CASE STUDY

LEGAL

PROACTIVE SECURITY

GAP ASSESSMENT

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

Business Challenges

- Meeting requirements of multiple regulatory compliances **(PCI, HIPAA, NIST, & MA CMR 17:00)**
- Identifying scope of systems subject to each regulation
- Lack of internal team's training & experience in cyber threats

Opportunities

- Compliance gaps remediated
- Ongoing consulting aids maintaining compliance as new locations added
- Outsourced network monitoring includes tools managing log data, human intelligence to confirm anomalous events & respond to protect interests

Foresite Solutions

- IT security assessment
- IT security and compliance advisory services
- ProVision security monitoring and alerting

BACKGROUND

When the American Bar Association issued a formal warning to law firms that they were key targets of international cyber criminals, it came as no surprise to the partners and board members of a large law firm with multiple offices and a wide range of commercial and personal clients. Still, as is the case in many law firms, they were uncertain their security measures met the highest standards necessary to protect the high value of data of their clients' intellectual property, personal data, financial information, and health records. They took immediate action. They charged the firm's IT director with hiring outside specialists who could help the team assess their current IT security best practices and applicable regulatory requirements compliance, and engaging these specialists in assisting the department in making recommended changes. Additionally, they pointed out the challenge of complications inherent in the firm's aggressive growth plans. Any newly acquired offices would need to be quickly brought under the same controls and managed from the same central office.

OUR **OBJECTIVES**

- ☐ Confirm types of data being transmitted & maintained to verify regulatory compliance guidelines
- ☐ Verify scope of systems for each compliance requirement
- ☐ Provide recommendations for meeting compliance requirements while minimizing scope to control cost of meeting compliance
- ☐ Engage specialists in PCI, HIPAA, NIST guidelines & IT security to assist firm's internal IT team w/new compliance & security implementations
- ☐ Engage specialists to provide expertise and manpower on an as-needed basis to eliminate full-time expense

OUR **SOLUTIONS**

Foresite's assessment first identified data types to confirm the regulations we needed to consider. We then compared the firm's existing state of current policies, procedures, and technical controls with appropriate requirements for compliance. Because of the firm's proactive approach to IT security, many required controls were already in place. Still, network monitoring was a challenge for its IT team - a staff of only five full-time employees, non of whom had formal IT security training or experience handling emerging cyber threats. We worked with the IT director on a proposal for ongoing assistance that was tailored to the firm's specific needs. It included:

1. Network security monitoring and alerting,
2. Incident response when the internal team needed to escalate investigation or remediation of a cyber incident to a trained security professional,
3. A block of consulting hours the IT director could use at his discretion for assistance with project planning and implementation to ensure new location were brought on with the same high level of IT security.

We presented the solution to the firm's IT committee to confirm it met the goals of all departments and made the case for proactive security to the board.

WORLD **HEADQUARTERS**
7311 West 132nd Street, Suite 305
Overland Park, KS 66213
+1 800-940-4699

CT **OFFICE**
1 Hartfield Blvd, Suite 300
East Windsor, CT 06088
info@foresite.com

UK **OFFICE**
A8 Ively Road, Farnborough
Hampshire, GU14 0LX, UK
+44 800-358-4915