The Liability of Technology Companies for Data Breaches

ADVISEN Productivity & Insight for Insurance Professionals

ZURICH®

Suits against technology companies sparked by breaches of customer data are relatively uncommon today, but they are likely to mushroom in the coming years. Settlements potentially can run into the millions of dollars. Even if a firm ultimately prevails in a lawsuit, defense costs still can run into the hundreds of thousands of dollars.

Every organization that keeps records about its clients or handles credit card transactions should be concerned about data security. Breaches occur with alarming frequency, and even a moderate breach can cost a company millions of dollars in response costs, system repairs, lawsuits, and fines and penalties. Like every other company, information technology companies should be certain their data is secure. Additionally, they must be vigilant when dealing with sensitive customer data and when building or integrating systems that are to be used with sensitive data.

A study by the Ponemon Institute, a data protection research firm, found that 85 percent of U.S. organizations may have experienced at least one data breach in 2009. These breaches cost American businesses billions of dollars. Forty-two percent of the cases involved errors by third parties such as professional services, outsourcers, vendors and business partners. Data breaches were more expensive when third parties were involved, according to the study.[1]

"For many technology companies, it is not a question of if they will be implicated in a data breach, but rather when they will be implicated."

For many technology companies, it is not a question of *if* they will be implicated in a data breach, but rather *when* they will be implicated. However, companies can take steps to avoid being sued and to mitigate the financial impact if named in a data breach lawsuit. In order to protect against suits by customers or by third parties damaged by a data breach, it is important that technology companies understand how data breaches occur, the sources of data breach liability and the various sources of loss following a breach.

The data breach plague

Information stored in databases and processed through computer technologies benefits both companies and their customers. With these benefits, however, come opportunities for a new breed of tech-savvy thieves, and heightened obligations and risks of those responsible for protecting sensitive information. A leading authority on data breaches, the non-profit Privacy Rights Clearinghouse, found that from 2005 through the end of 2009, more than 497 million records containing sensitive and personal information were breached in the U.S., more than 1.5 for each person in the country.[2] 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. Before this announcement, retailer TJX Companies held the dubious honor for the most stolen records when a hacker scam placed possibly 100 million records at risk. TJX uncovered the breach in January 2007.

Most breaches are the outcome of theft by employees with authorized access to sensitive information or as a result of errors by data owners. Many breaches occur outside a company's computer network, with lost or stolen laptops, discs, flash drives, Blackberries and other portable storage devices accounting for a significant percentage of serious breaches. Some breaches do not involve digitized data at

1 The Ponemon Institute, "2009 US Cost of Data Breach Study."

2 Privacy Right Clearinghouse (http://www.privacyrights.org/data-breach/new).

all, but rather occur because of the improper disposal of paper records. Many of the largest and most costly data breaches, however, have been caused by hackers. The Heartland and TJX incidents, as well as a 2008 data breach involving the Dave & Buster's restaurant chain, for example, have been traced to a U.S. based hacker, Albert Gonzalez, and two Russian associates. According to *The 2010 Verizon Data Breach Investigations Report, produced by Verizon in collaboration with the U.S. Secret Service,* organized criminal groups were responsible for 85 percent of all stolen data in 2009.[3]

Following a data breach, a company typically incurs costs for notifying customers and for processing claims for damages. The company may need to hire a public relations firm or a crisis response consultant for "damage control." Repairing the data breach problem and recovering lost or damaged data can be expensive and may involve hiring experts. Companies 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. Regulatory fines are another significant contributor to loss, and regulatory investigation defense costs are spiraling.

Lost business is often the most costly effect of a breach. The Ponemon study found that lost business accounted for $144 of the average cost of $204 per lost record in 2009.[4] Lost business includes both terminations by existing clients and target customers who choose not to have a relationship with the company as a result of the breach. Once a company's reputation is tarnished, it is difficult to recover and can become the first step toward the business failing.

Privacy and data security laws and regulations

The privacy and security of personal data first became an issue of significant concern in the 1960s and 1970s. With the emergence of the Internet, however, came unprecedented new possibilities for widespread loss and abuse of personal information, leading to legislation affecting almost every company operating in the global marketplace.

Laws that have a bearing on how companies store and use data largely fall into three categories. Privacy laws concern what companies can and cannot reveal about their customers, and their obligations for protecting personal information. Data security laws address how sensitive information is to be kept safe. Data breach notification laws provide instructions on what steps are to be taken following a data breach, and may define the relative responsibilities and liabilities of parties involved in a breach. Some pieces of legislation include privacy, data security and data breach notification components.

3 The 2010 Verizon Data Breach Investigations Report, Verizon and the U.S. Secret Service.

4 The Ponemon Institute, "2009 US Cost of Data Breach Study."

The United States has no one comprehensive privacy protection law. Rather, numerous federal laws address particular situations, including:

- Healthcare data (HIPAA and HITECH),
- Financial data (Gramm-Leach-Bliley Act, Red Flags Rules of the Fair and Accurate Credit Transactions Act of 2003, the Bank Secrecy 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 and the Computer Fraud and Abuse Act.

Most federal privacy and data security laws specifically address the responsibilities of data owners. The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (The Stimulus Act), also addresses the responsibilities and potential liabilities of "business associates," which can include developers, outsourcers and other types of technology firms. Subtitle D of the HITECH Act addresses privacy and security concerns associated with the electronic transmission of health information, in part, through provisions that strengthen the civil and criminal enforcement of HIPAA rules.

Forty-five states, DC, Puerto Rico and the Virgin Islands have enacted data breach notification laws requiring businesses, nonprofit organizations and state institutions to notify consumers when personal information may have been compromised, lost or stolen. Some states have gone beyond merely requiring notification and have passed more core comprehensive data security legislation. The Massachusetts Data Security Regulations, for example, addresses the selection of third-party vendors, requiring companies to take "reasonable steps" to select and retain vendors that have the capacity to maintain appropriate security measures for personal information. Vendors also must be contractually required to maintain safeguards.

"Three states, Washington, Nevada and Minnesota, have passed laws explicitly holding businesses and governmental entities responsible to financial institutions for certain costs arising from payment card information breaches."

Three states, Washington, Nevada and Minnesota, have passed laws explicitly holding businesses and governmental entities responsible to financial institutions for certain costs arising from payment card information breaches. Under the Washington legislation, which modifies the state security breach law, businesses that process more than 6 million credit or debit card transactions annually, "processors" and "vendors" that fail to reasonably safeguard card information can be required to reimburse financial institutions for costs related to the re-issuance of cards as well as attorneys fees in the event that a security breach involving payment card information is a proximate result. Vendors are defined as entities that manufacture and sell software and equipment designed to process, transmit or store account information that the vendor does not own. Businesses, processors and vendors can claim immunity from liability under the Washington law if they have complied with standards adopted by the Payment Card Industry Security Council (see below).

American companies conducting business outside the U.S. are likely to confront stringent privacy and data security laws. The EU has taken a global leadership

position in setting and enforcing standards for the protection of private data. The Information Directive of 1995 and the more recent Directive on Privacy and Electronic Communications of 2002 make it clear that EU residents are entitled to a right to privacy. Unlike the U.S., which has a patchwork of laws concerning principally the use of healthcare and financial information, the EU centrally supervises the private sector's use of personal data.

Outsourcing IT function can create compliance issues and, with them, potential liability exposures for data owners. Companies can outsource functions, but typically retain the liability if outsource vendors do not meet compliance standards. For that reason, more companies are becoming vigilant in assuring their vendors are compliant with all data privacy and data security requirements of their industry, and are increasingly likely to hold vendors contractually responsible for the consequences of any lapses or shortcomings.

Data security standards

There is no universally acknowledged standard for data security, though a number of organizations have promulgated guidelines. The most influential standards are the ISO/IEC 27000-series, which comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), and the Payment Card Industry Data Security Standard (PCI DSS), which was developed by the five major credit card companies as a guideline for organizations that process card payments.

The ISO/IEC 27000-series provides best practice recommendations on information security management, risks and controls within the context of an overall Information Security Management System. Nine standards are presently available, with several more under development. ISO/IEC 27000 certification typically is voluntary, though increasingly organizations are being forced to become compliant, if not certified, by business partners and regulators, or as the result of certain legal obligations.

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. The standard contains rules concerning how information is stored at the retail and card processing vendor levels, transferred to and from the entities, and payment information processed for the underlying bank's payment. Unlike many standards, PCI DSS has teeth. Compliance is assessed annually by independent assessors. Fines can be levied for non-compliance. However, *The 2010 Verizon Data Breach Investigations Report* found that 79 percent of data breach victims subject to the PCI DSS standard in 2009 had not achieved compliance prior to the breach.[5]

Data breach liability

Companies having a serious data breach have been sued under a variety of legal theories. Allegations of negligence, breach of fiduciary duty and breach of contract, individually or together, are common. Some recent cases have argued that data breaches are subject to strict liability.

5 The 2010 Verizon Data Breach Investigations Report, Verizon and the U.S. Secret Service.

"Potential targets for lawsuits include software developers, system integrators, system outsourcing firms, data storage companies and systems security consultants and auditors."

Negligence, which is alleged in most data breach suits, is typically defined in terms of a failure to use reasonable care or doing something a reasonably prudent would not do. Breach of fiduciary duty is a failure to fulfill an obligation to act in the best interest of another party. Plaintiffs may claim that federal privacy laws, such as the ones embedded in HIPAA, and state consumer protection laws create fiduciary duties that are breached when data is lost or stolen. Breach of contract, as the name implies, is the failure to fulfill a condition of a contract. In the case of data breach claims, the contract in question may not be a physical document signed by both parties. Plaintiffs may claim the defendant's written privacy policy is a contract or that state consumer protection laws create an implied contract. Strict liability is typically applied in product liability cases, and means that the manufacturer of a product is automatically responsible for any injuries caused by the product.

Those individuals whose personal information was lost or stolen typically are the plaintiffs in data breach liability suits – sometimes individually, but often collectively in class actions. Settlements of data breach class actions can be huge – data broker ChoicePoint, for example, agreed to pay $10 million to settle a class-action lawsuit brought against it over the 2004 theft of 163,000 personal information records by Nigerian identity thieves. However, many of these suits are dismissed. Legal experts note that the majority of courts have rejected data breach claims brought by affected persons that did not suffer any appreciable injury. Simply having one's personal information lost or stolen may not be sufficient, as the plaintiff must actually have suffered a loss in order to claim damages.

In cases involving stolen credit card information, banks and credit card companies may sue the retailer or processing company that experienced the breach. Heartland Payment Systems, for example, agreed to settlements of up to $60 million with Visa, up to $41.4 million with MasterCard, $5 million with Discover and $3.6 million with American Express as regards the 2008 theft of 130 million credit card records.

Potential liability of technology companies

"Take action against the vendor," advises attorney Susan Lessack in an article on limiting liability for data breaches.[6] A company experiencing a costly data breach is likely to assess whether technology vendors and service providers are available to help share the pain. Potential targets for lawsuits include software developers, system integrators, system outsourcing firms, data storage companies and systems security consultants and auditors.

One widely reported case highlights how IT firms can be sued for data security issues involving their customers. In June 2005, it was discovered that information on 40 million credit cards had been stolen from CardSystems Solutions, a credit card processing company. Subsequently, a lawsuit was brought by a merchant bank, Merrick Bank, against CardSystem's security assessment company, Savvis. The suit alleged that Savvis negligently certified CardSystem's security as compliant with Visa's Card Information Security Program ("CISP," the standard that predates PCI DSS). Merrick claimed to have incurred $16 million in payments to the card brands.

6 "Hacked! Limiting employer liability for breaches of employee data," Business Management Daily (businessmanagementdaily.com), Sept. 29, 2009

While not necessarily resulting in lawsuits, other examples of vendors being implicated in customer data breaches include:

- Health insurer WellPoint claimed that a failed security update performed by a third-party vendor was responsible for a data breach that could have exposed personal information belonging to 470,000 customers.
- Enterprise software solution vendor Hummingbird Ltd lost a piece of equipment belonging to Texas Guaranteed Student Loan Corp. that contained unencrypted personal information on 1.7 million Texas student loan recipients.
- An undisclosed number of Chase customers were sent notification letters after a vendor lost a tape containing sensitive information.
- Hackers disabled an e-mail verification service, enabling them to transfer $465,000 from a business bank account.

All companies that handle customer data are potential targets for cyber-thieves. This includes data storage and retrieval services, IT outsourcing and facility management companies, and Software as a Service (SaaS) vendors. Data security experts often remind customers that the onus is on them to assure that their vendors meet necessary security standards, including regulatory requirements for their industry. Larger, more sophisticated companies may audit key vendors, and companies of all sizes increasingly are pushing for provisions in contracts and subscription service agreements warranting the maintenance of predetermined standards. Some states now have data security laws that mandate such contractual provisions.

Beyond service providers, other categories of technology companies have exposure in the event that their product is involved in a data breach. For example, while security products (hardware or software) do not process or store data, if they fail to prevent a data breach their manufacturer could be implicated. Similarly, manufacturers of hardware involved in a security breach have the potential for liability.

Technology vendors once routinely disclaimed liability for lost or stolen data, but increasingly, purchasers of technology products and services seek to contractually limit their liabilities and to define technology vendors' responsibilities for data breaches. Because of the significant financial risk associated with poor data security and privacy, and the related regulatory requirements, considerable time, effort and expense often are expended drafting and negotiating data security and privacy terms. In some cases the vendor's potential liability dwarfs the value of the contract, creating enormous financial exposures.

Shrink-wrapped software is notorious for securities vulnerabilities, but manufacturers of these products generally enjoy immunity from liability as a result of contractual limitations in End User License Agreements. Custom developed software, however, does not typically enjoy the same protections. Since contracts for software development projects are usually negotiated, the buyer may be in the position to not only refuse the seller's limitations of liability, but also to insist on language designed to protect the buyer from the financial consequences of faulty code.

Wording developed by the State of New York to be used in software development contracts sets out performance standards as well as data security procedures to be followed by the vendor. Additionally, the New York wording calls for certification that the finished product meets all security requirements of the contract, and a warranty that it is free of "any code that does not support a necessary function of the application or that weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code." The highly-regarded SANS Institute has developed Application Security Procurement Language for the benefit of software buyers based on New York's model.

Some analysts predicted Merrick v. Savvis would open the floodgates for lawsuits targeting Qualified Security Assessors (QSAs) and other data security consultants. That has not been the case, in part because many of the liability issues raised by the case remain unresolved. Nonetheless, security assessors remain obvious targets if a client experiences a data breach. One of the key issues raised by the case is the responsibility of security assessors to third parties that may rely on their findings.

"Proactive risk management processes and a heightened awareness of security issues can help avert suits and lessen the potential consequences if a suit occurs."

Data breach-related lawsuits against technology companies have been relatively infrequent so far, but that is no reason for complacency. Greater awareness of the potential liabilities associated with data breaches, and of the various roles technology vendors may play in system security, has led to contract wordings that make lawsuits far more likely. Additionally, new legislation such as the HITECH Act specifically addresses the responsibilities of vendors and likely will spark a rapidly increasing number of lawsuits.

This report specifically addresses data breaches, but many of the same considerations apply to other aspects of system security. Infiltration of a system by a virus that takes over or inhibits an industry process can create substantial consequential loss. While extreme scenarios describe a third party wresting control of a portion of the power grid, the potential for industrial espionage, sabotage of processes and other forms of cyber warfare present remote but potentially significant liabilities. Whether a hacker steals credit card information or crashes a system, if a technology company was involved in writing the software, implementing the system, assuring security or providing other services, they increasingly are likely to be targeted for litigation.

Risk Management Controls

Technology companies need not sit back and wait for the lawsuits to pour in. Proactive risk management processes and a heightened awareness of security issues can help avert suits and lessen the potential consequences if a suit occurs. The risk management process should incorporate the following:

- **Security is not an "add on," it should be built into the product.** The product development process should specifically address security issues. This includes a rigorous process to identify and address threats and vulnerabilities, designing software and hardware controls to address these vulnerabilities, building time in the testing process to assure the quality and effectiveness of controls and developing documentation of the efforts. Responsibility for security features of products should be clearly identified.
- **Implement contractual controls.** Vendors may be compelled to assume some level of responsibility for data breaches in contracts, but they need to fully understand their potential liabilities and should strive for wordings that limit those liabilities as much as possible. The relative responsibilities of the developer, the implementer and the user should be clearly delineated. Checks on the process should be defined in the document. Additionally, review insurance requirements to assure that they can be addressed.
- **Clearly define implementation roles and responsibilities.** Client versus vendor roles should be specified in writing, including system configuration responsibilities and the migration of data from old systems.

Software as a Service, hosting and cloud computing companies should include additional elements in their risk management process:

- **Network controls must be in place.** These include firewalls, perimeter alarms, automatic logging, encryption (storage and transmission), user verification, password management, access controls, and patch maintenance procedures (applications and operating system). These controls should be tested periodically and log reports reviewed to identify anomalies.
- **Each customer's data should be separated from those of other customers.** This can be achieved by either virtual or physical means.
- **Human controls should be implemented.** Background checks, drug tests, and the like, should be routine practices for all employees with access to sensitive data. Additionally, conduct social engineering training for practices such as the use of passwords, storage practices, and the appropriate use of mobile devices.
- **Physical security systems should be deployed.** These include alarms, guards, fire protection devices, and power/communication feeds with backup. Also, regularly inventory physical data storage devices.
- **A data retention strategy should be implemented.** Back-up and archiving processes must be standardized.

Data Breach Liability Insurance

In recent years, insurance companies have introduced a number of products to address the liability exposures of technology companies. Typical commercial general liability (CGL) and errors and omissions (E&O) policies rarely cover claims related to loss of data, privacy breaches, and the like, making specialized coverage for data breach liability necessary. Data breach coverage becomes especially critical

for technology vendors as customers increasingly insist on contractual terms that explicitly define the liability of vendors for lost or stolen data. Additionally, customers often require technology vendors to have coverage.

Insurers offer specialized property and theft (first party) coverage and liability (third party) coverage related to privacy and data security. Data breach coverages often are bundled with other cyber liability coverages such as unauthorized access or use of an insured's computer system, alteration or destruction of electronic data and denial of service attacks. Technology E&O coverage protects IT firms against certain "wrongful acts" by, or on behalf of, the company. Policy terms and conditions can vary materially among insurers, so technology companies should work closely with their insurance brokers to be certain they are getting the best protection for their specific exposures.

Deciding whether to purchase a particular coverage and then comparing alternative policies often boils down to evaluating the policy in the context of questions such as:

- Does coverage respond to "failure of your product/service" as well as "loss of your data"?
- Is a data breach event clearly defined?
- Does it cover loss of business information as well as personal information?
- Will it respond to a regulatory action as well as litigation by customers?
- Will it protect the company if the breach is caused by a "rogue" employee?
- Will it respond to an employee suit against the company (HR information)?
- How does it work in conjunction with your E & O and GL policies?

The answers to these questions will help to decide whether the policy responds to an organization's needs, or whether the coverage contains gaps that need to be addressed with the underwriter.

Zurich

1400 American Lane, Schaumburg, Illinois 60196-1056
800 382 2150 www.zurichna.com

(10/10) 10-3289

Zurich HelpPoint

Here to help your world.

ZURICH®

Because change happenz®