netSPI Case Study

RISK COMPLIANCE SECURITY

Carlson Companies

Carlson Companies Uses NetSPI as Part of a Comprehensive Approach to Information Security

Expertise, Independence, Cost Cited as NetSPI Advantages

Carlson is a global group of integrated companies providing travel, hotel, restaurant, cruise and marketing services directly to consumers, corporations and government units. Carlson's brands, including Radisson Hotels, T.G.I Friday's, and Carlson Wagonlit Travel, operate in some 150 countries. It is one of the largest privately held corporations in the world.

To earn and keep the trust of customers and partners, Carlson must comply with an array of laws and industry standards concerning information security and privacy. For example, there is PCI, the Payment Card Industry set of requirements for handling credit card transactions. In addition, there are standards for data privacy and security mandated by HIPAA and Graham-Leach-Bliley legislation.

At the same time, the job of guarding confidential data is a much more complicated undertaking than it was a generation ago, when sensitive information was mostly protected in secure data centers. Today's environment is vastly different, with emails on cell phones, spreadsheets on tiny USB drives, and confidential plans on laptops that can be easily lost or stolen. Today, the environment is more challenging, and the rules are more demanding.

Designing a Comprehensive Approach

In 2006 Carlson Companies decided to take a comprehensive, holistic approach to managing information security. First, the company aligned itself with the relevant ISO

CASE STUDY AT A GLANCE

Client

Carlson is a global group of integrated companies providing travel, hotel, restaurant, cruise, and marketing services directly to consumers, corporations, and government units. Carlson's brands. including Radisson Hotels, T.G.I Friday's, and Carlson Wagonlit Travel.

Challenge

Carlson is required to provide Visa with an assessment of its compliance with Level 1 standards. PCI standards require an in-depth third-party assessment.

Solution

NetSPI helped identify some flaws in firewall management and determined what remediation was needed. NetSPI also performed penetration testing, both at the network and application levels.

Results

"NetSPI found some gaps in the firewall rules and drove the workflow in making the necessary changes… The results of NetSPI's penetration tests are not typical…They don't just give us a 10,000-foot view; they dig deep, and we are able to act on their recommendations. By the way, they also charge less than other QSAs."

standards, 17799 and 27002. Second, the company wrote an Information Security Charter, spelling out roles and responsibilities for providing governance, oversight and policy in this area. Third, Carlson embedded these standards and policies into an Information Security Framework that covers people, processes and technologies. And finally, to integrate these policies into regular business operations, the company established a company-wide Information Security Council, which is headed by Kathy Orner, Vice President and Chief Information Security Officer.

Each division has an Information Security Officer who sits on the council, which meets monthly and has an annual summit. The council drives IT security policies, incorporating HIPAA, Graham-Leach-Bliley and PCI requirements into global enterprise policies, ensuring these requirements have the necessary visibility and priority across the enterprise.

PCI Assessments and NetSPI

PCI standards in particular have become more detailed and rigorous, as the credit card industry has expanded its efforts to prevent fraud and ensure the security of card numbers and cardholder data. Moreover, the requirements of the standard increase with the number of credit card transaction a company handles. Carlson's volume of transactions makes it a Level 1 provider to Visa, for instance. As such, it is required to provide Visa with an assessment of its compliance with Level 1 standards. This kind of assessment used to involve only a self-administered questionnaire. Today, though, credit card companies require a more in-depth assessment, e.g., with detailed information on server and firewall configurations. And they want the assessment performed by a qualified third party.

To do this important job, Carlson brought in NetSPI, a Qualified Security Assessor, or QSA. NetSPI helped identify some flaws in firewall management and determined what remediation was needed. In the process, the NetSPI specialists created a taxonomy of the firewall rules and eliminate many that were overlapping or inactive. It takes considerable technical and administrative expertise to understand the sources of rules, the business reasons they were established, and the cascading effects of removing a given rule.

Next Steps: Automating the Process

As Kathy Orner noted, "NetSPI found some gaps in the firewall rules and drove the workflow in making the necessary changes. In the future, we look forward to working with NetSPI to potentially have an automated solution for mandated vulnerability reviews. It will be great to automate the workflow involved in maintaining compliance and be even more efficient."

Penetration Testing

NetSPI has also been helping Carlson with penetration testing, both at the network and application levels. To do this critical work, NetSPI has a team dedicated to application assessment and code review. This group has developed a comprehensive methodology that includes both commercial and proprietary tools, as well as extensive manual testing. In fact, 80% of the "high and severe" findings are discovered through the manual process.

Kathy Orner noted, "The results of NetSPI's penetration tests are not typical. They go to a much deeper level and get more granular. That enables us to understand better the areas of risk we need to remediate. They don't just give us a 10,000-foot view; they dig deep, and we are able to act on their recommendations. By the way, they also charge less than other QSAs."

"NetSPI found some gaps in the firewall rules and drove the workflow in making the necessary changes. In the future, we look forward to working with NetSPI to potentially have an automated solution for mandated vulnerability reviews."

Kathy Orner,
Vice President and Chief
Information Security Officer

An Independent, Objective View

Another NetSPI advantage is that Carlson can rely on it for independent, objective test results. Other companies can do penetration testing for Carlson, for example, but if another company is in a position to correct any vulnerabilities that are identified, that testing is not seen as truly independent. The natural temptation is strong to fix the problem, rerun the test, and present a clean report. As Kathy Orner said, "In my position, I feel much more comfortable with NetSPI saying there are certain vulnerabilities, because I know that NetSPI cannot change those vulnerabilities before the report gets to me."

The Differentiators

Kathy Orner sums up NetSPI's contribution to the global effort to manage information security across the many Carlson businesses: "NetSPI has been doing a great job for us. Their technical expertise is a differentiator, along with their in-depth, actionable reports, their arm's length objectivity and their lower cost."

> *""The results of NetSPI's penetration tests are not typical. They go to a much deeper level and get more granular."*
>
> Kathy Orner,
> Vice President and Chief
> Information Security Officer

A Better Approach to Risk, Compliance, and Security Consulting

NetSPI focuses on customized, responsive, product-independent consulting. Teams of security professionals with deep technical expertise and specific industry knowledge provide a range of advisory, assessment, and audit services that deliver objective, strategic, actionable results.The result is objective, strategic guidance for your security and compliance needs.

netSPI
RISK COMPLIANCE SECURITY

800 Washington Avenue North, Suite 670, Minneapolis, Minnesota 55401
www.netspi.com 612.465.8880 Telephone 888.270.0317 Toll free 612.455.6988 Facsimile