

Improving Security in a Conglomerate

Leveraging Strengths and Best Practices from Corporate to Subsidiaries

After several acquisitions and the creation of various subsidiary companies over the years, the corporate security department of a growing conglomerate was looking to get a picture of each division's current state. TrustedSec consultants performed independent program assessments for each subsidiary as well as the corporate entity to identify gaps in security and compliance and lay the foundation for establishing a robust, unified security program that met the needs of all parts of the conglomerate.

Problem

Organizations that have several subsidiaries (or independently-run divisions) face challenges in aligning each one and ensuring there are corporate standards for best practices. However, there is also the need to allow for flexibility so controls best meet needs, budgets, and risk tolerances of each group. The corporate IT and security departments ran lean, which made the separate entities that much more challenging to manage, as everyone had different strengths and weaknesses that were mostly unknown to headquarters—and each other. Without a full understanding of each division's current state and a unified standard to compare against, developing a corporate security strategy with actionable, achievable steps that applied to all parties simply was not achievable.

PERSONNEL PROFILE



Engagement Lead:
Alex Hamerstone,
Practice Lead, GRC

Alex Hamerstone leads TrustedSec's GRC practice and has designed security programs for both large and small organizations. He has advised and performed security assessments for companies ranging from small businesses to Fortune 100 corporations. Alex's experience covers a wide swath of industries, including retail, utilities, education, insurance, and healthcare, providing him with a unique view into the ways that organizations effectively integrate security into business.

Solution

The conglomerate sought out TrustedSec to perform independent security program assessments to make sure all of the subsidiaries shared a cohesive strategy for building a robust security program. GRC Practice Lead Alex Hamerstone and Principal Security Consultant Rick Yocum performed a thorough current-state assessment for each subsidiary as well as corporate. Their unified approach helped the organization to discern what was being done well and what needed improvement for an accurate understanding of the current state.

"Everyone at the subsidiaries was very receptive to us," Hamerstone noted. "We always start with understanding the big picture—corporate culture, risk tolerance, what the company does, how security functions, and governance. We not only looked for gaps, but also figured out what was being done well at each division that could be shared and adopted by everyone."

The TrustedSec team recommended domains and tasks that should be centralized and pushed out from the parent—and those that the subsidiaries should do themselves. For example, it did not make sense that each entity would need to go through the effort of writing independent firewall policies—an organization-wide policy would remove an unnecessary burden from the subsidiaries. And where some subsidiaries had great processes and systems in certain areas, Hamerstone and Yocum recommended an approach to share and adopt that which was working well already.

Benefits

TrustedSec was able to provide a strategy and roadmap for developing a robust security posture throughout the entire company. The team united the findings, recommendations, and plans into themes, trends, and issues that pertained to the entire company, effectively reducing costs and complexity. By taking the best parts of the security programs at each subsidiary and including them in the organizational security program, the new approach increased buy-in and cultural acceptance, which are some of the hardest things to achieve in any business.

"This is one of those engagements that really makes you glad to be in consulting. In the end, we were able to save them a lot of effort and time and set them on the path to improve the overall security program," Hamerstone said.

About TrustedSec

TrustedSec is an Information Security consulting team at the forefront of attack simulations with a focus on strategic risk-management. Our goal is to help organizations defend against threats of all kinds and change the security industry for the better.

With a team handpicked not only for expertise and technical skill, but for ethical character and dedication, TrustedSec is committed to increasing the security posture of organizations around the world.