

## Getting a Handle on Data Loss

By John Brandon

22 October 2010

*Processor*

According to a recent study by Kroll Ontrack ([www.krollontrack.com](http://www.krollontrack.com)), 21% of enterprises do not know where data loss occurs. Fortunately, many of these breaches can be prevented by establishing airtight security policies, enforcing them, and being proactive about data leaks.

According to Alyn Hockey, the director of product management at Clearswift ([www.clearswift.com](http://www.clearswift.com)), an email and Web security company, many security leaks occur through human error, such as leaving a laptop unattended in a public place or misplacing a backup tape with an important archive.

"Once you've identified the source of the leak, you need to plug it fast," says Hockey. "The first question is, how did it happen? If it was malicious, it's more than likely that the authorities should be contacted; if the leak was human error, then the individual should be retrained to ensure it won't happen again or moved to a position whereby the chance of a repeat occurrence is not possible. You may also consider making the security systems and processes stricter, but you have to get the balance right, as locking the system down too tightly will prevent business and will throttle the company further."

Hockey says one of the main issues with data loss is that many smaller companies do not have the resources of a larger organization that might hire a CSO who controls the processes around data security. Instead, they learn how to deal with breaches only after they occur and lack the expertise to develop the legal and technical process to prevent leaks.

Gary Bahadur, CEO of KRAA Security ([www.kraasecurity.com](http://www.kraasecurity.com)), a consultancy and managed security company, says the first step in figuring out how data loss could occur is through proactive monitoring, which examines end points, data stores, and client systems for possible leaks before they occur. He says there are a plethora of security tools that can provide DLP (data loss prevention) services. These tools can monitor every possible leakage point, from a USB thumb drive to email, FTP, and instant messaging.

### Preventing The Leaks

Proactive monitoring is a good first step because it means a company examines all points of possible data loss. This ensures that a company has taken action on leaks right away—a move to plug holes on a potentially dangerous scenario, such as hackers stealing data and using it nefariously. The very next step, Bahadur says, is to investigate the kinds of data that need to be protected. Part of this process, he says, is determining which data is mission-critical, because it's impossible to block all data. Instead, developing a security policy on which data has to be blocked is crucial.

Bahadur says policies are even more important in a smaller company than a larger one, which may be able to invest in enterprise-security software. But regardless of size, the real danger is in how employees use data: For example, someone might use a USB drive at work and then go home with sensitive company data that is then exposed. He says many SMEs probably know about potential security risks but lack the resources to really block gaps such as this. Creating policies about personal use of company drives, data transport, and remote access can all help reduce the risk. Policies are also a preventive move as opposed to reactionary.

Beyond policies, Bahadur says an SME needs to evaluate software that is available for ongoing monitoring and protection and decide if the tools are manageable within the organization, or if they need to go to an outside provider who can help manage data security functions.

## Ongoing Prevention

Blocking leaks that exist today, developing policies, and then using monitoring software will help keep a data center safe, especially when it comes to the most common leaks and employee mistakes. Yet, as Robert Hamilton, a product marketing manager with Symantec Data Loss Prevention ([www.symantec.com](http://www.symantec.com)), says, it's also important to develop a long-term strategy for understanding potential risks in data loss.

One aspect in the long-term strategy is continuing education about security risks, which helps employees understand the dangers in using company resources. This can include letting them know about the seriousness of the issue; the common ways criminals can steal data; and the established policies on using USB drives, email, instant messaging, and even social networking tools.

However, there are other steps to take, as well. "Long-term issues are best addressed by implementing improved data security controls . . . discovery to find where sensitive data is stored, and monitoring to understand who is accessing sensitive data and what they are doing with it," says Hamilton. "One of the most important things that a company can do is to perform an entitlements review. File access permissions are far more permissive than most organizations ever intended, and this is often the reason that people can access data they shouldn't. Locking down data by limiting access to only those with a legitimate business purpose is a strong data governance standard."

The education process and policy enforcement can help solve the critical problem facing many IT managers today, especially in smaller companies: They just do not know where leaks occur, and because they do not know about the potential leaks, they can't address the issue in the data center.

"Organizations do not know how much sensitive information they have, and they have no idea of the various locations where it is stored," says Hamilton. "They may not be aware of the role of the insider in data loss and they may be unaware of how aggressive outsiders have gotten with trying to steal data."

Taking steps to find potential leaks, blocking them right away, and instituting policies and ongoing monitoring services within an organization will all make computing operations safer and more secure.