customer fraud which may have exposed consumers' personal data; number updated periodically from initial 145,000.	
2/20/05	**T-Mobile**	400
	Mobile phone accounts of Paris Hilton and 400 T-Mobile customers compromised by hackers.	
2/23/05	**PayMaxx**	25,000
	Online payroll service provider shuts down its automated W-2 site after a researcher claims data on more than 25,000 W-2 forms was exposed.	
2/24/05	**Westlaw ***	Potential for “Millions”
	Accused by U.S. Sen. Charles Schumer of having “egregious loopholes” in one of its Internet data services that would allow thieves to harvest SSNs and financial identities of millions of people.	
2/25/05	**Bank of America**	1.2 million
	Announced it had lost computer data tapes containing personal information on federal employees, including some members of the U.S. Senate.	
3/8/05	**DSW Shoes**	1.4 million
	Announced credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from company database; announces on 4/18 the number of affected consumers could be 1.4 million.	
3/05	**Automatic Data Processing**	1,000
	Corporate payroll and benefits services company mistakenly distributes postcards imprinted with SSNs to more than 1,000 employees of Adecco Employment Services, an HR firm.	
3/07/05	**Nevada Department of Motor Vehicles**	8,800
	Personal information compromised when thieves stole a computer from a Nevada DMV office. The computer and other license-making supplies are mysteriously found June 1 at a construction site in Las Vegas.	
3/8/05	**Harvard University**	200
	Intruder gains access to admission systems and helped applicants log on to learn whether they had been accepted weeks before they were to find out.	

3/9/05	**Reed Elsevier, Seisint Unit (LexisNexis)**	310,000
	Announced that hackers gained access to sensitive personal information of about 32,000 U.S. citizens on databases owned by Reed Elsevier; later updates the number of potentially affected consumers to 310,000.	
3/11/05	**Boston College**	120,000
	Announced that hackers had accessed personal information of alumni in a computer system used for fund-raising.	
3/11/05	**University of California-Berkeley**	100,000
	Laptop computer stolen from a graduate division office contained the names and Social Security numbers of nearly 100,000 individuals.	
3/14/05	**California State University, Chico**	59,000
	Hackers broke into a computer system that contained names and SSNs of current, former and prospective students, as well as faculty and staff.	
3/18/05	**University of Nevada, Las Vegas**	5,000
	Administrators reveal that a hacker had been accessing the personal information of international students.	
3/23/05	**Mutual funds**	Unknown/Not disclosed
	Wall Street Journal reveals numerous mutual funds reported data security breaches, including Armada Funds; Pimco, a unit of German insurance giant Allianz AG; The Dreyfus unit of Mellon Financial Corp.; Bank of America Corp.'s Columbia Funds unit; Nuveen Investments; The First American Funds unit of U.S. Bancorp; AmSouth Bancorp's fund unit; CNI Charter fund unit of City National Bank of Los Angeles.	
3/25/05	**Northwestern University**	21,000
	Hackers broke into a graduate school server, exposing the Social Security numbers of students, faculty, and alumni.	
3/28/05	**San Jose Medical Group**	185,000
	Two computers stolen containing patient billing information, including names, addresses, Social Security numbers and confidential medical information.	
3/28/05	**Univeristy of Chicago Hospital**	Unknown/Not disclosed
	Announced an employee had been selling patient records.	
3/05	**Idaho State University (Pocatello)**	100
	Discovers that SSNs of students had been accessible to the public for more than three years on the university's Web site.	
4/05	**MCI**	16,500
	Long-distance phone company acknowledges in a 5/23 article in The Wall Street Journal the theft in April of a laptop computer that contained names and SSNs of current and former employees.	
4/8/05	**Eastern National (vendor for National Park Service)**	15,000
	Hacker infiltrated its "eParks.com" computer system and may have gained access to customer names, credit card numbers and billing addresses.	
4/10/05	**Carnegie Mellon University, Pittsburgh**	19,000
	Published reports on 4/21 said the university had sent letters to students, employees and graduates that their SSNs and other personal information was compromised in a breach of the school's computer network that was discovered on 4/10.	
4/12/05	**Tufts University**	106,000
	Begins notifying 106,000 alumni about "abnormal activity" on a computer that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers.	
4/13/05	**Polo Ralph Lauren / HSBC North America**	180,000
	Credit card issuer begins notifying consumers (who used General Motors-branded MasterCards to make purchases at Polo Ralph Lauren) that criminals may have obtained access to their credit-card information.	
4/15/05	**California Department of Health Services**	21,600
	Department confirms on May 27 the theft of a laptop computer that contained personal information (names, SSNs, health information) for 21,600 recipients of Medi-Cal services. The computer was stolen from the trunk of a car of an employee of a company that provides data services to the state.	
4/18/05	**Internal Revenue Service ***	Potential for "Millions"
	GAO reports computer-security flaws expose millions of taxpayers to ID theft. IRS confirms in June an investigation into potential data theft.	
4/19/05	**Ameritrade**	200,000
	Online discount broker reported it has notified current and former customers that it has lost a backup computer tape containing their personal information.	
4/23/05	**Georgia Southern University, Statesboro, Ga.**	Potential for "Thousands"
	AP reports on 4/28 that hackers broke into a GSU server that contained thousands of credit card and Social Security numbers.	
4/26/05	**Michigan State University, Wharton Center**	40,000
	Performing arts center says it learned of an intrusion on April 26 into a server that plays a role in credit card processing for ticket sales. The incident is not made public until media reports reveal the breach on May 5.	
4/26/05	**Foster Wheeler, Clinton, N.J**	6,700
	Engineering/construction company writes to employees, retirees, advising them that a hacker broke into the company's computer system in February and might have stolen personal data, including SSNs and bank deposit information.	
4/28/05	**Wachovia, Bank of America, PNC Bank of Pittsburgh, Commerce Bank**	680,000
	NBC reports bank managers/employees sold personal data of account holders.	
4/28/05	**Georgia Technology Authority (driver's license data)**	465,000
	Computer programmer arrested, charged with downloading state driver's license information – including names, addresses, driver's license numbers and possibly SSNs; "hundreds of thousands" of drivers may be affected.	

4/28/05	**Oklahoma State University**	23,000
	University confirms theft of a laptop computer that contained SSNs, genders, ethnicities, class levels and e-mail addresses of "the majority" of students who attended OSU over the past three years (23,000 annual enrollment).	
4/29/05	**Florida International University**	Unknown/Not disclosed
	Orlando Sun-Sentinel reports "recent computer break-in" potentially compromises personal data of students, professors and staffers. School says electronic intruders apparently dialed into FIU's computers from Europe.	
5/2/05	**Time Warner**	600,000
	Company announces that data on current and former employees stored on computer back-up tapes was lost by an outside storage company.	
5/4/05	**Colorado Department of Health**	1,600
	News reports reveal the theft of a laptop computer containing medical and other information about more than 1,600 children.	
5/5/05	**Purdue University**	11,360
	Computers breached over a 17-day period, compromising personal information of current and former employees.	
5/5/05	**Arbella Mutual Insurance**	Unknown/Not disclosed
	Boston Globe reports an Arbella Web site mistakenly offered unrestricted access to names, addresses, dates of birth, drivers license numbers and history, and SSNs, including Boston Mayor Menino and Mass. Gov. Romney.	
5/7/05	**U.S. Department of Justice**	80,000
	Justice Department says a computer containing the names and government credit card numbers for DOJ personnel was stolen between May 7-9 from Omega World Travel, which handles business travel for the department. DOJ doesn't believe personal information (SSNs, etc.) was compromised.	
5/11/05	**Stanford University**	10,000
	University confirms breach of computer network, stealing SSNs and other personal information of recruiters and students.	
5/12/05	**Merlin Information Services**	9,000
	Kalispell, Mont., data company acknowledges names, addresses, SSNs were compromised in fraudulent access incident(s) in March/April.	
5/12/05	**Hinsdale Central High School, Chicago**	2,400
	Two students are accused of hacking into a school database that contained the Social Security numbers of all of the school's students and staff.	
5/16/05	**Westborough (Mass.) Bank**	750
	Bank begins notifying customers that a former bank employee may have given SSNs and other confidential account information to a convicted felon.	
5/17/05	**Valdosta (Ga.) State University**	40,000
	University confirms breach of computer server containing SSNs, other information for multipurpose identification and on-line debit cards of students and employees. AP reports on 5/21 that 40,000 people could be affected.	
5/18/05	**Jackson (Mich.) Community College**	8,000
	University confirms breach of computer system, potentially compromising employee and student SSNs.	
5/18/05	**University of Iowa**	30,000
	University confirms breach of campus book store computer system, potentially compromising employee and student IDs, credit card numbers.	
5/23/05	**Brigham Young University**	600
	University confirms a hacker in April monitored e-mail activity and recorded keystrokes of students who used four computers in an open-access lab.	
5/26/05	**Duke University Medical Center**	14,000
	School says (on 6/3) that a hacker broke into its computer system and stole names, passwords and partial SSNs of employees, physicians and others.	
5/27/05	**Cleveland State Univeristy**	44,000
	University confirmes theft of a laptop computer from its admissions office, comprising students' addresses and SSNs.	
5/28-30/05	**Motorola**	30,000
	Confirms theft of computers from HR services provider, Affiliated Computer Services, exposing its U.S. employees' personal data, including SSNs.	
6/2/05	**Jackson High School, Jackson Township, Ohio**	Unknown/Not disclosed
	Two seniors convicted of illegally accessing school computers to change grades and acquire teachers' SSNs, credit card information and addresses.	
6/3/05	**Polk Community College, Winter Park, Fla**	At least 3
	Professor arrested for using students' names, SSNs to obtain department store credit cards. He allegedly had asked students to provide the data on a sign-up sheet for his class.	
6/6/05	**CitiFinancial**	3.9 million
	Consumer financial division of Citigroup begins notifying customers that computer tapes containing their SSNs and account data were apparently lost in transit via UPS some time between May 2 and May 20.	
6/10/05	**Federal Deposit Insurance Corp. (FDIC)**	6,000
	Begins notifying current and former employees of a 2004 breach that may have compromised their names, SSNs, DOBs, salaries and employment information.	
6/14/05	**Medica Health Plans (Minnetonka, Minn.)**	1.2 million
	Confirms that hackers twice stole sensitive and confidential data from its computer system in January and shut down parts of the system on four other occasions, exposing members' SSNs, addresses, DOBs, employment information and names of relatives.	

6/17/05	**Kent State University**	1,400
	Acknowledges the theft on June 14 of a laptop computer from an employee's car, which contained names and Social Security numbers of about 1,400 current and past school employees.	
6/17/05	**University of Hawaii**	150,000
	Acknowledges that two identity theft suspects had gained fraudulent access to the school's database, exposing SSNs, addresses and phone numbers of students, faculty, staff and library patrons between 1999 and 2003.	
6/17/05	**MasterCard International**	40 million
	Confirms hacking (discovered in late May) at CardSystems Solutions -- which handles transfer of payments between banks for consumer transactions -- exposes names, account numbers and verification codes of MasterCard, Visa, Discover, American Express card holders.	
6/22/05	**Eastman Kodak**	5,800
	Confirms it has begun notifying former employees that names, SSNs, birthdates and other information was on a laptop computer stolen from a consultant's car.	
6/22/05	**East Carolina University**	250
	Confirms May 2005 breach of an Internet server that contained SSNs, other personal information of students; says it believes the breach was limited to students and applicants in one department.	
6/24/05	**University of Connecticut**	72,000
	Confirms it has discovered a computer-hacking program had been placed in a server at the school in 2003, compromising names, SSNs, DOBs, phone numbers and addresses of students, faculty and staff.	
6/27/05	**Michigan State University, Human Resources Dept.**	Unknown/Not disclosed
	Media reports on 7/7 reveal a breach within the human resources department that may have exposed SSNs of all university employees and retirees.	
6/28/05	**Lucas County (Ohio) Children Services**	900
	Confirms current and former employees' names, SSNs, phone numbers contained in a personnel database had been e-mailed to outside computer.	
6/29/05	**Virginia Department of Criminal Justice Services**	3,500
	Confirms notifications due to potential theft of names, SSNs and phone numbers of people who had filed applications for jobs at the agency.	
6/30/05	**Ohio State University Medical Center**	15,000
	Confirms notifications to patients whose names and billing information was contained on a laptop computer stolen in April from a consultant's office.	
7/1/05	**University of California at San Diego**	3,300
	Confirms fourth hacking since April 2004. SSNs, drivers license, credit card numbers of students, staff and faculty compromised in incident in April.	
7/1/05	**Blue Cross and Blue Shield of North Carolina ***	Unknown/Not disclosed
	Files lawsuit against ProCare, a private group, for allegedly posting illegally obtained internal documents on the Internet (this incident is not currently included in our list as a "breach" pending more clarification).	
7/5/05	**City National Bank, Los Angeles**	Unknown/Not disclosed
	"Banker to the stars" confirms account holders' names, SSNs, account numbers and other info was on two backup data tapes that were lost in April.	
7/5/05	**Michigan State University, College of Education**	27,000
	Confirms discovery in April of a breach of a server in the College of Education that exposed students' names, addresses, SSNs, other info.	
7/8/05	**University of Southern California**	270,000
	Confirms a hacker (since 1997) may have gained access to students' names, addresses and SSNs due to a flaw in an online application database.	
7/8/05	**Blue Cross Blue Shield of Arizona**	57,000
	Confirms customers' addresses, SSNs, DOBs, phone numbers were on backup tapes stolen 6/29 from Arizona Biodyne, a managed care company.	
7/14/05	**University of Colorado**	42,000
	Breach of Wardenburg Health Center computer server exposes names, SSNs, ID numbers, addresses, birthdates of students, faculty, staff, visitors.	
7/14/05	**University of Colorado**	900
	Breach of server in the Visual Resource Center of the College of Architecture and Planning exposes names and SSNs of students and faculty.	
7/15/05	**University of Delaware**	343
	Confirms the December 2004 theft of three computers, one of which contained Department of Communications students' names, SSNs.	
7/18/05	**Iowa State University**	4,700
	Confirms the 7/6 discovery of a breach of its network exposing the SSNs and/or credit card numbers of Alumni Association customers since 2004.	
7/21/05	**San Diego County Employees Retirement Association**	32,000
	Discovers unauthorized access of two computer servers containing names, SSNs, birthdates, addresses of current and former county employees.	
7/25/05	**St. John's Regional Medical Center, Joplin, Mo**	27,000
	Acknowledges 7/7 theft of two computers containing patients' names, dates of birth and some medical account numbers.	

7/26/05	**California State University, Dominguez Hills**	9,613
	Discovers the unauthorized access of three desktop computers containing names and SSNs of students.	
7/27/05	**University of Colorado**	36,000
	Discovers breach of computer server (used to issue identification cards) exposing names, SSNs, photos of students, former students, faculty, staff.	
7/29/05	**Austin Peay State University, Clarksville, Tenn**	1,500
	Confirms exposure of students' names, SSNs, other personal info due to a problem with the search function on the school's Web site.	
7/29/05	**Cal Poly Pomona**	31,077
	Confirms 6/29 hacking of two computer servers, compromising names and SSNs of current and former faculty, staff, students and university applicants.	
8/3/05	**Anderson College, Anderson, S.C**	834
	A bag containing documents bearing students SSNs, gender and dates of birth is discovered off campus; college investigating possibility of theft.	
8/4/05	**Pennsylvania Unified Judicial System**	Unknown/Not disclosed
	Confirms "five to 10 minute access" via a Web site compromised SSNs, other confidential information of defendants on statewide computer system.	
8/8/05	**Sonoma State University, Rohnert Park, Calif.**	61,709
	Confirms unauthorized access of computer system had exposed names and SSNs of all students, faculty, staff and applicants from 1995 to 2002.	
8/8/05	**University of North Texas, Denton, Texas**	38,607
	Discloses "hacking" of system exposing names, SSNs, student IDs, phone numbers of current, former and prospective students from 1999 to 2005.	
8/8/05	**Huntington National Bank, Toledo, Ohio**	6,000
	Confirms distribution of notification letters due to theft of account information, including names, SSNs, signatures, account numbers of local customers.	
8/8/05	**J.P. Morgan Private Bank**	Unknown/Not disclosed
	Distributes letters on Aug. 25 advising of theft of a computer from its Dallas offices containing personal and financial information about its wealthy clients.	
8/9/05	**University of Utah**	100,000
	Confirms notification under way due to apparent "hacking" of a computer server containing names, SSNs of former employees from 1970 to 2003.	
8/9/05	**Iowa Student Loan Program**	165,000
	Learns from a vendor about a missing compact disc containing names, SSNs and states of residence of borrowers from the program.	
8/9-10/05	**Aims Community College, Greeley, Colo**	2,000
	Confirms on Sept. 12 the theft of a computer containing names and SSNs of students in fire science and emergency services programs.	
8/10/05	**Austin Peay State University, Clarksville, Tenn**	1,280
	Confirms additional exposure of students', vendors' names, SSNs, addresses, phone numbers, other info due to problem with school's Web site.	
8/10/05	**California State University, Stanislaus**	877
	Discovers a breach of a computer file server containing names, SSNs of student workers.	
8/18/05	**U.S. Air Force**	33,000
	Confirms "personal information" of officers and enlisted personnel was stolen from its online Assignment Management System in May or June.	
8/19/05	**University of Colorado**	49,000
	Confirms breach of computer server used by Registrar's Office, exposing names, SSNs, addresses, phone numbers of current and former students.	
8/19/05	**ChartOne / University of Florida Health Sciences Center**	3,851
	Confirms theft of laptop computer (on or about Aug. 1) containing patients' names, SSNs, dates of birth and medical record numbers.	
8/20-21/05	**U.S. Army, Fort Carson, Colo**	15,000
	Confirms on Sept. 12 the theft of four computer hard drives containing names, SSNs and personal records of soldiers processed at Fort Carson.	
8/21-22/05	**Kent State University**	100,000
	Confirms on Sept. 9 the theft of five computers containing names and SSNs of current and former students and professors.	
8/28/05	**Stark State College of Technology (Jackson Township, Ohio)**	Unknown/Not disclosed
	Acknowledges software "glitch" allowed students to inadvertently view personal information of other students, including SSN, GPA, course loads.	
8/29/05	**California State University Chancellor's Office**	154
	Confirms unauthorized access (via virus) of computer exposing names, SSNs of individuals who received student financial aid, two administrators.	
8/31/05	**Blue Cross Blue Shield of Florida ***	194
	Confirms insurance subsidiary sent letters to policyholders (all BCBS employees, relatives or retirees) with their SSNs printed on the envelope.	

9/7/05	**Children's Health Council, Palo Alto, Calif**	6,700
	Discovers theft of a backup tape containing names, SSNs and other personal information on current and former clients and employees.	
9/12/05	**Miami University (Ohio)**	21,762
	Acknowledges it had removed students' SSNs and grades from a Web folder where they had been accessible via the Internet for nearly three years.	
9/14/05	**North Fork Bank, Melville, N.Y**	9,000
	Distributes letters notifying mortgage loan customers about the theft in July of a laptop computer containing their personal information (perhaps not SSNs).	
9/19/05	**University of Georgia**	1,600
	Discovers unauthorized computers access, believed to be from another country, which exposed names, SSNs of current and former employees.	
9/21/05	**City College of New York**	9,000
	Acknowledges that CUNY Law School students' names, SSNs and other personal info were accidentally posted on a university Web site.	
9/22/05	**ChoicePoint**	5,000
	Makes notifications stemming from misuse of IDs/passwords by customers, including a police department, insurance company, P.I. firm and others.	
9/22/05	**World Trade Center Medical Monitoring Program**	10,000
	Sends letters re: 7/10 theft of computer from Mt. Sinai Hospital containing SSNs, other info of Ground Zero police/fire rescue and cleanup workers.	
9/27/05	**RBC Dain Rauscher**	100
	Notifies customers of illegal access to customer data by former employee who wrote anonymous letters saying he/she had compromised data.	
9/23/05	**Bank of America**	Unknown/Not disclosed
	Sends letters re: 8/29 theft of laptop computer containing Visa Buxx users' names, account numbers, routing transit numbers and credit card numbers.	
10/5/05	**Wilcox Memorial Hospital, Kauai, Hawaii**	130,000
	Discloses on 10/17 the theft of a computer hard drive containing patients' names, addresses, SSNs and medical record numbers.	
10/7/05	**Montclair State University, Montclair, N.J**	9,100
	Discovers students' names and SSNs were inadvertently exposed on a school Web site for nearly four months.	
10/12/05	**Vermont Technical College, Randolph Center, Vt**	1,100
	Discloses that all students' names, addresses, SSNs and other info was accidentally posted on the Internet for more than a year.	
10/16/05	**Georgia Tech Office of Enrollment Services**	13,000
	Reports burglary that included the theft of a computer containing names, addresses, birthdates and SSNs of current, former and prospective students.	
10/19/05	**Monmouth University, West Long Beach, N.J**	667
	Discloses that students' names and SSNs had been accidentally posted on a Web server accessible via the Internet for more than four months.	
10/21/05	**TransUnion LLC**	3,623
	Distributes letters to consumers whose SSNs and other personal information contained on a desktop computer stolen in a burglary in California.	
10/21/05	**University of Tennessee Medical Center, Knoxville**	3,800
	Announces the August theft of a laptop computer containing names, SSNs and birthdates of people treated at the hospital in 2003.	
10/26/05	**University of Virginia**	2,600
	Discloses that names and SSNs of students and contractors of the University Housing Division were accidentally accessible via the Internet.	
11/3/05	**Oregon Driver and Motor Vehicle Services**	"Thousands"
	During a drug bust, police discover a stolen laptop containing what state calls "outdated" DMV files, including names, addresses, birthdates, SSNs, etc.	
11/4/05	**Ohio State University Medical Center**	2,800
	Announces that patients' names, addresses, birthdates, phone numbers and SSNs had been mistakenly posted online for an unknown period of time.	
11/6/05	**Illinois Department of Human Services**	208
	Newspaper reports it found names, addresses, birthdates and SSNs on food stamp applications that were improperly discarded at Belleville office.	
11/9/05	**Firstrust Bank, Philadelphia**	N/A
	Man pretending to be with a cleaning crew is suspected of stealing a laptop computer containing account information for thousands of bank customers.	
11/11/05	**Scottrade / Troy Group**	140,000
	Notifies customers that names, SSNs, bank account numbers, other info was exposed in hacking of eCheck Secure service reported on 10/25.	

11/11/05	**University of Southern California - Keck School of Medicine**	50,000
	L.A. TV station reports theft of computer server exposed names, SSNs and other personal information of employees, donors and patients.	
11/11/05	**Indiana University - Kelley School of Business**	5,300
	Sends letter to students whose personal information was exposed in a computer hacking some time between August and early October.	
11/14/05	**University of San Diego**	7,800
	Discovers illegal access of computer server that exposed names, addresses, SSNs and personal income tax data of faculty, students and vendors.	
11/15/05	**City of Fernandina Beach, Fla**	267
	Discloses that City Clerk accidentally e-mailed the Social Security numbers of all city employees in response to a public records request.	
11/18/05	**Boeing Co**	161,000
	Confirms theft of a laptop computer containing names, SSNs and other personal information of current and former employees.	
11/21/05	**LaSalle Bank / ABN Amro Mortgage Group ***	N/A
	Discovers missing computer tape containing personal data of two million residential mortgage customers; reports on 12/10 it found the missing tape.	
11/23/05	**Washington Employment Security Department**	530
	Reports theft of a laptop computer containing names, SSNs and payroll information of employees of 49 Seattle area companies.	
11/23/05	**University of Delaware**	952
	Confirms two separate computer breaches in August exposed names, SSNs and other personal information of students, faculty members and others.	
12/1/05	**J. Sargeant Reynolds Community College (Richmond, Va.)**	26,000
	Notifies students that their names, addresses and SSNs were “inadvertently” posted on the college’s Web site for months.	
12/6/05	**SAM’S CLUB**	600
	Announces credit card fraud affecting cardholders who purchased gas at SAM’S CLUB stations between Sept. 21 and Oct. 2, 2005.	
12/7/05	**Guidance Software**	3,800
	Discovers hacking of company database in November compromised financial, personal data of customers, including law enforcement officials.	
12/7/05	**Idaho State University (Pocatello)**	100
	Discovers “illicit hacking program” on computer servers, exposing names, SSNs and other personal data of all students, faculty and staff for the last 10 years.	
12/9/05	**Oregon Community Credit Union (Eugene)**	200
	Discloses theft of an employee’s car containing insurance forms that included employee names, SSNs and other personal data.	
12/14/05	**University of Dayton (Ohio)**	74
	Discloses a programming error exposed on Internet the names, SSNs and other personal data of applicants to university’s pre-med program.	
12/16/05	**San Joaquin County (Calif.) Human Services Agency**	Unknown/Not disclosed
	Discloses investigation into the discovery in a dumpster of thousands of pages of documents containing clients’ names, addresses and SSNs.	
12/16/05	**University of Pittsburgh Medical Center**	700
	Six computers stolen from a medical office, compromising names, SSNs and dates of birth of patients.	
12/21/05	**Ford Motor Co**	70,000
	Informs active and former white-collar employees of theft of computer containing company data including their Social Security numbers.	
12/22/05	**H&R Block**	Unknown/Not disclosed
	Begins notifications that it had accidentally exposed their Social Security numbers on mailing labels of free copies of its tax return software it had mailed to customers.	
12/24/05	**Iowa State University**	5,500
	Confirms hacking of two computers; one containing credit card info of athletic department donors; the other held SSNs of university employees.	
12/25/05	**BancorpSouth**	6,500
	Announces deactivation of MasterMoney debit cards because “account numbers were either lost or they were somehow hacked into” via an unnamed merchant.	
12/25/05	**People First / Convergys**	Unknown/Not disclosed
	Tallahassee Democrat reports personal information of tens of thousands of Florida state employees was exposed due to defects in personnel data-scanning program.	
12/27/05	**University of Kansas**	9,200
	Shuts down Web site that potentially exposed names, addresses, dates of birth, credit card numbers, SSNs of applicants for university housing.	
12/27/05	**Marriott**	206,000
	Discloses missing computer tape containing credit card account info, SSNs of time-share owners and customers, as well as company employees.	

Total: 152 disclosed incidents, potentially affecting more than 57.7 million individuals

* ”Incidents‘ with asterisk (Westlaw, I.R.S., Blue Cross Blue Shield of North Carolina and Blue Cross Blue Shield of Florida, LaSalle Bank/ABN Amro Mortgage Group) have been listed but not counted in the above total. While concerns have been raised about their potential for exposure of sensitive, personally identifiable information, no actionable incident has been documented or disclosed.

Source: ID Theft Resource Center (www.idtheftcenter.org) as of 2/21/06.

Appendix II: Notice of Security Breach State Laws

(Last updated November 30, 2005)

Arkansas	**SB 1167**	Passed into law in 2005. Law provides notice to consumers of breach in the security of unencrypted computerized, personal information which is held by a person or business. Notice is not required if no reasonable likelihood of harm to consumers.
California	**Civil Code Sec. 1798.80-1798.82**	Effective July 1, 2003. Requires notice to consumers of breach in the security, confidentiality, or integrity of unencrypted computerized personal information held by a business or a government agency.
Connecticut	**SB 650**	Passed into law 2005, effective January 1, 2006. Requires notice of security breach by persons who conduct business in the state and have a breach of the security of unencrypted computerized data, electronic media or electronic files, containing personal information. Notice is not required if the breached entity determines in consultation with federal, state, and local law enforcement agencies that the breach will not likely result in harm to the individuals.
Delaware	**HB 116**	Signed June 28, 2005. Requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons doing business in the state. Covers sensitive personal information including medical information. Violations trigger triple damages plus attorneys fees.
Florida	**HB 481**	Signed June 14, 2005, Chapter 2005-229. Effective July 1, 2005. Requires notice to consumers of material breach in the security, confidentiality or integrity of computerized, unencrypted personal information held by a person who conducts business in the state. Time limits for the notice to be given and penalties if notice is not given on time. Penalties do not apply to government agencies.
Georgia	**SB 230**	Passed into law in 2005, effective May 6, 2005. Requires notice of breach that compromises the security, confidentiality, or integrity of computerized personal information held by a data broker.
Illinois	**HB 1633**	Public Act 094-0036, signed June 16, 2005, effective Jan. 1, 2006. Requires notice to consumers of breach in the security, confidentiality, or integrity of personal information in system data held by a person or a government agency.
Indiana	**Act No. 503**	Passed into law in 2005, effective June 30, 2006. Law provides notice to consumers of breach in the security, confidentiality, or integrity of computerized personal information held by a government agency.
Louisiana	**SB 205, Act 499**	Signed July 12, 2005, effective January 1, 2006, or such later time if the Attorney General completes regulations. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. No notice if, after a reasonable investigation, the data holder determines that there is "no reasonable likelihood" of harm to customers. Further exemption for those financial institutions which are in compliance with federal guidance. Authorizes civil actions to recover actual damages.
Maine	**LD 1671**	Signed June 10, 2006, effective January 31, 2006. Covers only information brokers. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information to residents of the state. Provides civil penalties for violations.
Minnesota	**H.F. 2121**	Passed into law 2005, effective January 1, 2006. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Does not apply to financial institutions or HIPAA entities.
Montana	**HB 732**	Passed into law in 2005, effective March 1, 2006. Law provides notice to consumers of breach in security, confidentiality, or integrity of computerized personal information held by a person or business if the breach causes or is reasonably believed to have caused loss or injury to a Montana resident.
New Jersey	**A4001/S1914**	Passed into law in 2005, effective January 1, 2006. Requires notice of breach of security of unencrypted computerized personal information held by a business or public entity. No notice if a thorough investigation finds misuse of the information is not reasonably possible. Written documentation of the investigation must be kept for 5 years.
New York	**A4254, A3492**	Passed into law in 2005, effective 120 days after September 20, 2005. Requires notice of breach of security of computerized unencrypted, or encrypted with acquired encryption key, personal information held by both public and private entities. The State Attorney General, the State Consumer Protection Board and the Office of Cyber Security and Critical Infrastructure Coordination must also be notified of the breach of security to protect the residents of New York. Authorizes Attorney General to bring actions on behalf of affected residents.
Nevada	**SB 347**	Passed into law 2005, effective January 1, 2006. Requires notice of breach of the security, confidentiality, or integrity of unencrypted computerized personal information by data collectors, which are defined to include government, business entities and associations who handle, collect, disseminate or otherwise deal with nonpublic personal information.
North Carolina	**SB 1048**	Passed into law in 2005, effective December 1, 2005. Requires notice of breach of security of unencrypted and unredacted written, drawn, spoken, visual or electromagnetic personal information, and encrypted personal information with the confidential process or key held by a private business if the breach causes, is reasonably likely to cause, or creates a material risk of harm to residents of North Carolina. Provides civil and criminal penalties for violations.
North Dakota	**SB 2251**	Passed into law in 2005, North Dakota Century Code Chapter 51-30, effective June 1, 2005. Requires notice of a breach of the security of unencrypted, computerized, personal information by persons doing business in the state. Includes an expanded list of sensitive personal information, including date of birth, mother's maiden name, employee ID number, and electronic signature. Exception for those financial institutions which are in compliance with federal guidance.
Ohio	**HB 104**	Signed into law November 17, 2005, effective February 15, 2006. Requires notice of breach of the security or confidentiality of computerized personal information, held by a state agency, political subdivision or business. Personal information includes information that describes anything about a person, including actions or certain personal characteristics, and can be retrieved from a system by a name, identifying number, symbol, or other identifier.

Rhode Island	**H. 6191**	Enacted July 10, 2005, effective March 1, 2006. Requires notice of a breach of the security, confidentiality or integrity of unencrypted, computerized, personal information by persons and by state agencies. Does not apply to HIPAA entities. Entities covered by another state or federal law are exempt only if that other law provides greater protection to consumers.
Tennessee	**SB 2220**	Passed into law in 2005, amends Tennessee Code Title 47 Chapter 18, Part 21, effective July 1, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons doing business in the state. Does not apply to persons subject to Title V of the Gramm-Leach-Bliley Act (financial institutions).
Texas	**SB 122**	Passed into law in 2005, effective September 1, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons who conduct businesses in the state. Authorizes Attorney General to seek civil penalties for violations.
Washington	**SB 6043**	Signed May 10, 2005, effective in July 24, 2005. Requires notice of a breach of the security, confidentiality, or integrity of unencrypted, computerized, personal information by persons, businesses and government agencies. Notice is not required when there is a technical breach of the security of the system which does not seem reasonably likely to subject customers to a risk of criminal activity. Imposes civil liability for damages caused by failure to give notice as required.

Source: Consumers Union

Appendix III: Glossary

Blog: An online diary or chronology, typically containing postings of the owner's personal thoughts. Also known as a weblog, or web log.

Denial of Service: A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.

Hacking: An attempt to gain access to a computer file or network illegally, or without authorization.

Identity Theft: A crime whereby the personal or financial information of an individual is obtained with the purpose of assuming that person's name to make transactions or purchases.

Phishing: A form of online identity theft whereby emails and web-sites are created and used to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then take that information and use it for criminal purposes, such as identity theft and fraud.

Spear Phishing: A version of phishing that targets a specific organization and seeks unauthorized access to confidential information. Typically, spear phishers send emails to businesses that look as if they come from the company's IT or HR departments, deceiving employees into revealing usernames and passwords, thereby gaining access to sensitive data.

Spam: Unsolicited email sent indiscriminately to multiple mailing lists, individuals, or newsgroups.

Spyware: Malicious software that secretly monitors and tracks information on an Internet user and then transmits it to a third party, such as an individual or company that uses it for marketing or other purposes.

Trojan Horse: An apparently harmless program that is actually malicious or destructive and destroys data or breaks the security of a system.

Virus: A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate.

Worm: An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.