After a breach, a retailer strengthens its security

How PwC helped establish a sustainable security program after a serious breach of customer data

Advisory Services
PwC Symantec Alliance

January 2014

Client's challenge

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

- The company did not have consistent processes to manage its IT environment and lacked a thorough understanding of where sensitive data resided, how it was used, who had access to it, and how it was protected. What's more, the retailer's compliance efforts for regulatory mandates like Payment Card Industry Data Security Standard (PCI DSS) were, for the most part, manual.
- The retailer did not securely store electronic health information and personally identifiable information (PII) of customers and employees.
- It also had unsecure documents detailing business procedures and processes that could potentially expose sensitive data.
- As a result of the breach, the company was facing possible action by the FTC in the form of a consent decree mandating that violations be mitigated.

The grocery retailer needed help remediating the security breach and developing and implementing a sustainable security program. It also required assistance in selecting and deploying supporting technologies that would help ensure security and data privacy.

PwC's Advisory solution

The retailer engaged PwC and our strategic Alliance, Symantec Corp., 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 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 for identifying and protecting sensitive data in the future.

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

During the planning and design phase, PwC collaborated with the retailer to ensure that its data security strategy, program, and business processes are 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.

pwc

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.

Our team of specialists 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.

PwC 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, we also assisted the grocery retailer in developing a comprehensive, sustainable data security program. Our solution delivered an end-to-end strategy for identifying and protecting sensitive data, for today and the future.

- PwC's solution provided the retailer with a thorough understanding of where its sensitive data resides and when it was accessed. This has enabled the company to apply the right controls to safeguard data and help prevent future breaches.
- We also helped decrease the enterprise footprint of sensitive data and helped migrate sensitive data to secure network environments, or protect this data using encryption or tokenization.

The retailer now has the technology, people, and processes in place to better understand where sensitive data resides in its environment, how it is used in business processes, and who has access to it. In addition the retailer can also detect and, when necessary, stop external dissemination of sensitive data. As a result, the retailer can better understand the scope of regulatory and industry pressures such as PCI. The company also has secured the PII of employees and customers, and implemented ad-hoc and scheduled data-validation processes as part of the new environment build 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