ADVISEN Productivity & Insight for Insurance Professionals

Swett & Crawford
Everything We Know Goes Into Everything We Do™

Data Security Issues Escalate as Risk Management Evolves

An Advisen Special Report

April 2010

Executive summary

With the proliferation of the Internet, and its integration with all areas of commerce, data security liability has been mounting. The issues behind this liability threat follow:

- Pervasive use of Internet-connected databases and electronic transactions has exposed companies across-the-board to malicious viruses and hackers. The growing use of WiFi-enabled transactions creates additional potential security holes.
- All credit and debit card transactions are electronically processed through computer systems, with payment processors acting as middlemen. Most of the largest data breaches have involved card-processors and retailers as the faulted parties.
- Laptops and other portable data storage devices, such as flash drives, increase the risks that lost devices end up in the wrong hands.
- Credit card companies have developed security standards for processors to improve safety.
- Information technology (IT) professionals must go beyond these standards, and view data security from an enterprise-wide endeavor to protect their organizations.
- Database and network security responsibilities should extend beyond the IT department, as policies need to be set by senior management and risk managers, and strategic outlook for data security should be viewed as a corporate governance issue at the board level.
- Insurance products mitigating the risk to data security are proliferating, and are part of the overall risk management of cyber liability. Being a relatively new product, these policies vary widely in their specific coverages.

Please see the Appendix for information on select large data security events of the past decade.

Introduction

Data security is a widespread problem for companies across-the-board. Any entity with a presence on the Internet, with sensitive data on servers connected to the Internet, or transmitting data such as credit card payments, is exposed to this risk. Today, this covers just about all businesses and other organizations, right down to the mom-and-pop shops performing credit card transactions. As data gets passed around at increasing rates, the liability of data breaches escalates with it.

Cyberspace was initially thought to be a domain with few risks for commerce with limited property and general liability exposures coming into play. These naïve concepts have long hardened into the realization that new sets of cyber liability risks have emerged; risks that are not often covered by standard property and general liability policies. Lost, stolen and hacked personal data unleashes a firestorm of customer resentment, litigation from aggrieved parties, and regulatory actions. Large lawsuits have risen over the past decade regarding breaches of data security, with the largest coming at the tail end of the past decade. Most of the vitriol in the court system has been directed toward credit (and debit) card processors and retailers such as Heartland Payment Systems and TJX Companies. Organizations of all stripes, however, are exposed to these risks, and one only needs to look as far as technologically-savvy Google and its Gmail break-in incident in China to learn that lesson.

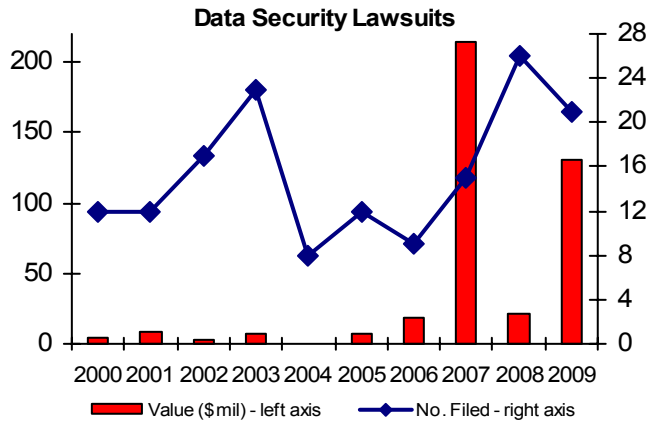
The large credit card brand managers, such as Visa and MasterCard, have developed IT standards to help credit card processing companies limit their exposure to fraud through increased controls around data. IT professionals of all companies, however, must provide holistic security that more than meets baseline requirements, and must view data security as an enterprise-wide and ever-changing process. Boards of companies are becoming more aware of their exposure to these risks, and should consider data security and broader cyber liability as a corporate governance responsibility. Senior management and risk managers also need to become involved in IT policies, as well as consider the rapidly expanding set of insurance products dealing with these issues to help mitigate the risks.

The scourge of the 21st Century

In the first decade of the 21st Century, database information was stored, shared, and processed at heightened dimensions, benefiting both commerce and consumers. With these benefits came opportunities for thieves, and the associated obligations and risks of those carrying coveted information. One of the leading authorities on data breaches, the non-profit Privacy Rights Clearinghouse, started tracking data breaches in 2005. From 2005 through the end of 2009, the organization claims that there were at least 345 million records breached in the US containing sensitive and personal information, more than one for each person in the US. They caution that the number should actually be higher because incidences are not counted when the organization is unable to confirm the number of records affected.

The Ponemon Institute, a leading research firm in the data protection arena, estimates in its 2009 Annual Study that 85 percent of US organizations (i.e., both private and government) may have experienced at least one data breach in 2009. A report from Javelin Strategy & Research, a data security consulting firm, found that 10 million cases of identity fraud occurred in the US in 2008, up 22 percent from a year earlier, and 11 percent of them were due to online theft and data breaches. The Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center, estimates that online fraud cost $265 million in 2008.

Advisen's Master Significant Case and Action Database (MSCAd)[1] confirms this trend of ballooning database breaches, which leads to lawsuits. MSCAd tracks large commercial lawsuits and other major events. The "Cyber Risks" section of MSCAd follows data security issues in the following categories: data lost or stolen, data security breaches, identity theft, improper disposal of records, fraudulent account access, unauthorized data distribution, and transaction processing. These types of lawsuits were almost non-existent before 1998, but the number filed reached 13 suits in 1998, and grew to 26 in 2008 and 21 in 2009. The cost to companies for these suits has mushroomed, from almost nothing before 1998, to $4.3 million in 2000, and reached $214.2 million in 2007. For suits filed in 2009, companies have paid out $130.1 million so far, but many of these cases are yet to come to fruition, particularly the largest cases. MSCAd captures the largest and most expensive events, but thousands of smaller and potentially crippling events happen to companies of all sizes every year.



In addition to increased awareness of identity fraud among regulators and the general public, the growing costs to companies reflects the growing number of records breached. Companies have come to rely on larger databases to conduct business, but many have lagged in beefing up security policies. Most of the largest breaches occurred in the latter years of the decade. For example, the largest known data breach, involving an estimated 130 million records of credit and debit card information, was announced by credit card processor Heartland Payment Systems in January 2009. The company claims that the breaches to their data security occurred in 2008. Before this announcement, the largest known breach found retailer TJX Companies, owner of TJ Maxx and Marshall's, the victim of a hacker scam, placing possibly 100 million records at risk, originally uncovered in January 2007 and occurring from July 2005 through January 2007.

How much do data breaches cost? The cost per security breach varies depending on who is counting, but all estimates are high. Forrester Research, management and IT consultant, estimates the average US data breach incident of sensitive data to cost $14 million, and they run as high as $50 million. In the "US Cost of Data Breach Study," conducted by The Ponemon Institute in conjunction with PGP Corporation, a data protection company, the estimate in 2009 was $6.75 million per incident.

The PGP/Ponemon study also estimates that data breaches cost US companies $204 per compromised customer record in 2009. Forrester Research gives a range from $90 to $305 per record – with the top end representing high-profile breaches in highly regulated industries like banking. Allied World Assurance Company keeps a data-loss-cost calculator on its *Tech//404* website, and its current estimate per record averages $166. The *Tech//404* site breaks the number down by the cost of an internal investigation, notification and crisis management cost, and regulatory and compliance costs.

[1] Advisen tracks significant lawsuits filed against companies and their directors and officers in MSCAd, as well as other major company events. MSCAd is the most complete and accurate database of such events, consisting of almost 40,000 events and over $900 billion in aggregate losses.

Companies will incur costs for notification and claims processing, activities that often are required by either state or federal laws, and may need to hire a public relations firm for "damage control." Fixing the data breach problem and data recovery is expensive in its own right and may involve hiring a forensic expert to discover the source of the breach. They will also often pay for credit monitoring services as a goodwill gesture, to help repair their image and mitigate against large damage awards in any subsequent civil suits.

The cost of lost business, however, is the most costly effect of any breach, according to the PGP/Ponemon 2008 study. The cost averaged $4.6 million per incident, or $139 per record, which was 69 percent of all data breach costs of $6.65 million per incident in 2008. Once a company's reputation is soiled, it is hard to recover and could become the first step toward the business failing. Regulatory fines can become substantial, and regulatory investigation defense costs are spiraling regardless of whether the firm is found liable. Costs can become uncontrollable if the company reacts off the cuff when data breaches occur. Having data breach scenarios as part of any disaster recovery plan (DRP) is imperative, which will allow the company to focus on priorities.

Settlement and awards for civil cases and associated defense costs are not part of any of these estimates. This area of litigation is evolving too quickly for any of the cost-estimators to produce reliable estimates. Consequently, these cost estimates vastly undercount the true costs, particularly for high profile data breaches. For example, TJX Companies set aside a $256 million fund in 2007 to deal with costs associated with their data breach, and has paid over $75 million in civil settlements alone from this fund thus far.

The risk of data security breaches is global. For example, in October 2007, disks containing personal banking information for 25 million people was lost in the UK. The disks were missing for three weeks before being found. Banks in the UK could end up spending as much at least $500 million dealing with the consequences. This is based on a conservative estimate of $20 per account, according to Gartner Inc.

Data security basics

With the risks of holding and transferring data being undeniable, data security has become a critical exercise in any organization. Data security is the practice of keeping data protected from corruption and unauthorized access. It helps to ensure privacy, protecting personal data, while allowing access to the proper users of the data.

The practice of data security goes far beyond protecting network databases from hackers and malicious viruses. Many of the threats to data security results from lost or stolen laptops, as well as other portable digital devices like external hard drives, flash drives, and even iPhones and Blackberries. For example, Brazos Higher Education Service Corporation, a non-profit company that originates and services student loans, endangered 550,000 records of personal customer data due to a stolen laptop incident in September 2004. Company policies concerning laptop use and portable storage devises, complemented by software locks and encryption, are the most effective way to mitigate potential problems. In the Brazos example, customer data was not encrypted. Access to company data through personal devices remains a thorny issue despite all of the technological locks used, making employee education paramount.

The specific technological forms of data protection include encryption, authentication, data masking, data erasure, backup solutions and hardware-based mechanisms. Encryption uses mathematical schemes and algorithms to scramble data into unreadable text. The party that possesses the key can

decode it. Full-disk encryption encrypts every piece of data on a disk or disk drive, which is recommended.

Authentication ensures that not only data is genuine, but also it validates that all parties accessing that data are who they claim to be. Logging into a system is one form, where users have various privileges. Strong user authentication systems use multiple factors, which may include an additional password, a one-time password, and hardware solutions such as smart cards and fingerprints.

Data masking is the practice of obscuring specific data within a database. This ranges from masking data from users, developers, vendors, and others. Data erasure is a method that completely destroys all data on hard drives or other digital media, which ensures that no sensitive data is leaked. Data security is not complete without backups, which ensure that lost data is recovered if something (when something) goes wrong. Software-based security solutions prevent data from being stolen, but a malicious program or hacker can corrupt the data, making it unusable. Hardware-based security solutions, such as biometric technology, can prevent access to the data, offering stronger protection.

Credit card companies get organized

Most of the major data breaches have revolved around credit and debit card processing, snagging retailers and credit card processors. Credit card processors are not the brand managers with their logo on the card, such as Visa and MasterCard. They are also not sponsoring banks, like Bank of America, which pays for transactions up front and bills consumers. Card processors are vendors that process credit card transactions. Retailers will contract with one to received approval information about each transaction, and the transaction information is transmitted to the appropriate bank sponsor for payment.

The Payment Card Industry Data Security Standard (PCI DSS) is a worldwide security standard created by the Payment Card Industry Security Standard Council in December 2004. The members are the card brand managers, like Visa. The goal of the standard is to prevent credit and debit card fraud through increased controls around the data. The PCI DSS is required by all organizations that hold and process cardholder information from any card with the logo of one of the Council's members. Compliance is assessed annually by independent assessors.

All of the major credit/debit card brand managers are members the Council, including Visa, MasterCard and American Express. The predecessor to this standard was the Cardholder Information Security Program (CISP) established by Visa, and other card brand managers required their own standards. All of the major and second-tier brand managers, however, recognized that a uniform standard was required to be effective and cost-efficient.

The standard contains rules around how information is stored at the retail and card processing vendor levels, transferred to and from the two entities, and payment information processed for the underlying bank's payment. Since the standard was first introduced in 2004, many updated versions have been released. In July 2009, wireless guidelines were published, which apply to the deployment of wireless LANs on sites that possess and transmit credit card data.

Critics of the PCI DSS feel that the standard is insufficient and point to a number of large and recent data breaches that were considered PCI DSS-compliant at the time of the breach. They feel that the guidelines are reactive, as the standard emerged long after standards were needed. New guidelines are developed, critics claim, only after major breaches bring holes to light.

For example, from January 2005 through January 2007, in one of the largest data breaches in history TJX Companies, fell victim to data breaches involving a gang of hackers using laptops. The gang decoded the data in the stores' Wireless LANs between payment scanners, resulting in up to 100 million records breached. The PCI DSS wireless guidelines were not released until more than two years after the announcement of this breach.

Global laws evolving

As global economies come to grip with the enormity of the data security challenge, many laws have been passed to help protect consumers from the associated risks, with privacy concerns at the core of these laws. Some of the major laws in the EU and US follow:

- EU Data Protection Directive (1995) requires that all EU members must adopt national regulations to standardize the protection of data privacy for citizens throughout the EU.
- UK Data Protection Act 1998 is a result of the above EU Directive. It ensures that personal data is accessible to those whom it concerns.
- EU Data Retention Directive (2006) is a controversial directive opposed by civil liberties groups. It compels all EU members to adopt laws that require Internet service providers and phone service companies to keep customer data for up to two years.
- US Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires the adoption of national standards for electronic healthcare transactions, and requires healthcare providers, insurers and employers to safeguard the security and privacy of health-related data.
- US Gramm-Leach-Bliley Act of 1999 protects the privacy and security of private financial information that financial institutions collect, hold and process.
- US Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 expands the reach of HIPAA data privacy requirements to include "business associates" of healthcare providers, such as accountants, law firms, billing agencies and other service providers. The law came into force in February 2010.
- US Red Flags Rule is a federal law, enforced by the Federal Trade Commission (FTC), that requires financial institutions and creditors with "covered accounts" to formulate and implement an identity-theft prevention program. The compliance deadline for this rule is June 1, 2010. The determination of whether an entity is covered by the rule is not based on industry, but rather by activities.
- Many US state notification laws require businesses, nonprofit organizations and state institutions to notify consumers when personal information may have been compromised, lost and stolen. In the US, 45 states, DC, Puerto Rico and the Virgin Islands have enacted similar consumer notification laws, with only Alabama, Kentucky, Missouri, New Mexico and South Dakota without such laws.
- Massachusetts Data Security Regulations require every person who owns or licenses personal information about a Massachusetts resident to develop, implement and maintain a comprehensive, written information-security program. The compliance deadline for this rule was March 1, 2010.

"But we had locks"

"But we had locks" exclaimed Carol Meyerowitz, CEO of TJX Companies, in June 2007 at the first shareholder meeting since the disclosure of its 100-million-record data breach. Data security has evolved beyond an IT function, and has become the ultimate responsibility of the executive suite and board of directors. Information security governance needs to be seen as a corporate governance issue, with responsibilities beyond the IT department, straight up to the board. In this day where floods of data are tossed around between systems that do not necessarily fit tightly together, simply ensuring that "locks" are installed at specific technological points does not ensure a comprehensive security system. Technology has advanced to this point much ahead of awareness of its risks, particularly within the executive suite.

Business continuity. A data security breakdown could cripple an organization, whether it is an accidental loss, malicious hacker and virus attack, or terrorist attack on an organization. All organizations need to have a business continuity plan (BCP) to deal with potential crises. Business continuity is a mechanism by which an organization continues to operate its critical business units as disruptions occur to normal business operations.

BCPs must be made at the company level, mandated by the board, and involves all business areas and overseen by risk management professionals. Although the best plans never completely stand up to reality as disasters occur, planning is invaluable. Any well thought out plan can help to reduce the cost of recoveries, keep everyone marching in the same direction, and prevent smaller problems from spiraling into disasters. DRPs are a subset of BCPs, which focus on specific steps to recover critical IT infrastructure, and are implemented immediately following disasters.

Outsourcing IT. Data security breaches often occur due to the fault of IT outsourced vendors and software providers, particularly vendors in the logistics and supply chain. Some companies may believe that outsourcing transfers liability to the vendor, but the perception of shifting liability is an illusion, as data owners remain liable for data breaches. Placing "hold harmless" and indemnity agreements in contracts with vendors is an issue between these parties, and have no bearing on customer liability. Bankruptcy of IT outsource vendors could cause data loss and could possibly lead to stolen data, and data owners need to respond quickly. If not properly planned for, this event could be disastrous for customers of failed IT outsource vendors. This scenario is an essential part of any BCP and DRP. As with all BCPs, senior management should take ultimate responsibility as they have the skills to assess the stability of vendors, and risk managers need to become aware of all issues of risk.

Critical data security issues for the IT department. Despite the importance of recognizing data security as an entity-wide responsibility, most issues lie within the IT department. Many types of data security breaches occur within the domain of the IT department, and the risk of incurring losses can be mitigated with proper IT policies. Beyond policies, vigilant and knowledgeable IT management is indispensable given today's multi-layered, complex and continually changing data center infrastructure.

According to the Ponemon Institute, not only have 85 percent of US organizations experienced at least one data breach last year, but 82 percent of data breach cases involved organizations with more than one data breach that compromised over 1,000 records per incident. An alarming 88 percent of all cases in 2008 involved insider negligence. This indicates that merely having proper IT procedures can avoid many mistakes, and background checks on IT professionals can help weed out those

subject to foul play. "We don't do background checks on IT people, but we give them the keys to the castle," said Thomas Katona, president and managing member of Apogee Insurance Group.[2] In December 2009, Cardiology Consultants fell victim to an apparent inside job when a thief, armed with an office security code for this medical center, stole a valuable computer used for ultrasound images that contained 8,000 patient records.

The risk falls far beyond company networks and IT professionals, but includes other hardware and personnel. Problems come from any employee that touches data, as well as vendors and contractors. Beyond PCs, laptops are a major source of lost and unprotected data, as are flash drives, iPods, iPhones and Blackberries, and any other portable storage devices like external hard drives. For example, in February 2010, a break-in at Arrow Electronics' offices in New York resulted in a stolen laptop containing 4,004 records of employee personal information, including some credit card and social security information.

The Ponemon Institute found, in its "US Survey: Confidential Data at Risk," 81 percent of respondents reported that their organizations lost one or more laptops containing sensitive or confidential business information. According to a survey by Kroll Inc., over a five year period data security breaches occurred: 22.4 percent due to lost or stolen laptops; 20.8 percent because of hacking; 15.3 percent via the Web; 4.8 percent in disposal of documents on computers; and 1.8 percent due to emails.

Some of the most critical data security issues for IT departments, which can help to mitigate the risk of data breaches, include:[3]

- Know who uses each bit of data and its location.
- Not all data is created equal. Organizations should prioritize data security activities to address the most sensitive and important data.
- Simply passing a regulatory audit does not in itself ensure comprehensive data security. Neither does passing a risk assessment like PCI DSS requirements. Companies should strive to follow their industry's best practices, rather than the least common denominator.
- Data security deals with many areas of expertise, so security strategy sometimes falls into silos that are not interconnected. Companies need to develop an enterprise-wide data protection strategy, focusing on how data flows through the organization.
- The IT department is not a fire department, as they are supposed to implement an IT structure that grows with the organization and changing technology.
- Outsourcing responsibility is a fantasy. Most all data protection and privacy regulations around the world state the organizations are responsible for their data, and responsibility cannot be shared.
- User education is important, but use automation tools as a backup, such as tools that monitor email, and controls on data manipulation.
- DRPs are critical. Creating a plan for various disaster scenarios, will minimize the risks associated with data breaches. It isn't a matter of "if" a data breach occurs, but "when."

[2] "Data Security Breaches Present Risks, Opportunities for Agents," *Insurance Journal*, April 27, 2009.
[3] This list was compiled with the help of *Processor* magazine, ITproPortal.com, and DataSecurityPolicies.com.

Emerging insurance coverage

In the past, data breach events were considered the domain of commercial general liability (CGL) and property policies. Some insurance coverage may be in place depending on the wording and industry of the insured. Privacy and data breach endorsements are sometimes added as well. As data breaches become more common and at higher potential severity levels, data breach exclusions are rapidly becoming the norm.

Furthermore, two important cases were decided in 2003, which have made relying on CGL and property policies for data breaches all but extinct. In Ward General Insurance Services v. Employers Fire Insurance, the court held that data is not considered tangible property in the context of property policies. In AOL v. St. Paul Mercury Insurance Company, the court found that computer data is not tangible property under a general liability policy.

In a recent court decision, Creative Hospitality Ventures v. United States Liability Company, the court may have potentially opened the door to coverage for third party claims within the Side B coverage for personal and advertising injury within the CGL policy. Insurers have not been forthcoming in extending coverage under this coverage for invasion of privacy claims, but future litigation may change their position or simply lead to new CGL exclusions.

Other types of major traditional policies that could respond to data breach events include errors & omissions (E&O) and media liability coverage. If an E&O policy is worded broadly enough, or if it has a specific provision about data breaches, it could cover data lost and damaged caused in the course of professional services. Media liability coverage is a type of E&O insurance designed for media professionals. The "invasion of privacy" provision in these policies may come into affect due to a data breach. Certain other specific types of policies can also come into play, such as kidnap and ransom policies if a hacker demands an extortion fee or threatens to distribute private information.

Data breach insurance evolving. Given that coverage of data breaches under traditional policies is muddy at best, and most likely covers only specific circumstances, companies need broader affirmative coverage for this area. Over 20 insurers including several Lloyd's syndicates have developed coverage to deal with these issues, and the market is still evolving at a rapid rate. The policies come by many names, which can be called network risk insurance, cyberliability insurance, privacy and security insurance, data security insurance, and data breach insurance.

Regardless of the name, data breach coverage usually comes in three parts: first-party; third-party; and coverage for other related issues. First-party coverage is for direct losses incurred by insureds as a result of a data breach, such as replacing and recovering lost and destroyed data, forensic investigation expenses, business interruption losses and extortion demands. Other first-party loss coverage includes notification costs when required by law, credit monitoring services provided to affected customers, call center services for affected customers, and expenses for emergency public relations teams to handle "damage control." For these first party coverage's, sub-limits are most likely apply but some carriers do include full limits.

Third-party coverage protects insureds from liability to outside entities such as customers, credit card companies, financial institutions and regulatory authorities. Coverage extends to defense costs and damages in civil lawsuits, and depending on the policy form, either full or partial limits for defense costs in defending regulatory actions. Some insurers may also offer full or partial sub-limits for fines and penalties imposed in regulatory actions. Other related coverages may include first-party crime coverage involving electronic theft as a result of a data breach and Internet-based media

coverage, including intellectual property, personal injury and advertising injury arising from online content.

Coverage forms are generally divided into two sections as respects third-party coverage: privacy and network security. Privacy in its most basic form is defined as unauthorized disclosure of private personal information in violation of privacy laws. Network security is the unauthorized access or unauthorized use of private personal information and confidential corporate information on an insured's computer system. Network security coverage normally provides coverage for denial of service attacks, introduction of malicious codes and viruses, and the destruction or damage of data stored on computer systems.

Data security coverage is an emerging area, so coverage terms vary widely compared to traditional areas. ISO does not have a standard application or policy, so insurers have different approaches to the types of risks covered, though in recent years they have been converging. Pricing is often inconsistent because underwriters are looking at a short and rapidly changing claims history to base their risk judgments. Pricing is based off gross revenue for most current policies. In the recent past, insurers used the number of records in an insured's possession as the basis for pricing, but due to the difficulty in ascertaining the number of records carriers have switched to the simplicity of using gross revenue. Some carriers offer policies with shared limit coverage with other policies, such as professional liability, while others offer data security policies with their own limit.[4] Because technology changes rapidly, risk issues associated with technology is in a state of constant flux. Insurance buyers should routinely check their policy forms to ensure that their coverage is adequate for this moving target.

With growing awareness comes mushrooming demand. Many insureds assume their traditional policies cover data breach liability. Companies should have their existing policies' coverage reviewed to understand the specific areas of coverage. A professional evaluation could be in order, as in-house risk management teams and generalist insurance brokers might not necessarily know the answer in this rapidly evolving field with little case law history.

Most likely, evaluations will reveal coverage with many holes, which could prove to be quite costly. Laws and regulations will often dictate certain responses in the event of data breaches, adding to costs, and regulatory actions such as FTC inquiries will make breaches more expensive. Brokers should be prepared to educate their clients about the total costs associated with data breaches, from notification, to credit monitoring services, to down time, as well as civil suits.

Data security was once considered merely an IT issue, for the geeks in the computer room to handle. It has, however, evolved into a legal obligation of the entire organizations. Senior management and the board of directors should become involved with setting policy and taking ultimate responsibility, and consider it a core corporate governance issue. Regardless of precautions, companies should be aware that no one is safe from this risk. With data flooding the Internet, and the growing use of WiFi networks contributing their own set of security exposures, it is virtually impossible to safeguard all data.

Once executives and risk managers of organizations and companies of all sizes become aware of their exposure to data breach liability, and of the shear size of possible associated losses, risk mitigation becomes essential for conducting business. In addition to reviewing IT policies and procedures, and considering appropriate DRPs and BCPs, data security insurance is an integral part of risk mitigation. Not just large businesses and institutions need to consider this insurance, but

[4] "Insurance for Breaches of Data Privacy and Information Security," Aon, December 1, 2007.

small shops on Main Street conducting credit card transactions will need it as well. It is potentially an enormous insurance market, which might some day rival the traditional coverage areas of CGL and property coverages in terms of market size as the economy is thrust further into the digital world.

Please see the Appendix for information on select large data security events of the past decade.

For more information about cyberliability insurance products, visit the Swett & Crawford Professional Services Group website at http://www.swett.com/main.php?page=PracticeGroupView&practiceGroupId=2.

This report was written by John W. Molka III, CFA, Senior Industry Analyst and Editor, 212.984.2753, jmolka@advisen.com.

About Swett & Crawford

Swett & Crawford, headquartered in Atlanta, Georgia, is owned by its employees and two private equity firms, HM Capital Partners and Banc of America Capital Investors.

In its national network of offices, Swett & Crawford serves independent agents and brokers through specialized Property, Casualty, Oil & Gas/Energy, Professional Services, Transportation and Underwriting Practice Groups. These groups provide access to commercial insurance products and programs, including property and casualty coverages, products liability, directors & officers and professional liability including cyber/privacy/security, commercial and public auto liability as well as a host of customized binding authorities and exclusive programs tailored to specific industries, businesses and professionals.

About Advisen

Advisen manages business information and market data for the commercial insurance industry and maintains critical risk analytics and time-saving workflow tools for over 530 industry leading firms. Through its work for the broadest customer base among information service providers, Advisen delivers actionable information and risk models at a fraction of the cost to have them built internally. Designed and evolved by risk and insurance experts, and used daily by more than 100,000 professionals, Advisen combines the industry's deepest data sets with proprietary analytics and offers insight into risk and insurance that is not available on any other system. Advisen is headquartered in New York. For more information, visit http://www.advisen.com or call +1.212.897.4800 in New York or +44(0)20.7929.5929 in London.

Appendix

The following are large data security events, which includes the top-three events in history as well as other select data breach events of the past decade.

Heartland Payment Systems

- A credit card and check processor, processing 100 million credit and debit card transactions a month for 250,000 US businesses.
- Malicious software breached their network, compromising the personal data of 130 million credit and debit cards, the largest in history. Visa and MasterCard tipped off the company to fraudulent card activity related to card transactions processed by Heartland's network.
- Occurred in October 2008, but perhaps began as early as December 2007. Announced in January 2009.
- The company estimated, in its quarterly report for the date ending September 30, 2009, that the data breach will directly cost $105.3 million. It is unlikely, however, that Heartland will ever pay the full cost of its alleged negligence, since that would bankrupt the company. Just looking at the cost of replacing the 130 million affected cards, at a widely considered conservative estimated cost of $30 per card, would cost the company almost $4 billion.
- The first consumer lawsuit was filed in federal court in January 2009, claiming that Heartland issued belated and inaccurate statements about the breach, and that the company does not appear to be offering credit monitoring services or any other relief to affected card holders.
- In March 2009, Visa removed Heartland from its list of companies compliant with the PCI DSS, pending re-certification by a third-party assessor. This action meant that merchants could not use the company to process payments if they themselves want to remain compliant. Most analysts agreed that it was unrealistic to expect merchant to switch processors in midstream, particularly since many have contracts with Heartland. This move was considered an attempt by Visa to avoid lawsuits, particularly from participating banks. It is important to note that Heartland was considered, by independent audit, as PCI DSS-compliant at the time of the breach.
- In May 2009, Heartland made it back onto Visa's list of PCI DSS Validated Service Providers.
- In September 2009, 30 financial institutions from 22 states filed a class action lawsuit against Heartland in federal court, claiming 10 counts including breach of contracts and negligence. The plaintiffs alleged that CEO Robert Carr knew that the PCI DSS was insufficient, citing remarks by the executive months before announcing the breach. He

called the standard "the lowest common denominator of data security" in a November 2008 earnings call.[5]

- In December 2009, Heartland won dismissal of a shareholder lawsuit against CEO Robert Carr and CFO Robert Baldwin, claiming that the company misled investors about its security before the breach. The judge ruled that investors failed to show that Heartland fraudulently concealed the attack and the state of data security.

TJX Companies

- Owner of apparel retailers TJ Maxx and Marshal's.
- The data breach was caused by hackers using laptops with wireless connections to decode data between wireless payment scanners at stores, by driving by or parking near stores in a technique called "war-driving." Once inside the network, the hackers collected personal credit card information and sold it to others that specialize in selling personal information over the Internet. It was first thought to have affected 46 million cards, but the estimate has grown to over 100 million, the second largest data breach in history.
- Occurred from July 2005 to January 2007, and perhaps as early as December 2002. Announced in January 2007. In 2007, the company put aside $256 million in reserve to pay for all estimated direct losses associated with this breach. Forrester Research places a total cost estimate at $500 million, and possibly as high as $1 billion.
- TJX was considered PCI DSS-compliant at the time of the data breaches. However, an investigation conducted by state attorneys general after the security breach was announced revealed that the company was not compliant with nine of the 12 PCI DSS requirements covering encryption, access controls and firewalls.[6]
- In January 2007, the first consumer suit was filed, accusing the retailer of negligence for not doing enough to secure customer data and for keeping quiet about the breach for months.
- In March 2007, the first shareholder suit was issued, asking for access to documents in order to assess if TJX's board has been doing its job in overseeing customer data.
- In April 2007, three New England Banking associations, Massachusetts Bankers Association, Connecticut Bankers Association, and Maine Association of Community Banks, and other individual banks, filed a lawsuit against TJX. Banks took on the primary brunt of the data breach, incurring expenses for replacing compromised cards and covering fraudulent charges. Since much of the transaction data was deleted by TJX, the full extent and exact cards affected may never be known. Visa claims that the toll from the breaches will continue to grow as stolen information finds its way into more thieves' hands.

[5] "Lawsuit: Heartland Knew Data Security Standard was 'Insufficient'," Government Information Security Articles, October 5, 2009.
[6] "TJ Maxx Settlement Requires Creation of Information Security Program and Funding," Client Alert, Pillsbury Winthrop Shaw Pittman LLP, July 1, 2009.

- In September 2007, TJX offered a settlement to its customers affected by the breach. It offered three free years of credit monitoring and identity theft insurance to certain customers confirmed as having data stolen. The company will also reimburse driver's license replacement expenses, including time spent at $10 per hour, if documentation is submitted. Others that submit documentation that claim lost time to deal with the effects of the breach, which are most of the claims, can receive a $30 store voucher.
- In November 2007, Visa settled with TJX for $40.9 million, which will be used to help recover losses by credit card issuing banks. Visa participating banks that did not accept this offer will need to pursue their own settlement. In an unrelated but significant case, a judge ruled that the banks suing TJX could not band together in a class, and must pursue their cases separately.
- In December 2007, given that the banks must pursue their own cases separately, most banks in the lawsuit led by the Massachusetts Bankers Association settled with TJX for an undisclosed amount. It appears the banks mostly accepted the Visa settlement.
- In April 2008, the FTC settled with TJX, saying that the company failed to use "reasonable and appropriate security for sensitive consumer information." The FTC ordered TJX to upgrade and implement comprehensive security procedures, and submit to audits by third-party security experts every other year for 20 years. No fines or penalties were levied because the FTC is prohibited from doing so in this instance.
- In May 2008, TJX settled with MasterCard for $24 million, which will reimburse its credit card issuing banks for the cost of replacing the cards.
- In June 2009, TJX settled a lawsuit brought by 41 state attorneys general for $9.75 million. The company will pay $2.5 million to create a data security fund for states, $5.5 million to fund data protection efforts by states, and $1.75 million to cover expenses related to the states' investigations. Additionally, TJX agreed to certify that its computer system meets detailed data security requirements specified by the states.
- In September 2009, TJX agreed to pay $525,000 to settle a lawsuit brought by several banks that were not part of previous settlements, which will reimburse the banks a portion of the expenses incurred in connection with the breach.

CardSystems Solutions

- A credit and debit card processor, which processed over $15 billion in credit card and online transactions each year.
- Hackers dropped a malicious script on the CardSystems application platform, in September 2004, injecting it through the Web application that customers use to access account information. The script extracted records and exported them to another site. Personal information was stolen from 263,000 cards, and exposed another 40 million cards to fraud. It is the third largest data breach in history and the largest at the time of the breach.
- The company claims that the only successful extraction of data occurred in May 2005, but extractions could have occurred as far back as September 2004. MasterCard first

discovered security violation in April 2005, and traced it back to CardSystems. It was announced in May 2005.

- CardSystems was audited by Savvis Inc. in June 2004, and certified the company as compliant with the CISP, the precursor to PCI DSS. After the breach was announced, Visa's investigation found that CardSystems was in fact not in compliance because it failed to maintain a proper firewall, failed to encrypt personal data, and improperly stored customer data. Visa noted that CardSystems did not pass an audit in 2003, which was performed by a company acquired by Savvis shortly before the 2004 audit.
- In June 2005, California credit card holders and merchants filed a class action lawsuit against CardSystems. The suit claims the company was negligent by failing to adequately secure credit card data. It also claims that the company, along with Merrick Bank, Visa and MasterCard violated their duty to properly inform consumers of the nature and degree of the security breach.
- In July 2005, Visa and American Express announced that they would terminate their relationship with CardSytems by the end of October 2005.
- In August 2005, CardSystems met its end of August deadline to become independently audited and considered PCI DSS-compliant. Visa and American Express, however, remained opposed to re-opening its relationship.
- In October 2005, Solidus Networks Inc (d.b.a., Pay By Touch Solutions) acquired CardSystems.
- In February 2006, the FTC settled with CardSystems and Pay By Touch. The settlement required both companies to establish and maintain a comprehensive information security program that includes administrative, technical and physical safeguards. It also requires them to obtain an audit from a qualified, independent professional every two years for the next 20 years.
- In November 2007, Solidus Networks declared bankruptcy, and in March 2008 CardSystems closed down.
- In June 2009, Merrick Bank filed a suit against CardSystems' auditor, Savvis, which certified that they company was CISP-compliant back in 2004. As a result of the audit, Merrick Bank claims, it signed a contract with CardSystems to process credit card transactions for its customers. Audits are simply a check to ensure that certain prescribed actions are implemented, or a point-in-time snapshot. They cannot account for the dynamic ebb-and-flow of IT decisions that may weaken security over time. It will be interesting to see how the court assigns responsibility beyond tracking the audit checklist.

Other select events of the past decade

- **RockYou** – A company that makes software and applications for users of social networking sites like Facebook. In December 2009, a hacker stole 32 million passwords from the company, and posted the list on the Internet. In addition to offering passwords and email information about these users, the posted list gave insight to would-be hackers and security experts about the password habits of computer users. For example, people using "123456" as their password are not alone. Also in December, an Indiana man filed a lawsuit against RockYou, alleging a failure to secure its network and protect customer data.

- **US Department of Veterans Affairs** – In May 2006, the US Department of Veterans Affairs (VA) announced that personal information on 26.5 million veterans and active duty personnel were stolen as a result of the theft of a laptop and external hard drive. The VA confirmed that records of every veteran discharged from the military since 1975 were stolen from the home of an agency employee. Included in the 26.5 million records breached was the personal information of 2.2 million active-duty troops.

- **RBS WorldPay** – An electronic payment processor owned by the Royal Bank of Scotland. It is a processor of non-cash transactions from merchant POS systems, websites and ATMs. In November 2008, the company's security was breached, potentially confiscating personal information of 1.5 million owners of prepaid payroll cards and gift cards, of which about 100 cards have been subject to fraud. The hackers orchestrated a global bank-robbing scheme in 49 cities, using personal cardholder information to duplicate ATM cards and withdraw $9 million in cash over a 30-minute time-span. In March 2009, Visa announced that RBS WorldPay was not PCI DSS-compliant and would need to become re-certified by a third-party assessor. In May 2009, the company successfully validated its compliance by an approved auditor.

- **Google** – This Internet software giant, along with 20 other US multinational corporations, fell victim to "a highly sophisticated and targeted attack" on their email accounts in China, exposing certain user-accounts to snooping by the perpetrators. The attacks were announced in January 2010 and were claimed by the company to have occurred in December 20009. Google clearly indicated that the attacks were orchestrated by agents of the Chinese government, which suggests that data security risks can come from state entities. This highly publicized event led to Google's defiant announcement that it will no longer censor Internet searches within China, as required by Chinese law, possibly endangering their presence in the country.