



AN RIS WHITE PAPER

CONQUERING E-MAIL AND DATA SECURITY RISKS

**Strategies to reduce risk and
seal off unsuspected new holes in the
communications perimeter**

IN CONJUNCTION WITH

SONICWALL

SECURITY-BASED INCIDENTS FROM THE INTERNET ARE RESULTING IN AVERAGE REVENUE LOSSES OF ALMOST \$2 MILLION PER INCIDENT ACROSS ALL INDUSTRIES AND FIRMS, ACCORDING TO ABERDEEN GROUP. RETAILERS ARE AN EASY TARGET OF EXTERNAL ATTACKS; RETAIL BRANDS ARE WELL KNOWN, AND CONFIDENTIAL DATA IS DISPERSED THROUGHOUT THE MANY MINI-NETWORKS RETAILERS OPERATE AMONG HEADQUARTERS, STORE AND DISTRIBUTION LOCATIONS.

Many retail companies have taken at least some steps toward protecting this infrastructure from external attacks. Less considered is their vulnerability to outbound security breaches, such as inadvertent or intentional exposure of data through employee use of e-mail, instant messaging, file sharing, Web posting, or portal activity.

Unfortunately the array of inbound and outbound data security risks are increasing, leaving many retail networks inadequately protected. While most companies have taken some steps, such as applying anti-virus services to e-mail or content filtering to employee Internet surfing, for many retailers dangerous gaps persist among these applications.

The risks of failing to fully protect both inbound and outbound flow of data for a retail business are increasing daily, from government legislation to customer trust. Fortunately, obtaining complete, enterprise-level protection is getting easier, thanks to newer solutions offering easy-to-use and affordable appliance-based and software-based services.

RETAIL IS A TARGET

Data has become the currency of modern retailing. Delivering inventory, financial, customer and other data to the places it can do the most good is critical in exploiting that data. Many retailers have deployed well-integrated software platforms for the purpose of enabling widespread access to information. But storing and moving that data carries risks and responsibilities.

Data enters retail networks via in-store, call center and online transactions, from structured and unstructured transactions with business partners, and through ad hoc communications with third parties. E-mail has become a critical medium for doing business, enabling customer service as well as employee and partner communications. Outgoing content travels through many of the same venues. These avenues must be maintained at peak operating efficiency to service customers and conduct business under today's real-time expectations.

That may be accomplished by controlling access to the network and managing the data that passes both into and out of it, through a combination of policies and technology.

The issue is more complicated for retailers than some other vertical markets due to the geography of the typical operation. What's more, employees within those sites require differing levels of access and control based on their role: a retailer might want a headquarters marketing employee to have wide access to other retailers' Web sites, for example, but not a store employee. It may be acceptable for an accountant to distribute customer data, but not a regional store administrator. A retailer may want a headquarters worker to verify the validity of e-mail content prior to distribution or receipt, but not want to disrupt selling activities of a

store worker in the same situation. Managing all that requires centralized, granular control.

WHERE ARE THE GAPS?

Analysts claim that many retailers only partially protect their data and networks from inbound and outbound data loss. Typical gaps include:

- Lack of a formal incident response plan for security breaches and failure to test that plan.
- Underestimating the threat of deliberate or accidental data outbound breaches by employees. Analysts expect this type of incident to increase in 2006.
- Failure to recognize the risks in ad hoc, unstructured network traffic such as e-mail.
- Misconception that they are not subject to privacy laws requiring protection of customer financial data, perhaps due to their small size.
- A piecemeal approach to security in which the retailer purchases point solutions as needs become evident, leaving them with gaps in coverage and high IT maintenance requirements for multiple solutions.
- Failure to adequately budget. "With narrow margins retailers tend to spend less than other sectors such as financial services, government and healthcare," says Stacey Quandt, research director, security solutions and services for Aberdeen Group. "Tight budgets and a lack of awareness of solutions to address this convergence mean retail will lag behind other industries."

Assessing these and other points of weakness is an essential step toward identifying appropriate solutions.



“ A small retailer is just as devastated when required to notify its 1,000 customers of a data compromise as a Tier One company is when alerting hundreds of thousands ”

RISKS ARE RISING

The consequences of a security breach continue to rise. In addition to customer trust, failure to adequately protect data means exposing the business to risks including: loss of investor confidence, degraded network performance and violation of commercial sector requirements such as PCI Data Security standards.

Regulatory penalties are also mounting, and failure to comply with regulations can lead to substantial fines and executive liability. Victoria's Secret is among the many retailers that have been the target of recent enforcement actions.

- Gramm-Leach-Bliley has implications for retailers that issue their own store credit cards, and are therefore considered a financial institution.
- Sarbanes-Oxley demands that companies establish financial controls and ensure their security policies are followed, a challenge when managing remote networks.
- FTC Act Section 5, which ensures companies keep the promises they make to consumers about privacy, applies to retailers that engage in interstate commerce. BJ's Wholesale Club was recently assessed the biggest fine in FTC history for violating this section due to poor information security status.
- HIPAA's Security Rule can apply in two ways: through retailers' use of e-mail to support administration of its employee health plan or information exchanged with customers, and, if the retailer has a pharmacy, e-mail related to a "doc in the box" (in-store clinic) and to the sale of related medical supplies and equipment.
- Laws requiring notification of parties whose personal financial data has been exposed have spread from California (SB1386) to many other states, and a federal law along these lines is a strong possibility in 2006, analysts say.

Then there's simply loss: In Aberdeen Group's The Security Spend Management Benchmark Report, best in class companies are losing 1.4% of their annual revenue to electronic security-related incidents, while organizations operating at the industry norm are experiencing loss rates averaging 7.7% of revenue and

industry laggards are losing an average of 8.4% of their revenue. Data security has become a competitive advantage.

A key point is that this is not a big-retailer-only issue; a small retailer is just as devastated when required to notify its 1,000 customers of a data compromise as a tier one company is when alerting hundreds of thousands.

RISKS TO RETAILERS ARE MANAGEABLE

As threats grow more sophisticated, so must retailers' approach to protecting their networks and data. According to IDC's The Time Is Now for Controlling Outbound Content, February, 2006, company policies alone are not enough to protect outbound breaches; several high-profile leaks have occurred despite the existence of written policies. Instead, guarding against the array of threats requires a holistic, customizable, multi-layered approach covering all networks and including:

- E-mail security, including protection from spam, viruses, zombie attacks, phishing, denial-of-service attacks, directory harvesting attacks and fraud
- Content filtering and automatic encryption of confidential outbound data
- Unified threat management
- Network security, including firewalls and VPN
- Policy management
- A framework for regulatory compliance
- Protection of mobile and wireless devices, including data on executive laptops

This broad range of risks and regulations can generally be addressed by a few common measures. These include:

A SET OF COMPANY-WIDE POLICIES. Executives must scrutinize existing practices to identify gaps, gain a clear understanding of laws, regulations and best practices, and then enact a clear, comprehensive set of data management rules by location and job that are also codified into their technology solutions.

INTERNAL DATA PROTECTION: It's important that policies govern not just movement in and out of the organization, but within it as well. A retailer needs rules about how data is protected, stored and backed-up.

EXTERNAL DATA PROTECTION: Technologies and policies must comply with regulations about data protection, such as making sure private data is not mistakenly sent out, and ensure everyone in the organization understands and complies with rules about data in all the situations they encounter.

MONITORING, REPORTING AND AUDITING: Some requirements not only stipulate security measures; they also demand that companies be able to prove they're in place. Technologies to monitor, analyze, report, and enable auditing of security activity are a key part of an appropriate solution.

Fortunately, solutions have emerged to simplify the application of the range of security technology through unified,

central management. These can be configured according to retailers' own rules, to ensure protection while not hampering productivity, and can be different for different users.

According to Aberdeen Group's Best Practices in Security: Governance, best-practice companies automate close to all of their security functions and controls, compared to only around half of industry average firms.

THIS IS THE TIME

The risks of failing to protect both inbound and outbound data are growing more pronounced just as the attacks themselves are growing more sophisticated and complex. Since none of these arenas fall into retailers' core competencies, it's time to take a holistic, comprehensive approach to protecting their data. Now that it's possible to obtain world-class protection in a way that requires a limited investment of resources, retailers must take action to ensure ongoing security without compromising productivity. ■

ABOUT SONICWALL

SonicWALL addresses the unique needs of retail e-mail security with a solution that leverages a global end-to-end attack monitoring network to deliver the highest level of protection from all inbound threats including spam, phishing attacks, and viruses as well as the outbound threat of employees sending noncompliant e-mails. With SonicWALL E-mail Security solutions, retailers can now take advantage of feature-rich, e-mail threat protection, as part of the company's extended security suite comprising network security, secure remote access, business continuity, and Web and e-mail security.

FOR MORE INFORMATION:

■ SonicWALL: <http://www.sonicwall.com/industries/retail.html>

