CASE STUDY

INSURANCE

INCIDENT RESPONSE

PROVISION

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

Business Challenges

- Cyber security talent shortage
- Single resource with skills to manage key infrastructure
- Outdated Incident Response plan
- No escalation path for Incident Response
- Log data not being collected and maintained

Opportunities

- Supplement internal resources with trained and experienced cyber security and compliance teams
- Proactive assistance with creation/ revision to Incident Response plans
- Seamless integration with Security Operations Center and Compliance and IR teams

Foresite Solutions

- Advisory Services
- Incident Response Retainer
- ProVision Monitoring & Alerting

BACKGROUND

An insurance company couldn't hire enough cyber security talent to meet compliance requirements and protect sensitive data. A multi-state provider of property and casualty insurance products faced the common challenge of growing cyber threats and compliance requirements without the funding to add to their internal staff.

OUR **OBJECTIVES**

- ☐ Supplement internal IT team with compliance and cyber security expertise
- ☐ Review Incident Response plan and have IR team on retainer in the event of an incident that requires outside expertise
- ☐ Monitoring for correlation of logs and increased protection against threats

OUR **SOLUTION**

Foresite's Advisory services allowed the company to have access to our PCI Qualified Security Assessor (QSA) team, first on a project basis to help them review the controls and confirm the SAQ document, then on an "as needed" ongoing basis. Next, we addressed their concerns around Incident Response. Foresite's consulting team found that updates were needed to align their IR plan with the current technical controls and procedures. We also noted that logs that would be needed in the event of an emergency were not being archived, and that led to another need – log monitoring and alerting. Although the company had basic log monitoring and alerting in place to meet PCI compliance, the solution did not include one of the most important components – Incident Response support. The existing contract did not include monitoring for all of the key devices that could indicate a compromise and did not provide immediate access to log data for incident response, or a trained incident response team for the internal IT team to use for escalation of issues that they couldn't resolve. We also could co-manage their firewalls as part of our service which addressed a concern of their management team of what would happen if their one Palo Alto trained team member was unavailable.

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