CASE STUDY: An insurance company couldn't hire enough cyber security talent to meet compliance requirements and protect sensitive data.

BACKGROUND

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.

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.

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 as new questions arise.

This quickly led to the question "What else can Foresite help us with?" and the next need was to address their concerns around Incident Response. While they had an existing IR plan, the document had not been updated in some time, and no table top exercises had ever been performed to confirm that it included all the information necessary to be useful in the event of a cyber incident.

Foresite's consulting team found that updates were needed to align the 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.

FORESITE BENEFITS

- Foresite allows you to supplement your internal resources with our trained and experience cybersecurity and compliance teams
- ProVision monitoring can cover a wide-range of devices, including firewalls, IDS/IPS, load balancers, servers, and endpoint.
- Incident Response
    - Proactive assistance with creation/revision to Incident Response plans
    - As needed access to trained Incident Response team
    - Seamless integration with Security Operations Center and Compliance and IR teams for fastest response and access to log information, as well as a well-rounded understanding of the client's environment.

INDUSTRY

Insurance sector

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

FORESITE SOLUTIONS

- Advisory Services for access to trained cyber security and compliance pros
- Incident Response Retainer for both proactive and reactive needs
- ProVision Monitoring & Alerting with co-management of firewalls