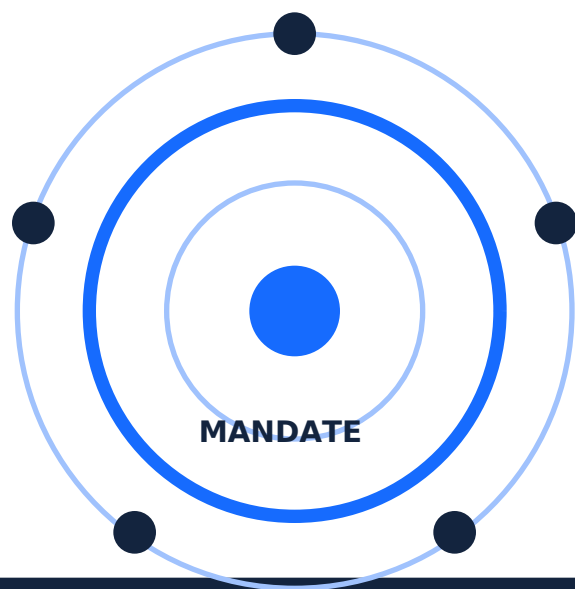


5 Things to Get Right Before Your CISO Search

A stronger search begins with a clearer mandate. Use these five decisions to define the leader your business actually needs.



THE FIVE MOVES

- 01** Start with business outcomes
- 02** Clarify authority and reporting
- 03** Agree on risk priorities
- 04** Define first-year success
- 05** Test leadership in context



THE EXECUTIVE BRIEF

A CISO search can move quickly and still miss the mark if the organization has not agreed on the job. The best starting point is a shared view of the business outcomes, authority and risk priorities the incoming leader will own.

1

Start with business outcomes

A search specification built only around tools, certifications or prior titles can obscure the work ahead. Identify the decisions the CISO must help the business make: entering a regulated market, protecting a digital product, integrating an acquisition or improving resilience. These outcomes should determine which experiences matter most.

Ask: What will be different for the business 12 months after this person starts?

2

Clarify authority and reporting

The reporting line signals how cyber risk enters enterprise decisions. A CISO may report through technology, risk or another executive function; the right arrangement depends on the organization. More important is explicit access to decision-makers, escalation paths and authority to coordinate across functions.

Ask: Where can the CISO make a decision, and where must they influence one?

3

Agree on risk priorities

No leader can fix every exposure at once. Give candidates a candid view of critical assets, current gaps, regulatory pressure and business constraints. Ask how they would sequence investment and where they would accept, transfer or reduce risk. This tests judgment rather than rehearsed technical answers.

Ask: Which three risks would leadership want addressed first?

THE THROUGH LINE

Write a one-page mandate before building the candidate slate: outcomes, decision rights, stakeholders, resources and first-year measures.



FROM INSIGHT TO ACTION

A candidate profile becomes useful when it reflects the decisions the CISO will need to make, the people they will need to influence and the results leaders expect.

4

Define first-year success

A vague directive to “improve security” creates mismatched expectations. Specify early milestones such as a baseline assessment, a prioritized roadmap, tested response roles and a board-ready reporting rhythm. Keep the measures tied to business exposure and execution, not activity counts alone.

Ask: What evidence would show progress at 90 days and at one year?

5

Test leadership in context

Technical depth is essential, but the role also requires communication, negotiation and team building. Use realistic scenarios involving a product launch, an incident or a funding tradeoff. Invite cross-functional interviewers to assess how candidates explain risk and bring others to a decision.

Ask: Can the candidate translate a security concern into a business choice?

START THE CONVERSATION

Bring the CEO, CIO, risk or legal leader and a board sponsor together to agree on a one-page CISO mandate. Then use it to shape the role profile, interview questions and first-year scorecard.



DAN DUFFY

Cybersecurity Practice Lead

Dan leads cybersecurity executive search and security solutions at Consulting Solutions. His work connects leadership requirements with the expertise and services organizations need to strengthen their programs.

FURTHER READING

NIST Cybersecurity Framework 2.0: nist.gov/cyberframework | NACD 2026 Cyber-Risk Oversight: nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/2026-cyber-risk-oversight/

Explore cybersecurity solutions and specialized talent

consultingsolutions.com