CASE STUDY

CONGLOMERATE OPTIMIZES HOLDINGS' SECURITY PROGRAMS

THE CLIENT

A privately held corporation with a large, diversified portfolio of companies.

THE CHALLENGE

The client wanted to ensure that the security risk at each of its subsidiaries was aligned with the parent organization's tolerance for risk, without severely hampering their autonomy.

THE SOLUTION

With the help of the Sirius Security practice, the client developed and implemented enterprise standards as the core of a new global security program that allows the parent organization to manage risk while still enabling each business unit to maintain autonomy. Sirius also helped the client develop a governance model to allow better visibility of risks across the organization. This included the creation of enterprise risk committees and a governance risk and compliance (GRC) platform. Finally, Sirius developed an organization-wide incident response program to dramatically improve the maturity of each subsidiary's ability to detect, respond to and report security incidents.

www.siriuscom.com
800.460.1237

It is Sirius policy not to identify clients featured in security case studies.

THE JOURNEY TO A HYBRIDIZED, CENTRALIZED SECURITY PROGRAM

With the help of Sirius, the client developed a modern, risk-based security strategy and individual programs at the holding levels, with oversight at the parent level. While each of the subsidiaries was free to develop its own programs, the holding company's standards clearly articulated a minimum set of security standards for each of the subsidiaries to follow, resources to assist with responding to security incidents, and a governance model that could help the organization manage risk on an ongoing basis. This helped the client right-size its security programs to emphasize what is most important and to frame every security issue in terms of risk to the business, with the right stakeholders involved in decisions on the best ways to proceed.

Sirius proposed a set of enterprise standards using ISO 27001:2013 and PCI controls as the basis for these standards, and then facilitated a meeting where each standard could be discussed and debated among each of the subsidiary CIOs. Ultimately, the organization developed a set of standards specifying what needed to be done rather than how to do it, allowing each of the IT leaders to retain autonomy over the methods by which they choose to implement solutions to fit their business needs. Examples of the standards include:

- All assets for the organization must be inventoried in an asset management system.
- All devices must run anti-virus client software.
- All structured and unstructured data will be tagged according to the organization's data classification and retention policy.
- All network traffic (both in and out) must be logged and monitored.
- Each organization will maintain an inventory of the applicable regulations with any known gaps in compliance status (e.g. GDPR, HIPAA, PCI DSS, and state and local requirements) to be tracked and managed on the organization's Enterprise Risk Register.

As each organization identified gaps in compliance with each of the new enterprise standards, roadmaps to deliver mature solutions supporting each of the standards were developed and included in budgeting exercises. To account for the varying size and nature of each of the subsidiary businesses, the enterprise standards were augmented to define five levels of maturity and a target implementation level for each standard and organization. Armed with these data points and strategic plans, the organization's new Enterprise Risk Committees can evaluate where additional investments and initiatives are required to align with the organization's tolerance for risk.

THE BENEFITS AND RESULTS

Sirius helped the client right-size its security programs to emphasize what is most important and to frame every security issue in terms of risk to the business, and with the right stakeholders involved in decisions on the best ways to proceed.

- The subsidiaries now have accountable owners for aspects of security programs.
- Changes in business technology, compliance requirements, economic conditions and security threats are continuously reviewed and evaluated using new risk management structures.
- A key stakeholders committee from subsidiaries meets periodically which leads to new strategic relationships and across holdings.
- The parent organization has significantly improved visibility into security incidents throughout the organization, and has supported investments into substantial improvements in each subsidiary's ability to detect and respond to security incidents.
- A detailed incident-response plan was created and is tested annually across the organization.

SIRIUS

SECURITY

Sirius provides leading-edge technology solutions, expert implementation and advisory services, top-ranked managed services, and proven methodologies backed by customized testing in our state-of-the art Technology Enablement Centers. We focus on the fundamental elements of an effective security program with an eye toward helping our clients address the cybersecurity skills gap, and leverage the cloud to boost agility and innovate faster than ever before. We help clients with solutions for:

- Program Strategy & Operations
- Identity & Access Management
- Infrastructure Security
- Data & Application Security
- Intelligence & Analytics
- Threat & Vulnerability Management

Call today to schedule a discussion of your security needs at 800-460-1237.