HEALTHCARE CASE STUDY

Foresite works with our healthcare clients to identify gaps and remediate against them when it comes to HIPAA and PCI compliance mandates and security best practice requirements

INDUSTRY: HEALTHCARE

BUSINESSINESS CHALLENGES

- Public HIPAA data breach
- Identifying gaps in compliance with new PCI DSS 3.0 standards
- Internal resources without sufficient time and expertise to quickly remediate issues

FORESITE SOLUTIONS

- PCI DSS 3.0 Gap Assessment
- Security and Compliance Advisory Services

OPPORTUNITIES

- Proactively find gaps in compliance and best practice
- Prioritize steps needed for remediation
- Ongoing consulting and assistance with remediation project planning and implementation in conjunction with the internal IT team

BACKGROUND

A hospital group was looking for outside assistance after suffering a very public HIPAA data breach, and subsequently realizing they were not meeting the compliance regulations for PCI DSS 3.0.

Foresite's Threat Mitigation Team met with their internal IT groups, and determined that while a recent HIPAA audit had provided them with steps for remediation, there was a lack of time for the internal team to oversee the remediation project. The team was concerned that the timeline to fix the issues would not be met. Further, it was unclear if the Cardholder Data Environment for PCI compliance had been accurately confirmed after many network changes.

OBJECTIVES

- Confirm current scope of the PCI Cardholder Data Environment
- Create a Prioritized Approach plan for remediation
- Provide ongoing support for project management and remediation assistance

SOLUTIONS

A PCI DSS Gap Assessment confirmed the current Cardholder Data Environment and the specific areas where compliance was not being met. This assessment allowed for creation of a prioritized list of items that require remediation, which could then be assigned to the hospital's various internal teams based on the expertise or systems involved.

Through an ongoing Security and Compliance Advisory service with Foresite, the hospital's staff is able to outsource oversight of the projects, and have access to resources with specific expertise that they don't have a full-time need for, but are required for aspects of the remediation, such as Payment Card Industry Qualified Security Assessors (PCI QSA), firewall security specialists, and Healthcare Information Security and Privacy Practitioners (HCISPP).

The flexible nature of the Advisory agreement means that resources can be both scheduled for specific projects and also utilized as needed for:

- HIPAA/PCI Consulting & Remediation
- Penetration testing and vulnerability scans
- Assistance with completing compliance documentation
- 3rd party vendor or solution evaluations
- Outsourced Security Operations team Incident Response

ABOUT FORESITE

Foresite is a global service provider delivering a range of managed security and consulting solutions designed to help our clients meet their information security and compliance objectives. In the face of increasingly persistent cyber-threats, Foresite's solutions empower organizations with vigilance and expertise to proactively identify, respond to, and remediate cyber-attacks and breaches where they occur.
Our team of industry veterans work as an extension of our clients' staff providing peace of mind while securing their most important assets. For more information, visit us at http://foresite.com or contact us at info@foresite.com.