CASE STUDY

Securing Transactions and a Company's Growth

The rise of the internet created massive opportunities for companies that figured out how to bring services and payments online. As e-commerce exploded, however, businesses took much longer to respond to cyber-thieves who steal credit card information stored on websites and internet-connected cash registers. That's changing. In the wake of a handful of high-profile retail breaches and the rollout of the Payment Card Industry Data Security Standard (PCI DSS) 3.0, companies small and large have realized they must adapt stringent security protocols—or face possibly ruinous consequences.

Trustwave®
Smart security on demand

CLIENT SPOTLIGHT

This major hotel booking system began at the founder's dining room table in the late 1980's. Over the past three decades, it has evolved into a huge online hub with its own payment processing technology—and has become the undisputed market leader in its country. Today, vacationers, government workers, student travelers, and corporate event attendees book hotels and other travel properties directly through its site.

THE CHALLENGE

A hotel booking system had responded to myriad technology- and market-driven changes over the past three decades, including building its own payment processing system. Allowing travelers to pay on its site was efficient for consumers and lucrative for the company—but also left the owners responsible for meeting increasingly tight payment card security measures. The booking system, which processes hundreds of thousands of credit card transactions, was struggling to respond to pressure to meet the PCI DSS. If it didn't comply quickly, the company faced a crippling blow: Losing its biggest travel management partner and its largest direct client.

> *"It's not a single step sort of thing. Getting the PCI DSS certificate was great, but now it's all about maintaining certification and staying secure. Trustwave gives us that."*
>
> – Managing director, travel booking company

THE SOLUTION

The booking company implemented Trustwave Compliance Validation Services. The package also included Trustwave Managed Security Testing, which performs regular scans of databases, networks, and applications, plus deep-dive penetration testing. As a result, the company gained PCI DSS compliance in 2014—and renewed its major contracts. This achievement increased customer trust and distinguished the firm from its main rival, allowing it to increase its total transaction value by more than 500 percent between 2014 and 2015. Executives explicitly attribute $3.5 million in monthly revenue to PCI DSS compliance and security enhancements.

Accordingly, the company became a true believer in Trustwave services. It added Trustwave Data Loss Prevention, Managed SIEM, Web Application Firewall, and File Integrity Monitoring to help ensure its staff had the support necessary to provide state-of-the-art system security. Outsourcing security concerns freed up the company's roughly 40 employees to focus on growing the payments business and expanding internationally.

INDUSTRY THREAT

Everyone remembers the major credit card breaches that felled huge retailers beginning in 2013, but the problems aren't over. Though security standards have increased and hacks on point-of-sale systems as a percentage of overall security attacks have fallen since those incidents, breaches still occur with alarming frequency. Even a relatively small breach can have major financial consequences. With cybercriminals changing their tactics at an astonishing rate, many companies just can't keep up.

> *"Trustwave knows what to do. We don't."*
>
> – Managing director, travel booking company

Trustwave®
Smart security on demand

CS-HOTELBOOKING-0218