ADVISEN Productivity & Insight for Insurance Professionals

July 27, 2008

Data Security: A Growing Liability Threat

An Advisen Briefing

Essence: *Digitized information has transformed the way business is conducted, but it also has created dangerous new liability exposures. Data security breaches can potentially cost companies tens of millions of dollars in fines and penalties, loss mitigation expenses, and settlements of lawsuits. Data security has been the domain of the Information Technology department, and the market for cyberliability insurance has been slow to develop. But as insurance products become more sophisticated and responsive to the data security risks of large companies, and as enterprise risk management processes are more widely implemented, corporate risk managers will be increasingly involved in the treatment of cyberliability exposures.*

In February 2005, ChoicePoint, Inc. announced that identity fraudsters gained access to personal data of 145,000 people. In June of the same year, a hacker accessed over 40 million credit card accounts serviced by CardSystems Solutions, leading to millions of dollars of fraudulent credit card purchases. Over a period of 18 months, 45.6 million credit and debit card numbers were stolen from the systems of retailer TJX Companies, resulting in a $41 million settlement with Visa Inc. and a $24 million settlement with MasterCard International Inc.

Modern technology enables massive amounts of information about individuals to be gathered, processed, and transmitted. But software vulnerabilities are pervasive. Surveys by Ernst & Young and the Computer Security Institute (CSI) reveal that 90% of businesses and government agencies have detected security breaches and 75% recognized financial loses from the breach.

Data security breaches can result in losses from a number of sources. Companies may incur fines or penalties if they are not in compliance with privacy and data security laws. A breach can result in millions of dollars in expenses for repairing the breach, tightening security measures, notifying customers and mitigating damages. Loss of trust and other reputational damages can have significant top line and bottom line impact: in extreme cases it can be ruinous. Lawsuits by customers, business partners and shareholders can result in tens of millions of dollars in settlements.

The insurance industry has been relatively slow to develop products addressing data security risks. The pace of development reflects both caution by underwriters and a general attitude of indifference on the part of insurance buyers. However, in recent years, the number of products available and the sophistication of the coverages have increased. Demand for coverage also has risen in the wake of large, highly publicized losses such as TJX.

Data security risks

Insurance market Lloyd's fends off 60 high-severity penetration attempts on its corporate IT infrastructure every day, according to Peter Hambling, the market's chief information officer. Most companies are not as forthcoming with these sorts of statistics, but it is fair to assume that Lloyd's is not unusual in the attention it attracts from hackers. According to Hambling, the nature of the attacks has changed in recent years, with a drop off in the number of attacks by "enthusiastic hackers" seeking only to break through firewalls and an increase in attacks by those seeking to extract funds or data.[1] Companies need to repel attacks not only from the outside, but also from insiders, especially those with administrative network access. Hannaford Bros supermarket chain recently reported the theft of 4.2 million credit and debit card numbers. The breach was determined to be the work of a company insider: malware that intercepts credit card information had been installed on the servers in each of the company's 300 stores.

It is not only hackers that companies need to worry about. Sensitive information can easily be compromised through human and administrative errors such as the loss or theft of a laptop or other portable devices. More than half of identity theft-related data breaches stem from theft or loss of a laptop or storage device. A major bank recently lost a backup computer tape with account data on 4 million customers. In another incident, a company reported that a laptop with personal information of nearly 400,000 current and former employees was stolen from an employee's car.

Large companies attract media attention when security breaches occur, but small businesses are typically more vulnerable to data security breaches. Since 2005, more than 80 percent of the instances of unauthorized access to card data have involved small merchants, according to Visa USA Inc.

Data security standards

There is no universally acknowledged standard for data security, though a number of organizations have promulgated guidelines. The ISO/IEC 27000-series, for example, comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The series presently consists of three published standards and eleven standards in preparation. The Payment Card Industry Data Security Standard (PCI DSS) was developed by the five major credit card companies as a guideline for organizations that process card payments to help prevent credit card fraud, cracking and various other security vulnerabilities and threats. Unlike many standards, PCI DSS has teeth: the major credit card companies can levy fines for non-compliance. In 2006, Visa levied $4.6 million in fines.

The current unsettled and evolving state of data security standards could prove to be the worst of all possible worlds for companies that experience a security breach. Ordinarily, standards can increase the potential liability of companies that fail to adhere to accepted standards, or can provide a strong defense for companies that followed standards but experienced a loss nonetheless. Except as concerns credit card processing, there are virtually no complete and universally accepted standards for data security, but the presence of some standards – however incomplete and inadequate they may be – could put the onus on a company that experienced a breach to explain why it had not adopted and adhered to some standard.

---

1 "Lloyd's faces up to threat of e-crime," *Computing*, June 26, 2006

Data security and privacy regulations

Concern over the privacy and security of consumer data first arose in the 1960s and 1970s. With the emergence of the internet, however, came new possibilities for widespread loss and abuse of personal information. Around the world, data protection concerns have led to legislation affecting every company operating in the global marketplace. Until the late 1990s, legislative attempts to address these issues were based largely on sector-specific legislation and self-regulation. The introduction of sweeping European Union (EU) legislation in recent years and the subsequent upsetting of the international status quo on the treatment of personal data have altered standards of privacy and data protection. An understanding of the differences in regulation that exist between industries and countries, as well as the potential liabilities for the misuse or improper handling of personal information is now essential for any company operating in the global online marketplace.

The protection of personal information in the US

Except for certain specific areas such as medical information, internet privacy and data security is largely unregulated at the federal level in the US. Attempts to introduce legislation, the most recent being S. 495: **Personal Data Privacy and Security Act of 2007**, have not been successful. S. 495 was intended to "prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information." The bill was considered in the Senate Judiciary Committee which recommended it to be considered by the Senate as a whole. However, it never came up for a vote.

Although there is no comprehensive privacy protection law in the US for Internet transactions, several laws address particular situations, such as for healthcare data (the **Health Information and Portability Accountability Act**), financial data (**Gramm-Leach-Bliley Act**), credit information (**Fair Credit Reporting Act**) and information obtained from children (the **Children's Online Privacy Protection Act**). Other federal laws that touch upon data privacy and security issues include the **Electronic Communications Privacy Act of 1986** – which principally addresses government surveillance, but also includes provisions concerning access to private computerized messages by third parties without legitimate authorization – and the **Computer Fraud and Abuse Act**, which prohibits accessing a computer without authorization to obtain certain types of information. The Act also prohibits knowingly accessing a computer with the intent to defraud and thereby obtaining anything of value.

A number of states have enacted laws addressing privacy and the protection of data. Breach laws, which have been enacted in over three dozen states, require companies to notify consumers when their personal information has been exposed to potential misuse. California was the first state to pass a security breach notification law with the **Security Breach Information Act,** which requires prompt public disclosure of any breach that might have compromised computer-based personal information about a California resident. In the wake of the TJX event, Minnesota lawmakers amended that state's data breach notification law to include security and liability components. California's **Online Privacy Protection Act (OPPA)**, which was signed into law in 2003, was the first state law to require owners of commercial Web sites or online services to post a privacy policy. OPPA applies to any person or company in the United States (and conceivably the world) that owns a commercial Web site or an online service that "collects and maintains personally identifiable information from a consumer residing in California who uses or visits" that Web site or online service.

The protection of personal information in the EU

The right to privacy is more strictly protected in the EU than in the US. **The Information Directive of 1995** and the more recent **Directive on Privacy and Electronic Communications of 2002** emphatically state that EU residents are entitled to a right to privacy. The 2002 EU Directive builds on the privacy protections that are contained in the 1995 EU Information Directive which defines "personal data" as "any information relating to an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity…" In the US, medical and financial records are protected under separate legislation, while most other private information acquired online does not have legal protection. The EU centrally supervises the private sector's use of personal data. A proposed amendment to the Directive on Privacy and Electronic Communications would mandate security breach notification.

The cost of data breaches

Data security breaches can expose a company to fines and penalties as well as to lawsuits. Although the damages associated with unlawful disclosure of private information are normally not large on an individual basis, collectively they can be massive, and defendants commonly join together in class action lawsuits. Settlements can include monetary damages as well as the cost of credit monitoring services and ID theft coverage. In addition, companies can incur millions of dollars in expenses to secure compromised networks, assess damages and notify customers. After retailer TJX Companies announced that information on more than 45 million customers' credit and debit account were partially exposed following a network breach, there were significant short term expenses to secure networks, investigate and mitigate the event, notify customers, and manage the public relations furor. Actions filed by business partners resulted in a $41 million settlement with Visa Inc. and a $24 million settlement with MasterCard International Inc. Additionally, TJX estimates that it will cost in excess of $150 million to clean up its security and settle with customers affected by the breach.

In a study of the costs of data breach, the Ponemon Institute found that of 23 million adults who had been notified that their data had been lost or compromised, 20 percent terminated their accounts and another 40 percent considered doing so. The damage to reputation is reflected not just in a loss of customers or clients over the longer term, but also in the reaction among investors who may sell a company's stock when a security breach becomes public. Research found that breaches in publicly traded companies result in a 1 percent to 5 percent loss in stock price within a month of notification of the incident.

A highly publicized failure to protect personal information can be extremely costly – and sometimes even fatal – for a company whose business depends on customer and client trust. In January 2005, a large credit card payment processing company, CardSystems Solutions, was forced to discontinue some of its core operations after a network security breach exposed 40 million accounts. Facing the prospect of being forced out of business, the company was promptly sold to a competitor.

The past several years have also seen increased federal scrutiny of poor information management practices. In one highly publicized case, the FTC levied a $10-million penalty on top of $5 million in restitution against data broker ChoicePoint Inc. – the largest civil penalty in the agency's history – for allowing sensitive consumer information to get into the hands of con artists. The FTC cited ChoicePoint for

violating the Fair Credit Reporting Act and for violating basic fair-practices laws. In addition, the company spent about $2 million to notify consumers whose data was exposed. The FTC also is aggressively pursuing companies that fail to live up to their stated privacy policies based on its interpretation of Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive trade practices.

Minnesota law, and similar laws proposed in other states, requires retailers, rather than banks or credit card companies, to bear the cost of losses when hackers steal credit card information. Such cost-shifting laws could significantly impact retailers; credit card fraud losses totaled more than $2 billion in 2006, according to the *Wall Street Journal*.

Risk management: Technology vs. insurance

Data security consultants frequently voice frustration at the generally poor state of security at many companies. Some companies have concluded that state-of-the-art data security measures are not cost efficient: the expected (or at least perceived) costs associated with bad press, angry customers, and network downtime may not be offset by the time, expense, reduced functionality, and frustrated end users that are nearly inevitable with enhanced data security. However, the prospect of mammoth liabilities in the wake TJX and other large data security breaches have led many companies to rethink their risk management strategies.

In most companies, data security has been the responsibility of the IT department. However, many IT security experts recognize that data security is an enterprise-wide activity that requires the involvement of corporate risk managers and senior management and managers throughout the organization. “The principal goal of an organization’s [data security] risk management process should be to protect the organization and its ability to perform their mission, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.” (“Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology”). An enterprise-wide approach to data security, while not mandated, is encouraged by internal control requirements of the Sarbanes-Oxley Act and by enterprise risk management standards such as those embedded in the controls for financial processes promulgated by Committee of Sponsoring Organizations of the Treadway Commission (COSO).

Protection from harm on any networked computer system will never be 100%. Internet security protection is a continual process that cannot be solved entirely by technical means such as firewalls, authentication systems, and antivirus software. To provide a financial backstop to data security technology, data breach insurance coverages have been introduced. Data breach coverage is still relatively immature and lacks uniformity from one carrier to another, but policies have become both more comprehensive and more focused as insurers have come to better understand the risk landscape of cyberspace as well as the specific business needs of their customers. Insurers now offer property and theft (first-party) coverage and liability (third-party) coverage related to privacy and data security. Some insurers also offer crises management benefits (including hiring a public relations team), customer notification expense coverage and risk-management services.

The rate of development of privacy and data security insurance products had been hampered by the fact that buyers were frustrated by the patchwork of non-standardized coverages and comparatively low limits available in the market, while

insurers were less than enthusiastic about developing products with significant underwriting challenges for which these was a perceived lack of demand. Inadequate understanding of exposures and relevant insurance products by many agents and brokers also may have impeded growth. As a result, the entire cyberinsurance market – of which data security products are a subset – is estimated to be only about $400 million in written premium (Betterley Risk Consultants), well below analyst forecasts of several billion dollars in premium by this point in time. Conning, for example, predicted in 2002 that the market would be as much as $6 billion by 2006.

The situation is rapidly changing, however. Highly publicized losses have stimulated interest in insurance solutions, which in turn has encouraged more insurers to enter the market. Companies now offering cyberliability products include AIG, Chubb, Travelers, Ace, CNA, Darwin, Beazley, Hiscox, Zurich, Evanston and Great American. As underwriters – both at primary carriers and at reinsurers – grow more familiar with the exposures, coverage will become both broader and better tailored to specific exposures, and policy limits will increase. Ultimately, coverages will become more standardized, making syndicated programs, and consequently much larger limits of liability, possible. At that point it is likely that the cyberinsurance market will experience the explosive growth that has long been predicted by analysts.

Almost every company maintains transaction and customer information on computers, and a great many companies transact at least a portion of their business electronically. Consequently, the vast majority of companies are exposed to electronic data security breaches. The financial consequences can be enormous – sometimes even devastating – but most companies have relied almost exclusively on technological solutions to manage the risk. While the market for data security insurance is still comparatively immature, increasingly sophisticated products, higher policy limits and competitive pricing, combined with a growing awareness at many companies that data security should not be exclusively an IT issue, will eventually make these products a standard part of data security risk management strategies.

This Briefing was written by Johanny Cruz, jcruz@advisen.com, and Dave Bradford, dbradford@advisen.com.

Cyberinsurance large losses and program benchmarking data can be accessed through the Advisen information platform. Losses can be accessed through MSCAd (Cases & Actions) under the Losses & Exposures tab at the top of the page. Select Cyber Risks from the Category menu under the Case tab. Benchmark statistics can be calculated by selecting Liability/E-business Liability in the Coverage and Lines of Business sections of both Advanced benchmarking and Express benchmarking, accessible from the Benchmarking tab along the top.