



Topics: Privacy, Regulatory Compliance

Case Study: SiegeWorks Provides Privacy & Compliance Solutions for Iowa Bank

Overview

SiegeWorks is a leading global enterprise security services, consulting and integration firm, serving as clients' critical first line of defense. A comprehensive portfolio of Digital Defense Services™ (SiegeWorks DDS™) and technology solutions is available, from digital risk assessment and management, to business continuity assurance services. SiegeWorks solutions enable proactive business and revenue protection and unconstrained information exchange.

The Issues

Organizations are under a tremendous amount of pressure, with networks and applications constantly under attack by increasingly sophisticated digital enemies. There is an essential need to ensure that privacy safeguards are in place to protect their customers and partners in addition to their own intellectual property.

In order to achieve and remain in compliance with corporate privacy policies and evolving regulatory requirements, SiegeWorks' team of information security experts help clients manage risk by providing security solutions to monitor, respond and adapt to an ever-changing, challenging environment. This is particularly crucial for organizations in highly regulated industries such as financial services, healthcare and government, where audits are conducted quarterly and violators of the law face steep fines or imprisonment for non-compliance.

The Situation

An Iowa-based bank was rolling out a new enterprise-wide CRM initiative to its vendors and wanted to make sure, that the software and operations were hardened against hacker, as well as unauthorized employee and vendor intrusion. In the process, they needed to assure that private customer information or proprietary corporate information could not, inadvertently, be shared with unauthorized parties.

The Challenge

SiegeWorks' client needed to assure that the new CRM system addressed security and privacy issues effectively and completely. This included meeting legal compliance requirements, according to the Gramm-Leach-Bliley Act (GLBA), SEC regulations, the Sarbanes-Oxley Act, and others.

Of all the issues presented, the most challenging would be the lack of specific ownership of the project by any single group. The bank's senior management realized that in order to execute a successful CRM rollout and security plan, they needed to bring in a consultancy with strong security and compliance expertise. This partner, together with the Project Manager, would assure that all departments worked together as a team, including

Information Technology, Information Security, Customer Service, Marketing, Finance, and other lines of business.

The Solution

SiegeWorks first reviewed the client's entire CRM implementation. Consultants looked at information data stores and business transaction processes that were affected, and also reviewed internal/corporate policies and regulatory compliance requirements. Then, they designed strong security measures around core business processes and confidential information.

Integral to SiegeWorks' process was an audit to identify the areas that were vulnerable to hackers or privacy breaches. Calling upon its Best Practices knowledge and expertise, consultants educated the Project Manager about potential issues and how they should be addressed. After interviewing each team member, SiegeWorks produced a documented CRM implementation and vulnerability remediation plan (with security measures prioritized according to criticalness). The plan would assure that important information and systems would be hardened against attack.

SiegeWorks trained and prepared all members of the team that would be instrumental in rolling out the CRM implementation or handling remediation tasks or management. At the end, SiegeWorks provided a final audit to assure vulnerabilities were adequately addressed.

Contact SiegeWorks today for a customized assessment of your privacy and compliance needs.