Data Loss Prevention in Financial Services

How to Grow Your Customers' Business in a More Regulated and Secure Environment

News of data loss continues to make newspaper headlines around the globe, especially when involving financial institutions—an industry already under the microscope by regulators, customers, and investors alike. According to Information Security Media Group's "2009 Data Breaches: An Interactive Timeline," the number of U.S. financial institutions targeted by various attacks reached 55 as of November 11, 2009. Those breaches included everything from insider theft and network intrusion to skimming and stolen or missing hardware (see page 5 for details).

> *"Brand and reputation have more heightened value especially considering recent scrutiny from both regulators and consumers."*

One noteworthy scandal involved an incident in which a computer technician was indicted in the New York Supreme Court, charged with stealing the identities of more than 150 bank employees and using them to pilfer more than $1.1 million from charities, non-profit groups and other entities. But the mayhem hasn't been contained to the States. In May, one of Germany's largest lenders said it was investigating possible violations of the bank's internal procedures involving activities associated with its security department. And a year ago, The World Bank Group's computer network—one of the largest repositories of economy information for every nation—was violated.

Executive ROI:
Financial services is one of the most highly regulated industries. And when it comes to the current regulatory landscape, banking examiners and practitioners alike are focused on data loss prevention (DLP). But it's not all about compliance. Now more than ever, reputations and deposits are at stake, forcing institutions to step up protection like never before. Read this paper to learn:

- **The regulatory imperative driving DLP;**
- **How financial institutions are tackling the DLP challenge;**
- **Strategies and tips to help you resolve your own DLP issues.**

It's no wonder that data leaks abound, explains Samir Kapuria, Sr. Director for the Enterprise Security Practice at Mountain View, CA-based Symantec Corporation, a worldwide leader in providing security, storage and systems management solutions. "Financial services organizations are a target of choice, rich in information that the bad guys want—not just for the glory, but for the economic return. Security postures need to constantly evolve to be commensurate with the morphing attack vectors and profiles."

That makes for quite a challenge. Government agencies worldwide are on the war path, putting financial institutions in the midst of a regulatory compliance crunch. But one-off compliance efforts—for example, stepping up to PCI requirements—aren't going to make the problem go away.

"Because today, risk has new weight to it," says Kapuria. "Brand and reputation have more heightened value especially considering recent scrutiny from both regulators and consumers." And that makes the right security posture a marketable asset. So in the fight for every deposit dollar, best-in-class institutions are harnessing both security professional services and technology like data loss prevention (DLP) to extend their effectiveness.

One Bank Shows Sustainability with DLP

"Banks have a total reliance on brand and integrity. It's a subjective issue, with very objective, tangible consequences," says David Krauss, Senior Manager of Global Financial Services at Symantec. And that makes data loss prevention a strategic initiative. From customer account numbers to employee

DLP Best Practices

When it comes to data loss prevention (DLP), experts offer sage advice to the financial community.

- Understand your data. Ask the three all important questions: Where is my data? Who is accessing it? And what are they doing with it? With the answers to those questions and the automation to do something about it, you can plug your leaks.
- Assess your risks. Take the time to evaluate where you're at and where you need to go. Understand the business risks and your compliance requirements; then prioritize what you need to do and when.
- Strategize from two perspectives. Plan for both proactive prevention and reactive response. How are you going to prevent something from happening? And are you responding appropriately when something inevitably does happen?
- Establish the right policies and controls. Set the ground rules. Identify users and groups and assign the appropriate access privileges. Classify your data and then define acceptable behavior parameters for interacting with that data.
- Make awareness a top priority. Good technology and intentions are for naught if folks don't know and abide by the policies. You must make training and awareness an integral part of your DLP initiative.
- Make sure you involve everyone. Data loss prevention is an executive-level initiative that impacts everyone, from human resources to accounting and legal. So rally the troops and make sure you have sponsorship from the top.

socials and intellectual property, "banks have become holistically tied to the security of information, perhaps more so than any other industry," he adds.

That's definitely the case for one large European financial institution that serves roughly 49 million customers. Offering both global investment and banking services, this long-standing institution operates in over 50 countries and employs approximately 150,000 people. The institution prides itself on a historically strong brand and saw the automation of its data loss prevention as a way to sustain that reputation.

This institution's primary goal was to understand its data: where it was, where it was going, the sensitivity of that data and the access rights involved. As one can imagine with an institution of this size, the magnitude of data bordered overwhelming. And globalization created its own set of complexities—different countries, different regulations, and different customer expectations. The institution needed a DLP toolset to protect all its data, from the network out to the endpoints whether in London or Los Angeles.

This innovative institution teamed with Symantec to automate compliance, as well as to implement a network security health check, network monitoring strategy, and endpoint security. Now that institution is full-speed ahead with all eyes on a strong and healthy brand that its customers trust with renewed loyalty.

The Regulatory Imperative

Every region has its own regulatory requirements, especially when it comes to the financial sector which has recently come under its own magnifying glass. Much of that legislation centers on non-public personal information (NPPI). For example, the Gramm-Leach-Bliley Act (GLBA) requires U.S. financial institutions to establish policy to protect information from foreseeable threats in security and data integrity. The Data Protection Act 1998 (DPA) is a United Kingdom Act of Parliament that governs the protection of personal data in the UK, defined through eight data protection principles. Even in Singapore, the Monetary Authority of Singapore (MAS) updated its Internet Banking and Technology Risk Management (IBTRM) Guidelines to help thwart data loss and increase security.

There are also regulations stipulating the policies and procedures for governing that protection; most notably the Payment Card Industry Data Security Standard (PCI) which dictates the terms for storage and transmission of credit and debit card transaction data. And there are even country- and state-specific mandates around the procedures for responding to violations and notifying customers of those breaches.

Of course, data breaches are scary. No good comes of them—from the public relations nightmare and distrustful customer base to the disgruntled board and worried stockholders—it's a huge reputational risk. Still, regulatory non-compliance, in its own right, is just as formidable a threat, explains says David Schneier, director of professional services for Icons, Inc., a Princeton, N.J.-based financial services consultancy. Audits can prove to be time-consuming, resource-draining exercises that suck up even the cushiest budgets. And sanctions for non-compliance can be devastating, not to mention the hefty penalties. GLBA non-compliance, for instance, can garner fines of up to

The Real Cost of Data Loss

So why should data Loss be a topic in the boardroom? It all boils down to the actual cost associated with a breach — and that's often in the millions of dollars.

According to a recent study by The Ponemon Institute, "2008 Annual Study: Cost of a Data Breach," those costs are real and cut very deep.

In the U.S., the firm reported total average costs of $202 USD per record compromised, an increase of 2.5 percent since 2007. That translates into an average total cost of more than $6.6 USD million per breach. In the U.K. the total average costs of a data breach grew to approximately $96 USD per record compromised, an increase of 28 percent since 2007. That's an average total cost per reporting company of more than $2.76 million USD per breach.

Most obvious, there are direct disclosure costs which include remediation such as customer notification and credit monitoring services. Other tangible costs such as customer churn and new customer acquisition losses as well as fines, legal fees, and public relations expenses add to the tally, as do intangible costs like brand damage, loss in customer trust, and even a decline in share price.

That math will catch the attention of any CEO, putting data loss in a whole new light.

$100,000 per violation and even imprisonment.

The Data Dilemma

So why is compliance so difficult?

Sure, there's some volatility in the regulatory requirements. Regulations evolve in a heartbeat, and new regulations pop up all the time. And with all those regulations, there's much subjectivity. Each calls for general information security and risk management programs, says Schneier. Institutions must demonstrate how they're protecting data and that they have effective controls in place. "But the regs don't go so far as to say how you have to do it," he laments. So adhering to something like Sarbanes Oxley (SOX) can be interpreted and implemented differently.

Still, the ever-evolving nature of banking in and of itself contributes immensely to compliance chaos. "Every change, every evolution has an impact on control," says Krauss, "and its effectiveness is compromised and stale in short order."

Just consider the many forces of change in the financial industry. Institutions are opening operations to accommodate new business models — going global and merging with other institutions. "Data knows no global boundaries which introduces new implications on risk posture as institutions merge," says Kapuria. The new consolidated, global bank has to balance both varying regulations, as well as, different paths to legal recourse. And engaging an army of third-party resources —especially as financial institutions look to outsourcing to drive down costs—only makes the chain of control more complex.

At the same time, institutions are rapidly evolving their infrastructure and expanding data reach. The network has become the Internet; storage has gone electronic. And the consumerization of IT has resulted in endpoint proliferation—from the iPhone and smart phones to home offices. Additionally, transparent channels present other vulnerabilities as institutions empower customers with 24x7 convenience terminals, online portals, and mobile banking, while communicating via email, text messages, and Twitter blasts instead of traditional post.

> *"Data is everywhere – it's in motion, at rest and in use. And most banks have exposures for which they're not even aware."*

Frankly, data is everywhere—it's in motion, at rest and in use. And most banks have exposures for which they're not even aware, warns Schneier.

So when it comes to this new way of business, Philip Alexander, the director of security operations for a fraud management company, and the author of "Information Security: A Manager's Guide to Thwarting Data Thieves and Hackers," poses some relevant questions for banking/security leaders concerned about DLP:

- How do you prevent sensitive data from leaving your network when employees have access to webmail?
- How do you stop contractors from downloading data to their laptop and walking out the door?

The Symantec Approach to DLP

Symantec doesn't take a single-minded or single-product approach to information risk management. "Our overarching philosophy reflects the holistic situation that banks are in today," says David Krauss, Senior Manager of Global Financial Services at Mountain View, CA-based Symantec Corporation. It's all about managing risk in an integrated, all-encompassing way to mitigate every threat.

The company believes that a centralized DLP strategy can make it easier to manage the complexity and volatility of current and future regulatory requirements. And through automation of key disciplines—such as endpoint security and encryption, data loss prevention, discovery and records retention, messaging management, and compliance monitoring—the company delivers a comprehensive view of everything, so financial institutions can react effectively to violations and more importantly prevent them from ever occurring.

Symantec Data Loss Prevention solutions enable financial institutions to protect confidential data such as customer identity and account information, intellectual property, and financial results.With a host of consultancy services—from infrastructure and operational assessments to DLP enablement and in-residence operational services—you can take your institution's security to the next level to protect your precious brand.

To find out how Symantec can help you, visit our resource center, which includes product and industry information, as well as DLP case studies:

To find out how Symantec can help you, visit our data breach resource center

- Even more problematic, how do you stop that data leakage when thumb drives have gigs of storage capacity, while bearing in mind that portable music players can also be used to store data files?
- How do you make sure that data from the '90s isn't sitting forgotten on the network?

What's more, access to that data runs rampant. From the executives in the boardroom to the tellers in the branch offices, privileged users are granted permissions or access to critical information—whether they need it or not. In fact, a recent study, the 2008 National Survey on Access Governance, conducted by the Ponemon Institute and Aveksa, finds that 70 percent of CIOs say that their employees have access to information that they don't need in order to do their jobs.

Still, many breaches are the result of well-meaning employees acting in an insecure manner or one-off process glitches set in motion by an unawares third-party. More sinister in nature, Ponemon Institute reports that 59 percent of employees who leave or are asked to leave a company are stealing data, while 67 percent used their former company's confidential, sensitive or proprietary information to leverage a new job.

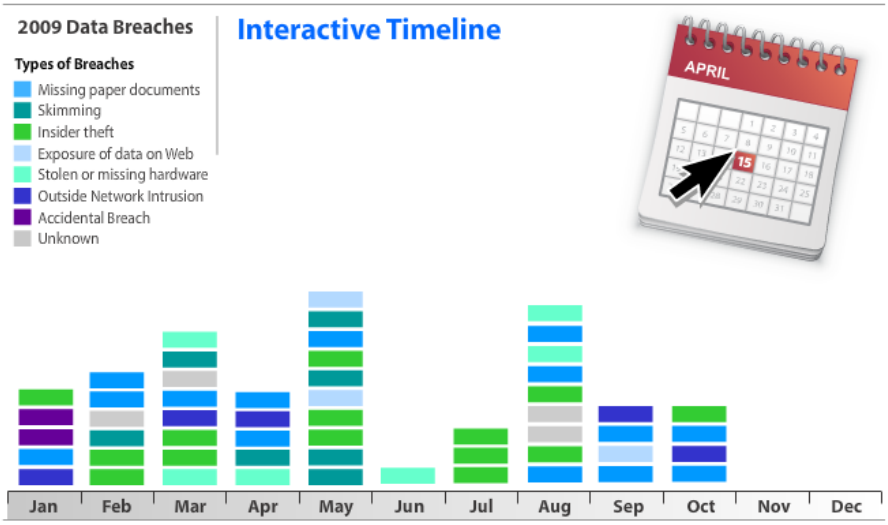
And all of this boils into the perfect storm for potential data loss. It's very hard to pinpoint exactly where sensitive information is, who has access to it, and how it is being used. But that's something financial institutions—from the global banks to the community credit unions—need to know. If they can answer those key questions, their compliance worries should be manageable.

DLP: The Right Protection in the Right Places

And that's where DLP comes into play within a bank's risk management strategy. These are systems designed to detect and prevent the exposure of sensitive information to outsiders. This would include customer identity and account information, non-public financial results, and the institution's intellectual property such as a proprietary trading platform. Whether that leak comes from a disgruntled insider, a process mishap or even an insecure endpoint, the right approach is a holistic matter, looking at all aspects of risk and implementing strategic layers of protection.

Of course, when it comes to the network, most banks have established fairly secure VPNs and other forms of perimeter control to keep hackers out. They're also scanning inbound mail for viruses, malware and other mal-intents like phishing. But to really protect against data loss, institutions must take measures to safeguard what's leaving the network. They need mechanisms in place to prevent instant messages from going out with customer data attached, and to stop emails from being sent with financial plans in tow. Automatic encryption of outbound email is a must. And security violation notifications should let users know when they've inadvertently exposed sensitive data—so they don't do it again.

Similarly, the access controls that banks have put in place help protect stored data. But the risk goes deeper than what may already be in place. Institutions really need to consider what's being stored and how. Procedures must be implemented to scan for inappropriately stored data and to find and remove aged data. They need to set up controls to prevent file sharing of sensitive data. And being able to provide auditors with an accurate inventory of data is key.



Information Security Media Group tracks industry breaches in its "2009 Data Breaches: An Interactive Timeline" with a total of 55 U.S. financial institutions targeted by various attacks as of November 11, 2009.

Perhaps most challenging are the vulnerabilities that lay just outside the realm of IT's control. With the new-found mobility of employees and the extension of business processes into third-party relationships, institutions must strictly control the data that's leaving the confines of their physical offices. Scanning laptops for sensitive data and disabling devices when employees leave the company is critical. What's more, it's important to take measures to stop that sensitive data from being copied onto USBs and thumb drives. Once data is mobile, it's near impossible to control.

"Endpoint systems are indispensable tools and these tools should be kept 'clean and ready' for productive use," according to a recent Aberdeen report. That means conducting the proper due diligence to make sure endpoints are secure, compliant and well-managed. "Deployment of endpoint management solutions is currently a strongly distinguishing characteristic of the companies achieving best-in-class results." But even at the best-in-class level, only 28 percent have adopted data loss prevention technology for endpoints, the report states.

In the end, technology is all well and good, but DLP has become a business issue. "You need technology to comply, but that alone doesn't mean you'll reach DLP maturity," warns Kapuria. After all, a substantial percentage of employees may not understand or internalize documented policies. So security awareness and education is a must at all levels of the institution. DLP should be a culture, with technology providing visibility into what policies are being followed and where violations are occurring.

> *"Leaders that automate the assessment process reduce their compliance costs by an average of 55 percent."*

The Simple Truth

DLP maturity may seem a tall order, but it becomes possible through program solutions, explains Kapuria. Automation allows institutions to implement consistent policies in real-time to prevent the inadvertent or criminal exposure of data, and to respond appropriately as necessary. And for compliance across the nuances of any number of different regulations, applying templates for key regulations—like GBLA, PCI, Sox and various state data privacy laws in the U.S.—means IT systems can enable an organization with accurate, consistent results.

Still, some institutions balk at the prospect of taking such comprehensive measures.

Symantec Financial Security Insights Series

For more insight into IT trends within financial services, check out our other white papers:

- **The 12 Business Benefits of Workspace Virtualization: For Cash-Strapped Financial Institutions, Bottom-Line Cost Savings Come with Added Manageability and Security Perks**

- **Resiliency, Not Just Recovery: With So Much at Stake Today, Financial Institutions Bank on Resiliency to Thrive in Trying Times**

"Deploying a compliance solution can be expensive," says Schneier. "That's a hard nut to swallow for some smaller institutions."

But the investment is certainly not without its rewards. In a recent benchmark report, called "Why Compliance Pays: Reputations and Revenues at Risk," the IT Policy Compliance Group concludes that there are leaders and laggards when it comes to compliance efforts. On average, those leaders faithfully monitor and measure compliance controls once every one to three weeks and experience two or fewer data losses or thefts of sensitive data annually. In contrast, laggards average six- to eight-month cycles and experience 22 or more data losses per year.

And, though it may seem an expensive task, it's important to note that those leaders that automate the assessment process reduce their compliance costs by an average of 55 percent.

"Compliance may be an unwanted, arduous mandate, but it brings good things," concludes Krauss. "It results in better business processes, improved service levels, and, of course, cost avoidance. But most importantly, it enhances customer trust in your brand."

To learn more about Symantec's solutions for financial institutions, visit:
http://go.symantec.com/financialservices

For more insight into the anatomy of a data breach and whether your organization could be at risk, visit our data breach resource center: One Breach Is One Too Many.