



A Websense® White Paper

The ROI of Data Loss Prevention

Introduction

One data loss incident can result in continuous cost. After making affected customers whole, conducting an internal investigation, repairing any damage to internal systems, and dealing with expected litigation, you can count on external audits, increased regulatory oversight, and a damaged reputation to stay with you for a while.

Organizations that rely on intellectual property (IP) for sale and use are subject to more long-term and far-reaching costs when data is lost. IP is the heart of today's technology, manufacturing, pharmaceutical, and even financial firms, and their most coveted sustainable advantage. When lost, it can have a direct and immediate impact on both the R&D costs, and the revenue estimates for the full lifecycle of the asset.

Without question, a data leak is not a one-time cost. Even after your operations have recovered, effects of the data loss could continue to impact your business for a decade or longer. One mistake can have far-reaching consequences, and a serious leak may mean that your business never recovers—or at least never returns to “normal.”

Fortunately, the threat of a leak is significantly mitigated through the use of technology—specifically, a data loss prevention solution, which can provide a clear return on investment (ROI) and a manageable total cost of ownership. Data loss prevention provides a sound cost-avoidance strategy and can positively impact revenue—saving hundreds of millions of dollars with little upfront investment. The risk of business as usual is clear, as is the reward for implementing diligent data control and data loss prevention measures.

Table of Contents

- The Challenge..... 3
- Determining the True Cost of a Data Leak..... 4
 - Direct Costs..... 4
 - Indirect Costs..... 5
 - Cost Summary..... 6
- The Extended Economic Impact..... 7
- Implementing a DLP Solution..... 9
 - Direct Costs..... 9
 - Direct Revenue Benefits..... 12
- Websense Means Real ROI..... 13
 - Direct Costs..... 13
 - Indirect Costs..... 13
 - Cost Summary..... 13
- Conclusion..... 14
- About Websense, Inc. 15
- About the Author..... 15
- Table of Figures..... 15.

The Challenge

A data loss incident can result in lost opportunity. The current business climate favors the informed, making intellectual property (IP), customer records, and other sensitive information vital to your competitive advantage. A single leak—be it proprietary data leaked to the public domain or customer information to a competitor—can have catastrophic consequences, from the cost of near-term remediation to the long-term damage to your credibility in the marketplace. A single leak can haunt your company, eradicating, in moments, the goodwill you worked decades to create.

The cost to remediate data loss can be high and can grow with time. Measured against the total cost of a leak, the total cost of ownership (TCO) of a data loss prevention (DLP) solution reflects a substantial financial savings in the short-term and an evident competitive advantage throughout the life of your company. Yet, the simple steps required to protect sensitive data are often overlooked.

A survey by the Ponemon Institute reveals that 85 percent of companies interviewed had experienced some form of data loss in the previous 24 months (See Figure 1).¹ The vast majority of these incidents came from inside the organization. While only 6 percent resulted from criminal activity and 6 percent from malicious employees, 42 percent of incidents were caused by the misplacement of devices (often without knowing exactly what data was stored on them). Other causes were employee negligence and third-party breaches, at 16 percent and 10 percent respectively. IT mishaps caused 7 percent of breaches, and missing backup media accounted for 4 percent of breach events.

Causes of Security Breaches

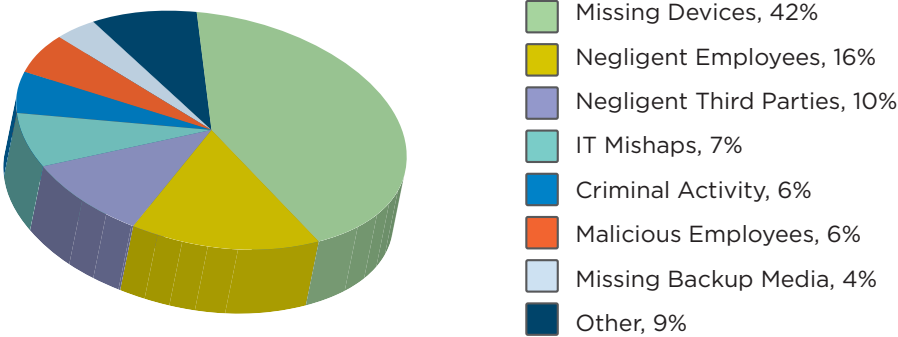


Figure 1: Causes of Security Breaches
Source: Ponemon Institute

¹ The Business Impact of Data Breach. Ponemon Institute LLC. May 15, 2007.

Determining the True Cost of a Data Leak

The loss of personally identifiable information (PII) and personal health information (PHI) carries great potential for financial loss. The risk of damage extends beyond your company, ultimately affecting customers, business partners, and other stakeholders. In response to such an incident, you are likely to face pressure from regulatory bodies, consumer watchdog organizations, and even the press. The possibility of litigation is significant, resulting in legal fees, a settlement or verdict, and other remedies that can affect your business for many years.

The direct costs resulting from a data loss incident of this kind typically consist of:

- The average cost per record associated with a leak to make affected parties whole
- Fees for legal representation
- Engaging a PR firm to minimize damage and restore reputation to the extent possible
- Consumer credit monitoring for all customers (not necessarily only those affected by the leak)
- Up to five years of system and process audits conducted by an independent third party

Intellectual property is a second, often overlooked category of data loss. Whether you are a computer chip manufacturer creating the next great processor or a Wall Street investment firm creating the next investment package of high-growth funds, intellectual property is the greatest competitive advantage a company has toward sustainability and profitability. Most IP data losses go unreported for two reasons: 1) there are no public disclosure laws, to date, that apply to intellectual property, and 2) the impact on valuation from a publicized loss would likely be tremendous.

The direct costs of intellectual property loss typically include:

- Fees for legal recourse to address who leaked the data and discover if it was being used inappropriately
- Short-term impact to R&D cost recuperation
 - Key variable(s): assets stage in its lifecycle
- Long-term impact to profitability/revenue projections
 - Key variable(s): assets stage in its lifecycle, reproducibility, market demand
- System and process audits to identify and correct the source of the data loss

Direct Costs

The cost of data loss can vary, especially as the far-reaching effects can be difficult to gauge. Forrester Research estimates that the average data leak results in \$1.5 million in economic damage, while The Ponemon Institute pegs the amount at \$4.8 million.² Ultimately, the cost of the data loss incident is determined by the size and nature of the organization, the sensitivity of the data that was lost, and the size of the incident itself.

Figure 2 outlines the major costs (according to Forrester Research) associated with data loss:

Cost Category	Description	Cost per Record
Discovery, response, and notification	Outside legal fees, customer notification, increased call center activity, marketing and PR, discounted product offers	\$50
Lost employee productivity	Employees diverted from normal duties, contractor labor	\$30
Restitution	Compensating affected customers for direct losses	\$30
Opportunity costs	Loss of future business opportunities	\$98
Total Direct Cost per Record		\$218

Figure 2: Direct Cost per Record of a Leak

A simple data leak that results in the loss of 100,000 customer records can turn into a direct and immediate cost of \$21.8 million. To put this number in perspective, an employee who generates \$1,000 in revenue per hour would have to work for 21,800 hours—a total of 109 years—in order to compensate for the loss.³

Indirect Costs

In the wake of data loss, an organization may face regulatory fines, additional security and audit requirements, and other liabilities that are directly related to the loss (e.g., replacement cards in the credit card business). In some states, compensating credit-bearing institutions for a loss that was the result of another organization is or may soon be a legal requirement. Such additional, indirect costs can exceed \$10 million, resulting in an average cost of \$2 million a year over an estimated five-year data loss impact.

In addition, a cost often overlooked in analyses of data loss impact costs relates to professional services. After a data loss event, organizations may face two costly professional service engagements: Periodic audits and process redesign.

Periodic audits may be imposed by regulatory bodies (as the Federal Trade Commission did to DSW in 2005), making the cost unavoidable and requiring the services of an independent third party. In DSW's case, the FTC required bi-annual audits for 20 years, though some cases have only required annual audits for five years. A third-party audit can cost a minimum of \$500,000 (note: the firm conducting the audit is not likely to have incentive to discount rates aggressively). If an annual audit is required for five years, the total cost can exceed \$2.5 million.

3. The author has only discussed direct costs of customer data to avoid confusion. It is difficult to calculate the impact of a loss of IP, simply because the loss is as unique as the asset, and any loss should be determined by the affected organization by those who are privy to such data points as: time R&D, cost, asset life start date, asset projected end life date, new asset projected end life date, forecasted revenue associated with asset, adjusted revenue associated with asset, expected profit margin, impact to operating margin, impact to profit margin, impact to sales (by region), impact to corollary IP/products, uniqueness of IP, reproducibility, market demand (by region), existing

Process redesign is a cost that can catch an organization by surprise. A periodic audit only ensures that its processes are effective in preventing future data loss, but the loss itself indicates that changes are necessary. In order to redefine information technology operations, particularly in regard to information security, an organization needs to engage a strategy and operations (S&O) consulting firm to develop and implement a new operational model. Typically, the cost of this type of S&O engagement can exceed \$1.5 million and takes two years to implement.

Cost Summary

Thus, the direct cost of a 100,000-record leak could amount to a minimum of \$35.8 million over five years, averaging \$7.2 million per year (See Figures 3 and 4). This amount does not include future damage to your business such as:

- Loss of market share
- Inability to retain existing customers
- Inability to acquire new customers

Cost Category	Description
Direct costs (100,000 records X \$218 per record)	\$21.8 million
Fines	\$10 million
Audit fees (\$500,000 per year X 5 years)	\$2.5 million
S&O engagement	\$1.5 million
Total Estimated Remediation Cost	\$35.8 million
Average Cost per Year (over 5 years)	\$7.2 million

Figure 3: Total Estimated Cost of Leak Summary

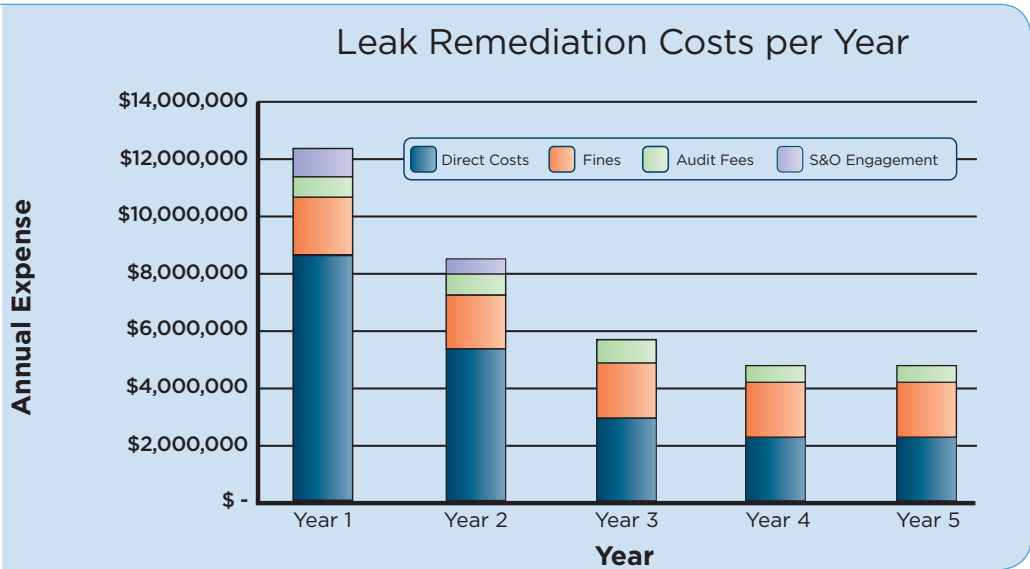


Figure 4: Estimated Leak Remediation Costs Over 5 Years

The Extended Economic Impact

The cost-per-record estimates from Forrester and Ponemon only address certain direct, indirect, and opportunity costs associated with the loss of customers affected by the leak. In high-profile cases, a company can expect to lose even more, as unaffected customers no longer find their business credible. Forrester estimates that a company can expect to lose up to 20 percent of their customer base because of a data loss. For a business with net annual sales of \$1 billion, with 80 percent of business coming from repeat customers, it can be devastating. If the business lost only 10 percent of repeat customers and saw a 20 percent decline in new customer acquisition, the net effect would be a revenue decline of \$120 million in the first full year following the loss (See Figure 5).

	Repeat Customers	New Customers	Total
Total annual revenue	\$800 million	\$200 million	\$1 billion
Lost business as a percentage of revenues	10%	20%	12%
Lost business in dollars	\$80 million	\$40 million	\$120 million

Figure 5: Estimated Revenue Impact of a Leak

The total economic impact could be a revenue decline of \$120 million, or a 12 percent drop in revenue the first year. Additionally, one must also consider that the costs to remedy the loss have led to higher expenses, putting substantial pressure on margins, percent-operating margin, and earnings per share (EPS). Before the leak, the company's expenses were compared against total revenues of \$1 billion. Post-loss, the \$1 billion is reduced by a hypothetical \$120 million in lost business and an estimated first year cost of \$12.2 million for loss remediation. Assuming other costs remain static, they have to be covered by \$867.8 million (\$1 billion less \$120 million less \$12.2 million) instead of the full \$1 billion.

Let us assume that this company has robust net margins of 20 percent, indicating a reasonable amount of operational efficiency. This would allow \$200 million to absorb the cost of the data loss. After lost business opportunities, only \$80 million in margin would be left to cover actual data loss costs. With an estimated first-year data loss cost of \$12.2 million, the net effect is a profit of only \$67.8 million when it otherwise would have been \$200 million; the loss results in a 66 percent drop in profits the first year. If the business can right itself in the wake of the loss incident, it can rely on revenue growth to absorb the costs for years two through five. However, reputation damage, pressure from watchdog groups, and negative media coverage are likely to constrain growth, ultimately making it difficult to absorb the costs of the loss from one year to the next. See Figure 6 for a breakdown of costs per year.

	Year 1	Year 2	Year 3	Year 4	Year 5
Annual Revenue (assuming 8% growth)	\$1,000,000,000	\$1,080,000,000	\$1,166,400,000	\$1,259,712,000	\$1,360,488,960
Annual Net Profit (assuming 20% margins)	\$200,000,000	\$216,000,000	\$233,280,000	\$251,942,400	\$272,097,792
Annual Leak Remediation Cost	\$12,220,000	\$8,450,000	\$5,770,000	\$4,680,000	\$4,680,000
Lost Business Costs	\$120,000,000	\$129,600,000	\$139,968,000	\$151,165,440	\$163,258,675
Total Leak-Related Losses	\$132,220,000	\$138,050,000	\$145,738,000	\$155,845,440	\$167,938,675
Resulting Annual Net Profit	\$67,780,000	\$77,950,000	\$87,542,000	\$96,096,960	\$104,159,117
Decline in Profitability Due to Leak	66%	64%	62%	62%	62%

Figure 6: Estimated Revenue Impact of a Leak Over Five Years

When you consider lost business opportunities and remediation costs within the context of revenue growth and stable net margins (before data loss costs), the long-term effects of the loss can be profound. As loss-related costs decline, the inability to attract new customers follows, resulting in estimated lost margin of 62 percent in the fifth year following the leak.

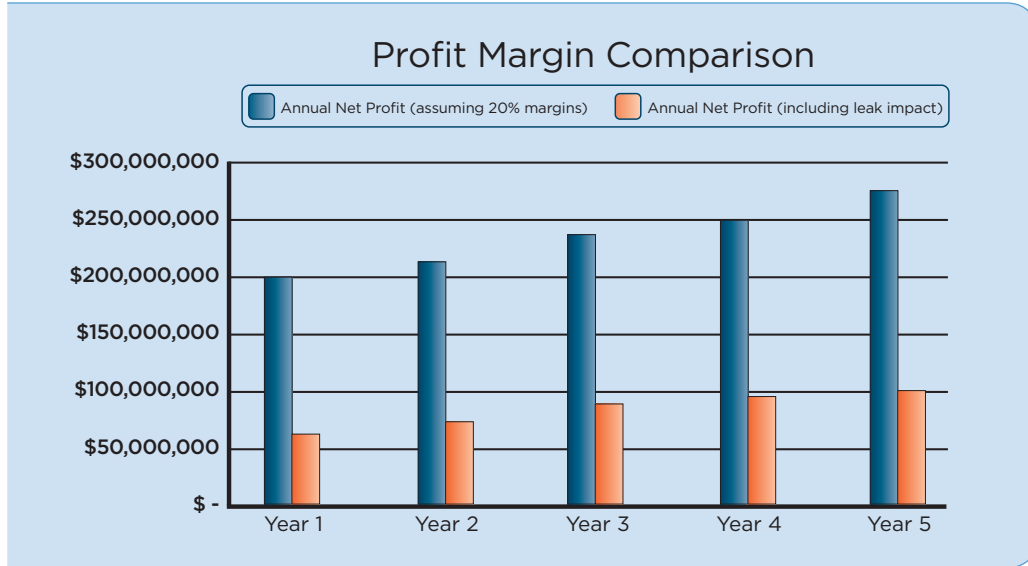


Figure 7: Estimated Impact to Profit Margin

Net profits are increasing every year, even after the leak impact is considered, but profits still reflect a net decline relative to what they would be if the loss had not occurred (See Figure 7). Implementing a DLP solution can save hundreds of millions of dollars with little up-front investment. DLP clearly delivers a cost-containment opportunity in a business environment characterized by both the unintentional information management accidents and by the threat of externally initiated data theft.

Implementing a DLP Solution

As Figure 6 shows, a company can suffer substantial losses because of a single loss event. For a \$1 billion company, for example, the economic loss could exceed \$100 million. While it is possible to protect against data loss, the cost of prevention is an obvious concern. What sort of investment delivers a return of more than \$100 million?

An investment in DLP software covers three categories:

- Software costs
- Installation and configuration costs
- Ongoing system administration and management

Direct Costs

Software costs consist of the fees necessary to acquire the software for use in the enterprise. Installation and configuration addresses how that software is put to work. This may include professional services support from the software vendor, as well as third-party consultants or additional software (such as integration utilities) needed to ensure that the DLP software meets the company's requirements. Ongoing system administration and management involves the daily expense of using the DLP solution, from power to system administrators to impact on business efficiency.

The cost of software varies based on the size and nature of the organization purchasing it, but Websense® estimates that a 10,000-user organization may spend \$17.50 per year, per employee on a DLP solution. Therefore, if you have 10,000 employees, expect to pay approximately \$175,000 in software fees per year.

While DLP software does automate the identification and prevention of potential data leaks, human involvement is necessary to:

- Oversee and manage the process
- Implement and enforce policy
- Handle exceptions
- Report on progress to key executives
- Identify and implement continued improvements to processes

Generally, an organization does not dedicate a single resource to DLP system administration; instead, these responsibilities are distributed across a number of team members who share both DLP administration roles and other information security roles in the Information Technology department. Websense advises that one full-time employee (FTE) administrator should serve up to 50,000 employees. Thus, in an organization with more than 200,000 employees, four FTEs would be appropriate. For extremely large organizations with straightforward data security policies, it may be possible to leverage economies of scale and reduce the administrator footprint in the organization.

Cost Category	Cost
Software per Year	\$175,000
Installation and configuration (i.e. professional services for the first year)	\$175,000
Administration and management (first year)	\$35,000
Total First Year Investment	\$385,000

Figure 8: DLP Estimated Cost Categories

After the implementation of a DLP solution, the environment must be managed in order to yield continuous results. Using a subscription model, the annual cost of the DLP solution is approximately \$175,000. For the first year, the total cost of DLP is \$385,000 which includes a comprehensive view of implementation. Ongoing management consists of the annual subscription fee for the DLP solution (\$175,000) and the cost of headcount to manage the DLP environment. Given that the technology involves a subscription model, the annual investment in DLP is typically an operational expenditure rather than a capital expenditure, facilitating budgeting activity and accounting practices.

The cost of data protection and management can be reduced through the deployment of a network-based solution rather than sole reliance on installing software at endpoints. Central management facilitates the rigorous enforcement of policy and protection of data in a manner that delivers economies of scale. Endpoint deployments require active management across the enterprise, which often leads to higher costs, increased likelihood of error, and the assumption of greater risk.

Of course, effective DLP programs require a certain amount of administrator involvement, even if a centralized model is used. However, the central implementation of a well-planned rules framework can reduce that cost substantially. Websense estimates that the practitioner cost of ongoing DLP system management is approximately \$18,750 per year, based on an hour of direct time applied to DLP management each week by an organization’s director of IT security (at \$75 per hour) and six hours of time by an IT security engineer each week (at a cost of \$50 per hour). Thus, the total cost of DLP management is a mere \$375 per week. Compared to the cost of a single security breach, the advantages of prevention are significant.

Cost Category	Director of IT Security	IT Security Engineer
Hours per Week	1	6
Cost per Hour	\$75	\$50
Cost per Week	\$75	\$50
Total Cost per Year (@ 50 weeks/year)	\$3,750	\$15,000
Total Cost		\$18,570

Figure 9: DLP Estimated Headcount Costs

After the implementation year, the annual cost of DLP is approximately \$200,000, which includes technology and administration. The technology component is fixed, but administration is variable. Some years see a higher investment as a result of improvement to business logic or other upgrades, but these costs are offset by the operational advantages they yield. In general, the annual cost of data management is linear after the year of implementation (See Figure 10).

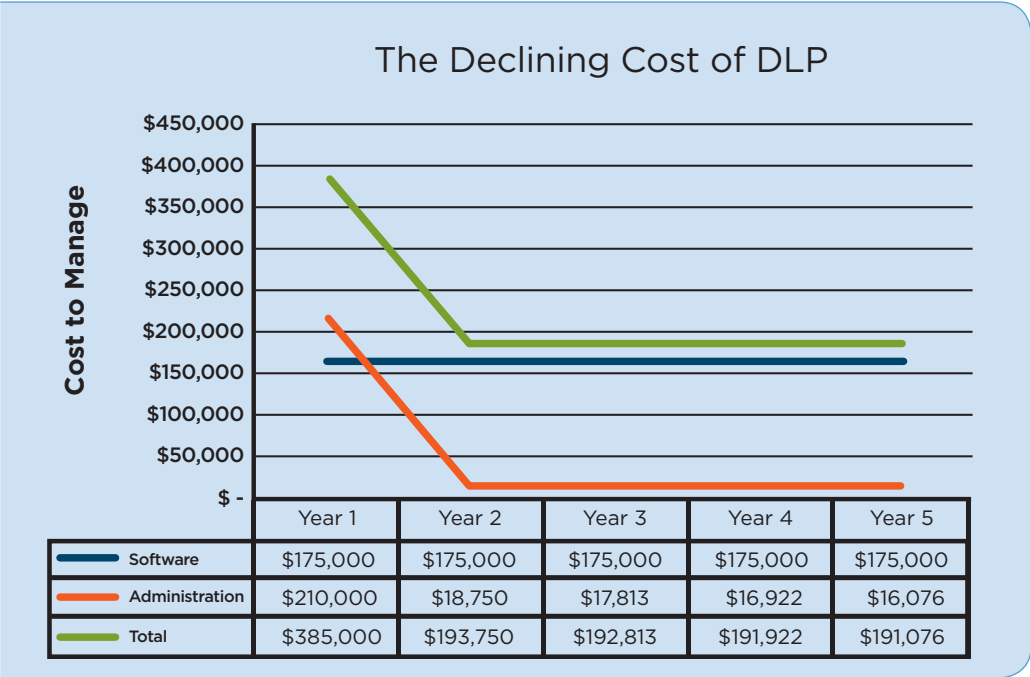


Figure 10: Declining Cost of DLP

This projection includes an annual decline of 5 percent in administration expenses after the first year to account for the accumulation of institutional knowledge. Quite simply, as an organization gets better at data loss protection, the process becomes less expensive.

DLP, as a percentage of the total data loss financial risk to which a company is exposed, is extremely cost-effective. In fact, DLP becomes more cost effective every year. From one year to the next, company growth increases the impact of a data leak, but also the operational efficiency of the DLP solution.

	Year 1	Year 2	Year 3	Year 4	Year 5
Total Leak-Related Losses	\$132,220,000	\$138,050,000	\$145,738,000	\$155,845,440	\$167,938,675
Total Cost of DLP	\$385,000	\$193,750	\$192,813	\$191,922	\$191,076
DLP as a % of Total Risk	0.29%	0.14%	0.13%	0.12%	0.11%

Figure 11: DLP as a Percent of Total Risk

The case for prevention is evident. For less than a half a percent of the risk to which a company is exposed, it can protect itself. Hundreds of thousands of dollars in expenses can lead to hundreds of millions of dollars in savings, every year.

Direct Revenue Benefits

Organizations that have implemented DLP solutions also derive extra value from their implementation by refining business processes and addressing operational inefficiencies. The key to maximizing the positive impact on revenue is focusing on affirmative business processes while identifying and fixing those that are broken. Many organizations have documented processes clearly but lack a monitoring and control mechanism to regulate written policy. Others have processes that restrict business but are required to mitigate risks. Without a control mechanism, once efficient processes often fall victim to employee vices (e.g., absent-mindedness, carelessness, ignorance, inconsistency, indecision, etc.).

There are two primary benefits to maximizing affirmative business processes and remediating those that are broken: 1) efficiency, and 2) effectiveness. By focusing on a core set of critical affirmative business processes, you can audit and enforce your processes with a DLP solution, helping to ensure that the organization is following the most efficient workflow possible and working toward maximum operational efficiency and increased transactions/volume. In addition, DLP solutions give you situational awareness to identify who is sending what data, where, and how, providing actionable intelligence to identify and remediate broken business processes. A more efficient business is a more capable and competitive enterprise. The second benefit, increased effectiveness, most closely translates to reduced operating margin—net savings, increased profits, etc. By increasing the effectiveness of affirmative business processes, you can decrease such variables as cost of sale, sales cycle, margin cost, cost per transaction, and thus guarantee an increase in rate of return, return on investment, etc.

The above described direct revenue benefits are illustrated in the following example of a fictitious Wall Street investment brokerage firm. The firm has a policy that encourages employees to use the Internet to research and gather investment and market information. The Internet is a key tool for analysts to keep track of investments, trends, and market-changing events. However, the policy has a specific parameter that prohibits employees from visiting social networking Web sites (e.g., blogs, chat boards, etc.) during work hours. The reason: the risk of employees posting confidential data on customers/investments is too great for the firm to accept. As a result, its financial analysts are barred from a great source of real-time investment/market information, and are either forced to uncover the information by other means (inefficient) or go without it, at a disadvantage to other analysts (ineffective). However, with a DLP solution that includes awareness and controls for users, data, and their destinations, the firm can set a control for an affirmative business policy that says, “A financial analyst can visit any blog or chat board, but cannot post confidential data to the site.” The policy can be applied to specific users, data types, destinations, and even categorically (e.g., all financial analysts, all chat boards, all confidential data). Thus, the affirmative business process is enabled, yet secured, making the employees both more efficient and effective for their customers, and potentially having a marked influence on revenue.

Direct revenue benefits are based on the specific business processes and operational inefficiencies addressed, and are unique to each specific organization. As such, no specific amounts will be aggregated into the model in this paper. The reader should, however be sure to account for such direct benefits when determining a ROI and should use the benefit to offset the cost of the solution.

Websense Means Real ROI

What does it cost to protect more than \$100 million in new business annually? To recover more than 60 percent of your net profits for more than a decade? For an organization with 10,000 employees, an initial investment of \$1 million provides the procedural and technological rigor necessary to keep customer records secure and proprietary data inside the company's walls.

The loss of data has the potential to alter a business completely, especially in a business climate characterized by increasing competition and rapid product obsolescence. Most leaks are preventable, through the implementation of DLP solutions and corresponding governance models, which can be used as the backbone of improved operations that reduce risk while delivering a competitive advantage.

Websense is unique in its approach to DLP. Websense has long been a content security provider, as the leader in Web filtering and Web security—protecting organizations from where their employees go on the Web, downloading malicious code (whether knowingly or not), and improving overall productivity. With Websense Data Security Suite, organizations get the market's most advanced DLP solution to discover data stored throughout the enterprise, monitor its use over a broad array of communication channels, and protect it, with business-centric controls that map to real business processes. What is unique to Websense DLP that no other vendor can deliver are three core components: detection accuracy, policy framework, and solution coverage.

Detection Accuracy

Websense Data Security Suite accurately discovers network shares and the data stored on them throughout the enterprise. The solution uses patented technology to analyze and report on the data, looking deep into the file and using advanced, proprietary technology to accurately classify the data—whether structured or unstructured. It includes patented fingerprinting technology that automatically integrates with databases and file repositories to discover and classify data on a recurring basis, without administrator intervention. A more accurate solution translates into fewer false positives and negatives, lowering administrative costs, overall cost of ownership, and delivering a faster, higher rate of return on your investment.

Solution Coverage

Websense Data Security Suite protects virtually all forms of data, including simple forms such as SSNs, birth dates, and accounts numbers, as well as complex forms such as CAD drawings, business plans, and other proprietary types. It also provides monitoring and protection for internal communications because quite external leaks are often precipitated by internal leaks, where borders are less secure and employees have greater access. The solution also provides coverage for over 250 built-in regulatory and policy templates for worldwide coverage, enabling administrators to apply policies to new geographies, regulations, and governance controls with the click of a button, as well as the ability to customize and/or create new policies unique to your organization. Websense Data Security Suite delivers unparalleled coverage for your business needs today and tomorrow, and helps ensure you continue to see a return on your investment in the years to come.

Policy Framework

Websense Data Security Suite intelligently maps data policies to business processes. The solution can discover broken business processes and provide a remedy. It includes intelligent, automated workflows to secure data and educate employees, which reduces help desk calls and administrator intervention, and solves what is fundamentally a business problem rather than an IT problem. Websense policy framework is unique in its ability to manage who can send what data, where, and how. This framework builds on over a dozen years of monitoring user activity on the Web, and integrates destination awareness from Websense Web filtering and Web security solutions with Websense Data Security Suite. Only Websense can enable policy controls with the click of a button to block sensitive data from going

to blogs, chat boards, phishing, gambling or other sites. Conversely, only Websense can authorize, with the click of a button, the transmission of patient records to an authorized partner, but only over encrypted email and automatically enforce the email's encryption. This intelligent policy framework, depicted in Figure 12, is not only unique to Websense, but is the cornerstone of an effective DLP solution—real policy controls for real business processes.

Who	What	Where	How
Human Resources	Source Code	Benefits Provider	File Transfer
Customer Service	Business Plans	Internet Auction	Web
Marketing	Employee Information	Business Partner	Instant Messaging
Finance	M&A Plans	Blog	Peer-to-Peer
Accounting	Patient Information	Customer	Email
Sales	Financial Statements	Spyware Site	Network Printing
Legal	Customer Records	North Korea	
Technical Support	Technical Documentation	Competitor	
Engineering	Competitive Information	Analyst	

Figure 12: Advanced Policy Framework

Many of the cases covered in this document reflect possibility more than certainty. If data loss occurs, the impact could exceed hundreds of millions of dollars. It might not happen to you. However, as businesses become more complex, experience employee turnover, and have to face the cleverness of hackers, the risk of a data loss increases. A relatively small price affords disproportionate protection.

Conclusion

Ultimately, every business seeks a competitive advantage. For the data-driven company, data protection and DLP increase the protection of sensitive data and deliver a foundation for aggressive growth. The cost reduction associated with data protection and process improvement frees operating capital for investment in the company's growth opportunities. Instead of reacting to data loss events, funds can be redirected to initiatives that attract clients, increase sales, and otherwise advance the business. Data that is not leaked retains its value longer. Once sensitive data leaves the company, its value can be decimated—along with the competitive advantage it offered.

Websense focuses on the normal flow of business. Instead of locking down your data and preventing employees from doing their jobs or allowing the free flow of data without any control, Websense is able to deliver business-centric security. Protect the data in your enterprise, but do not disrupt the business process.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, messaging and data protection technologies, provides Essential Information Protection for more than 42 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information, and enforce Internet use and security policies. For more information, visit www.websense.com and

Sign up for security alerts and threat reports:
<http://www.websense.com/securitylabs/>

View solution information and supporting educational materials:
<http://www.websense.com/global/en/ProductsServices/>

Download white papers or case studies and join webcasts:
<http://www.websense.com/global/en/ResourceCenter/>

Evaluate solutions:
<http://www.websense.com/global/en/Downloads/>

Locate and contact a Channel Partner:
<http://www.websense.com/global/en/Partners/Channel/FindPartner/>

About the Author

David Meizlik is the senior product marketing manager for Data Security Solutions at Websense, Inc., the leading provider of Web and content security solutions based in San Diego, California. His responsibilities include product positioning, go-to-market strategy and development, market and competitive analysis, and program development for Websense security products. Meizlik earned a bachelors degree from the Marshall School of Business at the University of Southern California, and went on to receive a graduate degree in communications management and technology from the USC Annenberg School for Communication. He has authored several technology papers, including [*Justifying Data Security: An Investment in Competitive Advantage, Deep Content Control™ Keeps Data in the Enterprise, There's More to HIPAA than Compliance, Prevent Leaks and Comply with PCI, E-Discovery Leaves No Stone Unturned, Protecting the Crown Jewels: Securing Intellectual Property,*](#) and [*GLBA Compliance Requires that Leaks be Sealed.*](#)

Table of Figures

Figure 1: Causes of Security Breaches	3	Figure 7: Estimated Impact to Profit Margin.....	8
Figure 2: Direct Cost per Record of a Leak.....	5	Figure 8: DLP Estimated Cost Categories.....	10
Figure 3: Total Estimated Cost of Leak Summary.....	6	Figure 9: DLP Estimated Headcount Costs.....	10
Figure 4: Estimated Leak Remediation Costs Over 5 Years.....	6	Figure 10: Declining Cost of DLP.....	11
Figure 5: Estimated Revenue Impact of a Leak.....	7	Figure 11: DLP as a Percent of Total Risk.....	11
Figure 6: Estimated Revenue Impact of a Leak Over 5 Years.....	8	Figure 12: Advanced Policy Framework.....	14