CASE STUDY

HITACHI
Inspire the Next

PCI COMPLIANCE

In order to ensure credit card payment security, the Payment Card Industry Security Standard Council (PCI SSC) defined a set of compliance requirements to safeguard credit card transactions and consumer personal and financial data under the Payment Card Industry Data Security Standard (PCI DSS). All organizations that handle cardholder information are subject to compliance with PCI DSS requirements.

QUICK FACTS

Industry: Media & Entertainment

Company Type: eCommerce and Information and Communication Services

Location: Canda

Needs & Requirements:

- Improve security posture to better protect corporate IT assets against vulnerabilities and intrusions
- Identify missing security controls
- Meet annual PCI DSS compliance requirements
- Report findings to executive team

THE CHALLENGE

The customer was facing several regulatory requirements involving important changes in its internal processes and technology. One of these requirements was from the Payment Card Industry (PCI). From an information security perspective, it was unclear the implications of such requirements as well as the required efforts to move forward to a compliance process.

The Payment Card Industry (PCI) Data Security Standard (DSS) is a set of specific security requirements for companies that process, transmit or store payment card information. This comprehensive standard is intended to help organizations protect customer account data and reflects most of the usual best practices for securing sensitive information.

THE SOLUTION

Since the customer had no clear understanding about PCI requirements implications, and given that its compliance project was in its initial stage, our approach for this mandate was to perform a comprehensive Gap Analysis in relation to PCI DSS requirements:

- We started by performing a business processes analysis in order to identify payment options as well as cardholder information to be protected.
- We evaluated the customer's security controls currently in place, in comparison to specific requirements established in the PCI DSS. During this evaluation, we considered human, technical and administrative aspects.
- We performed a comprehensive revision of all information security documentation available.
- Our network design team was also involved in the technical review of critical IT infrastructure elements, in particular, network architecture.
- As a result from this process, we produced a detailed report showing all gaps between security controls in place and PCI DSS requirements.
- Finally, we provided the customer with a list of recommendations and a proposed action plan in order to correct identified gaps.

MAIN BENEFITS

This project allowed our customer to:

- Understand the PCI DSS requirements implications;
- Identify missing security controls in relation to PCI DSS requirements;
- Develop administrative and procedural security controls as required by the PCI DSS;
- Identify cost-effective security measures that will help to reduce PCI scope and compliance costs;
- Design a detailed implementation plan to achieve PCI DSS compliance;
- Improve overall organization's security posture;
- Benefit from PCI DSS security controls implementation to achieve compliance to others regulatory requirements.

SERVICES PROVIDED

A team of Hitachi Systems Security Inc.'s Senior Cyber Security Experts collaborated on this engagement to:

- Support our customer through our PCI services portfolio including pre-audit and gap analysis services
- Provide proper recommendations about secure network architecture oriented to facilitate PCI DSS compliance

Hitachi Systems Security Inc.
955 boul. Michèle-Bohec, Suite 244, Blainville (Québec) J7C 5J6 Canada
Tel: +1 450-430-8166   Fax: +1 450-430-1858
www.hitachi-systems-security.com