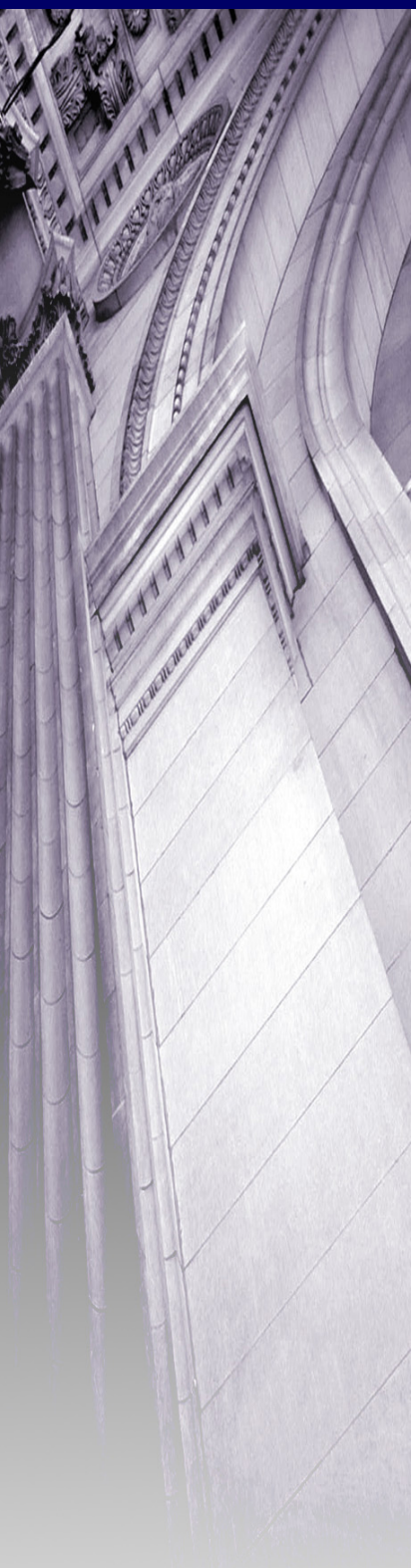


Information Security:
Meeting Today's Challenges

Sponsored by Websense

1. Introduction

1.1 The Complexity of Information Security

A 2007 survey found that the vast majority of organizations felt no better prepared to tackle information security than they did a year earlier.[1] This, following a year when organizations spent millions of dollars on improving security; new laws and regulations were created; and information security took center stage on an unprecedented level. Unsurprisingly, given the growing complexity of the legal and regulatory landscape for information security, the same survey found that companies listed "the complexity of security" as their number one challenge.

Information security today is indeed a complex challenge. Organizations must balance the cost of protecting information against the value of the information, while complying with hundreds (if not thousands) of laws, regulations, standards, and best practices that dictate information management techniques and technologies.

1.2 The True Cost of Information InSecurity

Since 2002, nearly 40 states have now passed some form of data breach notification law, and most of the rest are considering the same. These laws require organizations to notify consumers in certain cases where the organization knows or suspects that personal information was exposed through a security breach. Why the rush to create these laws?

> *"The Veterans Affairs Department has set aside more than $20 million to respond to its latest data breach . . [It] designated that much because the breach potentially puts the identities of nearly a million physicians and VA patients at risk . . ."*
>
> ***"VA sets aside $20 million to handle latest data breach," Government Executive.com***[2]

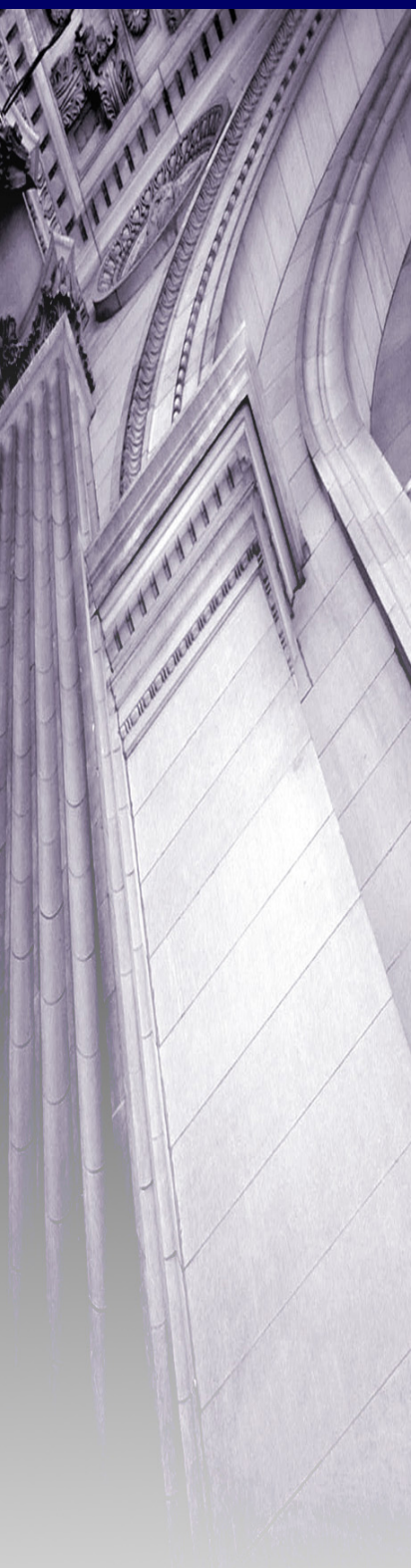
In 2006, consumer records containing personal information were exposed at a rate of 6 million per month. It is estimated that almost 2 billion personal records have been exposed by organizations in the US over the past 25 years. Furthermore, the number of reported incidents in 2005 and 2006 was greater than the previous quarter century combined. What is the cost of these information security lapses? A 2006 study found that retailers lost $2 billion because of consumer fears about the security of information.

August 2007

WHERE LAW & TECHNOLOGY MEET

KAHN CONSULTING INC.

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM



Are the years of headlines about lost data, hacked websites, misplaced laptops, credit card theft, exposed medical records, and so on having an affect? The answer is clearly yes.

This is one way to quantify the cost of information insecurity, but what is the true cost to an organization? What is the cost of dealing with the bad publicity; the impact on market valuations; replacing fired employees; lost productivity; restoring the trust of partners and suppliers; and cleaning up the mess? One study places the cost of data breaches at $182 per record, including direct costs, opportunity costs, and productivity costs. Another study places the cost at $90 to $350 per record.

1.3 The Benefits of Getting it Right

"Industry leaders are spending almost 50 percent more on IT security than are the laggards. For this increase in spending on IT security, the compliance leaders are experiencing 1750 percent fewer 'significant and material' deficiencies than the industry laggards."

"Improving IT Compliance," Security Compliance Council[8]

It is short-sighted to consider only the cost of information security *failure*. What about the *benefits* of getting it *right*? Today's leading organizations invest in information security and expect returns that offer business value and positively impact the bottom line; over the long term. Failing to comply with laws and regulations is not an option, but organizations benefit most when they use compliance requirements as a foundation, or jumping-off point, for building information security programs that protect and leverage the value of information assets, while offering competitive advantage.

For example, how can a bank offer its customers access to their account information anytime, anywhere, unless it has invested in tools, technologies and processes that protect that information as it flows from the enterprise to the consumer and back? Similarly, how can a manufacturer expose critical data to suppliers in real time unless it has done its information security and compliance homework? How does a technology company share its intellectual property with a business partner if it has not invested in the security technologies that will protect that asset and control access to it? A fortress mentality for data security is difficult to justify in today's networked business world.

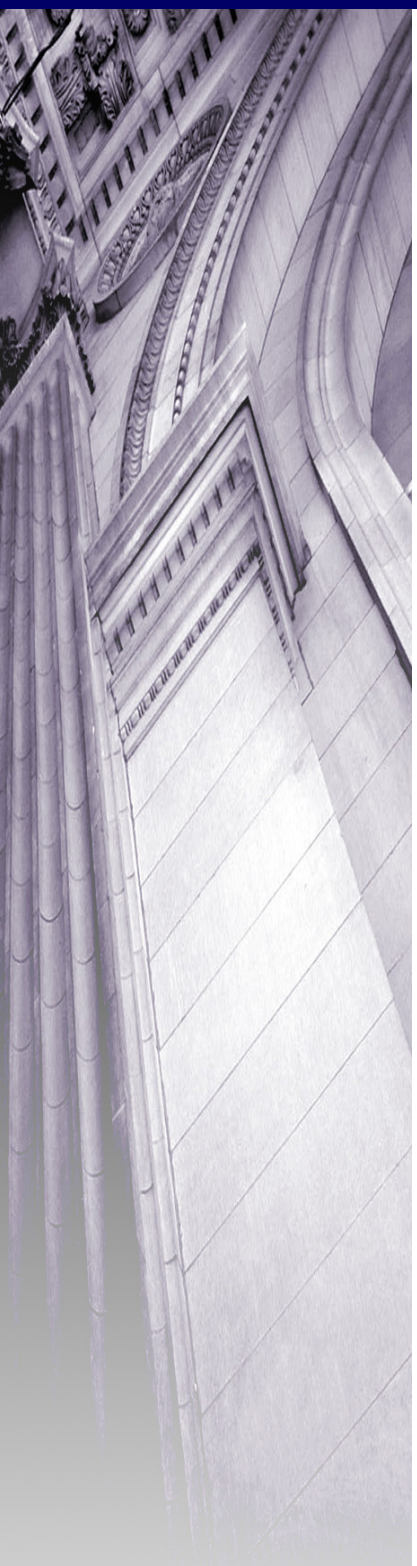
However, not every organization gets it right. In fact, a recent study found that that 60% of data breach incidents are caused by organizational mismanagement. Another survey found that 63% of companies surveyed believe they "cannot prevent a data breach," citing a lack of resources and internal governance processes as among the factors contributing to this inability. These numbers tells us that some organizations are their own worst enemies when it comes to information security.

1.3 The Benefits of Getting it Right

The reality today is that organizations have the mandate, the motivation, the information, and the tools to get information security right. This paper presents a series of industry-focused case studies designed to help organization understand what can go wrong, and how to get it right.

"You need to know where your data resides and who has access to it. This speaks to the integrity of the data that resides in your databases, the data that you use to carry out your business."

Director of US Homeland Security National Cyber Security Division[10]



The intent of these case studies is not to call attention to or embarrass any particular industry or organization, but rather to use the lessons of the past to help organizations succeed with information security today and into the future.

2. Information Security in the Financial Services Industry

"The payment-processing concern may have put the personal information of as many as 40 million consumers at risk . . . there is going to be a flood of lawsuits by both consumers and businesses."

"Security Breaches Of Customers' Data Trigger Lawsuits," Wall Street Journal[11]

2.1 Overview

Perhaps more than any other, the financial services industry has been in the information security spotlight for many years. As possessors of some of the most valuable information about consumers and businesses alike, the industry has long invested heavily in information security and compliance. Laws like the Gramm-Leach-Bliley Act (GLB) and its implementing regulations,[12] provide detailed requirements for the financial services industry regarding the way it must manage and protect customer information.

The stakes of security breaches in financial services continue to rise - both for organizations and individuals. It was recently reported, for example, that credit card numbers stolen via an email phishing scam in New Jersey were used by UK-based terrorists to finance their activities across the globe.[13]

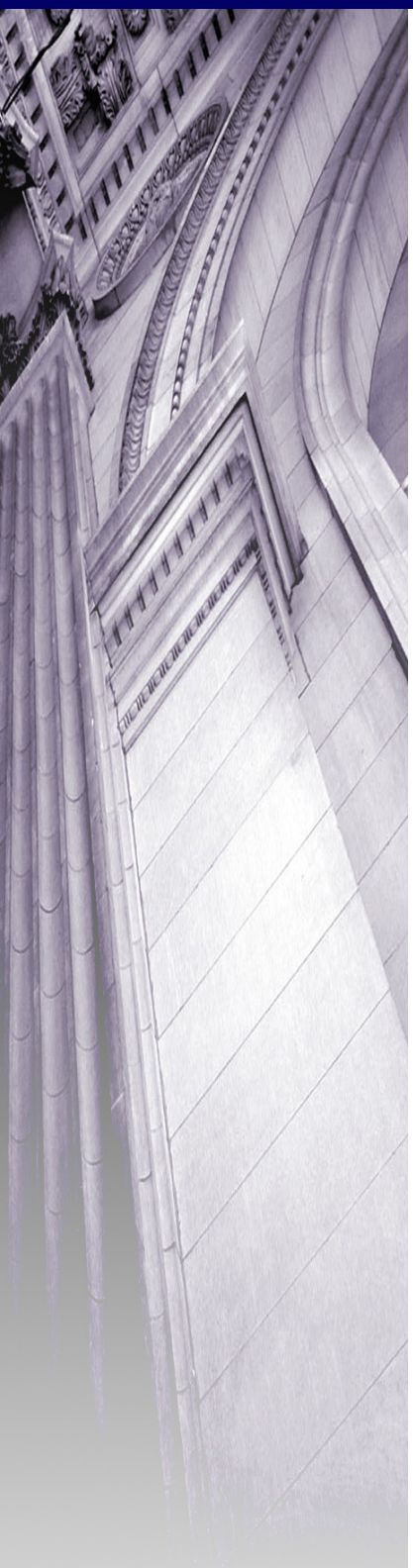
2.2 Defend Against Attacks By Trusted Insiders

A recent survey of senior information security professionals found that attacks by trusted insiders was cited as their most serious concern. Moreover, a majority of these professionals stated that they "do not believe that they have taken adequate measures to protect against 'data loss.'"[14]

Their concern may be justified. Unites States v. Shea[15] describes a case where a debt collection company discovered that its primary customer database had been corrupted by a disgruntled employee. The employee had placed a foreign program on its system that was coded to replace debt principal amounts with random numbers, switch client identification numbers and eliminate the Social Security numbers tied to each account. The program was coded to modify 5,000 records at a time and to repeat after each batch. The corrupted data was retrieved over a period of months with the help of the software manufacturer, costing thousands of dollars in consulting fees.

In another case, a computer software consultant stole personal information regarding 110,000 customers of an insurance company while he was there developing business software. He was caught when he tried to sell the information to an undercover law enforcement agent, and sentenced to five years in prison.[16]

A recent study by the US Secret Service found that most insider attacks are planned well in advance.[17] While the premeditated nature of insider attacks may make them more sophisticated,



it also increases the opportunity for organizations to detect and prevent such attacks using the right technology and techniques.

There are many steps that financial services firms can take to prevent insider attacks, including:

- Employ tools and techniques that are engineered to detect malicious activities both inside and outside the enterprise.
- Carefully design hiring programs to ensure that the right employees are hired in the first place, and that they have backgrounds and qualifications appropriate for their job.
- Create and enforce access controls that ensure employees only have access to the information they need to do their jobs.

2.3 Protect the Crown Jewels

In early 2006, the US Federal Trade Commission brought a case against a credit card processing company involved in what it called "the largest known compromise of financial data to date."[18] Throughout the course of the case, it was discovered that the sensitive information of tens of millions of consumers had not been adequately protected, resulting in "millions of dollars in fraudulent purchases."

In examining the company's approach to information security, the FTC found that the company:

- Stored unnecessary information, thereby increasing the risk of it being lost or stolen
- Had not performed vulnerability tests
- Did not implement strong passwords
- Did not implement readily-available technologies for protecting information or mandate the use of sufficiently strong passwords
- Did not have the ability to detect unauthorized access to information

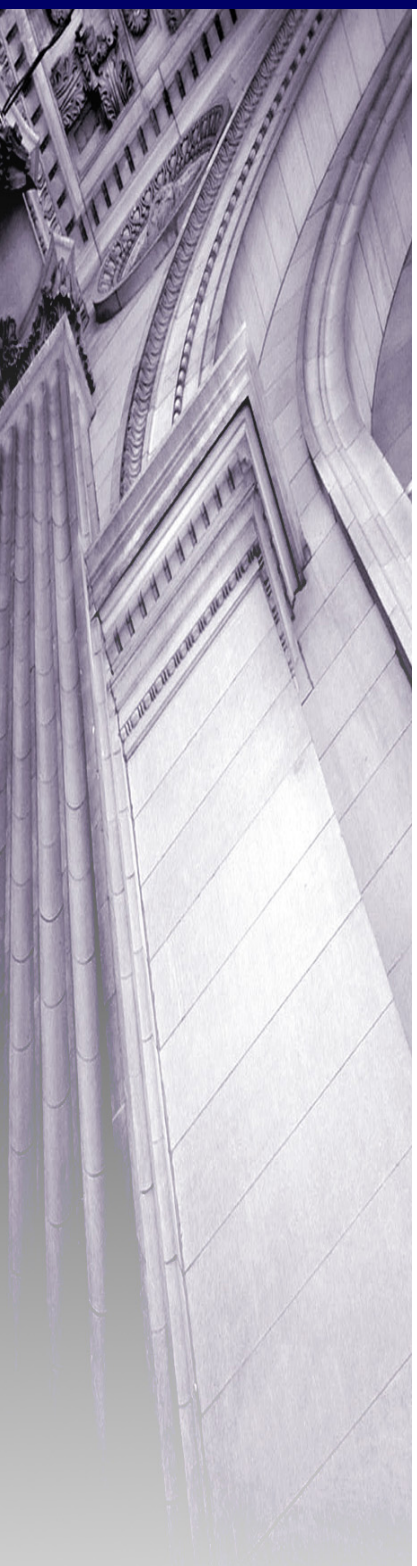
As part of the company's settlement with the FTC, it agreed to obtain an audit of its information security program every two years for 20 years.

This case illustrates the consequences that organizations can face when they fail to protect their data "crown jewels." The fact that this was the ninth such case that the FTC had brought at the time illustrates that this company was far from the only financial services firm with similar problems. Furthermore, this case demonstrates that even the most sophisticated institutions can overlook basic information security best practices.

3. Information Security in the Retail Industry

"Retailers lost almost $2 billion because of consumer security fears, with about one-half of those losses ($913 million) coming from people who avoided sites that seemed to be less secure and the rest (about $1 billion) came from consumers who were too afraid to conduct e-commerce business at all . . ."

"Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears"[19]



3.1 Overview

The dominance of electronic payment systems and the emergence of customer data warehouses have changed the face of retail. Today, retailers manage some of the largest databases in the world, allowing them to serve their markets more efficiently. At the same time, this has placed retailers in much the same position as financial services institutions – holders of massive volumes of financial and other data about their customers. In order for retailers to successfully leverage this data to serve their customers, they must properly manage and protect it. Retailers who get information security right build trust with their customers, which increases profitability. Those who get information security wrong pay the price.

3.2 Manage the Total Security Environment

To understand the critical role of information security in the retail industry, one needs to look no further than the Form 10-K for a major international retailer, filed with the SEC after the retailer had experienced one of the most extensive and publicized breaches of information security in history.

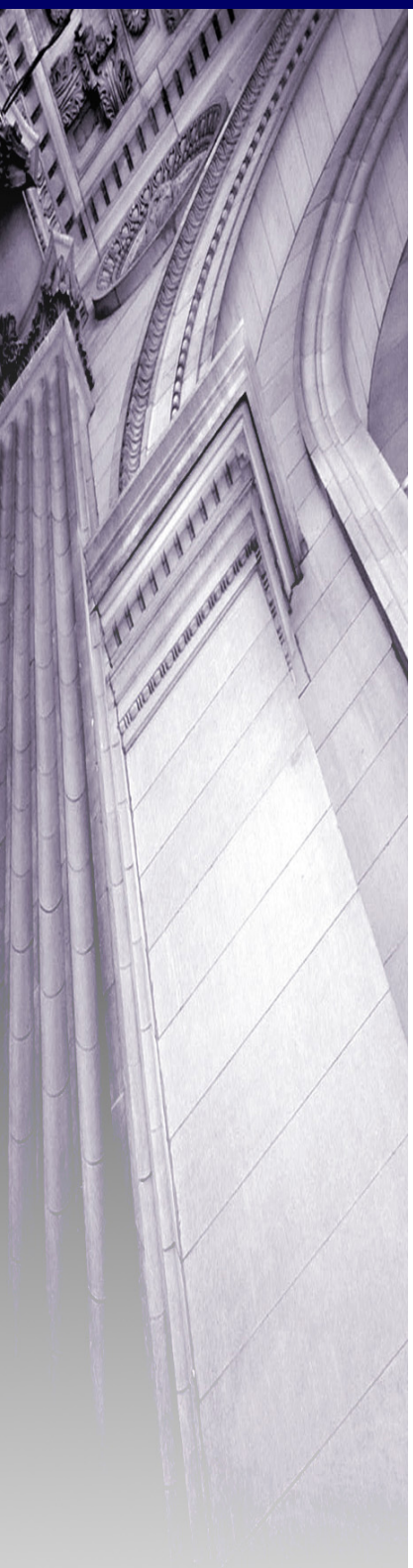
The document includes a ten-page section that details a two-year long saga of information security misadventures involving hacking, Internet worms, and encryption that the company estimates will cost it at least $20 million, and others estimate may eventually cost the company $1 billion. Millions of credit and debit card records were stolen and exposed, and the company faces multiple lawsuits. In addition, the filing reveals that the company seemed to know very little about what was happening on its own networks, over a period of years:

> *"We do not know who took this action and whether there were one or more intruders involved . . . or whether there was one continuing intrusion or multiple, separate intrusions . . ."*[22]

The company's filings with the SEC and other reporting around the incident reveal several details that are instructive for other retailers:

- The intruders appeared to gain access to the retailer's encryption keys, allowing them to decrypt critical information on the retailer's systems. Encryption keys should be highly protected and stored separately (logically or physically) from the information they are designed to protect.[23]
- The intruders appeared to have essentially unfettered access to critical company systems, which allowed them to install software, send messages to one another, copy files, move files between systems (e.g., from a US database to one in the UK). It is critical to monitor all access to critical systems, and establish and enforce strict access controls.[24]
- It was reported that, "the $17.4-billion retailer's wireless network had less security than many people have on their home networks, and for 18 months the company had no idea what was going on."[25]

Overall, it seems clear that the company had no comprehensive ability to monitor nor understand what was happening on its own systems. This, coupled with some rudimentary errors in the configuration and management of its wireless networks and data transmission practices led to the "biggest known theft of credit-card numbers" in history.



3.2 Understand Vulnerabilities Before Others Do

Retailers face not only the wrath of customers and regulators when information security is weak, but also possible threats of extortion. For example, as documented in the case of Unites States v. Ray,[27] a national electronics chain faced an extortion demand of $2.5 million from an individual who claimed to be able to exploit weaknesses in the company's network to access private customer information. The individual threatened to post the customer information online if the retailer did not pay up. Instead, he was caught, prosecuted, and set to jail.

This case illustrates the point that retailer's data is not only vulnerable, but is actually a target. No information security program can perfectly anticipate all possible attacks, but retailers can learn from the experience of others. Retailers should conduct routine vulnerability assessments and make necessary improvements on a regular basis. In addition, retailers should participate in industry groups to understand the challenges that others in the industry are facing and the solutions that they are employing.

4. Information Security in the Manufacturing Industry

"He admitted that he misappropriated more than 20,000 documents from the electronic database that DuPont has in Delaware. The value is set at 400 million dollars. [He] could face 10 years in prison and be fined up to $250,000."

"Man Pleads Guilty in DuPont Data Theft Case," eWeek[28]

4.1 Overview

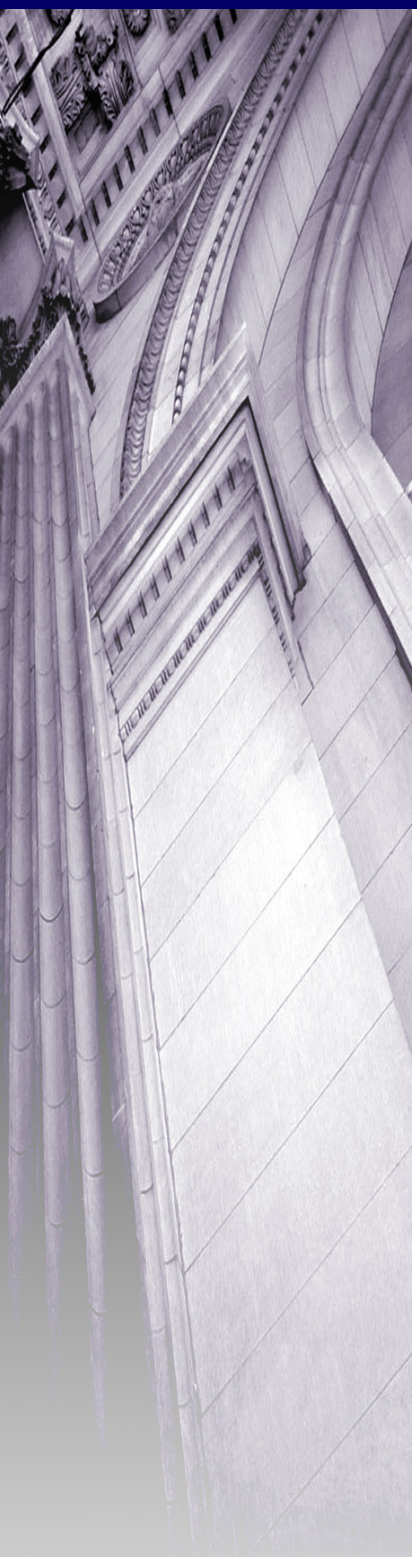
The manufacturing industry has leveraged information technology for many decades to assist in the automation and control of key processes. This history is certainly an asset but it can also present some challenges, especially when manufacturers connect systems to open networks (i.e., the Internet) that were not designed with the security needs of open networks in mind. This can be particularly challenging with industrial control systems such as SCADA (Supervisory Control and Data Acquisition) and DCS (Distributed Control Systems).

In addition, many organizations in the manufacturing sector outsource IT and help desk operations. The distributed nature of these operations and the complexity of supplier networks add security complexity that must be closely managed.

4.2 Apply Security to Key Control Systems

In 2005, an Internet worm named, "Zotob" spread rapidly across the Internet, infected several manufacturers, and impacted their control systems. Auto manufacturing plants from Illinois to Ohio were downed by the worm. Vehicle production by tens of thousands of workers ground to a halt as IT staff patched critical systems and brought them back on line. The company's suppliers were also hit with the worm, compounding the production problems.[29]

While the loss of production systems can have serious economic consequences, the consequences of losing private data, trade secrets, and other critical information can be devastating for manufacturing companies. Recently, 17, 000 employees at the world's largest drug maker had their



personal information posted on the Internet after the spouse of a company salesperson installed file sharing software on a company laptop, and the data was stolen.[30] At least one employee is suing the company.

These and other incidents in the manufacturing sector illustrate the importance of providing both inbound and outbound content protection. With highly distributed networks across global supply chains, manufactures need to invest in technologies that will secure the flow of information – both in and out of the organization.

4.3 Monitor and Enforce Access Controls

Between 2003 and 2006, a leading American airplane and aerospace manufacturer was the victim of a massive theft of hundreds of thousands of sensitive documents. It is alleged that a former employee stole 320,000 individual files and documents during this period - documents that the manufacturer estimated would have been worth between $5 and $15 billion to competitors.[31]

According to the criminal complaint in the case, the employee downloaded large amounts of information that "he ha[d] no responsibility or legitimate reason for accessing," and it is alleged that the employee "violated a company policy that limits access to areas relevant and necessary to perform work duties."[32]

This case illustrates the need for organizations to ensure that they have the ability to monitor and control access privileges. Too often organizations leave access controls to chance, especially outside the confines of structured systems that have sophisticated access control capabilities. For example, many organizations fail to control shared drives – a large and ever-growing storage location for valuable corporate information of all types. For example, Kahn Consulting recently consulted with an organization that had over 40,000 shared drive folders, with 40% of them open to anyone in the organization. Many of the folders contained confidential financial information and trade secrets.

Without the ability to monitor, track, log, and manage access controls, organizations have little hope of protecting their most valuable information.

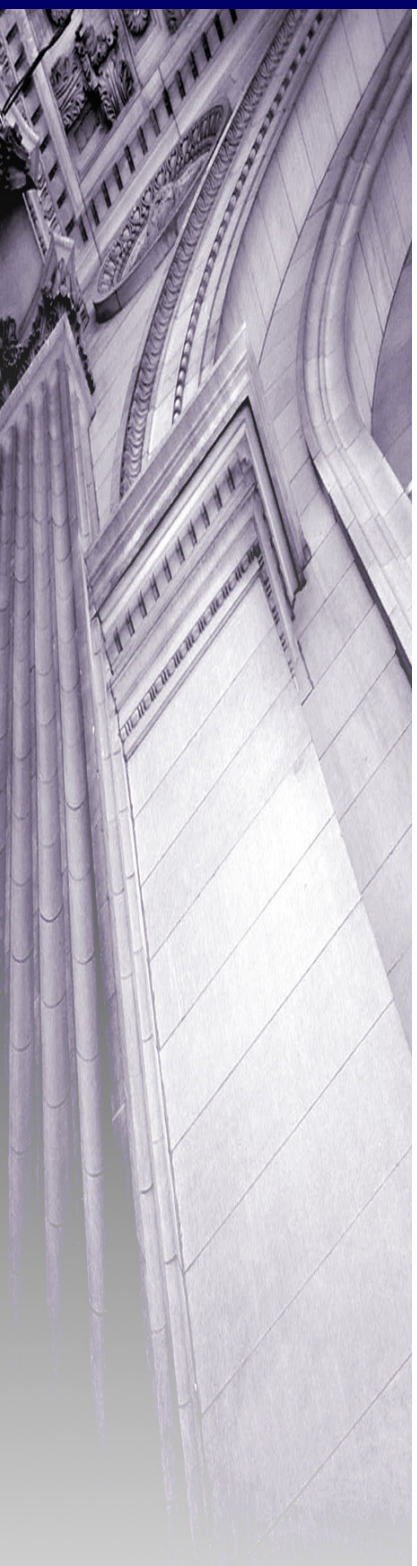
5. Information Security in the Technology Industry

"Experts say hundreds of thousands of computers each week are being added to the ranks of zombies, infected with software that makes them susceptible to remote deployment for a variety of illicit purposes . . ."

"An Army of Soulless 1's and 0's," New York Times[33]

5.1 Overview

The key assets of companies in technology industries are typically found in a form that makes them a challenge to manage - in other words, intellectual property in electronic form. But this is not the only challenge that technology companies face. Those in the information technology industry face the additional security problem of having a high number of workers that may have above-average computing skills, and as such may be more adept at circumventing security controls.



Recent surveys indicate that so-called "rogue" or "shadow" IT is a growing problem.[34] While such activities are not necessarily malicious, they should be prevented, as even the innocent action of a single employee can impact the entire organization when it comes to information security.

5.2 Protect Intellectual Property

The case of Expert Business Systems v. BI4CE, Inc.[35] illustrates the complexity that can occur in the technology industry when companies work closely together on developing intellectual property. It also illustrates the need to have procedures and tools in place to protect intellectual property throughout its lifecycle.

The case tells a story of two technology companies with complimentary technologies and markets who agreed to work together to develop a software program. At some point, the relationship soured:

> *The record shows that the relationship between the parties was, to put it delicately, unfulfilling. The record contains e-mails and other evidence indicating that plaintiff . . . regularly used very harsh language toward defendants, including frequent sarcasm and threats.*[36]

In any case, as the relationship deteriorated, the question of intellectual property emerged. The plaintiffs claimed that the defendants had installed a "remote access application on the plaintiffs' computers" thereby giving themselves "secret, unauthorized access to the entirety of [the plaintiff's] business and personal computerized records." They also claimed that the defendants had used their access to "intercept" email messages intended for the plaintiffs.

Had the companies put in place strong information security controls and technologies, the dispute perhaps could have been avoided, as the opportunity for malfeasance (or the appearance of it) could have been severely reduced.

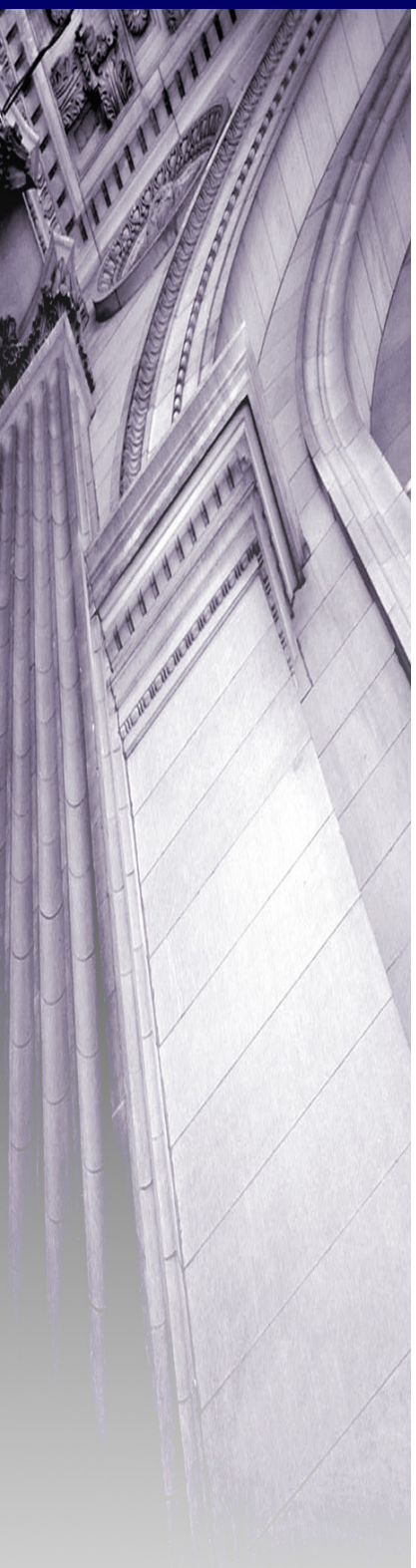
Organizations in the technology industry should ensure that intellectual property is properly protected, especially when it is shared with partners, suppliers, and other parties outside of the enterprise.

5.3 Manage Security Across All Systems

In 2007, it was revealed that a consultant working for the Los Alamos National Laboratory (funded by the federal government, but managed by a private consortium) sent classified information regarding nuclear weapons unencrypted through an open email network. The problem was further compounded when several of the email recipients (board members at the facility) forwarded the message to others.[37]

When notified of the breach, officials were dispatched across California to find and secure the computers containing the classified information. All of this came on the heels of several high-profile security problems at the facility, including one where classified data was illegally downloaded and removed from the facility on a thumb drive (an incident that has the administrators of the facility facing a potential $3 million fine).[38]

The email system is just one of many systems that even the most technology-oriented organizations might overlook when it comes to information security. It is critical that all systems, no matter how "informal" they may appear, are legitimized and brought under the information security program. This applies equally to instant messaging, text messaging, and other technologies such as peer-to-peer networks. The alternative can be devastating. For example, recently an employee at a large



drug company exposed the Social Security numbers "and other personal data" related to 17, 000 employees by installing "unauthorized file-sharing software on a company laptop provided for use at her home."[39]

6. Information Security in the US Federal Government

"A majority of federal government agencies still have significant weaknesses in their information security controls . . . as a result, the confidentiality, integrity and availability of critical information and information systems is in jeopardy government wide."

"Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk," GAO Report[40]

6.1 Overview

The federal government, as the keeper of some of the most sensitive information, has strict compliance requirements regarding information security. The federal government, unlike most commercial enterprises, has public watchdogs with mandates to regularly assess and report on the progress of federal government agencies in implementing and operating information security program. The General Accounting Office is one of these organizations, and much can be learned about information security from their examinations. Recent reports from the GAO have given many federal agencies a failing grade. Given that, it is not surprising that recent studies have found that the public's faith in the ability of government to protect their information is declining.[41]

6.2 Security and Data Integrity

"The key message to take away from my testimony last week is that agencies need to move away from mere compliance with the FISMA requirement and focus on effective security."

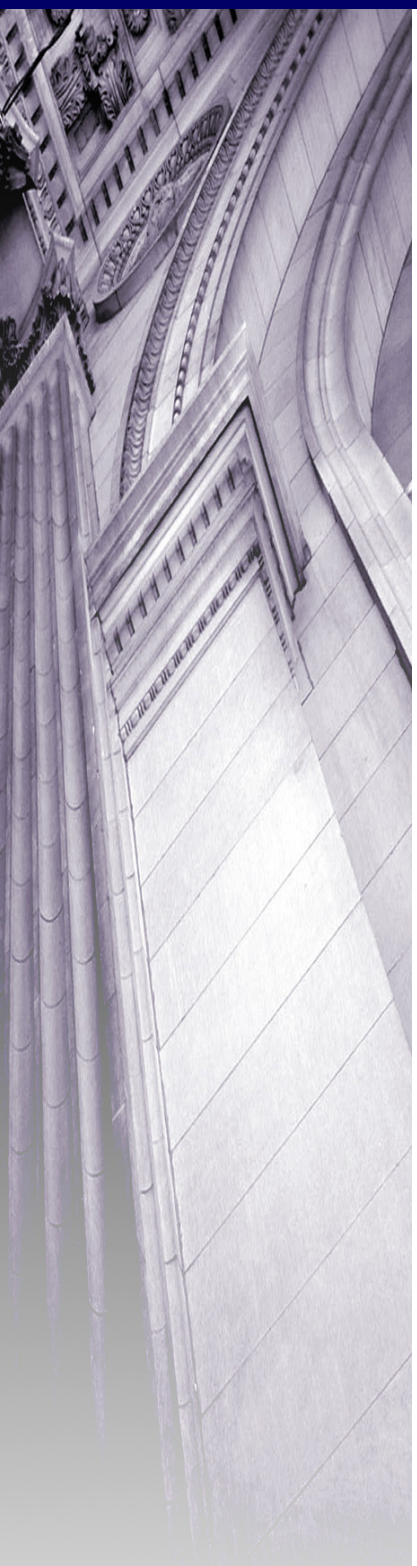
The Director of Information Security at the US Government Accountability Office[42]

Few cases involving information security - in any industry - are as dramatic as the case of Cobell v. Norton. Cobell v. Norton is a class-action lawsuit originally filed in 1996 that focuses on a dispute over funds paid (or not paid) to Native Americans by the federal government. There have been several decisions in the case, which is still ongoing.

One of the most dramatic developments occurred in 2001, when, "having been presented with extensive evidence of the lack of security for . . . data housed on or accessed by information technology systems at Interior," the court ordered the government to "immediately disconnect from the Internet all computers within the custody and control of the Department of the Interior. . ."[43]

In other words, in the courts view, the government's own information security program was so lacking that it ordered all computers housing the data in question to be immediately disconnected from the Internet. Only after the systems were deemed to be secure by an outside expert appointed by the court, were the systems allowed to be connected to the Internet.

This case illustrates a key point – that data integrity depends upon information security. In this case, where there were doubts raised about the accuracy and authenticity of records, the court



made a clear connection between the two - in fact deciding that information security was so lacking, that they only way the integrity of data could be protected was by unplugging the systems from the Internet.

7. Next Steps

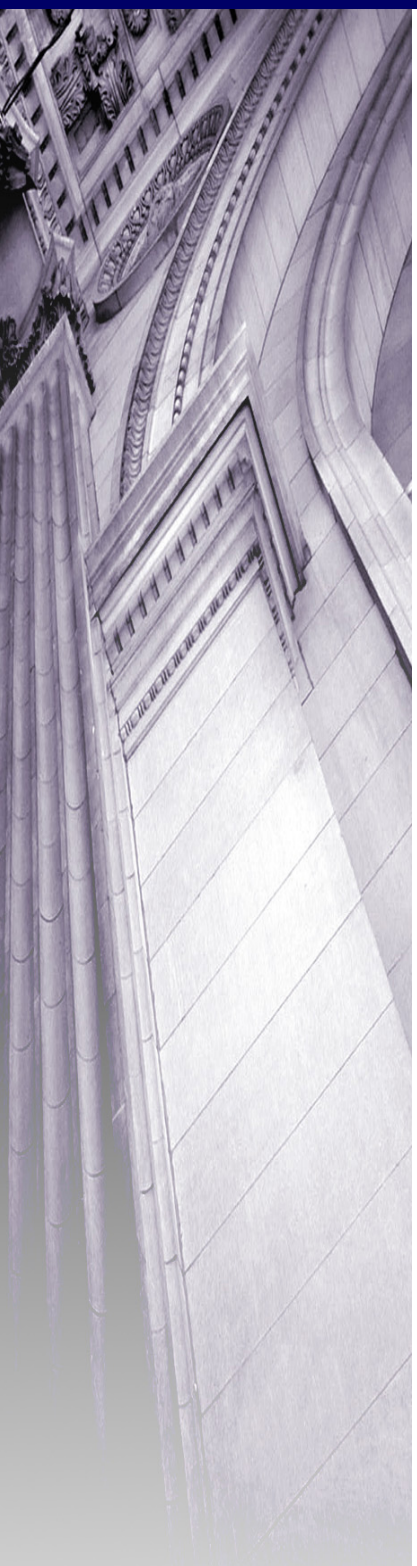
Organizations planning information security investments and building information security programs need to evaluate technologies, such as information leak protection applications, that are designed to help monitor, manage, and protect critical information. The complex reality of today's information security environment demands that organizations investigate technologies that can automate and otherwise streamline key information security activities. In addition, although the loss and theft of consumer information has attracted the most attention from the media (and perhaps, lawmakers), it is critical for organizations to realize that they must work to protect all information, throughout the enterprise.

The case studies explored in this paper highlight the capabilities that organizations should look for when evaluating such technologies:

1) Systems used to implement and monitor information security controls should be capable of detecting insider attacks.
2) Systems should support a risk-based approach to information protection that allows organizations to apply different levels of protection to different systems and types of information.
3) Information security tools should enable organizations to gain a complete, "360 degree" profile of their operational environment that allows them to identify and address weak points and correlate security events across systems.
4) Information security applications should support comprehensive vulnerability assessments.
5) Systems should support the monitoring and protection of both inbound and outbound content.
6) Systems should provide for the monitoring and management of fine-grained access controls.
7) Information security programs must address all systems used at the company – including the email, instant messaging, and other systems that might otherwise be less "managed" overall.
8) Security and data integrity go hand-in-hand, so organizations should look for solutions that that can help to ensure the accuracy and integrity of data, wherever it resides.

Given the current environment, it seems likely that organizations will face greater compliance pressures in the coming months and years than ever before. A federal data breach statute has been discussed by lawmakers for some time, but it is difficult to predict the impact of such a law should it come to pass. At the same time, increasing sophistication regarding information security on the part of those initiating and prosecuting lawsuits may put more pressure on companies to explain and justify their information security programs (or lack thereof).

In any case, all organizations, regardless of their industry, need to act today to get their information security house in order. As the case studies in this paper have demonstrated, information security is about more than just protecting information; it is about protecting the organization itself.



8. Endnotes

[1] InformationWeek Research's 10th annual Global Information Security Survey, quoted by, Greenemeier, Larry, "IT Security: The Data Theft Time Bomb," InformationWeek, July 14, 2007. Online at, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201001203

[2] Pulliam, Daniel, "VA sets aside $20 million to handle latest data breach," Government Executive.com, June 14, 2007. Online at, http://www.govexec.com/story_page.cfm?articleid=37191&dcn=todaysnews

[3] Government Accounting Office, "Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, June 2007.

[4] Erickson, Kris, and Philip N. Howard. "A Case of Mistaken Identity? News Accounts of Hacker and Organizational Responsibility for Compromised Digital Records, 1980–2006." Journal of Computer Mediated Communication 12, no. 4 (2007).

[5] Schuman, Evan, "Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears," Ziff Davis Internet, November 27, 2006.

[6] Poneman Institute, "2006 Annual Study: Cost of a Data Breach. Understanding Financial Impact, Customer Turnover, and Preventative Solutions," 2006.

[7] Kerber, Ross, "Analysts: TJX case may cost over $1b," By Ross Kerber, Boston Globe, April 12, 2007.

[8] Security Compliance Council, "Improving IT Compliance: 2006 IT Compliance Benchmark Report," 2006. Online at, http://www.securitycompliance.com

[9] Poneman Institute, "Ponemon Institute Study Shows Lack of Accountability, Resources at Root of U.S. Corporate Data Loss Problem," August 28, 2006.

[10] As quoted by, Greenemeier, Larry, "IT Security: The Data Theft Time Bomb," InformationWeek, July 14, 2007. Online at, http://www.informationweek.com/shared/printableArticle.jhtml?articleID=201001203

[11] Bank, David, "Security Breaches Of Customers' Data Trigger Lawsuits," The Wall Street Journal, July 21, 2005; Page B1

[12] Including, for example, the GLB Security Breach Notification Rule; GLB Security Regulations; and the FTC Safeguards Rule.

[13] Krebs, Brian, "Three Worked the Web to Help Terrorists," Washington Post, July 6, 2007. Online at, http://www.washingtonpost.com/wp-dyn/content/article/2007/07/05/AR2007070501945_pf.html

[14] Poneman Institute, LLC, "Database Security 2007: Threats and Priorities within IT Database Infrastructure," June 4, 2007.

[15] United States v. Shea, 2007 U.S. App. LEXIS 16388 (9th Cir. 2007).

[16] US Attorney for the Middle District of Tennessee, Press Release, July 9, 2007. Online at, http://www.usdoj.gov/usao/tnm/press_releases/2007/7_9_07.html

[17] Gaudin, Sharon, "Study Highlights Insider Threats," InformaitonWeek, August 25, 2006. Online at, http://www.informationweek.com/showArticle.jhtml?articleID=192300421

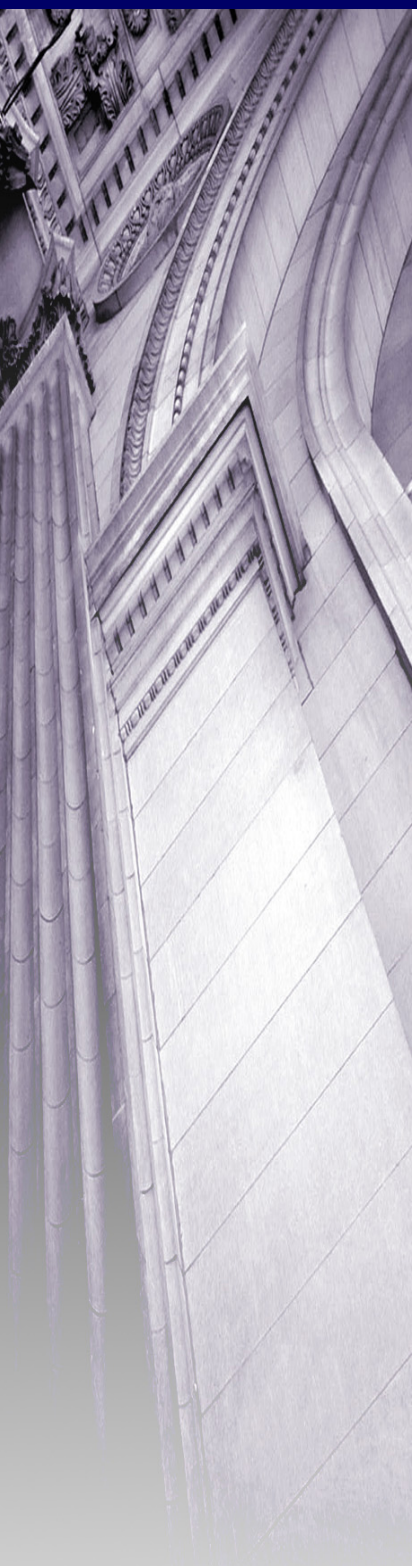
[18] Federal Trade Commission, "CardSystems Solutions Settles FTC Charges," FTC Press Release, February 23, 2006,

[19] Schuman, Evan, "Gartner: $2 Billion in E-Commerce Sales Lost Because of Security Fears," Ziff Davis Internet, November 27, 2006.

[20] Greenemeier, Larry, "Customers On T.J. Maxx Data Breach: Some Sue, Others Spend," InformationWeek, June 8, 2007. Online at, http://www.informationweek.com/story/showArticle.jhtml?articleID=199902768

[21] Kerber, Ross, "Analysts: TJX case may cost over $1b," By Ross Kerber, Boston Globe, April 12, 2007.

[22] The TJX Companies Form 10-K, for Fiscal year ended January 27, 2007.



[23] The TJX Companies Form 10-K, for Fiscal year ended January 27, 2007.

[24] The TJX Companies Form 10-K, for Fiscal year ended January 27, 2007.

[25] Pereira, Joseph, "How Credit-Card Data Went Out Wireless Door: Biggest Known Theft Came from Retailer With Old, Weak Security," Wall Street Journal, May 4, 2007; Page A1.

[26] Pereira, Joseph, "How Credit-Card Data Went Out Wireless Door: Biggest Known Theft Came from Retailer With Old, Weak Security," Wall Street Journal, May 4, 2007; Page A1.

[27] United States v. Ray, 428 F.3d 1172 (8th Cir. 2005).

[28] Rash, Wayne, "Man Pleads Guilty in DuPont Data Theft Case," eWeek, February 15, 2007.

[29] Roberts, Paul F., "Zotob, PnP Worms Slam 13 DaimlerChrysler Plants," eWeek, August 18, 2005. Online at, http://www.eweek.com/article2/0,1895,1849914,00.asp

[30] Associated Press, "Ex-Pfizer Employee Sues for Data Breach," July 20, 2007.

[31] Gaudin, Sharon, "Boeing Employee Charged With Stealing 320,000 Sensitive Files," InformationWeek, July 11, 2007. Online at, http://www.informationweek.com/story/showArticle.jhtml?articleID=201000820&cid=RSSfeed_IWK_News

[32] Miletich, Steve, "Ex-Boeing worker accused of downloading documents and leaking to reporters," The Seattle Times, July 10, 2007. Online at, http://seattletimes.nwsource.com/html/localnews/2003783055_webboeing10m.html

[33] Labaton, Stephen, "An Army of Soulless 1's and 0's," New York Times, June 24, 2005.

[34] Jowitt, Tom, ""Shadow IT Culture' on the Rise for Businesses," Techworld, July 5, 2007. Online at, http://www.cio.com/article/122459/_Shadow_IT_Culture_on_the_Rise_for_Businesses_

[35] Expert Bus. Sys., LLC v. BI4CE, Inc., 2007 U.S. App. LEXIS 11002 (4th Cir. 2007).

[36] Expert Bus. Sys., LLC v. BI4CE, Inc., 2007 U.S. App. LEXIS 11002 (4th Cir. 2007).

[37] Baker, Deborah and Talhelm, Jennifer, "Nuclear Weapons Secrets Leaked at Los Alamos," Sci-Tech Today, June 15, 2007. Also, Davidson, Keay, "Energy Dept. acknowledges lab's e-mail security lapse," San Francisoco Chronicle, June 16, 2007. Online at, http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2007/06/16/BAGG3QGHF01.DTL

[38] Vijayan, Jaikumar, "Univ. of California hit with proposed $3M fine for Los Alamos breach," Computerworld, July 16, 2007. Online at, http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9027143&intsrc=hm_list

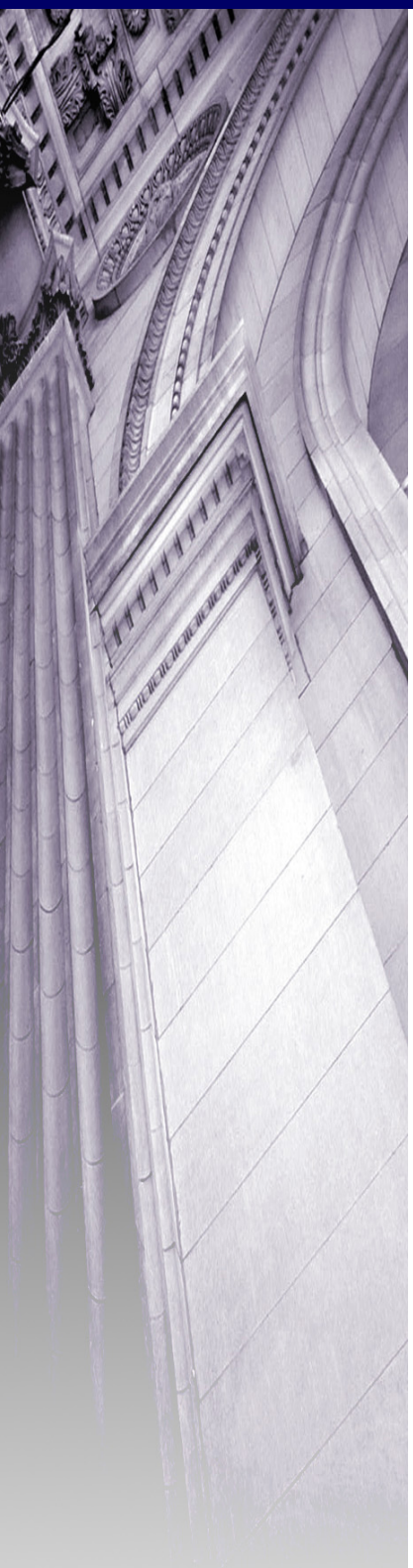
[39] Vijayan, Jaikumar, "Personal data on 17,000 Pfizer employees exposed; P2P app blamed," Computerworld, June 12, 2007. Online at, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024491&intsrc=hm_ts_head

[40] Government Accountability Office Report, "Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk," June 7, 2007.

[41] See, for example, Poneman Institute and Carnegie Mellon University, "Privacy Trust Survey," January 31, 2004, and Noyes, Andrew, "Study on privacy protections finds citizens distrust security agencies," National Journal's Technology Daily, February 20, 2007.

[42] Wilshusen, Gregory, director of information security issues at the US federal Government Accountability Office, as quoted by Jaikumar Vijayan, "Q&A: Federal info security isn't just about FISMA compliance, auditor says," Computerworld, June 14, 2007. Online at, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9024658

[43] Cobell v. Norton, Civil Action No. 96-1285 (RCL), Memorandum and Order.



9. About Kahn Consulting

Kahn Consulting, Inc. (KCI) is a consulting firm specializing in the legal, compliance, and policy issues of information technology and information lifecycle management. Through a range of services including information and records management program development; electronic records and email policy development; Information Management Compliance audits; product assessments; legal and compliance research; and education and training, KCI helps its clients address today's critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and government agencies in North America and around the world. Kahn has advised a wide range of clients, including Time Warner Cable, Ameritech/SBC Communications, the Federal Reserve Banks, International Paper, Dole Foods, Sun Life Financial, Kodak, McDonalds Corp., Hewlett-Packard, United Health Group, Prudential Financial, Motorola, Altria Group, Starbucks, Mutual of Omaha, Merck and Co., Cerner Corporation, Sony Corporation, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: www.KahnConsultingInc.com.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

www.KahnConsultingInc.com info@KahnConsultingInc.com 847-266-0722

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM