Preventing Information Leaks

By Aaron Weller, Protiviti Associate Director

July 30, 2007

There is a good chance that some of your organization's sensitive information is likely to have leaked into the outside world by the time you finish reading this article. Should that concern you? Can you identify the information that is important to your organization? If so, are appropriate controls in place to protect it?

To put these questions in context, an organization needs to understand the value of its information to external parties and the damage that it would suffer from a leak. Understanding the potential impact can help determine how much should be spent to manage the risks.

The good news is that most leaks are unintentional. This is a positive note because deliberate leaks are harder to prevent than accidental ones. Deliberate leaks tend to be either for personal benefit (e.g. stealing IP, insider information) or for perceived public benefit (e.g. "whistle blowing," or political leaks). By their nature, these leaks are made by people with legitimate access to information that often go to considerable lengths to cover their tracks. The opportunity for deliberate leaks to occur can be somewhat reduced by restricting access to sensitive information; however, there are always legitimate needs for access so this risk will always exist at some level.

A much more common occurrence is when information is leaked unintentionally, for example when someone loses a laptop (something that happened over 300,000 times in the U.S. last year). Suddenly, some aspect of internal operations, or competitive advantage, has the potential to become widely known, or sensitive customer information or financial information may be exposed to identity thieves or other criminals. Unintentional leaks can be significantly reduced through techniques such as increasing awareness of the consequences among your staff and putting in place monitoring capabilities. These topics are covered in more detail later in this article.

To disclose, or not to disclose. When is it a legal requirement?

For leaks of certain types of personal information, an organization may be required to report this to anyone who is affected, although this depends on which state the affected people live in. The first law of this kind in the U.S. was California's SB-1386, which was passed in 2002 and has been law since 2003. Many other states have since passed similar bills. SB-1386 requires individuals to be notified if there is a breach of certain types of sensitive information, including social security numbers in combination with other information.

Additionally, on January 1, 2005, California legislation AB 1950 went into effect, which requires businesses to protect certain "personal information." This extends the items covered by SB-1386 and includes medical information and other data types. There are also laws relating to the protection of educational records (FERPA), financial information (GLBA), and health information (HIPAA) among others.

© 2007 Protiviti Inc. All rights reserved. An Equal Opportunity Employer

When information breaches occur, companies may be held liable; however, criminal liability is rarely, if ever, incurred. Breaches are viewed as breaches of contract, not as felonies, which result in civil actions rather than criminal ones.

Gross negligence has not yet emerged as an issue, though it may as more incidents occur and the public demands action be taken. In one incident earlier this year, a company lost records containing 45 million credit card numbers, some of them connected to transactions dating back a number of years. Many of the credit cards had since expired, limiting the potential damage but raising the question: why was the company storing information it obviously no longer needed, all in one place? As more cases occur, it may be seen that certain steps are needed to show that due care is being exercised.

Determining fault and liability is not always straightforward, especially if legal actions are used as guidance. This often is the case in the United States, which does not have the same stringent privacy rights as Europe, with its EU Privacy Directive. Instead, the United States has individual acts focused on specific types of data—HIPAA focuses on medical data, for example—with no presumption of privacy across all types of data. There have been civil cases involving class action suits; however, it remains hard for individuals to obtain a reasonable remedy regarding lost credit card data—apart from being offered free credit protection, reimbursement for bank charges, and a new credit card(s).

Plugging the leak – Some initial steps

What are best practices for stopping leaks, and how much effort should organizations take in this regard?

The first step to understanding how to control your information, and to stop leakage, is to identify sensitive information, ensure that it exists only in the places you think it should, and only those with a legitimate need to access it can do so. To do this effectively requires an in-depth review of your business. Who creates sensitive information? When do you receive it from others? Where is it stored, used and transported? Who should have access to it, and who should not?

What needs to be protected?

Many types of data are potentially valuable to criminals or other parties that should not have access to them. Some data is inherently valuable, such as bank records, and some can be leveraged to generate value, such as obtain false ID, perform identity theft or facilitate other crimes such as blackmail. Information related to bank records is highly prized by criminals because of the direct monetary link to its exploitation. Credit card numbers are valued as well, particularly if the expiration date and other security data are bundled with them, permitting fraudulent transactions.

Other kinds of data are much more context-dependent. In most cases, publishing someone's home address on the Internet is not, in and of itself, a matter of high concern, simply because the opportunities for exploitation are limited. However, if this address was for someone in the witness protection program, this could be a criminal offence. Your organization's intellectual property will also need to be protected, but identifying what this is and where it is stored can be a significant challenge.

Who should access data?

The first step in preventing leaks is to clearly identify sensitive information and to tightly control access to it. This is easier said than done; particularly now that the majority of information is available electronically through a variety of methods. It is no longer sufficient to keep sensitive information in a locked filing cabinet—the electronic equivalent needs to be constructed. As the volume of electronic information stored by businesses is doubling every few years, this is going to become even more of a challenge in the future unless better methods of classifying and managing information can be widely implemented.

© 2007 Protiviti Inc. All rights reserved. An Equal Opportunity Employer

When new IT systems or business processes are designed, what considerations are made to the data that will be produced by those systems or processes; how it will flow between applications and departments; and from where else it may need to be accessible? Are all of those potential avenues secured?

Many business processes are designed around the assumption of free information flow within an organization, and will need to be revised to restrict information to only those people with a need to know. In security speak, this is known as the principle of least privilege. This also includes contractors and third parties who will need some level of access to information to be able to assist; however, all too often they are given the "keys to the kingdom" when they do not need them. Does your organization restrict information once a non-disclosure agreement has been signed? Or like many, do you assume that this should allow unrestricted access to internal information?

Controlling intentional leaks

In general, intentional internal security breaches result in higher financial losses for fairly obvious reasons: company employees are trusted and have access, so inappropriate acquisition of information can be more easily masked. Employees like to give—and are given—the benefit of the doubt. Therefore, when a breach occurs, it can be a long time before it is detected, allowing much more damage to be caused.

By assuming that intentional leaks will occur sooner or later, a well prepared organization will develop a media communications plan and other procedures to suspend or terminate the access of people who are suspected of leaking the information until an investigation can take place.

Preventing unintentional leaks

Oftentimes these types of leaks are unintentional. An unguarded laptop screen on an airplane or a loud conversation in the local café can easily result in unauthorized people gaining access to sensitive information. However, in the majority of cases people who gain information in this way will quickly forget it, as it is of little or no relevance to them. However, it is dangerous to assume that this is always the case.

In some instances, the people sitting next to you in the café are there on purpose. They know that this is the closest location to your office for people to get a caffeine fix and are specifically there to see what information they may overhear or otherwise gain access to that could be of value.

It is even easy for someone to offer a "Free WiFi Point" that could gather a significant amount of information from people who have not been trained to be cautious. There are also reports that these fake access points are starting to be seen on airplanes. Who would not want to have internet access from Seat 15B however unlikely it may be that the airline would provide this? In either case, a fake wireless access point could easily gather log-on credentials or other sensitive information that the user may supply without realizing.

This can also present another problem to organizations. By gathering user credentials in this way (often called "phishing"), transactions or data access can appear to be legitimately performed by valid users, and only later identified to be criminal activity. A development that has only recently received attention is so-called "spear-phishing" where a very specific group of users (e.g. who work for one company) is targeted with a specific purpose in mind (e.g. obtain specific information from that company). This is something else for companies to consider—once their users log-on, are there certain patterns of behavior that may indicate that an account has been compromised? Banks and financial institutions are ahead of the game in this respect as they have faced similar issues for years with credit card fraud, and now internet banking fraud. As a result, their behavioral analysis capabilities are quite sophisticated.

© 2007 Protiviti Inc. All rights reserved. An Equal Opportunity Employer

Another area to consider is the line between competitive intelligence and industrial espionage. The former is more benign—think of going on a blind date and Googling the person that you are meeting to find out some background on them before the first meeting. Publicly available information can provide useful information regarding the person's background, occupation, and activities.

Whilst competitive intelligence limits the search to material in the public domain, industrial espionage moves matters beyond that sphere, with its practitioners making connections from public information and then acting on it to gather added information that is not part of the public domain.

Industrial espionage is not necessarily cloak and dagger, but occurs when an asset valuable to a company is obtained through illegal or semi-legal means and is made available to competitors (or used to blackmail an organization), damaging the company's ability to compete.

Although being a victim of industrial espionage can be a serious issue for an organization, it does not require public disclosure. Also, it is difficult to identify the true amount of such activity that does take place. Interestingly, because companies can simultaneously "lose" and retain digital information, it may be some time (if ever) that leaks of this type are recognized to have taken place, even within an organization.

For example, if someone removes intellectual property when he or she leaves an organization, this may allow them to start a competing business without a major investment of time or effort to recreate that intellectual property. It is often hard to prove that this has taken place. Likewise, an argument can be made that China can now compete effectively with Western countries because knowledge that was originally acquired through significant investment in R&D has leaked via a variety of methods into an environment that lacks strong copyright protection laws where it can be reused without penalty.

Automated data leak prevention solutions

Over the last two or three years, technological solutions have appeared that are designed to address information leakage head on. Many of these applications initially focused on monitoring data leaving organizations over networks, via email, web traffic or other means. These systems sift through email, Web site postings, and so on to identify patterns (e.g. Social Security or credit numbers, hate speech, pornography, etc.), then either just log the incident, or raise an alert. They can also have custom rules defined to identify information specific to an organization (e.g. confidential projects) and alert on those as well.

Many of these applications, from companies such as Vericept, Vontu and WebSense can also block certain types of event-related traffic from leaving a network, if required. We do not recommend that this functionality is enabled until you are completely certain that this is what you want to do and you have a robust process in place to manage such incidents and ensure that business processes are not disrupted as a result.

In addition to monitoring network traffic (so-called "Data in Motion"), vendors have been adding functionality to scan hard drives and other data stores and detect information there. This functionality is often called "data at rest" or similar. Both Gartner and Forrester have released research comparing the functionality of the systems on the market and their strengths and weaknesses, and I refer you to those sources for more comparative details of the major players in the market. There are systems suitable for just about any IT budget and for any size organization.

Balancing business needs with security

All of the measures available to manage the risk of data leakage must be balanced with the requirement to facilitate business processes and transactions, rather than put a barrier in the way of performing legitimate tasks.

© 2007 Protiviti Inc. All rights reserved. An Equal Opportunity Employer

To facilitate this, we recommend that a good place to start is by understanding what data exists on your network and gaining a sense of overall information traffic patterns and access. Until you have a clear picture of your environment, it is difficult to create effective enforcements that do not have unforeseen side effects.

As your process matures, it is reasonable to identify areas that might require blocking, particularly from a compliance perspective. Ultimately, however, no technological solution alone will solve the problem—controls for both people and processes must also be effectively implemented as elements of an overall approach.

Some actions to consider:

- Identify "sensitive" information within your organization.
- Determine where this information is created, who has access to it, where it is stored, and where it is transmitted.
- Restrict access to sensitive information, both physically and logically.
- Develop an incident plan to respond to a significant data breach and ensure that relevant parties, (e.g. legal, PR, Executive Management), are involved.
- Review the functionality of automated "Data Leak Prevention" systems and determine if one is right for your organization.

Article from Protiviti KnowledgeLeader – www.knowledgeleader.com.

KnowledgeLeader is a subscription-based website that provides audit programs, checklists, tools, resources and best practices to help internal auditors and risk management professionals save time, manage risk, and add value. Free 30-day trials available.

Protiviti is a leading provider of truly independent internal audit and business and technology risk consulting services. We help clients identify, measure and manage operational and technology-related risks they face within their industries and throughout their systems and processes. And we offer a full spectrum of audit services, technologies and skills for business risk management and the continual transformation of internal audit functions.

Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

© 2007 Protiviti Inc. All rights reserved. An Equal Opportunity Employer