The Cost-Based Business Case for DLP

Aberdeen’s benchmark research in Data Loss Prevention (DLP) has shown that technologies to protect sensitive data against loss or exposure can indeed be deployed in a cost-effective manner, but business justifications for data protection can still be elusive. Because it is both quantified and business-oriented, identifying business value based on reducing the total cost of data protection is perhaps the most compelling way to make the business case for investments in DLP to safeguard your critical data. Leading the way are reducing the number of actual data loss or data exposure incidents, and reducing the number of audit deficiencies related to safeguarding sensitive data.

Business Context: If You Have to Do IT, Do IT Well

For most companies, current economic conditions amplify the relentless challenge of staying ahead of the vulnerabilities in their computing infrastructure, and protecting against the corresponding threats to their networks, systems, software and data. As noted in Secure, Compliant, and Well-Managed: The IT Security Approach to GRC (February 2009), Aberdeen’s research indicates overall budgets tightening in 2009, information technology (IT) budgets staying flat, and headcount slightly down compared to 2008. At the same time, budgets for security and security-related compliance are up – as are, unfortunately, the average number of security-related incidents over the past 12 months.

This creates a real problem: flat spending on information technology, and increased spending on security and compliance (viewed as a subset of the IT budget), literally squeezes out the organization’s ability to deliver new products and services. Yet organic revenue growth was identified as the leading organizational goal for 2009, and develop new products and services was second on the list of leading strategies (behind only improve operational execution). The widely-used phrase "do more with less" sums up the implied strategy for success – but how?

Skimping on security seems to be the wrong approach. For example, findings from The 2009 Aberdeen Report estimate the average financial impact of each data loss incident at $640K. The top 20% of all respondents in that study experienced 15% fewer actual data loss incidents over the last 12 months compared to the bottom 30%, which translates to a significant financial incentive to improve IT security for protecting data. Cutting corners on compliance seems an equally poor choice, at least to the extent that there is material cost or a meaningful stigma to non-compliance – or to the extent that the enforcement of regulatory compliance has "teeth."

www.aberdeen.com Fax: 617 723 7897
In Aberdeen’s IT Security research, the example provided by Best-in-Class (top 20%) organizations illustrates that once the business processes for security or compliance are accepted as tasks that must be done, the top-performing companies seek to optimize them for efficiency, allocate resources to minimize total cost of ownership, and ensure that incremental investments are in alignment with their strategic objectives for the business. If you have to do it, do it as efficiently and cost-effectively as possible.

**Best-in-Class Approach to Safeguarding Critical Data**

Over the last two years, Aberdeen’s benchmark studies have consistently found that Best-in-Class organizations have developed an overall strategy to discover, classify, protect, and manage their sensitive information, wherever it flows:

- **At rest** in back-end systems (e.g., applications, databases, file shares, storage, backup, and archive)
- **In flight** on the network (e.g., email, web)
- **In use** at the endpoints (e.g., hard drives, USB drives, removable media, and mobile endpoint devices)

Compared to all other respondents, these top performers have successfully deployed and managed data protection technologies to reduce data loss / data exposure incidents, to reduce audit deficiencies related to data protection, and to reduce costs associated with ongoing operations. But in Aberdeen’s benchmark-based research methodology, enabling technologies such as DLP or encryption are only one part of the overall story. Since the same technologies are equally available to everyone, the fact that some companies are able to achieve significantly better results than others also lies partly in the policy, planning, process, and organizational elements of ongoing operations.

The following high-level sequence of steps – each of which could be the topic of its own detailed analysis and discussion – will help any business leader to quickly assess their organization’s current state of play with respect to safeguarding its critical data:

1. **Identify and classify your data.** You can’t protect what you don’t manage, and you can’t manage what you don’t know about.

2. **Prioritize your security control objectives** for these information assets as a function of risk, audit and compliance requirements. Not all data is worth being protected; you should prioritize the protection of the data with the greatest impact on the business.

3. **Establish consistent policies,** as part of overall approach to safeguarding sensitive data at rest in the back-end, in flight on the network, and in use at the endpoints. Data is flowing everywhere, all the time.

---

Determined the Best-in-Class

To distinguish Best-in-Class companies from Industry Average and Laggard organizations in data protection, Aberdeen typically uses the year-over-year changes in select performance criteria such as the following:

- Number of actual security-related incidents (e.g., data loss or data exposure)
- Number of non-compliance incidents (e.g., audit deficiencies)
- Cost-related metrics (e.g., number of help desk calls, number of full-time equivalent staff)

Companies with top performance based on these criteria earn "Best-in-Class" status. See the respective benchmark reports for details.
4. Select and deploy data protection solutions, which will likely include a combination of enabling technologies, including DLP, encryption, key management, enterprise rights management, and other content monitoring / filtering solutions.

5. Invest in documentation, awareness and training for end-users, who should be made fully aware of their responsibilities for protecting the organization's sensitive data. Investments in technologies such as DLP can be eroded by insufficient investments in the people and process side of successful implementation.

6. Assign clear ownership and accountability for data protection initiatives to an executive or cross-functional team. The "one throat to choke" principle is highly correlated with the achievement of top results.

7. Automate enforcement whenever reasonable, with notification to end-users; standardize audit, analysis, and reporting. Both will reinforce awareness of policies and expectations for behavior.

8. Measure and monitor regularly; drive continuous improvements by finding and eliminating root causes for exceptions, security events, and audit deficiencies.

Every organization is somewhere along this path, and for the business-oriented purchaser / decision maker this list should be helpful in asking the right questions – both internally and externally (e.g., of product and services providers) – about proposed solutions and implementation plans. See Aberdeen's benchmark studies on Data Loss Prevention (June 2008), PCI DSS and Protecting Cardholder Data (June 2008), Managing Encryption (October 2008), Protecting the Database (November 2008), Endpoint Security (March 2009), and Unstructured Data (June 2009) for deeper insights in these areas.

What is the Business Value of Preventing Data Loss?

Those who would advise that the sole business justification for data security is protecting against data loss or exposure – which is an unrewarded risk (see below) – take a far too limited view. This perspective unfairly positions data security strictly as a cost, for which the benefit of investment is "so far as we know, nothing happened."

A more accurate perspective would be that the business value of data protection is not only associated with the value of the data, but also can be intertwined in many cases with the value of the business processes which it supports. That is, security is frequently a critical enabler for a given business process, and untangling the protection from the process is not always possible. In addition, the business value both for data and for a given business process is truly in the eye of the beholder: it is application-specific, company-specific, and industry-specific.

What all this means is simply that the business value of data protection (or of IT Security in general) cannot be captured as the result of a single set of...
formulas or templates, into which one can simply plug numbers and compute the one right answer. Unfortunately, it’s more complex than that. The good news is that the business value of data protection can be reasonably estimated – and understood – by mere mortals.

**Identifying and Classifying Business Value**

Just as every organization has to identify and classify its data, they have to identify and classify the business value derived from investments in data protection. Two decades of industry experience, combined with findings from two dozen Aberdeen benchmark studies over the last two years, can be boiled down to just four high-level categories for potential business value from investments in IT Security: manage **risk**, achieve and sustain **compliance**, enhance **revenue**, and reduce **costs**. This simple but powerful framework is summarized in Table 1.

**Table 1: Identifying and Classifying Business Value**

<table>
<thead>
<tr>
<th>Four Categories for Potential Business Value from IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>More Difficult to Quantify</strong></td>
</tr>
<tr>
<td>Manage <strong>Risk</strong></td>
</tr>
<tr>
<td>Enhance <strong>Revenue</strong></td>
</tr>
<tr>
<td><strong>Easier to Quantify</strong></td>
</tr>
<tr>
<td>Achieve and Sustain <strong>Compliance</strong></td>
</tr>
<tr>
<td>Reduce <strong>Cost</strong></td>
</tr>
<tr>
<td><strong>Stronger Technical Orientation</strong></td>
</tr>
<tr>
<td><strong>Stronger Business Orientation</strong></td>
</tr>
</tbody>
</table>

In many organizations, the two columns in Table 1 can represent a fairly significant organizational "divide." The topics of risk and compliance have a stronger technical orientation, and those who are evaluating solutions and working to build business cases are often more comfortable working within these perspectives. On the other side, the audience interested in the revenue and cost perspectives has a stronger business orientation, and may not always appreciate the implications of compliance and risk. As Aberdeen has previously noted, the most valuable IT security professionals in the months and years to come will be those who can successfully interpret the implications of risk and compliance in a business context, and more importantly who can successfully drive actions that positively impact the business.
Looking at the rows of Table 1, the "two C's" (cost and compliance) are relatively easier to quantify, while the "two R's" (revenue and risk) typically require both qualitative and quantitative analysis.

Let's examine each of these four categories in turn for the potential business value to be derived from investments in data protection.

**Manage Risk**

There are two types of risk. The first is un.rewarded risk, for instance when companies are compelled to make investments in security to protect against data loss or to address regulatory compliance. The second is re.warded risk, which are those investments that (hopefully) create value for customers and ultimately enhance the business. For example, a company may launch a web portal designed to increase collaboration and reduce the cost of processing transactions with its worldwide network of value-added resellers. The rewarded risks are obviously the more desirable investments, and yet as noted above under current economic conditions many companies are painfully limited from investing in these areas. Aberdeen's research has shown that in the Best-in-Class view of IT security, “governance” is now starting to be driven by business objectives and rewarded risks, rather than by technology, compliance, and unrewarded risks. See Aberdeen’s benchmark study on *IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs* (May 2009) for additional insights.

There are four possible actions that can be taken with respect to risk: accept it, ignore it (which is the same as accepting it), assign it to someone else, or mitigate it using appropriate security controls.

Estimating a monetary value for the risk to an organization’s data is a function of the value of the information, the probability of occurrence of data loss or exposure, and the impact of each potential occurrence. As noted above, this assessment is further complicated by virtue of each use case being application-specific, company-specific, and industry-specific – precisely why it is in the "more difficult to quantify" row of Table 1! The most useful models will blend both qualitative and quantitative approaches to make these estimates. Here is a simple but effective checklist to identify the most obvious high-value information:

- Information that generates revenue, either directly or indirectly (e.g., subscriptions, programs, services)
- Information that pertains to future revenue streams (e.g., research, new product plans, marketing plans, customer databases, intellectual property)
- Information which is essential for the smooth running of the company (e.g., financial data, administrative data, operations data)
- Information which must be protected by law (e.g., personnel records, patient records, student records, cardholder data)

"We are now using security and risk principles across our entire environment. Security is finally becoming more of an attribute, rather than the specific technologies that we invest in. The executive staff as a whole is not interested in the technologies, but you can bet they're all interested in who has access to the company's critical information, and where they take it at night."

~ CIO, mid-size high-tech firm
Once information has been identified and classified as high-value, a reasonable attempt can be made to quantify the impact of various security-related risk scenarios, for example:

- **Monetary loss** – what would the financial impact be if there were a security-related disruption of accounting system data, which led to delays in billing and shipping? If there were a diversion of funds?

- **Productivity loss** – what would the financial impact be if a security breach caused a sustained disruption of internal processes and communications? If the organization lost the ability to communicate with customers?

- **Indirect loss** – what would the financial impact be if a security breach caused the loss of potential sales? The loss of competitive advantage? The impact of negative publicity? (Indirect losses are the most difficult to quantify, but Aberdeen’s benchmark research shows that they are consistently among the most compelling factors driving current investments in data protection.)

- **Legal exposure** – what would the financial impact be due to failure to meet contractual milestones? Due to failure to meet regulatory requirements for the protection of customer data?

It’s worth underscoring again that the impact of risk to high-value information comes to life in the context of a specific business process, and the role that security plays in enabling that process and protecting its critical information.

### Achieve and Sustain Compliance

Mention the word "compliance" and for most people regulatory compliance comes to mind, but there are also other categories; two are compulsory and two are voluntary:

- **Regulatory** compliance includes both industry-driven (e.g., the Payment Card Industry Data Security Standard, or PCI DSS) and government-driven (e.g., the Commonwealth of Massachusetts data privacy legislation, the European Union Data Protection Directive) examples.

- **Competitive** compliance can include service-level agreements with customers or business partners, and to some extent the need to keep up with the current practices and capabilities of the competition.

- **Industry Standards and Best Practices** includes policies based on widely accepted frameworks such as COBIT and ISO 27002. In Aberdeen’s IT security research, Best-in-Class organizations are consistently more likely than their counterparts to map their security risks and corresponding controls to a matrix of compliance requirements, not the other way around. Chasing SOX, then chasing PCI, then chasing the next set of compliance requirements...
can lead to both overlaps (resulting in higher cost) and gaps (resulting in increased security incidents, and increased audit deficiencies) in controls. This focuses undue attention and resources on the "checkbox" approach to compliance, and makes it much harder to succeed at the game of "do more with less." Frameworks such as COBIT or ISO provide a solid foundation for Best-in-Class policies and controls.

- **Internal** compliance refers to addressing internal policies; these may simply embody some or all of the above, but in some cases they can also embody company-specific "C-level mandates."

Investments in data protection solutions should also get full credit for the business value of avoiding the costs of non-compliance, as well as for reducing the costs of sustaining compliance (e.g., through better effectiveness, greater efficiencies, or a higher level of automation).

**Enhance Revenue**

Investments in security that can legitimately be viewed as critical enablers for innovation- or growth-oriented initiatives make extremely attractive business cases, and examples in the area of data protection are increasingly common. On the one hand, companies must accommodate an ever-increasing volume of data, increasing numbers of both internal and external end-users, and ever-higher end-user expectations that data should be accessible any time, anywhere, and from any networked device. On the other hand, companies must also deal with an ever-changing array of security threats and vulnerabilities, a growing number of channels for potential loss or exposure of sensitive data, and more stringent regulatory compliance requirements related to data protection. IT Security practitioners are often caught between the desire to leverage the data to streamline and enhance the flow of the business, and the simultaneous need to safeguard the data — the very lifeblood of the business. Examples of business value from these processes, which may only be captured if the data security issues are adequately addressed, include:

- **Incremental revenue** examples include cross-selling, up-selling, and the acquisition of new customers, faster time to active status and more transactions per customer, lower drop-off rates and higher retention.

- **Additional channels** can drive both revenue growth and more cost-effective means of service delivery.

- **Competitive advantage** where security can make a positive contribution to image and brand, reduce costs to the end-customer, and increase the speed and agility in rolling out new services.

To be very clear, data security by itself does not produce revenue. But security-enabled business processes can and do enhance revenue. As in the risk discussion above, the most useful models will blend both qualitative and quantitative approaches to make appropriate estimates of business value.

"In the wave of globalization and collaboration, security and risk management are starting to be seen as facilitators for change. They help to manage the risks that are associated with change. And the CEO and Board are hungry for change."

~ CIO, mid-size high tech firm
Reduce Cost

Because it is both quantified and business-oriented, identifying business value based on reducing cost is perhaps the most compelling and reliable way to make the business case for investments in IT security. Cost-based business value is typically expressed as some combination of the following:

- **Cost savings** – the new or improved business process is less expensive; the organization spends less than it did before.
- **Cost avoidance** – the new or improved business process scales to higher levels; the organization can avoid additional spending in support of new capabilities or expanded scale.
- **Efficiency** – the new or improved business process saves time; the organization can accomplish the same in with fewer resources.
- **Effectiveness** – the new or improved business process increases productivity; the organization can do more or different things with the resources it already has.

As one concrete example of traditional business processes which are ripe for harvesting cost-based business value if they are enabled with the appropriate protections for sensitive data, consider document-intensive industries such as financial services, insurance, and healthcare. Cost reductions based on convenience and accuracy – not to mention the drastic reductions in the "four P's" of paper, printing, postage, and processing – are compelling, but not without the proper safeguards for sensitive information. This is especially true for sensitive data in "unstructured" formats, such as files, documents, presentations, spreadsheets, web pages, email messages, instant messages, images, audio files, video files, and so on. See Aberdeen's June 2009 benchmark study on Security for Unstructured Data for additional insights in this area.

Focusing Squarely on Cost: Most Direct Path to Value

For many organizations, keeping the focus squarely on reducing the total costs related to safeguarding critical data is the simplest way to communicate the business value of investments in data protection initiatives to a business-oriented audience. Total cost of ownership (or TCO) for a given solution is generally thought of as in terms of three distinct components: the cost of acquisition, the cost of deployment, and the cost to of ongoing operation and management, as illustrated in Table 2.

Of these three, the **cost of ongoing management** is the category for which Aberdeen has the richest benchmark data, as will be discussed in the following section. This is also the category with the largest impact on TCO, in that the cost of acquisition and the cost of deployment are generally incurred once, while by definition the cost of ongoing management of data protection initiatives is incurred year after year.

For convenience, the rows of Table 2 are organized in four areas: Product, Plant, People and Process. **Product** represents the cost items that an
organization would get directly from the solutions providers competing for their business. Plant, People and Process represent the infrastructure, organizational, and process elements of successful technology deployments that are the focus of Aberdeen’s standard benchmark research methodology.

**Table 2: Simple TCO Framework for Data Loss Prevention Solutions**

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
<th>Cost of Acquisition</th>
<th>Cost of Deployment</th>
<th>Cost of Ongoing Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
<td><strong>Endpoints</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Servers / Appliances</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Software / Licenses</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Services</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Maintenance / Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Plant</strong></td>
<td><strong>Facilities</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Business continuity</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>People</strong></td>
<td><strong>Specialists</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Administrators</strong></td>
<td><strong>Training</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Help Desk</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td><strong>Design</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Develop</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Deploy</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Manage</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Initiative Timing / Lifecycle: t = 0

Source: Aberdeen Group, June 2009

Using DLP solutions as a specific example, some of the factors that can have a large impact on the cost of ongoing management include:

- **Product costs** – how many servers are needed to scan for sensitive data at rest in back-end systems, in flight on the network, or in use at the endpoints? Are dedicated servers required, or can existing servers with spare CPU cycles be leveraged? What additional network costs, if any, will be incurred?

- **People costs** – how many staff must be allocated to respond to incidents generated by the DLP system? What is the rate of false positives? Can the solution correlate related incidents? Does it integrate with Security Information and Event Management (SIEM) solutions for incident handling, or trouble ticketing systems for workflow remediation?
• **Process costs** – what is the cost of developing and enabling consistent policies to secure sensitive data? What is the cost to adapt these policies over as the security and compliance landscape changes? What are the costs associated with setting up servers and deploying agents to scan for sensitive data?

By expanding the notion of TCO to encompass the total cost of the data protection **initiative**, companies can balance the costs (investments) in specific data protection solutions against the cost savings, cost avoidance, efficiencies and effectiveness that result from successful implementations. In Aberdeen’s benchmarking process, for example, the quantifiable benefits of Best-in-Class performance in data protection initiatives are repeatedly found to include fewer data loss or data exposure incidents, fewer audit deficiencies, and reductions in the ongoing cost of management (e.g., fewer help desk calls, fewer full-time administrators), among others.

### Benchmarking the Cost Advantages of the Best-in-Class

The model provided in Table 1 and the subsequent discussion, used as a general framework, should help most organizations work their way through a meaningful process of discovery and classification of the business value of incremental investments in preventing data loss. As an adjunct (i.e., not as a replacement) to that process, the findings from Aberdeen’s benchmark studies represent a quick, fact-based way to quantify the potential business value of achieving Best-in-Class performance at data loss prevention.

**Example 1: Fewer Security-Related Incidents**

As one example of the cost-oriented benefits that can be balanced against the TCO of an investment in a specific data loss prevention solution, Aberdeen’s benchmark research in DLP showed the average number of data loss or data exposure incidents (of all types) in the last 12 months to be as follows:

- **Best-in-Class** (top 20% of all benchmark participants): seven incidents
- **Laggards** (bottom 30% of all benchmark participants): 25 incidents

More specifically, the research showed that the average number of data loss or data exposure incidents with **known financial impact** in the last 12 months was one for Best-in-Class organizations, and eight for Laggards. Based on an average financial impact of each data loss incident estimated at US$640,000, the advantage of achieving top performance in data loss prevention – i.e., the relative performance of the Best-in-Class companies in comparison to that of Laggards – translates to seven incidents per year, times US$640,000 per incident, or US$4.5 million per year.

**Example 2: Fewer Audit Deficiencies (i.e., non-compliance)**

As another example, Aberdeen’s benchmark research in PCI DSS showed the average number of audit deficiencies in the last 12 months related
specifically to Section 3 ("protect stored cardholder data") and Section 4 ("encrypt transmission of cardholder data across open, public networks") to be as follows:

- Best-in-Class: 11 incidents
- Laggards: 31 incidents

If left unaddressed, these audit deficiencies could leave the companies exposed to actual data loss or data exposure incidents, which leads to the calculations in Example 1. But investigating, addressing, and demonstrating successful remediation of these audit deficiencies also consumes valuable time and resources. Based on an average estimated US$7,000 per incident for remediation, the advantage of achieving top performance in PCI-related data protection – i.e., the relative performance of the Best-in-Class companies in comparison to that of Laggards – translates to 20 incidents per year, times US$7,000 per incident, or US$140,000 per year.

Case in Point - A Technology Leader Benefits from DLP

Version 1.0 of Microsoft's internal "information classification and data handling" project was not successful. When Olav Opedal, Sr. Security Program Manager at Microsoft was tasked with taking over the leadership for the second round of this executive-driven initiative, he asked for and was granted six months for planning, quantification, collaboration, and evangelization. "Less time would be required now," he said. "But success is actually more about the planning, evangelism, and so on than about the technology. The executive mandate card will only get you so far; you have to get buy-in at the ground level as well as collaborate among the many internal groups that provide services to one another."

Microsoft’s initiative to protect its sensitive information stemmed from the same drivers as any other large enterprise organization, including:

- Compliance with PCI DSS (Microsoft is a Level 1 Merchant, processing more than six million credit card transactions per year), SOX, and other regulatory requirements
- Protection of customer information
- Protection of the company's intellectual property and financial information

The task was all the more challenging based on the sheer scale of Microsoft’s operations: 30,000 file shares containing more than 100 terabytes of data; 106,000 end-users, and 120,000 SharePoint servers.

But Opedal took the time to define the scope of the project and the risks associated with the company’s information very carefully. Information was classified not based on whether it applied to this or that specific regulation, but on whether the level of impact it has on Microsoft's business was high, moderate, or low. In collaboration with Microsoft's financial department, risks for High Business Impact information were quantified, and the team

"DLP by itself isn’t going to solve your data protection problem, unless you have a good understanding of the problem up front, solid definitions and processes, and the proper resources allocated. Every successful DLP initiative will also hinge on working within the organization’s unique cultural considerations and constraints."

~ Olav Opedal, Sr. Security Program Manager, Microsoft
presented multiple options to Microsoft's executives regarding how to address the data protection problem.

Microsoft's selection of the RSA DLP Suite from RSA, The Security Division of EMC, was based in part on its accuracy in discovering the sensitive content in this massive sea of information. Opedal was also able to automate many aspects of the workflow necessary for the initiative by leveraging the APIs in the RSA DLP solutions – capabilities which have subsequently been incorporated into later RSA product releases. Amazingly, the entire DLP scanning operation at Microsoft is now managed by just two full-time staff – one in Redmond and one in India – which is enabled by the advanced grid processing and incremental scanning capabilities of the RSA DLP offering.

What's next on the project roadmap? Building on the project's success and momentum, Opedal is expanding the initiative to include email, databases, and applications. In addition, they plan to expand the initiative to integrate the RSA DLP solution with Microsoft Rights Management Services (RMS), starting with an initial forest supporting 5,000 users and then expanding systematically from there.

**Solutions Landscape**

Solution providers for data protection solutions such as DLP can range from smaller specialists to multi-billion dollar firms. Table 3 provides an illustrative list.

**Table 3: Solutions Landscape for Data Loss Prevention (illustrative)**

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Solution(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA, The Security Division of EMC</td>
<td>RSA Data Loss Prevention Suite 7.0</td>
<td>The RSA DLP Suite discovers, monitors and protects sensitive data from loss, leakage, or misuse whether in the datacenter, on the network, or at the endpoints.</td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Data Loss Prevention 9 (Vontu)</td>
<td>Symantec Data Loss Prevention is designed to discover, monitor, and protect confidential data wherever it is stored or used, across network, endpoint, and storage systems.</td>
</tr>
<tr>
<td>McAfee</td>
<td>McAfee Total Protection for Data</td>
<td>McAfee's Total Protection for Data suite incorporates data loss prevention, encryption, authentication, and policy-driven security controls to help prevent unauthorized access to sensitive information, wherever it flows.</td>
</tr>
<tr>
<td>Websense</td>
<td>Websense Data Security Suite</td>
<td>The Websense Data Security Suite integrates four modules to discover and classify the data which is distributed throughout the enterprise; to monitor who is using what data, and how; to protect data with policy-based controls; and to integrate with endpoint security.</td>
</tr>
<tr>
<td>CA</td>
<td>Orchestria Product Suite</td>
<td>The Orchestria Product Suite addresses data loss prevention at multiple control points – including network, email servers, endpoints, and stored data – while leveraging a common infrastructure and management platform.</td>
</tr>
</tbody>
</table>

Source: Aberdeen Group, June 2009
In Aberdeen's benchmark study on Security for Unstructured Data (June 2009), respondents indicated their current and planned use for the DLP solutions listed in Table 3 (among others), which provides the data for the high-level comparison of these solutions shown in Figure 1. The x-axis is an index that measures the brand awareness (aided) that the participants in the study had for the respective DLP solutions – basically, a measure of whether or not they had heard of it when mentioned. The y-axis is an index that measures the value that organizations had derived from their deployment of the respective DLP solutions – calculated based on the percentage of current users of that solution earning Best-in-Class, Industry Average, or Laggard status in Aberdeen's benchmark study. Figure 1 also indicates the total "footprint" of users for each DLP solution in the research dataset, which includes both current users and those who indicated planned deployments within the next 12 months.

The research shows that McAfee, Symantec, and RSA are currently the most visible DLP brands within Aberdeen's benchmark dataset. In terms of value derived, current users of the RSA DLP Suite edged out those of both McAfee and Symantec based on the benchmark results of the participants in the study. In other words, although the RSA DLP solution is not as well-known as those from McAfee and Symantec, RSA DLP users were found to be more likely to have achieved Best-in-Class performance.

Figure 1: Benchmarking Current Users of Selected DLP Solutions
Summary and Recommendations

Business leaders and teams charged with leading the initiative to safeguard an organization’s critical data should:

- **Ask the right questions.** Have we identified and classified our data? Have we prioritized our security control objectives as a function of risk, audit and compliance requirements? Have we established consistent policies as part of overall approach to safeguarding sensitive data at rest in the back-end, in flight on the network, and in use at the endpoints? These steps are important precursors to making a business case and selecting specific technologies and services.

- **Make the business case.** Although business value from investments in data protection can be derived from multiple perspectives – including managing risk, achieving and sustaining compliance, enhancing revenue, and reducing costs – Aberdeen has found that balancing the costs (investments) of specific data protection solutions against the cost savings, cost avoidance, efficiencies and effectiveness that result from successful implementations is perhaps the most straightforward path. The research shows that reducing the number of actual data loss or data exposure incidents, and reducing the number of audit deficiencies related to data protection, may by themselves be ample to make the business case for a data protection initiative.

- **Select the right solutions.** Technical capabilities and current functionality should be evaluated among several important vendor selection criteria, including TCO, technical architecture, roadmap and strategic vision, financial stability, trustworthiness and reputation, service and support, and evidence of success by current customers. As noted using DLP as a specific example, companies can move the business case from the generic to the specific by balancing the costs (investments) required for specific data protection solutions against the cost savings, cost avoidance, and efficiencies and effectiveness that result from successful implementations.

- **Commit to the overall program.** The companies with top performance in data protection initiatives allocate the time and resources necessary to succeed, well beyond the selection and deployment of enabling technologies. Investments in awareness and training, steady movement towards automated enforcement of policies, standardization of audit, analysis and reporting, and consistent measuring and monitoring are also highly correlated with the achievement of top results.

Over time, the most successful initiatives will achieve what is perhaps the most difficult outcome: to change the company’s culture regarding how it protects and manages its sensitive data.

"The most important thing [for DLP solutions] is that they are accurate, and that they are unobtrusive. The referee can be ugly, as long as he makes good calls, doesn’t make bad calls, and let’s the game go on.”

~ VP and Business Unit Manager, mid-size enterprise
For more information on this or other research topics, please visit www.aberdeen.com.

## Related Research

<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online Assessment for DLP: interactive assessment and benchmarking tool</td>
<td></td>
</tr>
<tr>
<td>To Serve and Protect: Solving the Problem of Security for Unstructured Data</td>
<td>June 2009</td>
</tr>
<tr>
<td>IT GRC: Managing Risk, Improving Visibility, and Reducing Operating Costs</td>
<td>May 2009</td>
</tr>
<tr>
<td>Endpoint Security, Endpoint Management: The Cost-Cutter’s Case for Convergence</td>
<td>March 2009</td>
</tr>
<tr>
<td>Leveraging Logs, Information and Events: Three Use Cases for What to Do with All That Data</td>
<td>March 2009</td>
</tr>
<tr>
<td>Secure, Compliant, and Well-Managed: The IT Security Approach to GRC</td>
<td>February 2009</td>
</tr>
<tr>
<td>Protecting the Database: When (Most of) the Eggs are in One Basket</td>
<td>November 2008</td>
</tr>
<tr>
<td>The Encryption Key Lifecycle</td>
<td>November 2008</td>
</tr>
<tr>
<td>Managing Encryption: The Keys to Your Success</td>
<td>October 2008</td>
</tr>
<tr>
<td>Making Progress in PCI Compliance: Protecting Data at Rest, in Motion, and in Use</td>
<td>September 2008</td>
</tr>
<tr>
<td>Data Loss Prevention: Little Leaks Sink the Ship</td>
<td>June 2008</td>
</tr>
<tr>
<td>PCI DSS and Protecting Cardholder Data</td>
<td>June 2008</td>
</tr>
<tr>
<td>Trusted Computing and Data Protection</td>
<td>February 2008</td>
</tr>
<tr>
<td>Automating Encryption Key Management</td>
<td>January 2008</td>
</tr>
<tr>
<td>Protecting Data at the Endpoints: Combating Lost / Stolen Laptops, Thumb-Sucking, Pod-Slurping, and Other Threats to Your Sensitive Data</td>
<td>December 2007</td>
</tr>
</tbody>
</table>

Author: Derek E. Brink, Vice President and Research Fellow, IT Security (Derek.Brink@aberdeen.com)

Since 1988, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.2 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen plays a key role of putting content in context for the global direct and targeted marketing company. Aberdeen’s analytical and independent view of the “customer optimization” process of Harte-Hanks (Information – Opportunity – Insight – Engagement – Interaction) extends the client value and accentuates the strategic role Harte-Hanks brings to the market. For additional information, visit Aberdeen http://www.aberdeen.com or call (617) 723-7890, or to learn more about Harte-Hanks, call (800) 456-9748 or go to http://www.harte-hanks.com.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.