# FINANCE CASE STUDY

*Foresite helps a financial services firm take a proactive approach to cyber security in preparation for State and Federal regulatory audits.*

## INDUSTRY: FINANCE

### BUSINESSINESS CHALLENGES

- Preparation for upcoming regulatory audits with limited internal staff availability
- Identifying gaps in compliance - staff didn't know what they didn't know

### FORESITE SOLUTIONS

- Cyber Security Assessment with social engineering campaign

### 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 financial services firm had regulatory audits coming up, and wanted to be sure they identified and remediated any issues before being audited. Although they have internal IT and compliance staff, this initiative wasn't moving forward as quickly as they had hoped, and they became concerned that without outside expertise, they could easily miss new requirements that would cause them to be non-compliant.

Foresite's IT Security resource consulted with the firm's stakeholders to confirm their objectives for this project.

### OBJECTIVES

- Confirm current state of Cyber Security
- Prepare for upcoming regulatory audits
- Establish a relationship with a cyber security firm who can provide resources for aspects of cyber security that the firm does not need on staff full-time (such as Incident Response)

### SOLUTIONS

We recommended a Cyber Security assessment to compare the firm's current policies and controls against NIST standards and SEC regulatory guidelines. Third-Party vendors were included to verify that appropriate agreements were in place that confirmed the 3rd parties were following the firm's security practices. We also incorporated social engineering to test the human aspect of the firm's cyber security, as many breaches are caused by failure of staff to follow security awareness best practices.

Our findings for the firm were not unusual. Although they had much of the security best practice framework in place, missing security patches, use of default admin account credentials for devices like network printers and routers, and outdated account access policies in Active Directory left them vulnerable to attack, and not completely up to compliance standards. All of these issues were easily fixed by their staff and outside IT support firm once identified.

An email phishing campaign was developed to test the firm's staff on best practices for identifying and handling email scams. The firm was proud that their security awareness training proved to be effective, as despite multiple attempts and campaigns, staff alerted each other and the firm's executive team of the suspicious nature of the emails, and none of the users were tricked into providing their credentials. Although the firm had some documentation in place, they were missing some key policy documents that will be required for the audits, and some processes had not been documented at all. Again, a simple fix that will prevent them from a non-compliant audit status.

### 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.

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

WORLD HEADQUARTERS
7311 WEST 132nd STREET | SUITE 305
OVERLAND PARK KS 66213

www.foresite.com
(800) 940-4699