Five DLP Tips from Security Executives

DATA LOSS PREVENTION: WHAT YOUR COLLEAGUES ARE SAYING ABOUT IT AND HOW THEY TAKE ACTION

Executive Summary

With the rapid rise in data breaches, advanced threats and mobility, data loss prevention (DLP) has quickly evolved from a security issue to a business imperative. Once considered the concern solely of regulated financial services and healthcare organizations, companies across all industries are focusing on managing their data loss risk. As a result, C-level executives are turning to IT security to protect confidential data such as intellectual property (IP) and personally identifiable information (PII). DLP programs are emerging as the most effective solution. Security executives who use DLP as the cornerstone of their information security strategy are reaping significant tangible and intangible benefits; not only are they keeping their company out of the headlines, but they are also getting a seat at the table with their business peers.

This research paper examines the findings from a new study on DLP by Symantec . The goal of the study is to understand how DLP programs impact the effectiveness of security executives, while also protecting corporate data. Symantec surveyed more than 130 CISOs, VPs, directors and managers responsible for the evaluation, selection, deployment and governance of their organization's DLP solution. The study reveals that nearly half of the respondents believe they have improved their credibility with peers in other business units by implementing DLP. Key findings:

» **Improved boardroom credibility—**Forty-five percent of survey respondents say that DLP programs improved their credibility with peers in other business units, leading to more effective business leaders.

» **Increased executive visibility—**Eighty-nine percent of respondents say that their organization's DLP initiative originated from the top, either to demonstrate compliance or because management requested it.

CSO Custom Solutions Group

Symantec

» **Increased awareness of data loss risk—** Fifty-two percent of respondents' companies launched a data protection plan because they had either experienced data loss or felt such an event was imminent.

The Priority: Protect Business Data

Some of the top IT security issues troubling enterprises today have also become pressing business concerns. As industries grow more competitive and markets expand across the globe, C-level executives worry that intellectual property (IP), trade secrets and other strategic information is more likely to suffer unauthorized access or even theft, blunting an organization's ability to innovate and maintain a competitive edge. Business leaders are also plagued by the fear that when a data breach happens to a partner or competitor, the same thing could happen to them, complete with the negative publicity and high cost that stems from dealing with such an incident. Meanwhile, regulatory pressure from governments and industries continues to mount as enterprises are mandated to strictly guard customer and employee privacy, keeping data protection top of mind in the C-suite.

However, while the threat of a data breach is a serious concern for enterprises today, the need to protect data also presents an opportunity for CISOs to be viewed as more strategic contributors to the business rather than technical advisers (how they are traditionally viewed). However, since protecting data involves safeguarding both a company's crucial corporate assets and its reputation, CISOs have a chance to work with business users to develop strategies that protect data while lending credibility to their roles as strategic partners.

In fact, the survey conducted by Symantec shows that of the 130 respondents, 45 percent say their DLP program increased their credibility with peers in other business units.

"Data loss is a very real and very serious issue," says Tim Matthews, senior director, Data Loss Prevention, Symantec. "And DLP is the safest investment you could make."

The High Cost of Doing Nothing to Protect Your Data

Business leaders have opened their eyes to the need to protect data at a time when risks are higher than ever. This is in part due to the prevalence of advanced threats that are increasingly difficult to detect and thwart. Users are more mobile than ever, leveraging consumer devices that aren't owned or managed by the company to access corporate data. Greater access from more endpoints means employees create additional vectors for threats to infiltrate the corporate network and for crucial data to be stolen. In addition, attackers are growing more mature and patient, planting more sophisticated malware inside organizations.

The risk of data theft is also increasing because of changes in the way employees do their jobs today. In the race to be as productive as possible, users often don't stop to consider whether they are working with confidential data, or whether they are treating confidential data with the correct level of protection. Patient records are saved to a thumb drive; customer data is transferred to a laptop so an employee can work from home; unreleased product plans are emailed to personal webmail. While these actions may be unintentional, they still can expose sensitive information to unauthorized access. In fact, well-meaning insiders continue to cause the majority of breaches; the latest *Cost of a Data Breach* study finds that negligence was responsible for 39 percent of all data-loss incidents, with system glitches accounting for another 24 percent. Add to these threats the ongoing risk of malicious insiders stealing data, and it becomes clear that doing nothing isn't a strategy.

Not only does unprotected data expose a company to a possible breach, the fallout from such an event can threaten the viability of a business. According to the Cost of a Data Breach study, the average cost of a breach hit $5.5 million in 2011. These costs involve responding to breach notification laws, which are pervasive and mandate a rapid response, as well as lost business opportunities. What's more, customer confidence and the overall reputation of a company can take a serious hit once a breach is publicized. Having to bounce back from a data breach event is a struggle best avoided.

"Data loss is a very real and very serious issue. And DLP is the safest investment you could make."

— TIM MATTHEWS, SENIOR DIRECTOR, DATA LOSS PREVENTION, SYMANTEC

DLP as a Strategic Business Initiative

Results from the Symantec survey show that data protection is indeed growing in strategic importance, as the vast majority of respondents (89 percent) say that their company's data protection plan originated from the top; either to demonstrate compliance or because management requested it. And data theft is not an idle threat—more than half (52 percent) of respondents' companies launched a data protection plan because they had either experienced data loss or felt such an event was imminent. Of those survey respondents at companies that performed a risk assessment or proof of concept before installing a data protection solution, 82 percent found at least some sensitive data was at risk of unauthorized access or breach.

DLP solutions are increasingly being used to protect the crown jewels—IP, product blueprints, source code, financial documents, trade secrets, quarterly projections and so on. An organization's ability to compete in the marketplace and remain innovative is often dependent upon safeguarding such information, and thus doing so is a strategic imperative. DLP is also an effective way to protect regulated data and reduce business risk.

Five DLP Tips from Your Colleagues

DLP is more than just a security tool, it's a business process for managing risk, which affects every department in your company that touches confidential data." Therefore, DLP strategies require consultative input from CISOs to ensure the correct solutions are put in place and best practices are followed. In fact, DLP solutions are most effective when CISOs work with business users to identify and prioritize sensitive or confidential data, and apply policies to how it should be treated.

Symantec's survey respondents, who all have experience evaluating and deploying DLP solutions, recommend the following best practices for a successful DLP implementation:

1 » Clearly define your DLP requirements. It's important to understand how a DLP solution will integrate with your unique environment (cloud, mobile, endpoints, network and storage). Don't rely solely on paper evaluations and lab demos. Put DLP solutions through the paces in a production environment.

2 » Build a business case for your DLP program. DLP vendors can perform risk assessment to identify which critical data is leaving your network and thus is vulnerable to theft. The results, for example, quantified data loss risk, will arm you with a compelling business case to gain funding and support from key business stakeholders.

"Run the risk assessment and use the results to craft a strategy; don't [attempt to] boil the ocean with the tool," one survey respondent says. "The technology is great, but it's the processes built around it that are essential to success."

3 » Understand the total cost of ownership of DLP solutions. One survey respondent advises: "You evaluate all vendors and don't pick one that is the least costly." In addition to up-front software license costs, it's important to factor in hardware, maintenance, installation and staffing. Ninety percent of the effort of running a DLP program is reviewing and remediating data loss incidents.

Among survey respondents, 50 percent say that their DLP deployment costs are in line with the amount budgeted, and the majority of respondent companies dedicate one or less employee to DLP once the solution is up and running.

4 » Deploy DLP in waves to get quick wins. Attempting to deploy DLP across all of your users and systems simultaneously can be overwhelming and potentially disruptive to your business. Survey respondents recommend deploying DLP in stages: Develop a roadmap that starts with your highest-risk areas first and get some quick wins under your belt.

"Start out slow with a small number of key compliance policies enabled first, and do not attempt to block content from leaving your company until you are sure that the policies have been tuned to eliminate false positives," one respondent advises.

"The technology is great, but it's the processes built around it that are essential to success."

— SURVEY RESPONDENT

5 » Prepare for broken business policies. Before deploying DLP, enterprises are advised to determine how best to deal with broken policies, what methods will be used to prioritize and remediate them and how to keep those policies current as the business changes.

Other DLP best practices mentioned by survey respondents include using DLP to educate business units on the risks that exist and getting buy-in from business units and support from top executives before deploying.

Conclusion

Increased mobility and greater access to data are removing hurdles for employees to be as productive as possible and drive the business forward, but those trends also present a number of data protection challenges. Whether the goal is to comply with privacy regulations or protect confidential data, understanding how best to prevent data from falling into the wrong hands is a business imperative.

Recognizing the challenges and developing a long-term, sustainable data protection strategy that has the support of top executives and business units as well as the IT department is the best way to maximize risk reduction in a manner that's quick and doesn't tax resources. Choosing the right DLP solution helps enterprises develop and enforce better business practices regarding how to treat sensitive data as an integral part of a comprehensive security program. DLP solutions also help drive change across the organization and elevate the CISO's role to become a strategic partner to the business.

Understanding how best to prevent data from falling into the wrong hands is a business imperative.

Questions to Ask Before You Deploy DLP

To set yourself up for success, CISOs say it's important to understand what data is confidential to your business, how data owners want to respond to incidents and the overall corporate culture. Here are five questions to ask before you deploy DLP:

- **What data do you need to protect?**
Companies store hundreds of terabytes, even petabytes, of data. Understand what is confidential to your business and prioritize the most critical data first. Don't try to boil the ocean—that's a surefire way to kill your DLP project before it even starts.

- **What is your corporate culture?**
It's critical to understand your organization and tailor your DLP program to fit within the corporate culture. You want to be seen as "caring mother" not "big brother."

- **Do you have buy-in from business stakeholders?**
Data loss is not just a security issue, it's a business process that touches everyone from HR and legal to engineering and sales. Getting business-data owners involved early on will help you gain their support when it comes time to deploy and manage your DLP program.

- **How are you going to roll out DLP?**
CISOs recommend starting "slow and steady." First, monitor where data is stored and how it's being used. Once you've identified broken business processes and high-risk users, then you can start remediating data loss incidents. Next, turn on automated notifications to educate users about security policies—this dramatically cuts down repeat offenses. And prevent users from accidentally or maliciously leaking information by quarantining, encrypting and blocking outbound communications.