Executive Summary

2016 Data Protection Benchmark Study:

Visibility and Maturity of a Data Loss Prevention Program

When they start down the path of data loss prevention, major organizations around the world deal with an average of 20 data loss incidents every day. Incidents that need to be investigated, behaviors assessed, and mitigations implemented by a data loss prevention team that has probably not grown since the data loss prevention (DLP) solution was implemented an average of 4 years ago. Even though 83% of organizations report a fully deployed solution that meets most or all of their requirements, 33% report that they are still suffering from significant data loss, and many others may be without knowing it.

Intel Security and Ponemon Institute are pleased to present the findings of *2016 Data Protection Benchmark Study: Visibility and Maturity of a Data Loss Prevention Program*. The purpose of this research is to benchmark the current rate of data loss incidents across multiple industries and geographies, isolate the critical components of DLP maturity, and identify important focus areas to increase visibility and help prevent data breaches.

The research was conducted in North America (US and Canada), India, United Kingdom, and Asia-Pacific (Australia, New Zealand, and Singapore), and surveyed 1,000 IT and IT security practitioners in financial services, retail, government, healthcare and manufacturing, in commercial (1,000 – 5,000 employees) and enterprise (over 5,000 employees) organizations.

Key Findings

- Organizations dealt with an average of 20 incidents a day. The average number of incidents at the beginning was 20 per day, but about 17% of respondents reported less than 5, and 7% reported 50 or more. Organization size was directly related to the number of incidents experienced, ranging from 15 (1,000 to 3,000 employees), to 27 (more than 5,000 employees.
- Average cost of a data breach ranges from $80 to more than $350 per record. The loss or theft of patient records represents the most expensive data breach scenarios, while governmental organizations experience the least expensive data breach on a per capita basis.
- Average DLP deployment is 4 years old and is meeting most of the requirements. Like the number of incidents, length of deployment is directly related to organization size, with the smallest organizations running about one year behind. However, there is a wide distribution in responses, with just under half of all organizations with deployments between 1 and 3 years old.
- Symantec and Intel Security are the market leaders. This was a blind study, meaning the respondents were given no indication what company was the sponsor. Symantec and Intel Security were the predominant selection, with each the chosen solution of around 30% of respondents. Other vendors included Digital Guardian, Trend Micro, and Websense (acquired by Forcepoint).
- Most configurations are not generating enough visibility into potential data loss incidents. One of the biggest challenges with data loss prevention is the uncertainty around false negatives, or incidents that are not reported. Over 40% of the respondents are using only one of the available DLP configuration options, leaving them at risk of not getting enough visibility into potential data loss incidents. Even worse, 5% of the group said they did not know how the technology works!

- Organizations need to be more proactive in notifying users and sharing incident information. The majority of organizations are training their employees to consider the value of data they are processing. However, only 33% of organizations are sharing the outputs from their DLP solution outside of the security team. Without feedback, it is difficult to improve the protection of sensitive info.
- Organizations considered new project deployments (40%) and internal reorganizations (38%) to be the most likely causes of an increase in incidents, but the actual increases were reported to be 10% or less. The biggest percentage increases were caused by the least cited events: unpublished financial disclosures (25%), and employee use of social media (24%) were the most likely to trigger spikes of 20% or more in data loss incidents.

Critical components of DLP maturity

Set your DLP configuration to monitor and block incidents
Automated blocking of incidents not only reduces the load on the security team, it provides essential feedback to users to help change their behavior and reduce future incidents.

DLP implementations should use multiple data identification methods to catch incidents
Unstructured data, such as office documents, are increasingly the target of data theft, and may not be identified as confidential or sensitive if relying just on regular expressions. Additional methods, such as dictionaries and unstructured data analysis, are necessary to bring the security posture in line with today's attack methods, risks, and targets.

More incidents mean more visibility into data movement
More incidents are more work, but they also reduce the likelihood of false negatives and increase the probability that you will catch a data exfiltration. As the data loss prevention team gains experience with the nature of these incidents, they can use the advanced technique, such as user education, data classification, or automated blocking, to reduce them.

Make sure that you are watching multiple types of structured and unstructured data
While 48% of organizations are monitoring access to personal credit information, only 38% are watching employee and customer personally identifiable information and personal health information. These types of data are increasingly valuable to data thieves, and are making organizations of all kinds potential targets. The number of monitored activities has a strong effect on the number of daily incidents. Monitoring one activity generates an average of 17 daily incidents, whereas monitoring five activities generates an average of 58 daily incidents.

User education and ongoing feedback are necessary to change behavior
Relying solely on DLP products to identify and prevent data loss without the other training components does not appear to be the best approach. The vast majority of organizations are using DLP to reinforce data awareness, and are finding that this is helping to reduce the number of incidents. Unfortunately, many are not sharing the results of their DLP output with business leaders, potentially resulting in employees receiving contradictory information from the security team and their business leader.

Make sure that you are watching as many data movement vectors as possible
The majority of organizations are watching for suspicious uses of email. However, email is not the most likely vehicle for data exfiltration by internals. According to a previous Intel Security research study on data exfiltration methods, 26% of thefts by internal actors relied on stolen laptops or USB drives. Less than 40% of organizations had DLP visibility at the endpoint.

Important focus areas for future visibility

This study provides useful benchmarks that organizations can use to evaluate their DLP capabilities, configurations, staffing levels, and related data loss awareness and training activities. Understanding the underlying causes of data loss incidents and especially the activities that trigger fluctuations in the number of incidents are critical to building sustainable data loss

prevention methods. Knowing how your internal data moves provides the visibility to see attempted thefts when they are mimicking customer behavior or bypassing security controls, such as using unapproved apps or encryption where it is not needed.

An important result from the study is that regulatory compliance is no longer the number one reason for implementing DLP. Protecting data was cited by more than three quarters of respondents as their main reason for having a DLP solution. This is good news, because compliance is no guarantee of security and privacy. Instead, appropriate security and privacy controls are necessary to ensure data loss prevention, and thus compliance. At the same time, understanding and managing data was the least cited reason, and until this one moves to the top, data loss will likely continue to be a significant issue.

Data classification, finding and marking data throughout the organizations systems, remains an underused capability. For best results, data classification systems should offer a mix of automatic classification, using multiple data identification methods, and also manual classification that employees can use to augment the automated system. These classification prompts when creating or sharing documents provide additional training and awareness while employees go about their daily activities.

Conclusion

Data loss is a serious issue, continuing to affect many organizations around the world. All organizations are at risk, regardless of country, industry, or size. Visibility is at the core of data loss prevention, as you cannot protect what you do not detect. This means using multiple DLP configuration options to ensure that your corporate policies and procedures are being monitored and enforced. It also means deploying DLP solutions to cover data throughout the organization, at rest, in processing, and in motion, on the corporate network, endpoints, and clouds. Adequate staffing is also necessary to make all of this happen, whether that is developing the necessary configurations, processes, tuning them for optimal performance, or investigating incidents.

Visit **mcafee.com/DPbenchmarkstudy** to read the full report.