FORESITE
VISIONARY SECURITY & COMPLIANCE SERVICES

CASE STUDY

SECURITY ASSESSMENT

FUNCTIONAL TESTING

SOCIAL ENGINEERING

Business Challenges

- Client subject to annual audits
- Lack of trained cyber security internal staff
- Reliance on security personnel of commercial building for some of firm's physical security

Opportunities

- Identify vulnerabilities to be addressed
- Confirm building personnel are following security rules
- Verify security awareness of firm's staff to keep sensitive data protected

Foresite Solutions

- On site consulting to perform pre-audit functional testing of network
- Physical social engineering to validate building security and staff's adherence to establish cyber security policies and procedures

BACKGROUND

A firm in the finance sector performs audits to ensure they are doing everything they can to protect the financial data of their clients. Foresite has been contracted to send one of our auditors on site each year to perform functional testing of their cyber security controls and social engineering on the security personnel in the commercial building the firm is located in, as well as the firm's own staff.

OUR **OBJECTIVES**

□ Assist firm in maintaining secure environment to protect financial data

□ Preparation for outside audit to provide attestation of security to Board, clients and commercial insurer

OUR **SOLUTION**

□ Foresite Advisory Services allow the Foresite consultant to have flexibility to tailor testing in real-time based on observations while on site

OUR **RESULTS**

Functional testing of the technical controls shows that vulnerabilities are being patched in real-time and configurations are following best practices, however, several weaknesses were uncovered with the social engineering our consultant performed while on site. A document containing very sensitive information was found in the copy room. Another document found in the office included credentials to access the client database. Although physical access to the office would be necessary to retrieve the information, numerous vendors and cleaning staff have access and are allowed to move around the office unescorted. A recently purchased SIEM solution had been partially configured for the firewall logs, but is not providing any correlation with log data from servers, endpoint/AV or other network devices. Overall, the technical controls are strong but more focus is needed on training staff to adhere to the clean desk and document shredding procedures already in place. A recommendation was made to consider outsourcing log monitoring for 24/7/365 coverage and trained security analysts to review the log data, as well as increasing the scope of what is monitored to provide correlation that can identify both known threats as well as suspicious behavior.

ABOUT **US**

WORLD **HEADQUARTERS**
7311 West 132nd Street, Suite 305
Overland Park, KS 66213
www.foresite.com
(800) 940-4699

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.