At the Second Annual Identity Theft Summit held in Los Angeles, over a thousand representatives of law enforcement, the financial services industry, consumer groups and state and local government participated in the effort to find solutions to the growing crime of identity theft. Speakers, including Governor Schwarzenegger and Deborah Platt Majoras, Chairman of the Federal Trade Commission, took the podium to talk about the growing business necessity to protect confidential and sensitive customer data. Their messages were clear: (1) consumer concerns about the security of their sensitive personal data and the risks of identity theft are at an all time high; and (2) businesses must take reasonable measures to protect sensitive consumer data.

The growing concerns about identity theft are understandable. Nearly 10 million people in the United States are victims of identity theft each year. In 2005, this crime cost businesses and financial institutions more than $57 billion nationwide. As the damages caused by identity theft grow, so, too, have enforcement actions. The Federal Trade Commission has brought more than a dozen security cases against household names, like Microsoft, DSW Shoe Warehouse, BJ’s Wholesale Club and Choicepoint, for failing to take reasonable steps to protect sensitive consumer information. Perhaps the most well known enforcement action involved Choicepoint. The Federal Trade Commission obtained $10 million in civil penalties—the highest civil penalty ever levied in a consumer protection case—with $5 million in consumer redress for identity theft victims and significant injunctive provisions that require Choicepoint to implement a variety of new data security measures.

Another high profile data breach involved the theft of 40 million confidential customer records from CardSystems, a credit card processor. In this case, the Office of the Comptroller of the Currency (OCC) has taken formal actions against two banking employees—barring them from banking—for violating security requirements under the Gramm-Leach-Bliley Act by emailing confidential customer information to a third party. Another bank in Missouri is under investigation for sending confidential customer information via unencrypted network communications to a programmer. The lesson for corporate America is that reasonable security measures and safeguards must be implemented to protect sensitive consumer data.

Civil penalties and legal actions are only part of the damages that businesses can face for failing to implement reasonable security measures. Companies that suffer security breaches and the loss of consumer data also face:

- Expensive litigation, threats of class actions and significant clean-up costs
- Significant damage to corporate brand (estimated to range from 3% to 7% of the responsible company’s market capitalization)
- Loss of customer and employee trust
- Loss of shareholder value
- Damage to personal and professional reputations

Effective management of sensitive consumer data requires a consistent and proactive approach. Executives and their organizations must establish a culture of privacy and security—and take reasonable steps to manage sensitive information. Experience has shown that this is best accomplished with a holistic approach that includes administrative, physical and technical safeguards.

The problem for many companies is that their IT systems are complex and simply were not designed for the protection of sensitive data that is required in today’s regulatory environment. A typical company has numerous applications, distributed throughout the organization, using an array of protocols that reach across the company’s perimeter. As a result, each of these communication channels can potentially leak sensitive consumer data and, in fact, have been proven to do so. In most companies, employees can access sensitive data by sending Social Security or credit card numbers in, or as, attachments to emails or by dozens of other similar network activities that expose the company to serious risks.

---

1. OCC News Release NR 2003-27
2. The Federal Trade Commission recently stated that CardSystems, responsible for the loss of credit card information, faces potential liability in the millions of dollars under bank procedures and in private litigation for losses related to the breach.
4. Safeguarding Sensitive Data in the Financial Sector - Fighting Fraud and Identity Theft by Stopping Data Leaks, Intrusion Inc.
Financial services organizations are mandated by regulation: to ensure the security and confidentiality of customers’ nonpublic personal information, to protect the information against anticipated threats and unauthorized access, to identify all reasonably foreseeable vulnerabilities and threats to the information, and to implement prudent security strategies for protecting customers information including information sent through electronic channels. The Federal Financial Institution Examination Council has issued numerous guidance for financial institutions regarding the security of information assets. The FDIC has issued guidance specifically related to the use of instant messaging and warns institutions against transmitting unencrypted confidential or sensitive information. At a recent conference, NCUA Vice Chairman Rodney E. Hood encouraged credit unions to take proactive steps in managing credit union members’ data.

Powerful Technology – Cost Effective Solution

The challenge is to limit the exposure of sensitive consumer data by preventing it from leaving your company’s network unprotected. Intrusion’s Compliance Commander is powerful technology that provides a cost-effective tool to locate and prevent such security lapses – before they occur. Compliance Commander stops sensitive consumer data with 100% accuracy before it can leave your network unprotected. Compliance Commander’s Dynamic Application Detection technology protects all applications, ports and protocols against intentional and unintentional leaks of consumer data. This enables your IT team to mitigate areas of risk that frequently include common business processes involving:

- Business partners
- Customer support
- Mobile workers
- Other IT applications and services.

Compliance Commander’s Dynamic Application Detection technology protects all applications, ports and protocols. It also protects against targeted attacks, which are becoming more widespread as the value of consumer data grows.

Intrusion’s integrated Ticket Management Workflow tool provides a simple, yet powerful, process for fixing data leaks before they can cause damage. Advanced reporting and management capabilities quickly summarize your organization's risks, enabling you to focus your resources on the areas of highest risk to your company.

Ticket Management Workflow

You and your team have spent years building a successful business – working hard to develop trust with your customers and value for your stakeholders. Don’t risk your hard work by failing to implement effective tools such as Intrusion’s Compliance Commander. The Federal Trade Commission and other regulatory enforcement agencies expect you to protect sensitive consumer data like you would your company’s cash. Your customers demand it.

All Data Leak Incidents by Category

FFIEC Interagency Guidelines Establishing Information Security Standards
FFIEC Information Security Handbook