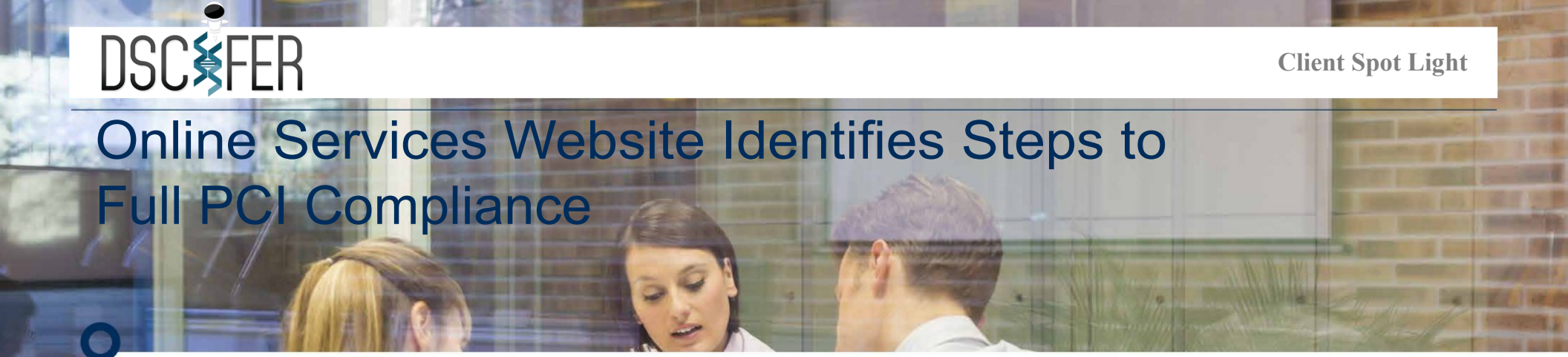

Online Services Website Identifies Steps to Full PCI Compliance

PCI compliance is just one piece of the security puzzle - how do you remain compliant while also addressing wider security weaknesses?

An online service's website processes hundreds of credit card transactions each day in many countries. Like most companies, the organization prides itself in creating the best user experience across all mobile and online platforms. Part of that experience is the peace of mind in knowing that sensitive credit card information is protected.

To answer these challenges, the company needed a thorough review of its overall security environment to help ensure that it was compliant with PCI standards in preparation for future audits.

What was the best way to approach this challenge?

- Provide an environment baseline assessment on the current state of security.
- Perform a PCI gap analysis to measure current controls against PCI Data Security Standards (DSS).
- Create a roadmap to PCI compliance.

PROJECT OVERVIEW

Organization Size:
Over two million users

Retail/online services website

Challenge:
To create a snapshot of the current cardholder

Organization Industry:
environment, identify and then remediate PCI gaps in preparation for future audits.

IMPACT

- Obtained holistic view into current security environment from PCI compliance standpoint.
- Identified areas for improvement to remain compliant.
- Enhanced current processes and technology.

PCI GAP ANALYSIS SERVICES:

Setting a Baseline and Finding Gaps

Information Gathering

To start, Dscifer collected data to understand how the client was processing secure information. This included cardholder environments, current policies, procedures and network diagrams.

Establishing a Baseline

Using PCI DSS, Dscifer established a baseline for analysis, including how the company builds and maintains a secure network, maintains a vulnerability management program, implements control measures and regularly monitors and tests networks.

Interviews and Onsite Testing

The baseline analysis also included interviews with staff responsible for information security to help make sure that processes were consistent. Dscifer also performed physical site walkthroughs, a data center review and an overall systems review to gain a holistic view of the organization.

Identifying Gaps

After these standards and expectations were set, Dscifer identified gaps in technologies, policies, standards and practices against the PCI DSS.

Roadmap

Dscifer provided the client with very specific remediation steps and a PCI Compliance Roadmap to secure the environment in preparation for upcoming audits.

Creating a Roadmap for the Future

PCI compliance is central to a retail organization's credibility and to maintaining a high level of security for its customers. It is important to work with a strategic partner that recognizes that while PCI is vital to running a secure business, it is not the only piece of the security puzzle.

Because PCI standards only address specific elements of data security standards, they don't necessarily speak to a company's entire security program.

As a result of the gap analysis, the client:

- Understood its existing security posture and current gaps and weaknesses.
- Attained tailored recommendations that were impactful yet cost-effective.
- Obtained a roadmap to PCI compliance.
- Reduced risk of data breach by working to eliminate gaps in the program.

DSCIFER

Dscifer.com

Dscifer specializes in comprehensive pure-play Cyber Security, Digital Forensic & E-Discovery, Risk Management, Healthcare, Aerospace and Defense Systems solutions. Our diverse and talented employees are committed to help businesses, governments and educational institutions plan, build and run successful management programs through the right combination of products, services and solutions. For further information visit www.dscifer.com