Lippis Report

White Paper

A Rational Approach to Data Loss Prevention

Issue 6

by

Nicholas John Lippis III
President, Lippis Consulting

December 2008

A Rational Approach to Data Loss Prevention

While the global economy slows down, network security spending continues to be robust as business and IT leaders seek to protect corporate assets and achieve compliance, thus avoiding a major distraction at a time when market focus is needed most. The largest corporate security vulnerability is data loss and it's getting harder to protect it. Here's why.

How To Prevent Data Loss From Compromising Your Company

Listen to the Podcast

The concept of work has changed significantly in the last decade. Gone for good are the days of nine-to-five working hours located in a headquarter facility. The modern concept of work is based upon anywhere and anytime electronic collaboration as computing and networking have gone mobile. Laptops and smartphones allow work to be done everywhere and work means sharing data and information from every place work happens to occur. Therein lies the rub; with greater work flexibility comes greater vulnerability to data loss. Employees are encouraged to share information and spread it freely between those with a need to know; but this comes with risk as information, potentially even customer information, is intellectual property, which becomes more vulnerable as employees work in the field and remotely.

But protecting data is not limited to mobile employees; it spans to all employees independent upon where they work. For example, compliance to regulatory, presidential directives and legislative initiatives require business and IT leaders to protect data loss or face significant penalties. Business and IT leaders need workable strategies to protect their intellectual property and customer data. The problem with implementing a data loss prevention solution is that data is everywhere and so too are vulnerabilities and harsh consequences. For example, details of 25 million child benefit recipients have been lost after two discs containing the data were sent from HM Revenue and Customs to the National Audit Office (NAO) but never arrived. The data included details of millions of bank accounts. In another example confidential records from more than 40 global businesses were stolen and stored on an unprotected server by a Russian cyber thief. The files came from Germany (621), France (322), India (308), Great Britain (232), Spain (150), Canada (86), Italy (58), the Netherlands (46), and Turkey (1,037), among others.

Data Leakage Worldwide: The High Cost of Insider Threats

Get the White Paper

It gets worse. Consider the following statistics:

70% of IT leaders say the use of unauthorized programs results in as much as half of data loss incidents.

44% of employees share work devices with others without supervision.

39% of IT leaders said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

46% of employees transfer files between work and personal computers.

18% of employees share passwords with co-workers. That rate jumps to 25 percent in China, India, and Italy.

Data loss incidents are usually high profile embarrassments with large consequences, such as an Eli Lilly executive who inadvertently sent confidential M&A documents to a NY Times reporter, costing the company tens of millions of dollars as the reporter wrote about the deal before an agreement had been signed. An Ohio State University administrator inadvertently e-mailed an attachment containing faculty and staff Social Security numbers to hundreds of students. A rogue Kaiser Permanente employee cut and pasted personal patient information on a blog in a successful effort to trigger a HIPPA violation and penalty. In the UK a hospital reported a staff member losing a USB memory stick which contained the medical records of 4,000 patients. The largest records storage management company, Iron Mountain, lost a GE Money back-up tape containing 230 different retailers' customer information, including Social Security numbers and credit cards. All told the unencrypted tape contained information on approximately 650,000 customers and held Social Security numbers for 150,000. GE Money is paying for a year of credit monitoring services to help protect those whose Social Security numbers were compromised. And everyone remembers TJ Max's wireless LAN breach where 45 million customer credit card numbers were stolen and used to buy over $8 million worth of merchandise.

Incidents like the above are difficult in good times and can be catastrophic in bad economic cycles, which serve only to give customers spending pause with your company. Clearly businesses are not the only entities vulnerable; governments and their agencies are too. Not all data loss is intentional, but accidental loss occurs as well with unfortunately the same consequences. Further, data loss is not just concerned with loss of electronic information but the loss of information contained in physical documents or portable storage entities, all of which need protection as well.

What is Data Loss Prevention?

So what is data loss prevention or DLP? It's a business problem that starts with the concerns of executive management about intellectual property and customer information being lost or stolen. For many business leaders DLP is intellectual property protection, avoidance of unwelcome media coverage of a security breach and regulatory compliance assurance. DLP discussions usually start with executive management, in order to understand data loss concerns which leads to a comprehensive DLP strategy. A DLP strategy does not include just one technology; to mitigate data loss risk a successful DLP strategy needs to include people, process, and technology. A DLP strategy is about educating and managing employee behavior, then using policy to enforce that behavior which is accomplished via security technology.

From a risk perspective most executives think of DLP in terms of communication channels such as e-mail, web, and devices such as end-points, USB sticks and encrypting backup tape compromises. Another way to think about DLP is to protect data when in motion, while at rest on storage media or in use on end-points and portable storage devices such as USB, iPods, MP3 players, etc. All of these areas of risk need to be mitigated and assessed from a regulation compliance perspective such as HIPPA, GLBA, PCI, Basel II, etc.

A Governance Philosophy of Non-Disciplinary Communications

In addition to DLP technical solutions, addressed below, governance and corporate culture play a large part in a DLP mitigation strategy. Changing behavior is difficult without a significant event, such as some of the firms mentioned above have experienced. The risky behavior statistics, again mentioned above, will not change overnight, but one approach has proven helpful. Educating employees to the dangers and risk of data loss is an important step in its prevention. By instilling a culture of non-disciplinary communications between employees and IT where employees feel comfortable reporting a real or potential data loss to IT is a huge step in containing damage when it occurs. The quicker the data loss is identified the quicker its damage can be contained. The reality is that data is going to get out. With all the data that flows throughout a corporation on a daily basis, there will be an accidental case periodically. The larger problem for business and IT leaders is when employees are fearful about

acknowledging their mistakes and don't sound an alarm; then all of a sudden business and IT leaders find their company in the news, in damage control mode and answering uncomfortable questions from regulators.
Two Technical Approaches to DLP

The DLP Overlay Approach

DLP technology is based upon content-level inspection which is fundamental to the DLP overlay and network-based approaches presented here. The DLP overlay is based upon IT identifying content it needs to monitor and the DLP overlay does so at every point in the IT infrastructure to prevent data loss. DLP overlay solutions provide large amounts of information concerning how data is used and is thus effective at protecting against accidental data loss. But DLP overlays have to be used in conjunction with other data security technology to protect against all types of data loss such as accidental, negligent, data theft, identity theft, etc. Therefore, DLP overlay delivers auditing and compliance in respect to monitoring specific content throughout the network, but it ultimately cannot solve the business problem of data loss prevention unless it is paired with other security technology.

Over the past several years firms such as Vontu and Reconnex, which have been acquired by Symantec and McAfee respectively, specialized in the overlay approach. But these overlay solutions are complex, require too much time to deploy and are costly to manage; many business leaders realize that the overlay approach cost them $10.00 to protect $5.00 worth of data. In short, the DLP overlay is an additional layer of content security on top of an existing security infrastructure. As a result few DLP providers are still in business as IT and business leaders recognize that DLP needs to be implemented as part of a broader system rather than a point solution for larger enterprises. The question is what kind of broader system?

The Network-Based DLP Approach

McAfee, Symantec and others believe that DLP is a separate security system while others such as Cisco believe that data loss is best mitigated by understanding what data needs to be protected, and then leveraging the network to prevent data loss as the network touches every IT asset. In short Cisco believes that DLP is best achieved by leveraging existing investments in network infrastructure, which already contains key security technology which mitigates data loss. For example, a strong security network contains web application firewalls, VPN, Network Admission Control (NAC), data link encryption and extensive security for data in motion with technologies such as TrustSec.

By examining DLP from a risk-perspective, and integrating content analysis plus targeted data security into the network fabric, data protection within all communication channels is achieved, providing the broadest defense of loss. For the above-mentioned content analysis Cisco has recently acquired IronPort, an e-mail security concern, which allows Cisco customers to implement content aware policy within security technology in an effort to mitigate unauthorized e-mails from being sent out of their corporation. Its Cisco Security Agent (CSA) offers an approach to mitigate unauthorized documents, data and applications from being copied on USB sticks and other personal data storage devices too in a single end-point security solution.

The network-based DLP approach is an efficient and reasonable way to achieve data loss prevention. The network approach to DLP allows IT leaders to measure risk by identifying its most valuable data and then creating the right strategy to prevent data loss. In addition data security policy is augmented while providing content monitoring and inspection over high-risk channels in the network. This affords a broad approach to DLP as every corporation has unique data loss vulnerabilities it needs to mitigate.

The network-based DLP approach is both comprehensive and does not require a large capital outlay; nor does it increase operational spend for its management as the overlay approach does. In short, DLP controls are distributed throughout the network infrastructure with data loss prevention achieved by configuring existing networking devices, turning on features, adding policy rules, and taking advantage of new security features added to existing network products and appliances. Network infrastructure policies can be changed to address different risks with different profiles all within the existing network. For example, web application firewall is not addressed by many DLP strategies, but web applications are most compromised. As hackers get through the web application firewall to a

back-end credit card database, a company will find itself in a nightmare scenario. A network-based DLP approach addresses the widest range of risk with the tools to lock data down.

Enforcing content policies at high-risk points is an effective data loss defense, which is very useful for auditing and accident loss control. For example, content filtering of e-mail, web traffic and end-point devices ensure that accidental data loss is mitigated. With content filtering Outlook mail may notify a user that he/she tried to send an e-mail to the wrong person and it contained Social Security numbers. Or content enforcement over the e-mail channel may notify the user that there are Social Security numbers in the e-mail they are sending which is not supposed to be sent externally, thus providing a strong warning to prevent data loss. Putting content enforcement over channels where employees can easily leak information is an important aspect of a network-based DLP strategy of risk mitigation. Cisco, for example, has integrated content enforcement into security devices rather than forcing customers to buy a separate device to monitor e-mail.

Reasonable Steps To Maximize Data Loss Prevention

Data loss events are increasing thanks to today's mobile corporate environment, which offers many ways to lose data. For large global and multi-national firms, there are different social, cultural and business practices in various countries that need to be factored into a DLP solution. In addition, in today's global economy many business leaders do not have the patience or the budget to undergo a large complex and costly DLP overlay project. The network-based approach to DLP offers a wide range of defenses and solutions to mitigate data loss while leveraging existing network infrastructure and personnel investments.

We offer the following considerations to develop a network-based DLP implementation.

Identify Data Loss Risks: Business and IT leaders should identify data loss risk and associated liability. This is perhaps the easiest part of DLP, as high visibility data loss scenarios are straightforwardly identified. Working together, business and IT leaders with their strategic network vendor should identify all the risk scenarios that are of concern. This includes data at rest, in motion and in use as well as regulatory compliance requirements for data and applications. Consider communication channels such as e-mail, web, remote access, personal data storage such as USBs, mobile devices, lost or stolen laptops, physical security such as building access, and data resident on physical assets too, which if lost or stolen would constitute a security breach of intellectual property and/or customer data.

Network-Based DLP Planning: With data loss risk scenarios identified IT leaders can now review their network infrastructure to assess its ability to mitigate these liabilities. Two important network-based DLP areas for IT leaders to focus on are e-mail and storage. Clearly large firms have deployed switches, WLANs, firewalls, routers and remote access network infrastructure devices. But has Network Admission Control and TrustSec been turned on? These are two important DLP network features providing authorized access to data and network encryption protecting data in motion, at rest and in use. Content enforcement of e-mail via the network mitigates both unauthorized and accidental data loss from e-mail systems. Other considerations are the network's ability to provide remote access via SSL VPN ensuring that remote connections are encrypted or ensuring that remote desktop applications are cleared of confidential information after use, mitigating specific data loss scenarios. There are numerous opportunities for data loss; IT leaders can close these vulnerabilities by leveraging their network.

Employee Data Loss Prevention Training/Education: IT leaders are encouraged to develop training that sensitizes employees to risky behavior. Many may not view their behavior as risky. Usually it's not until events such as those presented earlier take place that employees fully understand the risk that they put their corporation in with password sharing, accessing unauthorized applications, sharing computers, transferring files between home and work computers, etc. Boundaries and acceptable use policies on better data usage are often viewed favorably, as most employees are good corporate citizens.

Data loss governance: Consider a corporate culture that encourages employees to inform managers and IT leaders of a data loss without incrimination. This will allow IT to react quickly to data loss, contain damage and even potentially avoid its consequences.

Most IT leaders are concerned about losing data over personal storage devices such as USB sticks and through email systems. A good DLP solution needs to provide strong risk mitigation solutions to these two concerns plus additional risk scenarios identified by business and IT leaders. The global economy is entering a difficult cycle, which can be made worse with the high profile visibility associated with data loss security breaches. The opportunities for breaches are increasing as corporations have expanded the diameter of their business processes and operations thanks to mobile devices and remote access network solutions. The network-based approach to DLP offers a rational method that expands data loss defense options by leveraging existing investments in network equipment and skilled personnel.