CASE STUDY

FINANCE

SECURITY ASSESSMENT

NIST GUIDELINES

FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

Business Challenges

- Preparation for upcoming regulatory audits with limited internal staff availability
- Identifying gaps in compliance

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

Foresite Solutions

- Cyber Security Assessment
- Social engineering campaign

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 had internal IT and compliance staff, this initiative wasn't moving forward as quickly as they had hoped. They became concerned that without outside expertise, they would 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.

OUR **OBJECTIVES**

- ☐ Confirm current state of cyber security
- ☐ Prepare for upcoming regulatory audits
- ☐ Establish a relationship with a cyber security firm

OUR **SOLUTION**

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. Although they had much of the security best practice framework in place, missing security patches, use of default admin account credentials for devices, and outdated account access policies in Active Directory left them vulnerable to attack and non-compliant. 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. 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. The firm had some documentation in place, but they were missing some key policy documents that will be required for the audits, and some processes had not been documented at all.

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