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

CARLSON

The Challenge

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 Gramm-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.

1. **ISO Standards:** The company aligned itself with the relevant ISO standards, 17799 and 27002.
2. **Information Security Charter:** The company wrote an Information Security Charter, spelling out roles and responsibilities for providing governance, oversight, and policy in this area.
3. **Information Security Framework:** Carlson embedded these standards and policies into an Information Security Framework that covers people, processes, and technologies.
4. **Information Security Council:** 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.

About Carlson Companies

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. For more information, visit carlson.com.

Industry
Hospitality

Headquarters
Minnetonka, MN

Reach
Global

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, 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 transactions 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 eliminated 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.

> 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 at Carlson Companies*

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.”

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.”

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.

Website
www.NetSPI.com

Email
Info@NetSPI.com

Phone
612.465.8880