

## JOB DESCRIPTION

# Chief Information Security Officer

**Reports to:** Chief Executive Officer, with a direct reporting line to the Audit & Risk Committee of the Board of Directors

## About the role

---

The CISO is accountable for whether the company, including its people, partners, systems and AI agents, can be trusted with what it cannot afford to lose. This is an enterprise risk leadership role, not a technology operations role. The CISO works as a peer to the CIO, Chief Scientific Officer, General Counsel and CFO, and is independent of the teams whose work the CISO is expected to evaluate.

## What you will be accountable for

---

- Telling the CEO and the board the truth about cyber risk in business terms: dollars, downtime, reputation and regulatory exposure, including the risks the company has chosen to accept.
- Owning enterprise AI governance, including approval criteria for AI tools, oversight of AI agents and other non-human identities, and policy on employee use of AI.
- Chairing a standing risk council with research, business, legal, finance and technology leaders, where controls are shaped with the people who live with them before they are imposed.
- Designing a security model for research and development that protects the organization's most valuable work without slowing it: guardrails over gates, monitoring over blocking, and a short list of non-negotiable rules.
- Independently verifying that foundational controls (encryption, identity and access, asset inventory, segmentation and recovery) are in place and working, and reporting plainly when they are not. Technology teams do this work; the CISO certifies it.
- Measuring and reporting resilience through tested time to detect, contain and recover, rather than activity counts such as training completion.
- Leading incident response at the executive level and communicating with the board, regulators and insurers.

## Authority that comes with the role

---

- An independent budget, approved by the CEO and reviewed by the board, separate from the IT budget.
- Standing time on the board agenda, with private sessions without other management present at least annually.
- Authority to escalate any unresolved risk directly to the board.
- A required seat in decisions on technology adoption, acquisitions and major vendor relationships.
- Coverage under the company's directors and officers (D&O) insurance.

## What you bring: the technical test

---

*These qualifications are not optional.*

- Deep, current technical fluency: the ability to read an architecture diagram, question an engineer and spot a vendor's overstatement in the first meeting.
- Hands-on familiarity with AI tools and AI-specific threats, including prompt injection, agent permissions, model and data theft, and deepfake fraud.
- Threat knowledge drawn from peer networks, industry information-sharing groups (ISACs) and red-team work, not primarily from vendors.
- Typically 15 or more years of experience across security engineering, operations and architecture. Degrees and certifications are welcome but secondary to demonstrated depth.

## What you bring: the judgment test

---

- A track record of recommending that leadership accept a risk when that was the right business call, and the ability to explain why.
- Experience translating security decisions into business trade-offs that boards act on.
- An understanding of how people actually behave under pressure, and the ability to design around that behavior rather than blame it.
- Evidence that research, product or operations leaders sought you out rather than routing around you.
- The standing and temperament to tell senior executives “no, not like that,” and the partnership skills that keep them asking for your opinion anyway.

## How success is measured

---

- Tested recovery and containment times improve year over year.
- Material risks are known, priced, and consciously accepted or addressed, with no surprises at the board level.
- AI and research initiatives move at full speed inside agreed guardrails, without a rise in shadow AI or workarounds.
- Business and research leaders rate the security function as a partner in an annual survey.

## What this role is not

---

*This is not the head of IT infrastructure, the owner of the help desk or a compliance checklist manager. It is not a gatekeeper whose success is measured by what it blocks.*