

Protecting Confidential Information in a Down Economy

Source: Symantec.com

(http://www.symantec.com/business/solutions/article.jsp?aid=20090828_protecting_confidential_information_in_a_down_economy)

Did you know that an estimated 90% of data loss incidents are accidental?

That may be surprising news in light of the fact that **cyber-criminals have never been busier**. But according to a recent survey by TheInfoPro Inc., data loss is “more the result of non-malicious activity as compared to malicious actions.” (“Why Data Loss Prevention?” TheInfoPro Inc., October 2008)

What does that mean for your business? For one thing, it means that the loss of critical data is more likely to result from the actions taken by one of your users in the course of doing business than from someone hacking into your network.

Now consider the findings of another recent survey, which puts the spotlight on a little-known aspect of the current recession: namely, that as companies downsize, data loss risks increase.

According to a Ponemon Institute survey of 945 employees who lost or left a job in 2008, 59% of them admitted to stealing confidential company information. In addition, researchers found that many of these instances of data theft could have been prevented with better data loss prevention policies and technologies. (“Data Loss Risks During Downsizing,” Ponemon Institute, February 2009)

Taken together, these surveys offer a strong and timely argument for re-examining your company’s approach to protecting sensitive data.

This article looks at how a great deal of data loss is preventable through the use of clear policies, adequate controls on data access, and better communication with employees.

Get answers to these critical questions

What can you do to ensure that your company is protected against a data breach? Start by looking at the data itself. You want answers to some fundamental questions. Here’s a simple checklist:

- Where is my confidential data?
- Who are the owners of this critical data?
- How is it being used?
- On a more technical level, do you know which file servers and databases contain exposed confidential data?
- Do you know which laptop and desktop computers contain confidential data?
- Do you know who has unauthorized access to your confidential data?

Your ability to answer these questions is critical, given that employees today have so many options for extracting sensitive information, such as media devices with large storage capabilities, USB storage devices, PDAs and smartphones, digital cameras, and Web-based email.

Data Loss Prevention (DLP) technologies are particularly well suited for today's midsize companies. An effective DLP solution enables you to discover, monitor, and protect your confidential data:

- **Discover.** Find confidential data—customer contact lists, employee records, email lists, financial information—wherever it is stored, create an inventory of sensitive data, and automatically manage data cleanup.
- **Monitor.** Understand how confidential data is being used—whether the user is on or off the corporate network—to gain visibility across your organization.
- **Protect.** Automatically enforce security policies to proactively secure data and prevent confidential data from leaving the organization.

Perhaps most importantly, DLP can go beyond simply preventing information loss. In the event that information is removed from the system, a strong DLP solution can provide logging and reporting features that identify the user and provide details on what information was removed, when it was taken, and how it was extracted from the corporate system. These forensic capabilities provide you with a great advantage in recovering from the loss of critical data as well as any legal actions that may follow.

DLP is a key component of the new Symantec Protection Suite Enterprise Edition. The advanced content filtering and data loss prevention of Symantec Protection Suite Enterprise Edition help you control sensitive data, reduce the risks associated with data loss, and meet regulatory compliance and corporate governance demands.

Of course, technology alone can't protect your sensitive information. Nor should information security be the job of just a few individuals within your organization. Rather, all of your employees should be educated and empowered to protect company data. This [document](#) provides guidelines and recommended best practices for promoting information security. Use these guidelines and best practices to re-engage with employees and improve existing company information security efforts or to develop a baseline information security communications plan.

Conclusion

The explosive rise in the amount of data that companies handle every day has led to a situation where just about anybody can access and distribute sensitive information in unlimited volumes. Increasingly, the loss of sensitive information is having a severe financial and brand-related impact on businesses of all sizes. That impact is multiplied in tough economic times, as employees who leave or lose a job may take data with them via USB and other devices.

As a result, you need to know exactly where your sensitive data resides and how it is being used so that you can prevent it from being copied, downloaded, or sent outside the company. It's not enough to secure your network. It's time that you focused on protecting your important data.