

How to protect your critical information easily

Safeguarding massive amounts of sensitive, confidential data—from legally protected personal information to intellectual property and trade secrets—from malicious attacks and accidental loss is one of IT's biggest challenges. With employees having greater mobility than ever before to work outside the office, the job of protecting data has never been more difficult. Organizations must find a balance between protecting data and allowing it to flow easily around the business and between employees and partners. This white paper identifies the areas an effective strategy needs to address and describes how organizations can make data protection easy and cost-effective.

By Jonathan Tait, Product Marketing Manager, Sophos

How to protect your critical information easily

Summary

Safeguarding massive amounts of sensitive, confidential data—from legally protected personal information to intellectual property and trade secrets—from malicious attacks and accidental loss is one of IT's biggest challenges. Forrester Research says 288 million records were lost in the United States in 2008 and that 52% of the nation's large organizations lost confidential data in 2007 and 2008. From a financial perspective, the Ponemon Institute estimates each lost customer record costs a business more than \$200, with about \$150 of that in indirect costs, including abnormally high levels of customer turnover. That translates to an average organizational cost per data breach of more than \$6.6 million (Ponemon Institute LLC, "Fourth Annual US Cost of Data Breach Study," January 2009). Such breaches can damage a business's reputation, destroy customer trust and adversely affect the bottom line.

With employees having greater mobility than ever before to work outside the office, the job of protecting data has never been more difficult. Organizations must find a balance between protecting data and allowing it to flow easily around the business and between employees and partners. This white paper identifies the areas an effective strategy needs to address and describes how organizations can make data protection easy and cost-effective.

Avoiding the usual problems

There are a couple of common approaches to implementing data protection, which ordinarily end in pain:

- Some companies may choose to implement a dedicated data loss prevention (DLP) solution. However, this can often prove to be costly and hopelessly complex—often taking too much

time to complete and even sometimes never getting done at all.

- Other companies may choose to deploy multiple solutions addressing different aspects, but not in a consistent way. This comes with its own problems. It affects the performance of computers and causes pain for IT with multiple management consoles, licenses and support numbers to call.

The goal for an IT manager is to secure sensitive data without exceeding your operating budget or overloading your team. This is an especially daunting challenge when data is on the move. Sending data via email, putting it on a USB thumb drive or burning it to a disk all increase the potential for malicious attacks or careless handling of sensitive information.

With that in mind, there are four key areas that IT should consider for building a solid yet manageable data protection strategy. You could approach each of these four areas in turn, but addressing them all together will give you a comprehensive strategy whose whole is greater than the sum of its parts:

1. **External threats and malware:** Stop malware and hackers from maliciously stealing data and compromising your security.
2. **Complying with policies:** Make sure that users are adhering to the policies you put into place.
3. **Preventing data loss:** Stop users from being careless with data.
4. **Securing mobile data:** Ensure that sensitive data can't be compromised if users lose devices, while still allowing data to be exchanged among authorized users.

Protecting against external threats and malware

Today's malware targets any data that can be sold—from financial information to blueprints. If it's valuable, the bad guys want it. Stopping the threats and keeping your network clean gives you a strong foundation on which to build your data protection strategy.

To stay ahead of these escalating threats, your organization needs a solution that detects and defends against known threats—preventing most from getting into your system in the first place—while also being able to effectively detect, block and remotely clean up emerging, unknown threats. Such comprehensive performance will give your business the advantage it needs in the battle against malware and external threats.

Stopping threats and keeping your network clean

The first steps to ensuring your sensitive data is protected involve stopping threats before they cause potentially devastating damage and keeping your network clean. Look for a solution that features proactive protection that detects known, unknown and emerging threats. Such a solution will block malware from reaching the system in the first place. But if something malicious does actually make it onto your network and attempt to steal data, your security will detect, block and remotely clean it, ending the threat before it begins.

Complying with policies

Regulations regarding securing confidential, personal data continue to grow more numerous and more stringent. Retailers and healthcare providers are now joined by virtually every other type of business that handles customer information under the microscope of regulatory compliance for data security.

It's one thing to have all your policies neatly documented, but it's an entirely different thing to get people to comply. Deploying a technology solution enables you to enforce policies and monitor activity across your organization. This also helps you to prove that you are taking appropriate action to protect the sensitive and confidential data on your network.

Making compliance easy

When it comes to policy compliance, you need to quickly create and deploy policies across your organization. Plus, you need to monitor and control the use of all your devices and programs, from USB storage devices and instant messaging applications to email and web access and blocking the use of P2P software. So you should look for a comprehensive yet simple solution. Such a solution should identify specific devices to which data can—and cannot—be written. The result will be that you'll protect your data without slowing the information superhighway down to the speed of a winding country road in the name of security.

Preventing data loss

An organization that has successfully implemented a dedicated DLP solution is an exception to the norm. Most businesses wrestle with this issue and are unsure of the best way to attack the problem. For the vast majority of organizations, implementing a dedicated DLP solution is like using a sledgehammer to crack a nut.

A better, more cost-effective approach is to integrate data loss prevention into the anti-virus solution your company is already using. Having a single endpoint agent not only stops the external threats but also monitors the movement of sensitive data keeps the organization protected while reducing the impact on system performance.

One potential nightmare for an organization—and its IT manager—is a user who sends an email with

confidential data attached and accidentally copies an unauthorized, external recipient. Once he or she pushes the send button, that data is off to where it shouldn't go—unless your DLP solution features a gateway that can identify that the data in question shouldn't be sent to an external recipient and stops the transfer before it is completed. That's how easy it would be if your anti-virus product could also manage your DLP needs.

An integrated solution

An integrated endpoint agent should monitor all of the common ways users can move data off the network using various devices or programs—removable storage devices, CD/DVD/floppy drives and internet-enabled applications such as web browsers, email clients and even instant messaging. It also should offer varying levels of control so you can choose the one that works best for your business and help to educate your users on the importance of protecting sensitive data. For example, you could choose the gentle approach and have the product tell the user he or she is being careless with data. Or take a stronger approach and block a user's ability to place sensitive information—such as a customer billing database—onto a USB drive or burn it to a CD.

Also consider gateway protection to catch any accidental attempts to send protected data to the wrong person. It will prevent disasters and keep that proprietary or confidential data where it should be—within your company.

Securing mobile data

Several solutions, such as encryption, are available to protect data at rest on the network. But when data starts moving, it is at a much greater risk of being compromised or lost, whether it's moving because someone is taking it off the network or because it's on the laptop of an employee who's traveling.

Much of the time when data is lost, it's not due to a malicious attack but to human error. People lose

things, and that can compromise data security. Each week, more than 12,000 laptops are lost at airports—that's more than 600,000 laptops per year. Most are left behind at security checkpoints and up to 70% of those are never reclaimed, according to the Ponemon Institute (Ponemon Institute LLC, "Airport Insecurity: The Case of Missing & Lost Laptops," June 30, 2008). Further exacerbating the situation, more than half of the business travelers surveyed by Ponemon said they store sensitive data on their laptops, and the majority of those admitted they do not back up or secure that data. Encrypting the data significantly reduces risk. It enables employees to do their jobs and helps your company avoid becoming another data-loss headline.

It's easy to say, but is it easy to do?

The best way to prevent data loss from mobile devices is to encrypt the files stored on them. However, organizations need to share data in the normal course of business and that's where problems arise. It's difficult to secure data on removable media and share it as needed. You could ask everyone to use encrypted USB drives, but that's not always practical. The idea is to maintain mobility and productivity while protecting data and minimizing the impact on the end user, so evaluate solutions that make it easy for users to secure data on any USB storage device—otherwise they are more than likely to avoid doing it altogether.

Even if your organization's employees don't lose their laptops, some of them inevitably will forget their passwords while they're traveling and your IT team will get their SOS at any time of the day or night. Look for a solution that delivers a simple way for users to recover passwords themselves wherever they are—it will speed up the process for them and avoid costly IT hotline calls.

Encryption is a great solution for preventing data loss, but the reality is that there are a lot of different hardware specs out in the real world, which makes deploying a single effective

encryption method a problem. To deal with this reality, you need a solution that will assess computers during implementation and automatically notify you of any potential installation issues so you can take action before it is too late.

And for confidential data that does have a valid reason for being emailed to customers or partners, you don't want to deal with the hassle of building a complex infrastructure, undergo painful software installations or create time-consuming or confusing processes for your users. Instead, you should seek a gateway solution that will automatically encrypt confidential information so that it is protected as it heads across the internet to its recipient.

Conclusion

According to the Open Security Foundation, since 2000, the most prevalent types of data loss are from stolen laptops (21%) and malicious attacks/hacks (16%). So it's clear there's a problem. But the cure shouldn't be as complex as the problem itself. Therefore, look for a solution that handles external threats and malware; prevents data loss; secures mobile data; and helps you comply with policies and regulations. The ideal solution will allow you to use these features separately—although combining the four areas will give you the solid yet manageable data protection solution that you are looking for.

To learn more about how Sophos provides anti-malware and data protection in one simple-to-manage solution, please visit:

<http://www.sophos.com>

Boston, USA | Oxford, UK
© Copyright 2009. Sophos Plc

*All registered trademarks and copyrights are understood and recognized by Sophos.
No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any
form or by any means without the prior written permission of the publishers.*

SOPHOS
WWW.SOPHOS.COM