PROFILES IN *Confidence*

ELLIOTT FRANKLIN

SVP, CISO
Fortitude Re

Headquarters: Bermuda

Employees: 550+

Annual Revenue: Private Company

Elliott Franklin leads security at Fortitude Re with a perspective shaped by both technical experience and a deep understanding of the human side of cybersecurity. Elliott is responsible for protecting sensitive data and ensuring resilience in an environment where risk is constant and expectations are high.

His approach to security and leadership reflects a broader shift in the role of the CISO. Security is no longer just about controls and compliance. It is about enabling the business, adapting to rapid change, and building programs that can withstand both technical and human pressures.

STAYING GROUNDED IN THE FUNDAMENTALS

In the face of geopolitical and economic uncertainty, Elliott's approach is intentionally steady. "You cannot ignore it, but at the same time, we do not change," he explains.

Rather than reacting to every new threat or headline, his team remains focused on core disciplines such as identity and access management, monitoring, and response. Threat intelligence from industry groups like ISACs provides additional context, but it does not change the foundation of the program.

For Elliott, consistency is what allows organizations to remain effective even as the external environment evolves. "We try to stay focused on the basics regardless of what is going on," he says.

SECURITY AND BUSINESS LEADER

Elliott sees a clear shift in how CISOs must operate today. "We have to be business leaders now," he says.

Rather than leading with regulatory requirements or security mandates, his focus is on understanding business priorities and aligning security to support them.

"We are asking the business for their priorities," he explains. "How can we help the company make money or be productive?"

This shift changes how security is perceived. Instead of being a gatekeeper, the CISO becomes a partner who helps accelerate outcomes. "If we can accelerate things," he says, "they will not even see it as a security project."

AI AS OPPORTUNITY

Elliott describes AI as a rapidly evolving force that is already reshaping how security teams operate. "We are definitely taking advantage of what AI has to offer," he says.

At Fortitude Re, AI is being used to automate operational tasks and improve response times. The team has implemented agents and automated playbooks that support detection, triage, and response, allowing them to act faster than traditional processes would allow.

"We have implemented over 100 automated responses and playbooks," he explains. This includes taking decisive action when needed. "We have given them permission to take action," he says, noting that in some cases that may include shutting down systems to stay ahead of a threat.

For Elliott, the priority is clear. Speed matters, and automation is essential to keeping pace.

BALANCING SPEED WITH CONTROL

While the business is eager to adopt AI, Elliott emphasizes the importance of doing so responsibly. "Right many, many businesses want everything immediately," he says.

Elliott believes the role of security is not to slow that momentum, but to guide it. He explains, “We cannot say no. Instead, the focus is on helping the business move forward safely by establishing clear guardrails and frameworks.”

At Fortitude Re, that guidance is grounded in established standards. “These are not our rules,” he says. “If we follow the NIST AI risk management framework, it makes it easy to explain.” This approach allows the team to support innovation while maintaining consistency and control.

IDENTITY AND DATA AS THE CORE PRIORITIES

Beyond AI, Elliott remains focused on foundational areas that continue to drive risk. “Identity and access management is an important area to focus on,” he says.

As organizations adopt more SaaS applications and AI systems, managing both human and non-human identities becomes increasingly complex. APIs, tokens, and service accounts expand the attack surface, requiring greater visibility and control.

At the same time, data protection remains a constant challenge. Understanding where data lives and how it moves across environments is critical, particularly as employees adopt new tools at a rapid pace.

For Elliott, these are not new problems, but they are becoming more urgent as the environment evolves. “We are trying to understand what is being uploaded and where it is going,” he explains.

RESILIENCE AS A CORE DISCIPLINE

Resilience is another key area of focus, particularly as organizations face a growing range of disruptions.

Elliott emphasizes the importance of planning for outages, ransomware, and other operational risks. This includes ensuring that backups are secure and the organization can continue operating even during an incident. “It is an insurance policy,” he explains.

While resilience may not always be a visible priority, it is essential to long-term success.

THE HUMAN SIDE OF CYBERSECURITY

Looking ahead, Elliott believes one of the most important areas of focus will not be technology, but people. “Technology really is last,” he says.

As AI continues to reshape the industry, it is also creating new pressures for security professionals. Concerns about job displacement and constant exposure to risk can take a significant toll. “AI is making practitioners even more afraid,” he explains.

Elliott is particularly focused on the impact this has on mental health, both within the workplace and at home. “We cannot continue to sustain the pressure that CISOs have to always be protecting the company without having health issues,” he says.

This perspective reflects a broader leadership responsibility. Building a strong security program is not just about tools and processes, it is about supporting the people behind them.

LEADING THROUGH CHANGE

For Elliott, the future of cybersecurity will be defined by how leaders balance technology and risk with human impact.

The pace of change will continue to accelerate, driven by AI and evolving threats. But success will depend on more than technical capability. It will require clear communication and a focus on both business outcomes and team well-being.

At Fortitude Re, Elliott is building a program that reflects that balance, one that stays grounded in fundamentals and recognizes that behind every system is a team that must be supported to succeed.