

timely news on accounting and operational issues

QuickBrief*

Retail & Consumer

Protecting Sensitive Data within Retail and Consumer Companies

In working with large global retailers and consumer products manufacturers (Retail & Consumer companies), we have observed that management and boards of directors are talking a great deal about identifying and managing their companies' key business risks, and many are taking steps to manage and mitigate those risks. For Retail & Consumer companies, data protection is an increasingly critical business risk that must be carefully measured and managed, particularly when it comes to privacy and the protection of credit card and other sensitive customer data. In addition, the growing trend toward electronic payments and the rapidly growing importance of the Internet as a sales channel has heightened the awareness of this issue for Retail & Consumer companies, their customers and other stakeholders.

Few would dispute the idea that consumer identity theft and fraud are growing business problems across the board and that there is pressure on Retail & Consumer companies to do something about it. Retailers are increasingly being targeted by professional hackers, as well as supposedly trusted insiders. They are arguably second only to financial institutions in terms of the amount of personal customer information stored on their information systems, including valuable credit card information, and are seen as (and often are) easier targets for data thieves. Consumer products manufacturers are also a target due to their growing direct-to-consumer sales through

online channels and outlet stores, and the increasing amounts of sensitive data they capture and store.

According to Privacy Rights Clearinghouse (www.privacyrights.org), an estimated 101 million records containing sensitive personal information have been involved in security breaches since January 2005. In 2007 alone, there have already been over 40 reported breaches where sensitive personal information has been compromised. Many of these breaches garnered scant media attention. However, when a well-known consumer-facing company is involved, the media focus can be overwhelming.

The pressure is coming from all sides. Consumers are more aware than ever of the threat of identity theft and expect Retail & Consumer companies to take the necessary steps to protect their personal information. The media's white hot spotlight, Wall Street analysts, shareholders, business partners, and more recently, legislators — are all seeking assurances that companies are doing all they can to protect the sensitive customer data stored on their systems.

Unfortunately, these higher expectations and increased focus have surpassed the efforts of many Retail & Consumer companies to protect customer data. Given what is at stake and the growing risks in data protection, Retail & Consumer companies may need to ask themselves whether they have invested

enough time, attention, and resources in data protection.

Make no mistake, a security breach involving customer data can be devastating to a Retail & Consumer company, leading to a host of problems, including negative publicity, loss of customer trust, fines, investigations, and litigation. Certain state and federal regulations require full and immediate disclosure when a breach occurs, and bills have recently been proposed that would hold Retail & Consumer companies liable for failing to protect customer data. A company could also be subject to fines by the Federal Trade Commission and credit card companies, as well as years of costly mandated audits.

Perhaps most importantly, the damage to a company's reputation and the faith and trust of its customers and other key stakeholders could take years to mend. The damage to the business in terms of lost revenue, while difficult to quantify, is a constant concern. From an internal perspective, estimates from the *2006 Annual Study: Cost of a Data Breach* conducted by Ponemon Institute, LLC suggest that data breaches cost companies an average of \$4.8 million per breach and \$182 per compromised record. And the legal, strategic, operational, and financial issues that result from a breach can often consume a company's attention and resources over an extended period of time. As a result, concerned boards of directors and audit committees are asking CEOs, CFOs and CIOs pointed questions about data security risks and the steps they have taken to manage and mitigate those risks.

Are Retail & Consumer companies doing enough to protect themselves?

Despite strides being made in improving data protection and information security, Retail & Consumer companies may still be taking on more risk in this area than they realize or wish to accept. Our experience shows that managers and executives may not have a clear idea of how prepared their companies are to prevent or detect a security breach or to respond quickly and appropriately should a breach occur. Indeed, some senior executives may operate on hopes and assumptions when it comes to data protection with little clear or concrete evidence that their companies' information is secure. Others may allow data protection to become an afterthought as they cut or re-allocate information security and related budgets in favor of more pressing priorities.

A complicating factor for Retail & Consumer companies is the fundamental challenge of not knowing exactly where sensitive data is in the organization — how it gets created, how and where it enters the organization, how it flows through the organization, where it is stored, where it leaves and leaks out of the organization, to which third parties it is being sent, and when and where it is disposed of and/or destroyed. This entire “data lifecycle” process is often not well understood or controlled, and the massive volume of electronic data as well as the ease with which data can be transferred makes compliance with internal policies and external rules and regulations a difficult undertaking.

According to a survey of 434 information technology and security professionals working in Retail & Consumer companies conducted by PricewaterhouseCoopers and CIO Magazine, 43 percent of respondents said that their companies are not in compliance with state and local privacy regulations and 30 percent said that their organizations are not in compliance with their own security policies. In addition, Retail & Consumer companies' spending on information security and data protection lags behind the averages across other industries.

Ongoing cost and budget pressures and competing priorities often prevent Retail & Consumer companies from fully identify-

ing and addressing data protection at an enterprise-wide level and from complying with privacy and other regulations and industry standards and requirements, such as the Payment Card Industry (PCI) Data Security Standard, in a timely way. The PCI standard is designed to help safeguard customer credit card data and other sensitive information (see the sidebar on page 3) and defines control objectives that companies must meet in order to comply with the standard.

In August 2006, Visa confirmed that only 36 percent of level one merchants (companies that process more than six million transactions per year) were in compliance with the PCI standard. With compliance at such low levels, it becomes clear that company executives may not realize exactly how much and what type of customer data is stored on their systems and, therefore, do not realize the critical nature of this risk. In fact, some companies face fines from credit card companies for retaining too much customer information on their systems, particularly “track” data that stores sensitive information such as the card verification value (CVV2, CVC2 or CID) code printed on all cards and commonly referred to as the “security code.” In rare cases, suspension of processing rights has also occurred.

Some Retail & Consumer companies may also be under the false assumption that if they are in compliance with the PCI standard, they are adequately protected from all threats and vulnerabilities to customer and credit card data. More specifically, Retail & Consumer companies may not have identified or addressed all of the vulnerabilities across the enterprise even if they are PCI compliant. In addition, companies that are only required to perform the PCI self-assessment may not have undertaken a comprehensive, in-depth review of the protection of their credit card processing and storage systems. Moreover, they may not have considered how to protect other sensitive data such as information collected through loyalty programs, customer and employee personal information, and employee health information.

How to improve your company's data protection

Compliance with specific PCI mandates and broader information security policies,

although a good start for avoiding risk and protecting data, is typically a tactical exercise and cannot be relied upon to ensure a company's protection against a security breach. In order to strengthen their position against attack and the all-consuming business issues that can result, Retail & Consumer companies need to take a strategic view of data protection and establish comprehensive and sustainable programs to identify and mitigate risk throughout the organization.

If Retail & Consumer companies are to protect their sensitive data throughout its lifecycle, they must begin at a high level with a comprehensive data protection risk management strategy. This calls for the commitment of executive management to address data protection and sustain protection efforts going forward. Data protection needs to be on the agendas of both management and governance bodies, such as boards of directors and audit committees.

Furthermore, Retail & Consumer companies need to have a thorough understanding of the complete data lifecycle of their credit card and other customer data both within and outside the boundaries of their organizations. This can be accomplished through data inventory and data flow analysis activities. In our experience with working with large global Retail & Consumer companies, we have found many instances where companies were not aware of all locations where credit card and customer data was being stored and where this sensitive data was being transferred unprotected across international borders and to multiple third parties.

Another area within the data lifecycle that requires attention is data loss prevention or data leakage. Too often, companies focus heavily on protection from outside attacks while insufficiently addressing the biggest threat which is the inside threat posed by employees, contractors, and temporary staff who can unintentionally or intentionally cause a loss of data or leak sensitive information to an inappropriate party. Based on our experience, credit card and customer data exits Retail & Consumer organizations undetected and unprotected through many channels, such as e-mail, file and web transfers, USB devices, CDs, DVDs and laptops. Retail & Consumer companies need to develop and implement mechanisms to detect,

block and prevent this sensitive information from leaving the organization.

After gaining a thorough understanding of where sensitive data resides and how it flows through and out of the organization, Retail & Consumer companies can begin to assess the risks and the adequacy of controls and security across the data lifecycle. This often means conducting a risk assessment to identify appropriate preventive and detective controls, developing an incident response plan, and aligning data protection risk management activities with the company's overall risk management and business activities, goals, and objectives. This approach allows for a more holistic view of these risks — how data protection risks interact with and are affected by other risks and activities throughout the company and, more importantly, how the company can prevent a data breach from happening and how to respond appropriately if a data breach were to occur.

From there, companies must develop an overall data protection program that includes compliance with applicable government regulations and industry standards, such as the PCI standard, while also addressing broader risks that fall outside of those requirements and standards.

Conclusion

Data protection is a daunting issue for today's Retail & Consumer companies and only promises to grow in importance, size and complexity. To develop a comprehensive strategy for addressing data protection risks, Retail & Consumer companies can begin by considering the following five questions:

1. Does the company have strategic compliance efforts underway?
2. Is there support for and a commitment to data protection among senior management and the board of directors?
3. Is the company clear on where it stands regarding its PCI compliance requirements, including its assigned merchant level, and its ability to comply with PCI requirements?

The Payment Card Industry (PCI) Data Security Standard

The Payment Card Industry (PCI) Data Security Standard encompasses 12 security domains for the protection of cardholder data. The requirements fall into four categories: (1) building and maintaining a secure network, (2) protecting cardholder data, (3) maintaining a vulnerability management program, and (4) regularly monitoring and testing networks. All merchants that process more than six million transactions per year must undergo an annual security assessment and external vulnerability scans by a certified assessor or the company's own Internal Audit department. Noncompliance with these requirements can lead to significant fines. For more information, go to: www.pcisecuritystandards.org.

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data by business need-to-know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Specific areas of focus where Retail & Consumer companies typically face challenges in meeting the PCI standards include:

- Encrypting credit card data in accordance with PCI standards so that full credit card data is not readable, or implementing appropriate compensating controls.
- Securing and controlling remote access to credit card-related systems, especially in cases where remote systems (i.e., employee's home computers) are able to access the corporate network remotely.
- Securing and segmenting wireless networks, particularly wireless at retail store locations, from the corporate network and credit card systems in order to protect them from attacks originating on wireless networks.
- Managing user IDs and passwords at retail locations, particularly on point-of-sale systems, where generic and default logins are often used to access systems and are seldom changed, therefore allowing ex-employees and others a way to easily access the system without being able to track their actions.
- Properly segmenting store networks from the main corporate network, and further segmenting critical credit card processing and storage systems to prevent compromised systems from store and other network segments from being used as launching points for attacks.
- Improving auditing, monitoring, and logging capabilities for credit card-related systems to ensure any malicious activity is detected and responded to in a timely manner.
- Maintaining software security patches to ensure that systems are not susceptible to known vulnerabilities.
- Writing secure web applications that prevent common web-based attacks, such as SQL injection.

4. Can the question “Is our data protected throughout the data lifecycle?” be answered with confidence and supported with evidence?
5. Where is the credit card and other customer data processed and stored and is the company storing “track” credit card data?

Once these questions have been answered, Retail & Consumer companies can begin to create and implement an effective strategy for protecting their sensitive data and can begin to address their information security and risks across the enterprise.

With senior level management commitment, an understanding of the risks facing the company, and a comprehensive data protection program in place to address those risks, Retail & Consumer companies will be well on their way to protecting their systems and sensitive data.

PricewaterhouseCoopers Contacts

For more information about the subject of this *QuickBrief*, please contact:

John G. Maxwell 973-236-4780
Americas Retail & Consumer Industry Leader

Nadia Alaudini 513-361-8185
Retail & Consumer Assurance Partner

Gerard Verweij 617-530-7015
Retail & Consumer Advisory Partner

Ron Kinghorn 617-530-5938
Retail & Consumer Systems & Process Assurance Partner

www.pwc.com

This document is provided by PricewaterhouseCoopers LLP for general guidance only, and does not constitute the provision of legal advice, accounting services, investment advice, or professional consulting of any kind. The information provided herein should not be used as a substitute for consultation with professional tax, accounting, legal, or other competent advisers. Before making any decision or taking any action, you should consult a professional adviser who has been provided with all pertinent facts relevant to your particular situation. The information is provided ‘as is’, with no assurance or guarantee of completeness, accuracy, or timeliness of the information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability, and fitness for a particular purpose.