Engineering Consulting Firm Improves Security with a Formalized, Top-down Risk Management Program

Case Study

- **Industry:** Consulting
- **Country:** United States
- **Size:** Mid-size

Challenges

- Business disruption due to a ransomware attack.
- Lack of formalized security policies.
- Insufficient endpoint protection.

Solutions

- The Arete Cyber Strategy and Defense team conducted a comprehensive vulnerability and security controls assessment.
- Ongoing Arete virtual CISO (vCISO) partnership for best-practice guidance on formalizing policies and creating a robust risk management program.

Benefits

- Established an information security oversight committee to ensure a top-down approach to security accountability and policy enforcement.
- Created a new, secure business service in collaboration with business development managers.
- Developed a mature risk management program.

When hit by a ransomware attack, an engineering consulting firm was quick to put its incident response (IR) plan into action, immediately calling its insurance carrier and engaging the Arete IR team to assist with mitigation and restoration. Within 48 hours, the firm had the decryptor keys in hand and within two weeks, had fully resumed normal operations.

"Despite getting back online relatively quickly, I couldn't shake that feeling of having been violated," said the firm's IT manager. "It was the worst experience of my professional career. We thought we were secure, but the bad guys had walked right in, taken control, and shut us down. I never want to feel that way again."

The fastest way to improve security

The best time to strike is while the iron is hot or, in this case, when the pain of a bad experience was still fresh. Knowing that no one from his firm ever wanted a repeat ransomware experience, the IT manager solicited executive support to conduct a vulnerability assessment.

"The executive staff was extremely motivated to get security right and uncover any other possible gaps," he said. "When they gave me the green light, I called on the Arete Cyber Defense and Strategy team to run the assessment."

The Arete team began with a review of CIS controls, walking the IT staff through questionnaire after questionnaire to identify weaknesses and prioritize risks.

"My team was brutally honest with every question," the IT manager said. "We'd already been exposed and had nothing to hide or fear. Plus, sugarcoating wouldn't have gotten us anywhere."

Once they'd completed the initial assessment, the Arete team presented their findings to the leadership team, pointing out weaknesses, reviewing the function of the various controls, and laying out a roadmap for how the firm could improve its score.

"Our score wasn't terrible," the IT manager said, "but we knew we could do better. And Arete advised us on the fastest and easiest way to get started: Formalize our security policies."

> "It was the worst experience of my professional career. We thought we were secure, but the bad guys had walked right in, taken control, and shut us down. I never want to feel that way again."
>
> **IT Manager**

The IT department alone cannot protect a company

To help with the formalization process, the IT manager partnered with an Arete virtual CISO (vCISO), who provided templates and samples for developing best-practice information security policies and defining who is responsible for cybersecurity. Hint: It's not just IT.

More than words on paper, security policies are designed to set behavior. And while the IT team had standard practices in place, they'd neither formalized them into written policies nor instituted a process for reporting up the chain of command to establish accountability and ensure enforcement.

"Accountability alone would improve our security score," the IT manager said. "Risks identified at the bottom of the organization can't stay at the bottom. They must be addressed by those with decision-making power.

> "The flexibility of the Arete vCISO program has been a perfect fit for our needs."
>
> **IT Manager**

"We understood that we needed a top-down approach. We needed buy-in and support from our president and executive staff. And today, everything we do comes from the top."

As part of this approach, the firm created an information security oversight committee comprised of the IT manager, the Arete vCISO, an HR manager, a controller, and an operations manager — all high-level employees with a stake in cybersecurity and a duty to know, understand, and treat risks either by accepting them or mitigating them.

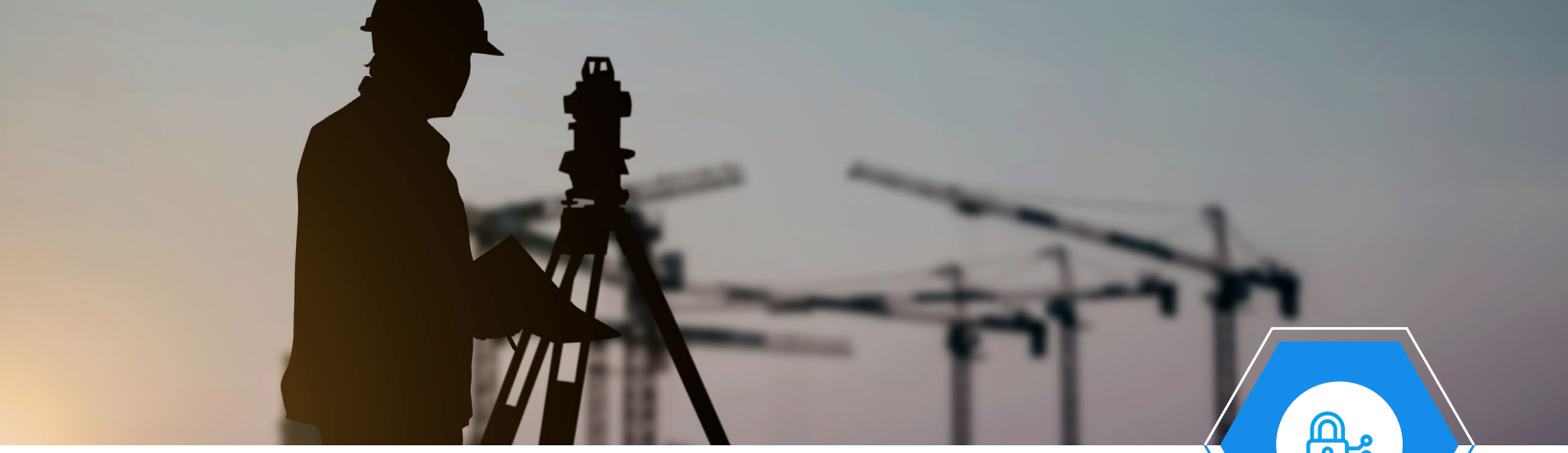
"In the past, for example, we ran internal phishing campaigns, but because they weren't formalized, there were no repercussions if someone failed," said the IT manager. "Today, those programs are formalized and if anyone fails, HR follows up with those individuals to ensure they complete mandatory training. That's accountability."

Additional steps to improving security

In addition to formalizing policies and establishing the oversight committee, the firm made technical advancements, implementing the robust SentinelOne EDR solution across all endpoints, and ensured that all employees, including the executive team, completed extensive security training. What's more, the IT manager created a risk management structure from scratch, crediting the Arete vCISO with giving him the building blocks to get started and mature the project into a formal program within a year's time.

"The flexibility of the Arete vCISO program has been a perfect fit for our needs. If we need to meet, we meet. If we don't have anything to discuss on a particular week, we can skip the meeting at no charge," said the IT manager. "By the same token, if something more urgent arises, we have a direct line to help."

"In security, so much comes down to relationships and finding someone you can trust and learn from," he added. "I have complete faith in our Arete vCISO. He brings years of real-life experience and wisdom that we can apply to our own environment."



Security as a business enabler

As part of its business, the firm collects all manner of geographical information and stores it in a database. Via an internal web portal, employees can access and search within this data and create various reports or maps.

Recently, some of the firm's department managers and business development professionals asked if they could extend access to their clients and in essence, create a new product. The idea was to allow clients to view the data, create dashboards, and print maps.

"My initial thought about allowing external people onto our network was, how could I safely administer this service?" said the IT manager. "If I gave one client a password, I'd have no way of preventing them from sharing it with another 20 people. The idea got really complicated, fast. So, who did I immediately call to discuss possible options?"

The IT manager and Arete vCISO arranged a brainstorming session with representatives from key teams, including product/application development, firewall, internal applications, human resources, to discuss the desired outcomes and security concerns. Together, they devised a solid plan for how to safely offer the new service.

"We decided to segment certain aspects of the data and place the client portals in a DMZ. That way, clients were separated from the rest of our network," said the IT manager. "We found the bare minimum protocols needed so we can shut everything else down and only allow those protocols. To boot, we're configuring SentinelOne to offer another layer of protection."

So now, the IT department has helped the firm create a new, secure service. And should clients ever have security concerns, the IT manager is available to explain exactly how everything is configured and why it's safe.

"In security, so much comes down to relationships and finding someone you can trust and learn from. I have complete faith in our Arete vCISO. He brings years of real-life experience and wisdom that we can apply to our own environment."

IT Manager

Arete is transforming the way organizations of all sizes prepare for and respond to cyberattacks. With decades of experience fighting cybercrime, our global team has been on the frontlines of some of the world's most challenging data breaches. Our core skills — managed detection and response, digital forensics, threat intelligence, threat hunting, remediation — help organizations address the full threat life cycle while also improving their overall cyber posture. To learn more, visit www.areteir.com or follow us @Arete_Advisors.

Arete