



Topics: Business Process Security, Business Process Outsourcing

Case Study: BPS for BPO

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

In today's challenging business environment, many companies are looking for ways to streamline business processes. Often, they choose to outsource certain processes, a practice which is known as BPO—business process outsourcing. BPO can include the following key functions: administration, finance and accounting, human resources, payment services, sales, marketing and customer care, supply chain management, software development, and more. There are many benefits to BPO; in addition to the promise of major cost savings, for example, there's the ability to respond more quickly and flexibly to changing market conditions while focusing on core competencies to bring in revenue and growth.

However, ensuring the security of business processes can be a challenging endeavor, and a risky one—especially when outsourcing.

The Situation

For SiegeWorks' client, an enterprise F100 retail software company based in the Silicon Valley, California, security became a key factor in its BPO initiatives. They wanted to outsource backend processing for customer support as well as certain software development. When they ran these as pilot programs, security was not an issue, however going into production they needed to assure that systems were secure, complied with internal policies, and met compliance requirements for regulations such as the Gramm-Leach-Bliley Act and the California Security Breach Information Act, Section 1798 (CA1798). They also wanted to assure that customers would be comfortable with the way they were handling their outsourcing initiative—that they would know the company remained in compliance with laws and its systems were hardened against hackers and malware (viruses, etc.). Finally, they needed to ensure that outsourcing partners were unable to gain access to confidential systems via "back doors".

SiegeWorks worked with this client to plan and implement a security solution to fit its BPO needs.

The Challenge

While outsourcing can be extremely cost effective, layering security expenses on top can render such projects too costly. However, security breaches can cost a company more than they ever bargained for.

SiegeWorks' client could have hired one of the largest consulting firms to address its security needs, which would have sent representatives to each of its overseas outsourcing locations; however, those consultants wouldn't have understood local laws, nor be able to translate the company's needs clearly. This client wanted a global company with local expertise and highly focused security proficiency to oversee this important initiative, train its partners and assure universal compliance with policies.

They had two primary concerns, the first of which was the security of their network. Outsourcers would need access to the company's systems and databases in order to provide customer support. Dedicated networks would need to be put in place to assure security of confidential corporate and customer data. They would require a combination of the right technologies and processes, including access control, identification and authentication, and hardened applications and databases.

Secondly, the client needed to assure that applications being developed by partners were secure and of the highest quality, while cutting costs and time to market.

The Solution

SiegeWorks' client needed guidance in considering the many security factors involved in its BPO initiatives. It took the client through a series of Best Practices to help them understand the consequences of security risks to its network and externally-developed software.

To assure network security, SiegeWorks provided the client with system and process audits and vulnerability penetration tests, producing risk reports by location. Comprehensive training was offered to all local staff members, outlining and assigning remediation priorities and responsibilities in order to assure that all partners were adhering to a single set of guidelines, and in compliance with corporate policies and standards. Technology solutions were implemented where lacking, such as firewalls, intrusion detection and prevention systems, authentication mechanisms, and so forth.

For software development, SiegeWorks provided training classes that followed a series of Best Practice documents. Testing and code reviews were conducted early, at the design and build phase, with re-testing prior to production. Outsourcers were audited at their individual locations so that problems could be fixed locally, saving time, money and other difficulties by a factor of 4x for the client.

Because SiegeWorks' client took the right measures up-front and proactively (rather than reacting to problems later), they enjoyed major cost and time savings, peace-of-mind security assurances, and had a positive experience overall. They were able to maintain business continuity through the entire process, and they are now always prepared for regulatory audits. Last but not least, they now have a standard, policies and procedures in place, so they can choose to outsource more, and more easily, to achieve the market advantage.

Contact SiegeWorks today to find out how we can provide a customized security process to fit your BPO needs.