

*Managing the risk of leaking customer information requires a technological solution. Insurance cannot repair an organization's reputation nor regain customer trust.*

## Reducing the Risk of Information Leakage

ADAM NELSON AND DAVID ETUE

All organizations today are completely dependent on their digitally stored customer information. Credit card numbers, home addresses, Social Security numbers, and other personally identifiable information are essential for doing business in today's economy.

Safeguarding this information is of the utmost importance — when this information is leaked or stolen it imposes real costs on citizens (time, money, and security) and organizations (market, brand, legal, operational, and financial implications). The loss of this information through fraud or incompetence is undermining consumer faith in Internet-based commercial transactions and raising significant challenges for risk managers.

In the past few years, there has been a sharp increase in information leakage from large organizations, including commercial, government, and education institutions. (See Exhibit 1.) These events have been referred to by many names, including information loss, information leakage, extrusions, and unauthorized disclosures. According to the 2005 CSI/FBI Computer Crime and Security Survey, unauthorized access to information and theft of proprietary information showed “significant increases in average loss per respondent” as compared to previous reports.<sup>1</sup> This increase in information leakage and the negative impact associated with it have become large problems for major organizations. This risk is so great that 66 percent of information

## Exhibit 1

## Examples of Recent Information Leakage Incidents

COMPANY	DATE	# OF PEOPLE AFFECTED	AFFECTED INFORMATION	SECURITY BREACH	RESPONSE
<b>ChoicePoint</b> — compiler of consumer information	Feb. 15, 2005	About 145,000 consumers; at least 750 fraud cases are known.	Addresses, Social Security numbers, and credit reports.	Thieves posing as legitimate customers bought information.	Informed federal authorities. Will no longer sell sensitive personal information to clients other than governmental agencies, accredited corporate customers, or other businesses whose use is driven by a consumer-initiated transaction.
<b>Bank of America</b> — bank and credit-card company	Feb. 25, 2005	Holders of as many as 1.2 million federal-government charge cards.	Social Security numbers.	Computer backup tapes were lost.	Contacted federal authorities, then consumers.
<b>LexisNexis</b> — consolidator of legal and business information	Mar. 9, 2005	Initially, information for as many as 32,000 consumers; a month later, raised to about 310,000, though only 59 incidents of illegal action are known.	Social Security numbers and driver's license numbers.	Unauthorized use of customer logins and passwords occurred.	Informed federal authorities and consumers, improved security, limited customer access to personal information.
<b>Time Warner</b> — media conglomerate	May 2, 2005	About 600,000 current and former U.S. employees back to 1986.	Social Security numbers and details on beneficiaries and dependents.	Backup computer tape was lost in shipping by an outside information-storage company.	Notified those affected.
<b>Citigroup</b> — financial conglomerate	June 6, 2005	3.9 million consumer lending customers.	Social Security numbers, names, account history and loan information.	UPS confirmed it lost a package shipped by Citigroup containing computer tapes.	UPS and Citigroup launched internal investigations. Citigroup notified all 3.9 million customers.

technology (IT) security personnel surveyed in the 2004 Ernst & Young Global Information Security Survey have a high level of concern regarding a “loss of customer data privacy/confidentiality” in the next 12 months.<sup>2</sup>

### Key Drivers

There are two key technical drivers of this increase in information leakage: the conversion to digital assets and the increase in available technology “channels” to communicate information. Organizations have spent many years converting information to digital formats to make it more accessible to employees, consultants, suppliers, business partners, and customers. This digitization has provided huge gains in productivity for all parties involved, but it has also driven a significantly higher level of risk.

Before the age of digitally based intellectual property assets, various physical security controls were put in place to ensure that an organization’s information was properly protected. These controls included policies and procedures to implement access control, physical security, and anti-forgery measures. These controls still exist today, but organizations have had to adapt and expand their control measures to deal with the digitization of information. Once information is stored in an electronic format, securing and preventing unintended disclosure, either accidental or intentional, of these digital assets present significantly larger challenges.

### Digital Assets Are Harder to Protect

Digital assets have some unique and important differences that make them much more challenging to protect than their physical counterparts. Before assets were stored digitally, physical access was required to take or copy large amounts of information. In today’s networked enterprise, information can be accessed from virtually anywhere and is frequently shared in the course of commerce, situations which have increased the number of potential threats to an organization’s information. In the paper age, the asset had to be taken, which meant it could be discovered actually missing, or copies had to be made that were typically of a lower quality. In the digital age, the original is usually never removed and copies are perfect replicas of the stored information.

### Proliferation of Communication Channels Increases Risk

In addition to the increased exposure presented by the digital assets themselves, the proliferation of additional network channels has lessened organizations’ abilities to control the exposure of information. With the ubiquity of Internet-based communications, it has become increasingly simple to share digital assets via a variety of technologies.

---

*Once information is stored in an electronic format, securing and preventing unintended disclosure of these digital assets present significantly challenges.*

---

E-mail systems were the first widespread mechanism for interorganizational communication and remain the most popular. Most people have more than one account and often as many as five. As recently as five years ago, e-mail was the primary method for exchanging information electronically. Today, the addition of channels such as instant messaging, Webmail, peer-to-peer networks, and other real-time communication channels greatly increases the risk of disclosure of sensitive or confidential information. These additional channels create additional points from which information can leak and, when unmanaged, greatly increase the risk of unintended disclosure of information.

### Internal Nontechnical Factors Also Pose a Threat

However, companies today are also dealing with a nontechnical driver — the internal threat. The Gartner Group estimates that “70 percent of security incidents that actually cause loss to enterprises — rather than mere annoyance — involve insiders.”<sup>3</sup> Requirements for productivity gains have made employees work harder and longer. Outsourcing and globalization have eliminated jobs. All of these factors greatly increase the chance that a disgruntled employee or contractor could be motivated to disclose information. To make matters worse, a black market

for information such as credit card and financial account information has evolved. This makes it easier for a dishonest employee, contractor, or third party to turn raw data into a financial profit.

As technology continues to evolve and organizations rely on it more and more to accomplish their mission, the likelihood of information leakage and the negative impact that accompanies such leakage has increased greatly.

## Regulatory Impact

In response to these threats, government bodies in the United States and Europe continue to implement comprehensive regulations to ensure the privacy and integrity of corporate, financial, and personally identifiable information. In addition, private associations and other groups have recommended and encouraged organizations to implement information privacy processes and technologies.

---

*Any legislation or regulation that results from Congress' deliberations will significantly affect the way organizations and their customers address information privacy.*

---

The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach Bliley Act (GLBA), California SB 1386 and AB 1950, and the industry-based Payment Card Industry (PCI) Security Standard are examples of these regulations. It is estimated that at least 22 states will have adopted some type of information privacy or security law by mid 2006. Absent federal legislation, this number is only expected to grow.

The Federal Trade Commission (FTC) takes enforcement of the regulations very seriously. Recent enforcement actions against violators, including ChoicePoint, DSW, and BJ's Wholesale Club, have resulted in fines and/or requirements to establish

comprehensive information security programs. The requirement to obtain audits of the program by independent third parties for up to 20 years has also been imposed.

In addition to SB 1386, California enacted another significant piece of legislation, AB 1950. This legislation requires specified businesses to use data safeguards to ensure the security of Californians' personal information, which California defines as name plus Social Security number, driver's license or state ID number, or financial account number, and to contractually require third parties to do the same. However, this bill does not apply to businesses that are subject to other information security laws, such as the federal financial and medical information security rules.

Given that it covers any company with information on a California resident, SB 1386 has been called "a de facto national information privacy law." But that's a misnomer. SB 1386's provisions differ from those of other state laws. As a result, large organizations must tailor their processes and procedures to not only SB 1386 but also other, different state laws. For example, a health insurance company that accepts credit card payments could be required to comply with the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act of 1996, up to 22 state privacy laws, and the Payment Card Industry Security Standard.

The U.S. Congress is now proposing to address information privacy in a comprehensive manner. Passage of federal legislation is uncertain. But any legislation or regulation that results from Congress' deliberations will significantly affect the way organizations and their customers address information privacy. Not only will this have an impact, in a fundamental way, on how information is handled in an organization, but it will also influence how technological solutions are developed to effectively manage risk and ensure compliance.

## Managing the Risk

According to the Risk and Insurance Management Society's glossary, risk "is the possibility of loss or exposure to loss." Risk equals the likelihood of a given threat taking advantage of a particular vulnerability to accomplish a particular goal — in this case, disclosure or leakage of sensitive or confidential information.

This equation simply measures the presence of risk and not the resulting impact of that adverse event on the organization, which is often measured by expected value and probability metrics.

Most organizations strive either to maintain a fixed expected value from a risk or to lower the expected value over time. The rise in vulnerabilities from the technical and social drivers has greatly increased the expected value of information leakage risk, forcing the organization to make a decision on how to handle this leap.

There are four options for managing a risk:

1. accept the risk;
2. transfer the risk to a third party;
3. mitigate the risk; or
4. avoid the risk altogether.

If you look at the information leakage risk, you unfortunately find that two of these are not reliable options. It is difficult to transfer this risk. Insurance is the typical method used to transfer risk. While a few providers write policies to insure against information loss, the market is still underdeveloped. Avoiding the risk is also not an option. This risk is unlike the risk of skydiving, where you can choose not to pursue the activity. Your employees (and many contractors, customers, suppliers, and business partners) require access to information for your organization to function. Avoiding the risk would require ceasing operations and, therefore, is also not an option.

This leaves the organization with two viable options: accept the increased risk delivered by these additional unmanaged communication channels; or take action to mitigate the risk through the implementation of process changes, technology, or a combination of the two.

### **Risk Mitigation Options**

If an organization decides this risk must be mitigated, it has a variety of options. It is important to segment the focus into two areas — “data at rest,” which is information stored on computer hard drives and tapes, and “data in transit,” which is data flowing across a computer network.

### *Data at Rest*

Data at rest can be protected with traditional IT security controls and are typically addressed with access control and encryption. Encryption protects the information if the hard drive is accessed outside of a specific application, if the data are stolen, or if a backup tape is lost during transportation to offsite storage (as has happened multiple times in the past year). Access control permits only authorized users to view the information. However, it is important to note neither option does anything to protect the information when it is accessed by a legitimate user — or someone impersonating one.

---

*Solutions provide content-based analysis to monitor the outbound network traffic and identify whether the content leaving is compliant with organizational policies.*

---

### *Data in Transit*

Data in transit requires a different approach from the traditional IT security controls used to mitigate technology-based threats. Traditional IT security approaches have allowed or disallowed technologies to access data but have done nothing to control the content flowing through allowed technologies. For example, suppose users are allowed to use e-mail, http(s) (hypertext transfer protocol), instant messaging, and FTP (file transfer protocol) but are not allowed to use peer-to-peer technologies. If a user has access to a piece of information, he or she can send it via any of the approved channels regardless of organizational policies regarding the content. Therefore, the traditional data in transit controls do not prevent a threat agent from using an allowed technology for unauthorized purposes.

### **A Technological Solution is Needed**

In order to prevent the unauthorized use of approved channels, an approach fundamentally different from traditional security tools is needed.

### Inspection and Analysis

One solution is to find a technology that actually inspects the content flowing across channels and analyzes it based on its content rather than its technical attributes. This is a significant challenge, as information on a computer network is typically spread over a variety of “packages” called packets — and the solution must actually inspect and correlate the contents of each packet. The need to solve this problem has created a new market of IT security solutions. However, the industry has not yet agreed on a common name for these systems. Names currently in use include extrusion detection and prevention systems, content monitoring and filtering, and egress-point security. Regardless of the name, all of these solutions were developed to provide content-based analysis to monitor the outbound network traffic and identify whether the content leaving is compliant with organizational policies.

### Encryption

Encryption is also a useful tool for data in transit, but its use needs to be controlled. Providing users with encryption capabilities can have two very different consequences, one positive and one negative. On the positive side, encryption enables an organization to apply more security to information sets that require it. For example, a positive use would be encrypting the network traffic containing insurance files between a health-care organization and an insurer in order to prevent the information from being seen when it is crossing the Internet. On the negative side, that same encryption could be used by a rogue insider to subvert content controls in order to send customers’ financial account information to the insider’s home computer, from whence the insider could sell it on the black market. It is important to consider solutions that provide feedback as to how encryption is being used in the organization.

### Mitigation Requires Identification and Prevention

It is important to note that a solution that merely reports on information loss does not actually mitigate risk. Risk mitigation requires more than simply reporting on the state of the organizations’ compliance position. It requires preventing the loss altogether.

### Conclusion

Enterprises face an increasingly complex array of

regulations governing how they use and store digital information. These regulations, along with potential negative impacts on brand and customer trust, greatly raise the impact of information leakage to an organization’s reputation and financial bottom-line. Managing this risk is quickly taking its place among the top concerns of risk managers and corporate officers. While insurance will play a role in comprehensive risk management solutions, that role will necessarily be a small one. Insurance cannot repair an organization’s reputation nor regain customer trust. The solution lies in preventing information leakage. That translates into process changes as well as the deployment of new technologies. IT managers do not view solutions in terms of risk reduction. However, risk managers in consultation with the IT department can and should take the lead in introducing information leakage risk reduction strategies to their organizations.

### Endnotes

1. Gordon, Lawrence A., Martin P. Loeb, William Lucyshyn, and Robert Richardson, *2005 CSI/FBI Computer Crime and Security Survey*. Available at [www.usdoj.gov/criminal/cyber-crime/FBI2005.pdf](http://www.usdoj.gov/criminal/cyber-crime/FBI2005.pdf).
2. Ernst and Young, *Global Information Security Survey (2004)*. Available at [www.ey.com/.../file/2004\\_Global\\_Information\\_Security\\_Survey\\_2004.pdf](http://www.ey.com/.../file/2004_Global_Information_Security_Survey_2004.pdf).
3. Pescatore, John, “High-Profile Thefts Show Insiders Do the Most Damage,” GartnerResearch, [www.gartner.com](http://www.gartner.com) (November 26, 2002).

---

Adam Nelson, Esq., is an attorney and security and privacy consultant living in Chicago, IL. Nelson was a senior consultant in the security and privacy practice of IBM Global Services. He can be reached at [acnels@gmail.com](mailto:acnels@gmail.com).

---

David Etue, senior security strategist and director of marketing at Fidelis Security Systems, brings a deep understanding of information and network security industry trends needed to protect digital assets through extrusion prevention. Prior to working with Fidelis Security Systems, Etue was manager of information security at General Electric. He can be reached at [david.etue@fidelissecurity.com](mailto:david.etue@fidelissecurity.com).

---

Founded in 2002, Fidelis Security Systems is a privately held company headquartered in Bethesda, MD. Fidelis provides a network security solution that prevents the unauthorized network transfer of critical or sensitive information at gigabit speed.