Strengthening security after a breach of a retailer's customer data

A large global retailer establishes a sustainable security program after a serious customer data breach.

Consulting
Information Security

June 2014

Client's challenge

A global grocery retailer with more than 1,000 U.S stores suffered a public data breach that compromised millions of customer credit- and debit-card numbers. The retailer faced numerous shortcomings in its overall security practices, including:

- A lack of consistent processes to manage its IT environment, and a lack of knowledge about where sensitive data resided, how it was used, who had access, and how it was protected.
- Compliance efforts for regulatory mandates like Payment Card Industry Data Security Standard (PCI DSS) were, for the most part, manual.
- A lack of secure storage of electronic health information and personally identifiable information (PII) of customers and employees.
- Unsecured documents detailing business procedures and processes that could potentially expose sensitive data.

As a result of the breach, the retailer faced possible action by the FTC in the form of a consent decree mandating that violations be mitigated. The retailer needed help remediating the security breach, and developing and implementing a sustainable security program. They also required assistance in selecting and deploying supporting technologies that would help with security and data privacy.

PwC's Advisory solution

The retailer engaged PwC to design and implement a comprehensive program for data security and privacy. A core component of this initiative entailed the design and deployment of a data loss prevention (DLP) solution.

Our team of specialists met with members of the retailer's security and compliance groups to help identify the location of critical data across the enterprise; design and apply appropriate controls based on business processes; and draft a roadmap to identify and protect sensitive data in the future.

pwc

Drawing upon knowledge of the retailer's unique business needs gleaned from previous engagements, we helped select the Symantec Data Loss Prevention solution. Our team crafted a strategy to integrate Symantec DLP into the retailer's existing Governance, Risk, and Compliance (GRC) tool to better manage its risk and compliance issues.

During the planning and design phase, we collaborated with the retailer so that its data security strategy, program, and business processes seamlessly integrated with business requirements. The Symantec DLP solution was employed to scan and identify sensitive data in multiple repositories across more than 1 petabyte of storage.

We also helped craft a strategy to inspect and identify sensitive data in transit to outbound networks and to discover sensitive data in use on high-risk endpoint assets, such as retail transaction databases and file shares on the corporate network. We identified business processes that allowed unnecessary user access to data, enabling the retailer to remove data from unauthorized and unsecured locations. It also paved the way for deployment of mitigating controls like encryption and tokenization.

We collaborated with the retailer's security and compliance teams to develop incident-response plans. We also helped design employee training for the DLP solution, including policies, operational processes, and configuration for continuous detection and remediation. Finally, we helped develop controls, including classification and separation of data into various network segments, which can be applied in the future as necessary.

Impact on client's business

PwC's solution not only helped remediate a serious data breach, but we also assisted the retailer in developing a comprehensive, sustainable data security program. We delivered an end-to-end strategy to identify and protect sensitive data for today and the future.

The retailer now has the technology, people, and processes to better understand where sensitive data resides, how it is used, and who has access. The retailer can detect and stop external dissemination of sensitive data and they can better understand the scope of regulatory and industry pressures such as PCI. The retailer also has secured the personally identifiable information (PII) of employees and customers, and implemented ad-hoc and scheduled data-validation processes.

For more information, please visit

www.pwc.com/security

Or contact

G. Christopher Hall
Principal
(724) 396-3677
g.christopher.hall@us.pwc.com

Robert Boyce
Director
(404) 877-2478
robert.boyce@us.pwc.com