

A FORSYTHE CASE STUDY

PCI DSS Compliance

A Consumer Goods Company

Business Challenge

A consumer goods company with a Web-based ordering system supporting 70,000 customers was faced with meeting the compliance requirements of the PCI Data Security Standard (PCI DSS), which is designed to ensure the security privacy of customer credit card and transaction information. PCI DSS defines a standard of care developed by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International for securing consumer cardholder data, wherever it is located. Compliance is required of all entities storing, processing, or transmitting consumer cardholder data. Merchant processors must comply and are responsible for ensuring compliance for all payment channels including retail (brick-and-mortar), mail/telephone order, and e-commerce.

PCI DSS compliance encompasses 12 basic security requirements:

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software
- Develop and maintain secure systems and applications
- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data
- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes
- Maintain a policy that addresses information security

The consumer goods company was looking for help with managing its entire PCI DSS compliance effort.

Solution

Forsythe performed a security assessment in order to create a roadmap for achieving PCI DSS compliance. Based on the results of the assessment, Forsythe also performed a comprehensive information security policy review, which focused on the requirements documented in the PCI DSS security audit procedures and reporting methodology. Our approach also incorporated industry best practice frameworks such as ISO-17799 standard and National Institute of Standards and Technology (NIST) standards.

Forsythe then worked with the company to develop an integrated information security policy to serve as a formal representation of management's strategy, intent, and commitment to protect company information assets. The policy was documented in logical sections addressing key control areas, assigning responsibility, and referencing ancillary documents. In this way, any security assessor evaluating the company's security program can clearly determine that their policy and documentation satisfy the PCI DSS requirements.

Results

The benefit of Forsythe's 35-plus years of IT-infrastructure experience combined with our

expertise in security solutions could be measured in terms of time and cost savings for this client. Forsythe's recommended creation of a request for information (RFI) to select suitable vendors that would enhance the security program based on the PCI DSS Compliance Review. The vendor evaluation and selection process in the Technology Evaluation Center significantly reduced the selection period for this client.

With Forsythe's assistance in choosing the vendor that would best meet its requirements, the client selected a mid-tier vendor solution which would not have been the obvious choice had their selection been made through a traditional procurement process. The chosen vendor solution brought an additional unforeseen 60% savings to the client when the cost of the selected technology was compared to its nearest competitor. Savings related to operational support of the new solution were also quickly recognized by the client.

In summary, Forsythe performed the following services during the course of the engagement:

- PCI DSS Gap analysis
- Remediation Roadmap
- Vendor Solution Analysis and Evaluation Support
- Solution Implementation

As a result of these projects, the client was able to successfully pass a formal PCI DSS audit.

