Data Loss Prevention for Financial Services

By David Miner

The scenario any executive fears is a loss of confidential customer data. Data breaches come unexpectedly and present threats to proprietary information for financial institutions and their clients. Lost or stolen information can be especially worrisome, as both immediate and long-term costs of responding to a data breach threaten customer trust and loyalty and ultimately the bottom line.

Financial services organizations are aware of threats posed by breached information and are looking for preventive solutions—automated, cost-effective data loss prevention (DLP) tools that will effectively control the operations for every person, process or interaction to protect confidential customer information while also helping them demonstrate compliance with multiple data privacy regulations and company policies.

With these tools, retail banks, investment brokerage firms, insurance companies, credit card and credit reporting agencies can prevent the wrongful disclosure of sensitive data while protecting customer trust and the company brand.

A particularly difficult aspect of a data breach is minimizing the inevitable firestorm of damage to an institution’s brand and reputation. Trust quickly dissolves when data breaches make customers unsure of their financial protection.

The Ponemon Institute found that for each data breach, a financial institution lost on average nearly $240 per record, compared to other industries that lose $200 per record. This statistic reinforces the fact that financial services institutions stand to lose millions of dollars resulting from breached data.

Laws and Standards
Today, most states require that individuals be notified if their confidential or personal data has been lost, stolen or compromised. If a breach occurs, the responsible organization must notify all affected individuals and immediately move forward to prevent further breaches from happening.

Current laws and regulations are in place to help protect consumers and prevent lost data. Payment Card Industry Data Security Standards (PCI-DSS) define how companies must handle credit cardholder and card authentication information. The rules outline how data must be stored, managed and processed to keep it secure. The Gramm-Leach-Bliley Act of 1999 stipulates additional security measures, requiring financial organizations to develop a comprehensive information security program to safeguard sensitive customer information such as social security and credit card numbers.
The consequences of noncompliance are serious. Monetary penalties for violating PCI-DSS can be as high as $500,000 per incident, as well as loss of interchange discounts. Gramm-Leach-Bliley Act noncompliance can lead to severe civil and criminal penalties, including fines of up to $100,000 per violation and even imprisonment.

**A Look Inside**
Customer identity and account information, intellectual property, financial results and network passwords are all pieces of valuable company information. Even if an institution has layers of perimeter protection in place to halt the progress of external threats, internal threats certainly exist. By some estimates, insiders are responsible for 70 percent of security incidents that incur losses.

Proprietary information can be at the fingertips of various employees. Customer social security numbers or personal account numbers may accidentally be exposed on a file server in violation of PCI or state data privacy regulations. Merger and acquisition plans could be innocently copied to a USB drive. Confidential financial results may inadvertently be e-mailed to the press or analysts ahead of a public announcement, and a laptop containing customer credit card information could suddenly be lost or stolen.

There are many scenarios, but the loss of any sensitive information—intentional or not—can trigger a domino effect that can ultimately bring business to a screeching halt. Clearly, information must be protected not only from external threats but from internal ones as well. To protect and prevent data breaches, organizations must use up-to-date DLP technology and services—maintaining complete control of stored data. To be effective, institutions must know where the data is headed and who has access to the information.

**Counting on DLP**
Based on best practices that include financial services-specific policies, user roles, recommended response rules to remediate incidents, and predefined compliance and risk reports, DLP technology is the best solution. Once the data is discovered, DLP technology automatically applies data protection policies through integration with data encryption, storage tiering and archiving systems.

Deploying comprehensive DLP technology can examine all data usage and prevent confidential information from exiting any network gateway or endpoint, from laptops and servers to USB devices, CDs/DVDs and iPods. The technology leverages advanced detection and deep content inspection to ensure high accuracy and minimal false positives. It enables administrators to monitor and prevent the transmission of data, encrypted or not, that violates company policies. After all, just because information is encrypted doesn’t mean it has been approved to leave the organization.
To protect employee privacy and meet regulatory requirements, DLP can also control the amount of incident information so only appropriate, authorized personnel have access to employee identification or incident details. In addition, it can scan employee laptops, including offline machines, for a complete inventory of which laptops in each department may contain exposed confidential data so that appropriate steps can be taken to remove, encrypt or relocate this data.

DLP provides workflow that is automated, prioritized and correlated. From pre-defined compliance reports and scorecards to automatic incident notification and enforcement, intuitive incident presentation, severity-based remediation and business unit report, these capabilities offer financial services organizations proven workflow and business unit enablement.

Data loss has become a rising threat for the financial industry, and it will become critical for institutions to have insight into what sensitive information they have, where it’s stored, and how it’s being used—both on the network and at the endpoint.

*David Miner is senior director financial services, industry worldwide marketing, for Symantec Corp.*