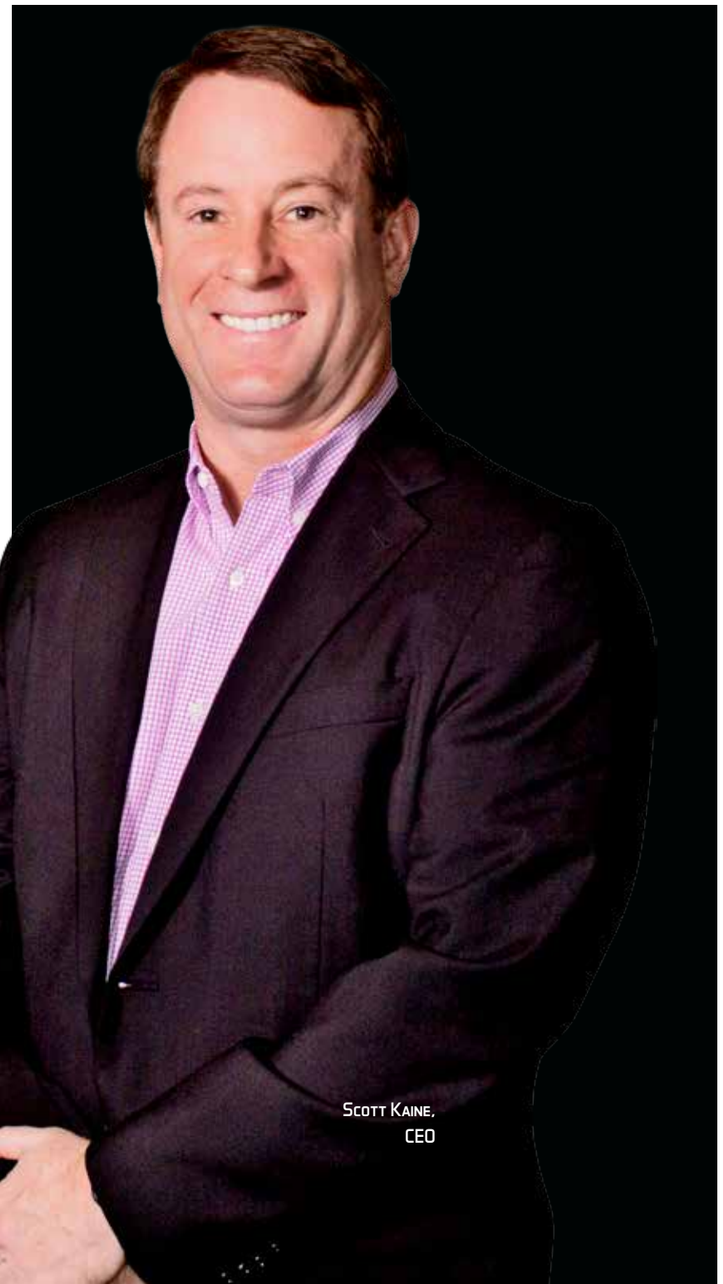
Delta Risk LLC

Delivering Security at the Speed of Business

When organizations transition to the cloud, there are often many security considerations they neglect. Delta Risk has identified the crucial demand for cybersecurity expertise that organizations seek at this point, and aptly positioned its managed services value proposition in the industry.

Scott Kaine, CEO of Delta Risk, explains how his team begins by identifying potential threats to the client's networks, taking a proactive stance towards security. While the complexity varies with the size of the organization—such as mid-sized firms' issues relating to the cloud environment and large organizations struggling with their DevOps practices—Delta Risk supports its customers by delivering security at the speed of business. As one of the leaders in the cybersecurity arena for commercial and government clients worldwide, the firm offers a full suite of strategic consulting, advisory, incident response, and managed security capabilities, along with cloud security solutions.

Founded as an information security services consulting firm in 2007, Delta Risk now focuses on helping mid-sized and large businesses, as well as government agencies, be prepared, defensive, and resilient against growing threats. Here are some of the key insights that Kaine shares about the firm's proactive approach, and how it helps clients improve their cybersecurity operational capability to protect their business operations.



Scott Kaine, CEO

> Through the use of cloud and the Internet, businesses are moving faster than ever. Our job at Delta Risk is to help our clients keep pace on the risk and security front

Taking a Proactive Approach

Our approach is primarily based on three core units: people, process, and technology. On the people side, we deliver tabletop exercises for our clients. Individuals are walked through many scenarios to help them be better prepared in case of a security event or an attack. After the exercise, our team offers suggestions on how their response to the situation can be improved.

When it comes to process and governance, we review clients' existing security policies and compare them with the best practices. During this process, we examine important questions such as, "What happens if an organization's operations harmful to its infrastructure or the cloud? Do the current governance and policy address those issues?" After we've built a process that's in alignment with best practices for our clients, we investigate their technology and figure out the existing gaps.

The cloud environment is assessed in two ways—by ensuring that the configuration has been set up correctly and that it is monitored on a continual basis. We deliver full visibility into the activity of our clients' cloud environments and accounts and allow their teams to run development operations while ensuring that there are no unknown risks. We also use advanced analytics to detect inappropriate use of resources from internal or external attackers.

Holistic Managed Services Delivery

There is no single security solution that answers all needs. We take an agile and data-driven approach when it comes to designing our solutions to respond to changing requirements. This involves co-discovery and joint problem-solving with clients and partners to find the optimal response for unique challenges.

Delta Risk incorporates methods from the national security arena to evaluate and improve cyberoperational readiness in the private sector. Within large enterprises, we extend our expertise to provide organizations with guidance on the most appropriate usage of their security resources. We can also train their operational staff on how to be prepared and effectively deal with future threats.

For mid-tier and small organizations, we offer turnkey services around outsourcing the client's security programs and act as a trusted advisory partner as well as an extended technical arm of their staff to take care of their security issues. For most of the companies that we cater to—despite practicing the preventative approach—the client usually makes the call after an issue arises. In such cases, we respond to the case-in-point by deploying the necessary resources to do the forensics and evaluations, depending on the type of threat.

In addition, we take a multi-faceted approach to evaluate the client's cyberdefense strategies with tailored risk assessments and framework-based gap analysis. If a client decides they want a third-party to take over security for them, our ActiveEye platform comes into play. Through our ActiveEye managed security services, we combine people, processes, and technology to continuously monitor the client's systems from inside and outside their network.

Growing with the Evolving Market

The next phase of our journey will see us increasing the use of machine learning and response capabilities into our platform. As we continue to focus on the U.S. market, we will deliver mechanisms and algorithms to ensure this platform learns from the exposure that it gets and makes the required changes automatically, improving the overall process to reduce human intervention.CA