Professional services firm targets cyber risk and rapidly upgrades security

AT A GLANCE

A rapidly growing professional services company appointed a chief information security officer (CISO), completed a targeted risk assessment, and executed a prioritized security action plan.

CHALLENGE

The board of directors of this rapidly growing, privately funded professional services firm recognized the company faced escalating cybersecurity risk. The board noted competitors that had suffered service disruptions and security incidents, and concluded that its security architecture needed a refresh to protect its "crown jewels."

APPROACH

The project's first phase was a targeted risk and controls assessment. Coalfire personnel interviewed the board and executives, and analyzed key business processes to identify the company's high-value assets. Coalfire also reviewed security controls, using the NIST 800-53 Revision 4 (medium) framework. Finally, they developed 40 business-oriented risk statements, each of which named assets, vulnerabilities, threat actors, and potential attack vectors, yielding a semi-quantitative estimate of residual risk.

These risk statements, along with risk treatment options, were presented to the executive team and the board. "We had a fact-based discussion on the risks we faced and our options for treating, transferring, or avoiding them," explained the firm's CISO. "Then, we prioritized our security investments and obtained the necessary budget and resources. Every action item had a sponsor, budget, and realistic implementation schedule."

Over the next six months, the company rapidly implemented and improved dozens of administrative and technical security controls. Several improvements, which are described in Table 1, aligned with the NIST Cybersecurity Framework (CSF) Core Functions (Identify, Protect, Detect, Respond, and Recover).

> *"We took a targeted approach to our risk assessment because we had an informed board with specific ideas on what risks they wanted to address."*
>
> – CISO AT THE PROFESSIONAL SERVICES FIRM

Table 1: Aligning security updates with NIST CSF

Identify (ID)	• **ID.GV:** Updated the firm's information security governance program and information security policy. • **ID.SC:** Identified critical vendors and services, and adopted supplier risk management processes.
Protect (PR)	• **PR.AC:** Re-architected the document storage solution to improve service, control unauthorized access, and reduce operating expenses; and implemented single sign-on (SSO) multifactor authentication (MFA) solutions. • **PR.AT:** Defined security roles, created an employee handbook, implemented a security awareness program, and trained the board and executive teams. • **PR.IP:** Established baseline workstation configurations, eliminated unnecessary administrative privileges, and enhanced the vulnerability management program. • **PR.PT:** Restricted the use of removable media.
Detect (DE)	• **DE-AE:** Upgraded the logging and monitoring solution, and enhanced alerting and response procedures. • **DE.CM:** Upgraded the email security solution to enhance its ability to detect malicious malware.
Respond (RS)	• **RS.CO:** Clarified incident management team, roles, and responsibilities. • **RS.AN:** Documented, implemented, and tested incident response procedures.
Recover (RC)	• **RC.CO:** Developed a recovery communications plan.

RESULTS

Throughout remediation, the CISO updated executive leadership and the board. Several projects were completed ahead of schedule, allowing for additional security enhancements.

During the project, several well-known enterprises reported massive data breaches and cyber-related operational disruptions. Due in part to these security improvements, the company avoided similar problems. "You can never prove the negative," said the firm's CISO, "but it's clear that our enhanced endpoint security program kept our patches current and guarded us against some nasty weaponized malware. I'm thankful the board funded the program, and I'm delighted with our team's performance and our solution providers to-date."

CS_ProfSvcs_110617