



Don't Let Data Loss Burn a Hole in Your Budget

How to implement a data loss prevention strategy

By **Payal Mehrotra**, Product Manager

Let's face facts: the office-based worker is a thing of the past. Users access corporate data from anywhere at any time from any device. While mobility offers organizations significant productivity benefits, it also increases the risk of data loss that could cause irreparable harm. This paper guides you through the steps necessary to implement a practical data loss prevention (DLP) strategy. We'll start by quickly looking at what's driving data loss prevention and the consequences of data loss. We'll then provide practical implementation advice.

What's driving DLP?

There has been a fundamental shift in how employees interact with IT, driven by hardware (laptops and smartphones) and services (webmail, IM, social media and remote access). Access to corporate data remains the lifeblood of the organization. But the risk of it leaving your control is now significantly higher. The days when a solid perimeter firewall was enough are long gone.

To prevent data breaches and keep sensitive data, such as personally identifiable information (PII), out of the wrong hands, security professionals need the right tools to minimize risk. Vendors have responded by developing technology that, used properly, can significantly reduce the risk of data loss.

Costs and consequences of data loss

PII is any piece of information that can be used to uniquely identify a single individual. Examples include name, Social Security number, credit/debit card numbers, date of birth or health record.

Loss of PII can have far-reaching, devastating effects. Regardless of how your company handles a data loss incident and its disclosure, your security and privacy policies will come under intense scrutiny by auditors, your customers and the press. Inevitably, customers can lose confidence in your company, which means lost business.

Studies now put the total cost of a single data breach in the millions of dollars. According to the Ponemon Institute, the average cost of a data breach in 2012 was \$199 per record compromised in Germany, and \$188 per record in the U.S.—the two countries with the highest costs. The average total cost for a data breach in Germany was \$4.8 million and \$5.4 million in the U.S.¹

Not surprisingly, reputation damage has major consequences. The biggest single contributor to the cost of a data breach is lost business, accounting for 56% of the total cost for U.S. organizations, the Ponemon Institute reported. Other costs are associated with customer support, such as information hotlines, reputation management, productivity and legal fees.

Organizations also face fines due to a number of laws and regulations that seek to protect PII, including PCI DSS, HIPAA and Sarbanes-Oxley in the U.S. To reduce the risk of data loss, maintain compliance, and avoid the associated costs, companies need a tightly integrated, multi-layered approach to data loss prevention.

¹ 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, May 2013, https://www4.symantec.com/mkt-ginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

Cost of a Data Breach 2012



**COST PER
COMPROMISED
RECORD**
(U.S. dollars):
Germany: \$199
U.S.: \$188



**TOTAL COST PER
DATA BREACH**
(U.S. dollars):
U.S.: \$5.4 million
Germany: \$4.8 million



**LOST BUSINESS
ACCOUNTS
FOR 56% OF TOTAL
COST OF A
U.S. DATA BREACH**

Implementing a multi-layered approach to DLP

A holistic, multi-layered DLP strategy begins with content monitoring at data exit points such as portable storage devices, external hard drives, IM and email messages. Your strategy should also include encrypting data at rest and in transit to prevent unauthorized individuals from accessing information that leaves the organization. Finally, a multi-layered DLP approach must include end-user policy compliance. This means enforcing rules for proper data use.

Companies should prioritize management of data by choosing a DLP solution that monitors and controls distribution of PII at exit points. You can simplify configuration, deployment and management by choosing a DLP solution that protects data at both the endpoint and the email gateway. DLP product that integrate scanning for sensitive information into an existing scanning mechanism—the antivirus engine, for example—reduce the need for separate solutions.

"The biggest single contributor to the cost of a data breach is lost business, accounting for 56% of the total cost for U.S. organizations."

PONEMON INSTITUTE

End user policy compliance

Controlling what end users can do on their devices is one of the easiest and most effective ways to reduce the risk of data loss. There are three main areas you should focus on as part of your DLP strategy.

- ▶ **Storage devices and network interfaces:** Manage the use of connected devices (e.g., thumb drives, external hard disks and smartphones).
- ▶ **Applications:** Manage the use of applications (e.g., file sharing, online storage, remote access, IM clients, web browsers).
- ▶ **Web filtering:** Manage which websites users can access (e.g., web-based email, hosted IM, anonymizers).

Don't Let Data Loss Burn a Hole in Your Budget

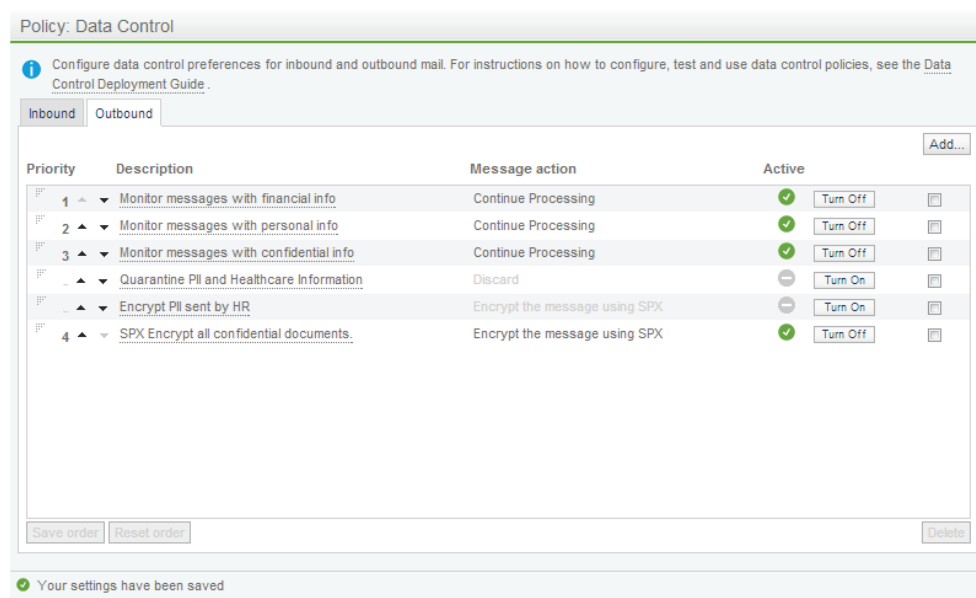


Figure 1: Creating DLP policies on outbound emails

Assessing your DLP needs

Implementing the technical components of a DLP strategy—content monitoring, encryption, and policy compliance—requires preparation. You can make the roll-out process a lot easier with careful planning beforehand, so let's go step-by-step through the process of preparing for a DLP project.

- 1. Understand what industry and government regulations impact your organization.** For example, data protection legislation and industry regulations in the U.S. include PCI DSS and HIPAA. Be sure to know which laws apply to you in your region. If necessary, consult a corporate attorney to get clarity on detailed requirements.
- 2. Kick off an internal project.** You need to define and document the business drivers, regulatory requirements, business case and high-level objectives for DLP/data security implementation. For example, your primary goal may be to protect PII stored by your organization and improve your auditing. A secondary goal may be to protect intellectual property specific to your organization.
- 3. Secure sponsorship from within the senior management or executive team.** As with all IT projects, you need support from management if your DLP strategy is to succeed. Inform senior management of the goals identified in Step 1 and the benefits of implementing the data security policy.
- 4. Gather a project team with representatives from across the organization.** Consider including someone from the senior management team (ideally your sponsor), human resources, finance, legal, etc. Sensitive data exists throughout your company, and data loss affects the whole organization. These representatives can help you identify sensitive information and define appropriate security policies.

Don't Let Data Loss Burn a Hole in Your Budget

5. **Identify the types of data you have within your organization.** For example, you should identify data covered under regulations and intellectual capital. Determine where this data resides so you can identify the systems you need to monitor. Learn how the data is used and by whom so you understand the data's role and who could accidentally expose data. Don't forget to include your IT staff, like systems administrators, who may not actually use the data but have access to it.
6. **Evaluate the risk and impact of a data breach for each data type.** Based on this information, prioritize risks and address the most serious first.
7. **Plan policies for identifying sensitive data types and remediation actions.** For example, if a user attempts to send customer or confidential data via email, you may want to block that action or encrypt the data. You could also log the action and/or warn the user that he or she is violating security policy. Solicit feedback from your peers and colleagues on your policy recommendations.
8. **Educate users.** User training, guidelines and acceptable use policies are critical to the success of your DLP strategy and should be factored into the project alongside any IT activities. Your objectives for user training should be two-fold: to manage their concerns and, more importantly, to make all employees aware of the new policies and to enlist their help in protecting data. Whether in person or online, user training can be included as part of more general training about data security. Once users know what is expected of them, you can hold them accountable.

Once you complete these eight steps, you've established a solid foundation for your DLP project. Now you're ready to address the technical aspects of implementing your policies. Next we'll show you how to do this using Sophos solutions.

DLP made easy with Sophos

Sophos offers two solutions that feature content-aware data loss prevention technology. Each monitors user actions at common data exit points.

- Sophos Secure Email Gateway secures your email gateway and provides simple yet powerful protection from spam and phishing attacks.
- Sophos Enduser Protection Suites protect your desktops, laptops, mobile devices, data, web and email—all in a single license.

Each solution uses data control rules to identify and trigger a response when a user attempts to transmit sensitive or proprietary data outside of the company. A data control rule is made up of three elements:

1. **Items to match:** Options include file content, file types and file names.
2. **Points to monitor:** Monitoring points include email, storage types and applications.
3. **Actions to take:** Monitor, block or request user authorization.

Don't Let Data Loss Burn a Hole in Your Budget

The data types protected include a wide range of PII and financial data formats, all of which are kept up to date by SophosLabs. The full list can be reviewed within the Sophos solution or by requesting a list from a Sophos partner. As necessary, you can also define custom lists.

Data control rules should be written for specific types and quantities of data. For example, data control rules can be defined on outgoing emails to prevent users from sending financial information like bank account numbers in the email body, subject line or in an attachment.

Defining sensitive data based on content can be complex. Sophos has simplified this task by providing a pre-built library of sensitive data definitions, known as Content Control Lists (CCLs).

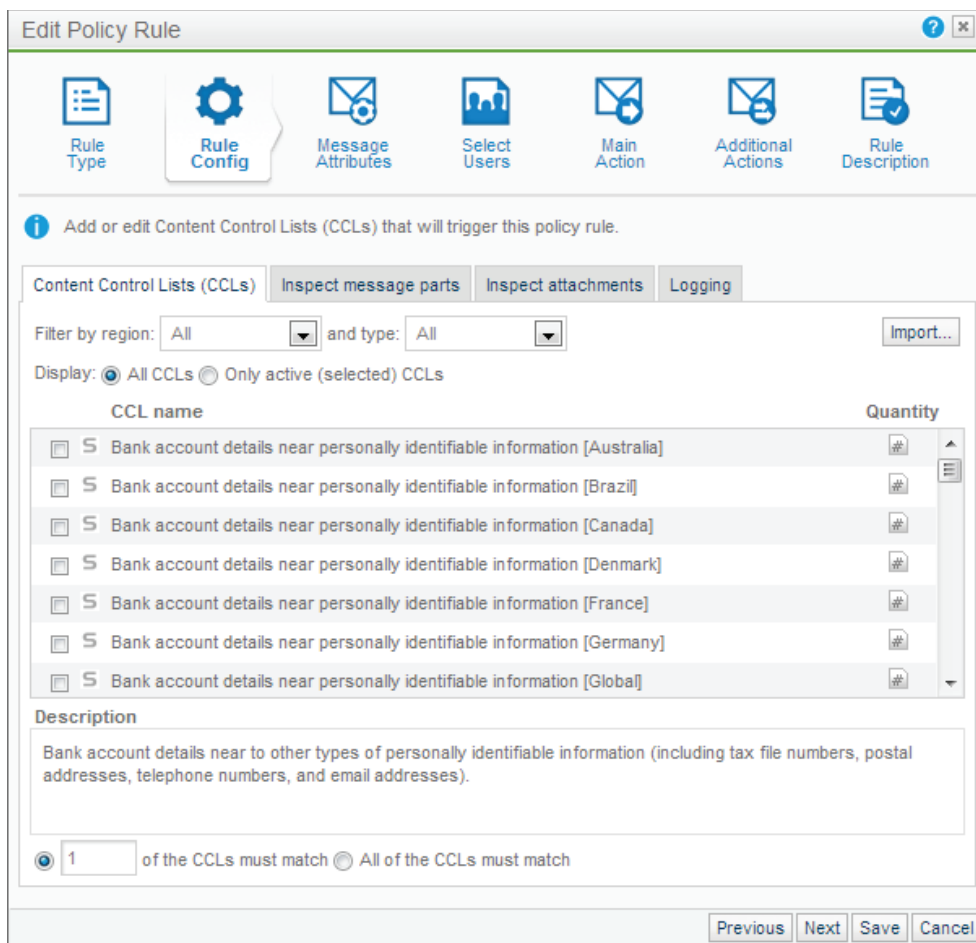


Figure 2: Sophos's Content Control Lists are easy to use.

Don't Let Data Loss Burn a Hole in Your Budget

Besides choosing which CCLs you want to implement, you must determine how you'll enforce your policies. With Sophos Enduser Protection Suites, the options include silently logging the event, logging and warning the user with a prompt to proceed (similar to a training mode), or logging and blocking the transaction. With Sophos Email Appliance and Sophos Secure Email Gateway, the options include logging, quarantine, blocking or encrypting the content before sending.

It's important to use clear and well-formed rule names that explain to the user why their action was blocked. You can also customize the message and point to a policy page on the intranet and/or provide help desk contact information.

Common use scenarios

Identifying PII

The most common data loss policies relate to identifying PII and financial data. The following two scenarios explain how to configure such policies to protect these sensitive assets.

Scenario 1: You want to identify any credit or debit card details that are sent via email with Sophos Secure Email Gateway. When an event is generated, you'll want to encrypt the data.

Scenario 2: You want to challenge users who transfer large blocks of customer contact information. To do so, use Sophos Enduser Protection Suites to detect when PII or financial data is uploaded to the web (which also covers webmail) or transferred onto removable storage devices. Set the system to query the user and audit his or her response when an event is generated.

Combining PII definitions and custom data sets

To increase accuracy, you can combine PII definitions provided by SophosLabs with custom data sets. For example, an educational institution may combine PII definitions for email and postal address details with its custom data set that lists students and staff names. The same can be done with a list of employee Social Security or National Insurance numbers.

Using document markers to monitor sensitive data

Sophos solutions that include DLP technology can also be used to identify documents that contain sensitive data that cannot be classified as PII or financial data. This can be done in one of two ways.

For single-purpose documents that contain sensitive information—for example, a confidential performance review or acquisition document—you can add an invisible string of characters to the document. The string may be inserted into the header, footer (using a white font on a white background), or metadata of the document.

Don't Let Data Loss Burn a Hole in Your Budget

When sensitive data is created and handled by a wider group within the organization, it makes more sense to use a document classification system. Keep it simple by using only two to three classification markers (e.g., "Internal confidential" and "Partner confidential"). Make sure each marker is unique to avoid false matches. Making sure markers are inserted into the appropriate documents can be a challenge, so embed the markers into document templates.

Once the document marking process is in place, you can configure a series of rules in your Sophos DLP solution to identify the relevant strings. Using this approach provides a picture of how the data is being shared across the organization and how.

Best practices for launching your DLP strategy

Traditional security measures are no longer adequate. In the past, you simply deployed an antivirus, and users had to accept its limitations. However, because DLP deals with user privacy and PII, you need user buy-in. Here are some best practices for a successful rollout of your strategy.

1. **Begin with a transparent security policy.** Give your users a document explaining the key aspects of your DLP policy to answer questions about user privacy. Focus on the types of data you're trying to protect and make sure the organization's motivations are clear.
2. **Deploy data protection technologies to prevent accidental data loss.** Accidents happen—people lose laptops, or send emails to the wrong address. Protect against data loss by deploying security solutions such as content control, device control and encryption to render data unreadable without a password.
3. **Start with a small subset of prioritized data and slowly expand the rules.** If you turn on all the rules at once, the number of events will be significant. IT will be overwhelmed, and users will be inundated with messages warning them of their actions. Either productivity will be impacted (and IT will be accused of hindering the business) or users will begin ignoring these warning messages.
4. **Avoid accusatory language in notices.** Instead of accusing the user of sending sensitive data, tell the user that it looks like he or she might be sending data in a manner that breaches policy.
5. **Link to specific advice on how to send data securely.** Your goal shouldn't be to catch users violating the rules, but to educate them so they become part of the DLP process.

Don't Let Data Loss Burn a Hole in Your Budget

Conclusion

Loss of customer data or corporate proprietary information can cause permanent harm to your business and reputation. Your DLP strategy should have multiple levels, consisting of content monitoring, data encryption, and policy compliance.

But data loss prevention doesn't have to be difficult or expensive. With DLP technology integrated into our endpoint, server and gateway solutions, you can have a complete DLP strategy that is simple, practical, effective and within your budget. And because DLP is integrated with our endpoint and email protection solutions, there's no additional investment.

Sign up for a free trial at Sophos.com
Sophos Email Appliance
Sophos Enduser Protection Suites

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA
© Copyright 2013. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

NP 10/13 wpna

SOPHOS