Banks Guard Against Data Breaches

Understanding the potential for critical breaches helps mitigate operational risks

Banks face the constant risk of unauthorized exposure of sensitive financial business data and customer information. The recent security breaches disclosed by retailing giant TJX Companies and the U.S. Department of Agriculture, as well as last year's breach of Veterans Administration data, demonstrate the severity of this problem.

When banks report on information that comes from their legacy systems or pass it around, they share the information via FTP transfers. This is exactly where they are at great exposure to risk from loss of data. Data may be downloaded to a PC, and if the PC is lost or gets into the wrong hands, the bank is faced with potential data loss and a possible security breach.

> "Banks must understand what their big picture is."
>
> **Chris Yaldezian**
> Industry marketing executive, financial services
> Sterling Commerce

There are enormous costs associated with data breaches. Since they are not strictly limited to financial costs, they can seriously impact a firm's bottom line.

First, a data breach can have severe reputational costs to both the bank and its brand. Following a data breach, a bank likely will suffer loss of market capitalization and shareholder value. In addition, it will encounter some opportunity costs within sales and customer service. Customers may also begin to have some negative associations and uncertainty with a bank after a reported data breach, which would soon affect the bank's ability to sell and cross-sell.

As if the reputation and opportunity costs aren't enough, the direct operational costs of a data breach can be staggering. Notifying all customers whose information has been breached has a significant cost, as does implementing a plan for fixing it. The plan may require a bank to provide customers some sort of freebie, like putting monitoring measures on their accounts or giving them a year's subscription to a credit reporting service. There are also costs associated with the fines levied on any bank that fails to meet the data protection requirements mandated in Gramm-Leach-Bliley Act (GLBA) regulations.

The total monetary cost of a data breach could easily reach up into millions of dollars for banks that experience this kind of incident. There are intangible costs, as well. According to the 2006 Annual Study: Cost of a Data Breach, a study performed by The Ponemon Institute, which aims to advance ethical information and privacy management practices in business and government, the total cost of a data breach currently averages $182 per lost customer record, taking into account

STERLING MEFG ADVANTAGES
It's all in the Platform

- Streamlines external financial data transmissions
- Simplifies diverse financial communications
- Provides enhanced visibility and management capabilities
- Addresses potential data security issues before they happen
- Predicts future demands

sterling commerce
An AT&T Company

direct incremental costs, lost productivity costs and customer opportunity costs.

A Holistic View

In today's global environment, Banks must take a holistic view of the potential for serious data breaches. This kind of holistic approach to the risk of a data breach will enable banks to avoid taking hits to shareholder value, reputation, opportunities and operational costs.

"Banks must understand what their big picture is," says Chris Yaldezian, industry marketing executive, financial services at Sterling Commerce. "They need to determine the real likelihood of a breach occurring and consider the costs they would incur in the event of a serious data breach, and then weigh the two."

Say that a bank estimates that it has a one-in-a-million chance of a data breach. But a breach might cost $20 million in operational costs, and potentially much more in terms of reputational and opportunity costs. The best bet? It would make sense for the bank to implement stronger measures to proactively guard against data loss and security breaches.

"So the money it will cost you to truly secure your data will be money well spent," Yaldezian points out. "The bank will be protected against hits to its reputation or to shareholder value, and it won't take hits in terms of operational and opportunity costs."

Taking a holistic view also means that banks must view data security as part of their overall operational risk management strategy, according to Yaldezian. "Data security is not just a compliance issue. It should be part of an operational risk management strategy," he notes. "Most banks have operational risk management assessments. And because of Basel II, larger banks are required to have them, and the top 25 banks in the U.S. perform these assessments. So that's driving the holistic view, in a sense."

The holistic picture allows banks to take into account the likelihood of a data security event and weighing against the operational, reputational and opportunity cost. After they have taken a big-picture view of the data security issue, incorporating it into their overall operational risk management strategy, they can look to software to help mitigate their risk of data breaches.

In order to ensure their long-term financial viability and regulatory compliance, banks need a trusted ally to fight against data theft and guard against data loss. A solution partner that will help them achieve a holistic view that will protect their organizations.