Best Practices in Data Protection

Survey of U.S. IT & IT Security Practitioners

Sponsored by McAfee

Independently conducted by Ponemon Institute LLC

Publication Date: October 2011

Best Practices in Data Protection

Survey of U.S. IT & IT Security Practitioners

Executive Summary
October 2011

Part 1: Introduction

Ponemon Institute is pleased to present the results of the *Best Practices in Data Protection* survey. This research was conducted to determine data protection practices in leading organizations and to provide guidance on how best practice status can be achieved. Sponsored by McAfee, the survey focused on issues relating to the use of data protection solutions such as endpoint encryption and data loss prevention within the workplace.

The study surveyed 718 IT and IT security practitioners in the United States. Respondents were asked to self-report if they believed their organization has achieved best practice status in data protection. Twenty-three percent or 168 respondents say their organization is an industry leader for data protection best practices.

Most of the respondents in our study (550) say their organization's mission is to achieve substantial compliance with regulations, laws, public standards, internal policies, procedures and agreements. These are referred to as "mainstream organizations" in this report. Eighty organizations that self-reported that they do the minimum as required by internal or external policies were excluded from the survey.

Survey respondents have an average of 10 years of experience in their field. More than half (53 percent) report directly to the CIO. The majority (81 percent) of respondents are at the supervisor or higher level in their organizations. Almost half (47 percent) work in organizations with a headcount of 5,000 or more.

We believe this study is important because it provides insights on how organizations can be more successful when investing in and building a data protection program. According to the findings of our research, the top three reasons why organizations support and fund data protection programs are:

- Need to comply with regulations, laws and other mandates.
- Response to a recent data breach incident within the organization.
- Public reports or news stories about data breach incidents concerning other companies.

Specifically, the study's findings reveal that the following are the five key success factors in a data protection program:

1. A formal data protection strategy for the organization and metrics to determine if the strategy is effective.
2. Key metrics from a management console and observation and regular testing of data protection solutions.
3. Data protection technology features that focus on privileged users, restriction of access and outbound communications are considered critical.
4. Centralized management of the data protection program with such features as actionable information, policy administration, reporting, automatic securing of endpoints and monitoring.
5. Automated policies for detection and prevention of end user misuse of information assets.

Part 2. Key overall findings

In this section, we present the consolidated findings for both best practice and mainstream organizations in our study. The research study report is organized according to these three main topics:

- The main drivers for the existence of a data protection program
- The steps taken by organizations in our study to mitigate risk to sensitive and confidential data
- The key success factors for a data protection program

The main drivers for data protection programs are compliance and response to a data breach incident. According to the findings, 50 percent of respondents agree or strongly agree that senior management in their organizations believes that the need to comply with regulations, laws and other mandates followed by response to a data breach incident are the main reasons senior management will fund and support a data protection program. Only 28 percent say it is because of a sense of responsibility to protect information assets, followed by 26 percent who say it is a desire to protect the company's reputation and maintain customer trust and loyalty.

When asked what information assets their organizations are most worried about if they had a data breach, respondents say they are most concerned about intellectual property and less concerned about consumer data**.** Lost or stolen source code, design documents and spreadsheets would present the most risk to organizations. Of least risk to these organizations is loss or theft of consumer data. In fact, more than half (57 percent) of respondents say their organizations' data protection effort is most concerned with safeguarding intellectual property.

Steps taken to mitigate risk are most often an approach that involves ongoing manual compliance monitoring and informal observations. Respondents identified the two greatest threats to their organization as the lack of data protection across all devices and the increased proliferation of end user devices containing sensitive data.

Currently the steps most taken to identify risks are ongoing manual compliance monitoring (62 percent of respondents), informal observations by supervisors and managers (59 percent of respondents) and ongoing automated compliance monitoring using a DLP tool (46 percent). Fifteen percent of respondents are not aware of the steps taken to identify risks.

According to 44 percent of respondents, the greatest benefits of a data loss prevention solution and endpoint encryption is to reduce the risks associated with mobile workers and their use of portable computing devices. These benefits are followed by 39 percent of respondents who say the greatest benefit is enhanced end-user accountability.

According to the majority of respondents in our study, endpoint encryption (EE) and data loss prevention (DLP) are critical to achieving their security objectives. However, these solutions are not widely deployed. Sixty-nine percent of respondents say EE and DLP are either very important or important to achieving their security goals. On average, respondents say that 41 percent of their organizations' endpoints are secured using EE. Fifty-one percent of respondents say that DLP has either not been implemented or only partially implemented.

Barriers and key success factors to achieving best practices. The most significant barriers to having a successful data protection program are lack of monitoring and enforcement of end users, complexity of compliance and regulatory requirements and lack of skilled or expert personnel. Only nine percent say it is the lack of effective data protection solutions.

The following are five key success factors identified by respondents who self-reported that they are their industry's leader for data protection best practices. The analysis below describes the current state of all organizations in our study to adopt these key success factors. In Part 3 of this paper we analyze the differences between the industry leaders and the mainstream respondents.

1. **Strategy.** Many organizations are lacking a formal strategy to determine if they are effective in addressing threats to their information assets. Only 19 percent of organizations in our study have a formal strategy that is deployed across the enterprise and 26 percent have a strategy that is partially implemented. Thirty percent of respondents say they have an informal strategy and 25 percent say they have no data protection strategy.

2. **Metrics.** Key metrics from a management console and observation and regular testing of data protection solutions are the top two ways organizations determine if their data protection solutions are effective at minimizing data loss.

   Fifty percent say they have no specific metrics for determining the effectiveness of data protection efforts and six percent are unsure. The most popular metrics used by respondents are percentage of endpoints secured with encryption and other data protection tools, number of end users trained, number of records or files detected as compliance infractions and number of policy violations**.**

3. **Data protection technology features that focus on privileged users, restriction of access and outbound communications are considered critical.** According to 76 percent of respondents, the most important feature of a data protection technology is to be able to conduct close surveillance of privileged users.

   This feature is followed by 74 percent who say it is to restrict access to sensitive data, 73 percent who say it is to prevent questionable or suspicious outbound communications and 72 percent who say it is to prevent or curtail insecure endpoints from accessing sensitive applications or systems. Considered less important are identifying where sensitive or confidential information is located (48 percent) and prioritizing of threats and vulnerabilities (44 percent).

   In terms of governance and controls practices considered, organizations believe vendor or business partner data protection management procedures and monitoring of business partners, vendors and other third parties are most important.

4. **Centralized Management.** Success of a data protection program is dependent upon centralized management, according to the majority of respondents. Sixty-five percent of respondents say that centralized management is considered very important or important to the success of data protection efforts. The top five factors essential to centralized management are: actionable information, policy administration, reporting, automatic securing of endpoints and monitoring.

5. **Automated Policies.** More than half (53 percent) of organizations in this study agree that automated policies are much more effective in terms of detecting or preventing end user misuse of information assets than manual methods. This is followed by 49 percent who believe enforcement of policies is among the most important deterrent to end user misuse.

Part 3. Best Practice Organizations Vs. Mainstream Organizations

In this section, we look at what separates the best practice organizations from the mainstream organizations. In many cases, best practice and mainstream organizations perceive data protection practices quite differently. The following are the most salient differences between a best practice organization and a mainstream organization in this study.

Executive Sponsorship. Organizations with best practices are better able to secure C-level and senior management support and funding because there is a greater sense of responsibility for the protection of information assets and a desire to protect the company's good reputation. In contrast, mainstream organizations secure funding and support because of such external factors as compliance, the need to respond to a data breach and as a result of negative publicity.

Proactive, Internally Driven Goals. The leadership of best practice organizations understands the importance of safeguarding sensitive and confidential information. C-level executives are more likely to consider data protection a top priority in best practice organization (55 percent vs. 35 percent of mainstream organizations).

Endpoint Solutions. Data loss prevention (DLP) and endpoint encryption (EE) are more important to a best practice organization's security mission. In best practice organizations, 76 percent of respondents say DLP is important and 75 percent say EE is important to meeting their security objectives. In contrast, 67 percent in mainstream organizations say these solutions are important. Further, best practice organizations are more likely to believe the mandatory use of endpoint encryption is among the most effective ways to reduce data loss (52 percent vs. 44 percent of mainstream organizations).

Effectiveness. Determining effectiveness of data protection solutions differs between best practice and mainstream organizations. Best practice organizations are most likely to use key metrics from a management console (60 percent vs. 38 percent of mainstream organizations) and results from internal or external audits (20 percent vs. 11 percent of mainstream organizations). Best practice organizations are also most likely to see reduced risks associated with mobile workers and their use of portable computing devices as one of the most important benefits of data protection solutions.

Vendors. Both best practice and mainstream organizations agree that vendor support and scalability are important features when making a DLP or endpoint encryption purchase decision. However, mainstream organizations are more likely to consider cost as an important feature. Best practice organizations consider vendor support as most important. In addition, best practice organizations favor the consolidation of data protection vendors to reduce complexity of IT security operations (49 percent vs. 41 percent of mainstream organizations).

Responsible Group. IT security often plays a more important role in data protection in best practice organizations. Twenty-five percent of respondents from best practice companies say that IT security is most responsible for setting strategy, overseeing deployment and ongoing management of data protection activities. In contrast, only 15 percent of mainstream organizations say this is the case.

Strategy. Best practice organizations are most likely to have some type of formal strategy for data protection. Sixty-four percent of respondents in best practice organizations say that they have a formal strategy that is partially or fully deployed across the enterprise. Twenty-eight percent of respondents in mainstream organizations say they do not have a data protection strategy and 33 percent say it is informal. Best practice organizations also are more likely to view data protection as having a higher priority than other security practices.

Barriers. Best practice organizations have different perceptions about what are the most significant barriers to achieving effective data protection. The top two barriers, according to best practice respondents, are dealing with the complexity of compliance and regulatory requirements followed by lack of leadership. Mainstream organizations are more likely to see lack of monitoring and enforcement of end users as a barrier. Best practice organizations are less likely to see insufficient resources or budget as a barrier.

Identifying Risk. Steps taken to identify data protection risk also differ. Specifically, best practice organizations favor ongoing automated compliance monitoring using DLP and respondents in mainstream organizations favor ongoing manual compliance monitoring. Best practice organizations also are more likely to conduct formal risk assessments.

Metrics. Best practice organizations are more likely to have metrics in place to determine the effectiveness of their efforts. The top two metrics they use are the percentage of endpoints secured with encryption and other data protection tools followed by the number of records or files detected as compliance infractions.

Policies. Best practice organizations are more likely to consider the enforcement of policies as among the most important deterrents to end users' misuse of information assets (56 percent vs. 47 percent of mainstream organizations). They also believe automated policies are much more effective in terms of detecting or preventing end user misuse of information assets than other methods.

Part 4: Insights and Implications

Taken all together, the findings of this research suggest that small improvements in a company's data protection practices can provide substantial benefits in terms of loss prevention, reputation or brand protection and other negative consequences caused by data breach.

In general, we find that enabling security technologies are important and should be used concurrently with other data protection practices in order to move a company into the zone of best practices. Other steps have to be taken concurrently, especially:

- Create a formal, enterprise-wide strategy with appropriate policies, procedures and guidelines.
- Implement education, training and awareness activities.
- Deploy monitoring and enforcement practices.
- Automate policies for detection and prevention of end user misuse of information assets.
- Consolidate the data protection program with centralized management with such features as actionable information, policy administration, reporting, automatic securing of endpoints and monitoring.
- Measure with key metrics from management console and observation and regular testing of data protection solutions.

In addition, the complexity of data protection activities or operations within the typical organization requires clearly defined governance practices, in-house expertise, unambiguous leadership and support from the top (preferably the CEO).

Finally, our results support the notion that data loss prevention and endpoint encryption solutions can significantly impact an organization's data protection and information security posture. The majority of respondents say EE and DLP are critical to achieving their security objectives.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO),** we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

McAfee

Delivering Comprehensive Data Protection and Management

McAfee delivers a comprehensive range of endpoint data protection solutions with an integrated, centralized management platform to protect against loss, theft or unauthorized access and transfer of confidential information.

McAfee endpoint encryption and DLP solutions enable strong encryption, access control, user behavior monitoring, and policy-driven security. The McAfee® ePolicy Orchestrator® (McAfee ePO™) management platform provides centralized management, policy administration, monitoring, automation and reporting, proof of protection, and actionable security analytics that delivers comprehensive visibility of an enterprise's security posture.