PROFILES IN *Confidence*

JAY MODY

CISO & Head of IT Infrastructure
Chimera Investment Corporation

Headquarters: New York, NY

Employees: 400+

Annual Revenue: Total revenues of $821 million and a GAAP net income of $144 million ($1.72 per diluted common share)

Jay Mody has spent nearly three decades evolving alongside technology itself. Over the course of a 28 year career spanning infrastructure, engineering, cybersecurity, and financial services, he has witnessed wave after wave of transformation. Through it all, one principle has remained consistent: security must enable the business, not slow it down. “I’ve always looked for gaps in business processes and controls, and tried to be proactive rather than reactive,” he says.

That mindset has shaped his leadership at Chimera Investment Corporation, where he serves in a dual role as both CISO and Head of IT Infrastructure. Since joining the company, Jay has helped guide Chimera through rapid growth, major acquisitions, evolving regulations, and the transition to a cloud-first environment, all while building a mature cybersecurity program designed to support the business as it scales. Jay sees his role as helping the organization grow securely while preparing for whatever comes next.

“I’m always trying to be a business enabler,” he says, “My goal is to let the business drive the car fast while making sure we have the right guardrails and brakes in place when needed.”

SECURITY AS A BUSINESS ENABLER

One of the defining shifts in Jay’s career came when he stopped viewing cybersecurity as purely a technical discipline and began aligning it directly with business priorities. “What are the challenges the business is facing? What is the CEO’s vision?” he says.

That perspective became especially important after Chimera brought in a new CEO focused on growth and acquisitions. Jay recalls a conversation where the company’s leadership made clear that expansion would move quickly and security needed to keep pace.

Rather than positioning cybersecurity as a blocker, Jay focused on demonstrating readiness. He highlighted the company’s investments in compliance, governance, and resilience while building new programs to support brand protection and digital trust.

One example involved protecting executive identities and the company’s public presence online. “I implemented a program to protect our digital brand,” he explains. “Making sure there is no impersonation and no lookalike domains out there.”

That business-first mindset now shapes how he approaches nearly every security initiative. Whether discussing infrastructure modernization, acquisitions, or AI adoption, the conversation always starts with business impact.

BUILDING AI AND DATA GOVERNANCE

As AI adoption accelerates across financial services, Jay is focused on ensuring governance evolves just as quickly. Two of his largest priorities today are AI governance and data governance, both of which he recently presented to senior management and the board.

“AI is something our CEO sees as essential,” Jay explains. “But he wants to make sure we have proper governance and guardrails.”

Jay approaches AI through three distinct lenses: AI as an asset, AI as a threat, and AI as a tool. That framework has helped structure how they evaluate risk and manage adoption across the organization.

At the center of the strategy is governance. Chimera established an AI task force that brings together stakeholders across enterprise risk, legal, business intelligence, and technology to define policies, training requirements, and

operational controls. “We need proper training. We need policy clearly defined,” he says. “Then the operations team can create the controls and processes based on those policies.”

The challenge, however, is the pace of change. Jay notes that vendors are increasingly embedding AI capabilities directly into enterprise platforms, often without customers actively requesting them. “They are already introducing AI features into their applications without asking anyone,” he comments.

For security leaders, that creates a difficult balance. Organizations cannot afford to fall behind, but they also cannot introduce AI without understanding the risks. “We don’t want to be left behind,” Jay shares. “But we also need to adapt our controls to this changing environment.”

To support that effort, they are using the NIST AI Risk Management Framework as the foundation for the governance strategy, while also implementing additional monitoring around AI agents and cloud environments.

PREPARING FOR AI-DRIVEN THREATS

While AI presents opportunities, Jay is equally focused on how it changes the threat landscape. One of the biggest concerns is how quickly attackers can weaponize vulnerabilities using advanced AI models. “Our response time is narrowing,” he reflects. “We used to get days to patch systems. Now as these models evolve, bad actors will eventually have access to these capabilities as well.”

His response centers on two priorities: response time and resiliency. Jay’s team focuses heavily on protecting internet-facing systems through continuous threat exposure management while maintaining strong internal segmentation and zero-trust controls. But he also recognizes that prevention alone is not enough.

“If a bad actor breaches our network and brings systems down, I’m going to rely on our established backup and disaster recovery process,” he explains. That preparation is something Chimera has invested in for years. Jay emphasizes that resiliency is not built during a crisis. It must already exist before one occurs.

“My team is prepared to respond to any breach or ransomware threat,” he stresses. He also sees AI playing a growing role in recovery itself. They are implementing AI-driven recovery capabilities designed to identify the safest restore points following an incident, reducing recovery time during a potential attack.

SCALING SECURITY THROUGH GROWTH AND ACQUISITION

The company’s recent acquisitions introduced another major challenge: integrating organizations with very different levels of security maturity. Rather than immediately imposing controls, Jay focused first on awareness and alignment. “These are the gaps we identified in your environment,” he recalls telling leadership teams. “Here’s the roadmap to bring you into Chimera’s secure operating environment.”

That roadmap included deploying visibility tools, integrating vulnerability management, and aligning systems with the controls already established within Chimera’s environment.

Jay approached both situations the same way: transparency, collaboration, and education. “Technology evolves. Risk evolves,” he explains. “It’s a changing landscape.”

LEADING THROUGH COLLABORATION AND ACCOUNTABILITY

Jay describes his leadership style as collaborative and execution focused. “I want my team to collaborate and work across the business,” he says. “The business needs to understand why we are doing this and where the end state will be.”

He also emphasizes accountability. For Jay, projects are not complete when technology is deployed. They are complete only after monitoring, backup, disaster recovery, compliance integration, and documentation are fully operational. “I don’t want someone telling me the project is done,” he says. “I want to know the monitoring is in place, the backup is configured, and the documentation is complete.”

At the same time, he is intentionally preparing his team for larger leadership opportunities by gradually giving them ownership over critical systems and initiatives. He comments, “Many team members want to grow and work on different technologies, so I’m giving them more responsibility as they develop.” That investment in people mirrors the support Jay says he has received throughout his own career.

Since joining the organization, he has grown from Director of Infrastructure to CISO and Head of IT Infrastructure, gaining direct access to executive leadership and the board along the way.

“They’ve given me that growth ladder,” he says. “I have a seat at the table, and I can share risk very transparently.” For Jay, that transparency is essential to effective leadership, especially as AI, cloud adoption, and cyber risk continue to evolve simultaneously.

The pace of change may continue to accelerate, but his focus remains consistent: build resilient systems, support the business, and prepare the organization for what comes next.