CDW PEOPLE WHO GET IT

DATA LOSS PREVENTION AND THE FINANCIAL FIRM

The right DLP solution helps capital markets firms protect their data from exposure and reputation from scrutiny.

Executive Summary

The capital markets industry runs on sensitive information. From confidential customer data and payment card account numbers to sensitive financial analyses, the lifeblood of financial firms is their ability to protect secrets.

Many financial firms invest significant time and energy into identifying sensitive information. Still, many fall short in their ability to detect and control the unauthorized leakage of that information.

Data loss comes in many forms. These range from the malicious insider seeking to sell a competitor proprietary information to an undertrained administrative assistant accidentally attaching the wrong file to an email message.

Data loss prevention (DLP) technology offers information security staff at financial companies the ability to monitor hosts and networks for potential leaks and stop any loss before it is too late. The software offers a comprehensive, content-aware solution designed to monitor and protect confidential data wherever it is stored or used.

TWEET THIS!

Table of Contents

The Situation

The information held by financial firms makes them attractive targets for data thieves interested in corporate espionage or committing identity theft. Unfortunately, one of the largest threats facing these firms is the intentional or accidental disclosure of information by company employees – the so-called "insider threat." Insiders seeking to steal sensitive information may target client records, trading strategies or even closely guarded business algorithms.

At the same time, financial firms are encountering significantly increased regulatory scrutiny. Compliance obligations imposed by government and industry regulators require that firms implement strict security controls and safeguard sensitive information placed under their stewardship.

Unfortunately, security is not always high on the priority list of capital markets firms that are focused on seeking profitability in an environment of fast-paced financial transactions. In fact, the UK Financial Services Authority (FSA) recently issued a report concluding that "Financial services firms, in general, could significantly improve their controls to prevent data loss or theft."

Quite simply, there is still more that needs to be done to protect client data.

Taking a Proactive Stance

As financial firms face the combination of increased scrutiny and a riskier threat environment, they must begin to shift their focus to a proactive stance designed to reduce the likelihood that a data breach will occur. The FSA report cited five fallacies that financial firms often fall victim to and that lead them to assume a reactive stance toward data breaches:

1. Senior managers at many financial firms believe their organizations do not hold sufficient personally identifiable information to be of value to cyberthieves.
2. Many stakeholders in the financial services industry believe that identity thieves target only high-net-worth individuals.
3. The staffs at small firms often believe that their operations are not large enough to attract the attention of identity thieves.
4. Many financial professionals view the insider threat to their data as insignificant.
5. Some firms believe that a lack of breach reports is evidence enough that they have adequate controls in place to prevent loss. (When, in fact, a lack of reporting may be because their controls are not sophisticated enough to detect a breach.)

Each of these misconceptions can lead firms to adopt the wait-and-see approach of dealing with breaches after they occur. In reality, firms should proactively implement security controls to protect their data from both internal and external threats. DLP systems can play an important role in this control environment.

TWEET THIS!

What Is DLP?

DLP solutions are designed to protect organizations against the mishandling of confidential information by insiders.

These solutions monitor a wide variety of transmission mechanisms including email, removable media, mobile devices, peer-to-peer (P2P) communications and social networks. When a DLP tool detects an apparent leak of confidential information, it will block the transmission and notify security administrators so they can take any additional action if needed.

DLP Technology

DLP solutions detect and prevent the unauthorized use and transmission of confidential information at three stages:

1. While the data is being used ("in use")
2. While it is being transmitted across a network ("in motion")
3. While it is stored for future use ("at rest")

These technology suites protect data by performing three critical security functions:

1. **Inventorying sensitive information** – Once a firm has gone through a data classification exercise and identified its most sensitive data elements, DLP products can help identify all of the locations in the enterprise where that information is stored, processed or transmitted.

   The technology is especially reliable in the financial industry, where many sensitive data elements follow known and recognizable patterns. For example, Social Security numbers use a 10-digit pattern in the format XXX-XX-XXXX. Credit card numbers also tend to use similar patterns and include a verification code that provides an additional safeguard.

2. **Monitoring the flow of information** – Identifying the locations where sensitive information is stored is only part of the solution. IT chiefs must also be confident that they understand the flow of confidential information around the enterprise.

   DLP systems can help a firm identify the points where sensitive information enters, log its routes and note where it exits the network. Running a DLP system in monitor mode may uncover previously unknown business processes that manipulate sensitive information, prompting a thorough information security review.

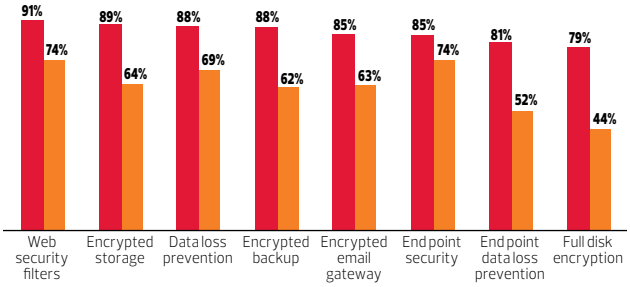
3. **Blocking data leaks** – The most important reason that many financial firms choose to deploy DLP products is to prevent a data breach from occurring at the most vulnerable moment: as data is about to leave the enterprise network. In addition to being able to detect potential data breaches, DLP products include the ability to intervene and prevent a breach from taking place.

DLP technologies can be an important weapon in the arsenal of a firm's security team. They are designed to operate in

conjunction with other controls as part of a defense-in-depth approach to information security. When combined with firewalls, encryption, intrusion detection and prevention systems (IDPS), and a security information and event management (SIEM) system, DLP solutions provide a solid control environment to protect sensitive information.

Organizations with top data security programs layer nearly all available data loss prevention measures — others pick and choose:

- Those that grade their data security as **A** (35%)
- Those that grade their data security a **B–F** (65%)



Source: 2012 CDW Data Loss Straw Poll

DLP Solution Categories

DLP solutions fall into three broad categories designed to protect data while in use, in motion and at rest, respectively. These include endpoint protection, network protection and storage protection.

1. **Endpoint DLP systems** — They reside at the host level and consist of software agents installed on end-user computing devices to monitor data while it is in use or stored on the endpoint. These agents have privileged access to the operating system that lets them detect data stored on or transmitted by the system. In many cases, this privileged access lets them bypass encryption controls and detect even surreptitious attempts to remove sensitive information.
2. **Network-based DLP systems** — These are attached to the network perimeter and monitor data traffic as it enters or leaves the organization's internal network. These systems are often designed to integrate with firewalls, email gateways and other products to provide a secure border and thwart the unauthorized removal of sensitive information.
3. **Storage-based DLP systems** — They provide dedicated protection for data at rest. These systems offer specialized monitoring of network-attached storage (NAS) and storage area network (SAN) systems, identifying locations that store confidential information and reporting the unauthorized use of that information.

Many DLP solutions combine features from one or more of these categories to provide a comprehensive control environment. These approaches are of particular interest to organizations that must comply with multiple regulatory requirements.

Maximizing Preventive Measures

Financial services firms implementing data loss prevention technology for the first time should consider following some industry best practices that will maximize the effectiveness of the investment:

- **Classify your data.** The only way to prevent the loss of sensitive information is to configure a DLP system to recognize it in the first place. This requires the creation of a thoughtful data classification scheme that identifies the sensitive information under care. This effort should include close collaboration with business units.
- **Set appropriate policies.** DLP systems may be seen as an intrusion into the privacy of end users. Before deploying DLP technology, ensure that you have appropriate language in your security policies defining such use.
- **Develop a slow and steady implementation plan.** As with any IT project, use professional project management and create a detailed implementation plan that includes adequate testing and a phased approach.
- **Check your identity management capabilities.** DLP relies upon the accurate identification of individuals within the organization and their roles. For example, customer service agents might be expected to exchange sensitive account information with individual customers, while analysts might not need access to that information. A DLP system works best in an environment that also uses strong role-based identity management.

Keeping Compliant

In the wake of the Enron accounting scandal and identity theft cases too numerous to count, the financial services industry is now arguably one of the most regulated industries in the world.

Government and industry regulators have stepped in to create a patchwork set of laws, regulations and standards that impose a wide variety of security requirements on financial firms. DLP systems can play an important role in ensuring that data governed by these compliance obligations is adequately protected against loss.

Dodd–Frank Wall Street Reform and Consumer Protection Act

The Dodd–Frank Act, signed into law in July 2010, implements a wide-ranging set of financial reforms designed as a response to the recession gripping the country during the years leading up to its passage. The most notable provision of the act for financial services firms is that it eliminates a safe harbor previously afforded to many financial advisers and requires

them to comply with Security and Exchange Commission (SEC) regulations. They must:

- Preserve electronic records for at least five years.
- Take reasonable measures to safeguard electronic records from confidentiality, integrity and availability risks.
- Limit access to electronic records to authorized individuals.

DLP technology can assist firms seeking to comply with these requirements, as it is an important confidentiality control, protecting sensitive e-records from unauthorized access.

Gramm–Leach–Bliley Act

The 1999 GLBA requires that financial firms adopt a set of security controls designed to ensure the privacy of sensitive financial information.

The GLBA Safeguards Rule requires that firms:

- Implement administrative, technical and physical safeguards that ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

DLP technology can offer the proactive prevention called for by GLBA and limit the chance of exposing sensitive data.

Health Insurance Portability and Accountability Act

Established in 1996, HIPAA imposes privacy and security requirements on healthcare providers, health insurance programs and healthcare information clearinghouses.

Although financial firms may not fit this definition at first glance, the human resources departments within such firms may handle HIPAA-regulated information or they may have clients in the healthcare industry that provide data requiring HIPAA protections. DLP systems can help safeguard this information from unauthorized disclosure.

Payment Card Industry Data Security Standard

PCI DSS is a contractually imposed set of security requirements that affect any organization that stores, processes or transmits credit and/or debit card information. Firms subject to PCI DSS may use DLP technology to block potential security breaches involving cardholder information.

In addition, DLP products may serve as a "compensating control" – an alternative security method used when a PCI-regulated firm is unable to meet one or more PCI DSS requirements. The use of DLP as a compensating control requires explicit permission from the firm's merchant bank.

Sarbanes–Oxley Act

The SOX act requires that publicly traded companies institute controls to ensure the integrity of financial statements. This includes an obligation to protect financial information from unauthorized access. DLP solutions can be used in partial fulfillment of this requirement.

DLP Solutions

Financial firms seeking to implement a DLP solution have a number of products from which to choose including:

- **McAfee Total Protection for Data Loss Prevention** – McAfee provides a suite of tools that protect against loss of data while in motion, at rest and in use. The Discover, Monitor, Prevent, Endpoint and Device Control modules may be centrally managed and integrated with other controls through McAfee's ePolicy Orchestrator solution.
- **Symantec Data Loss Prevention** – This suite discovers, monitors and protects sensitive business information. When used in combination with other controls, it can also prevent unauthorized devices from connecting to enterprise networks and automatically encrypt devices and media containing sensitive information.
- **CA Technologies DataMinder** – The CA product incorporates a series of data protection controls that includes DLP technology and full-lifecycle data management. It has components to protect data in use, in motion and at rest.
- **Trend Micro Control Manager** – Trend Micro has integrated DLP modules in its product for endpoint security; mail server security; SharePoint; gateway messaging and network security. These solutions also integrate with other Trend Micro security tools to provide unified control and analysis.

As financial firms seek to identify an appropriate set of DLP technologies, they may wish to consider combining components from multiple vendors to meet their unique business needs.

To learn more about data security solutions, contact your CDW financial services account manager, call 888.706.4239 or visit CDW.com/financial-solutions

TWEET THIS!

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.
All other trademarks and registered trademarks are the sole property of their respective owners.
Together we strive for perfection. ISO 9001:2000 certified
122218 – 130226 – ©2013 CDW LLC

CDW PEOPLE WHO GET IT