A CISO Cannot Lead Every Operating Model the Same Way

By: Jaiz Anuar

18 February 2025 · Cybersecurity · Leadership · 6 min read

The CISO title may remain the same, but authority, accountability and the leadership style required can change completely with the operating model.

A CISO may have many years of cybersecurity leadership experience.

But experience can become a weakness when it is applied without understanding the organisation's operating model.

A CISO who previously controlled the SOC, security engineering, architecture and governance may join another organisation where operational cybersecurity sits under the COO or CTO, while the CISO reports to the CRO.

Another CISO may move from a second-line governance role into a full-scope position where the entire cybersecurity function reports directly to them.

The title may remain the same.

The authority, accountability and leadership style do not.

One of the biggest mistakes a CISO can make is assuming that a leadership approach that worked in a previous organisation can be applied unchanged in a different operating model.

Past experience should provide judgement.

It should not become a fixed playbook.

Three CISO Models Require Three Different Leadership Styles

Cybersecurity leadership is commonly structured in three different ways.

Each model can work.

But each requires the CISO to behave differently.

The CISO must first understand where decision rights sit, which teams are directly controlled, where independence is required and how accountability is distributed.

Without that understanding, the CISO may overstep authority, weaken governance or fail to provide the leadership the organisation actually needs.

Model 1: CISO, TISO and BISO

In some large or complex organisations, cybersecurity leadership is distributed across a CISO, Technology Information Security Officer and Business Information Security Officers.

The CISO normally provides enterprise-wide cybersecurity direction, strategy and governance.

The TISO focuses more closely on technology security, including infrastructure, cloud, applications, engineering and technical control implementation.

BISOs connect cybersecurity with individual business units. They help business leaders understand cyber risk, prioritise remediation and align security requirements with business objectives.

This model requires the CISO to lead through coordination.

The CISO cannot behave as though every decision, programme and security team sits under one central command.

A CISO coming from a fully centralised organisation may struggle in this model. The CISO may try to control decisions that should sit with the TISO, bypass BISOs or interfere directly in business-level security matters.

That approach can create duplication, weaken accountability and reduce trust.

The effective leadership style is influence, alignment and common direction.

The CISO must ensure that:

Responsibilities are clearly defined

Shared security objectives are established

Risk reporting is consistent

Escalation paths are understood

Cross-business risks have clear ownership

Minimum security expectations are applied across the organisation

In this model, the CISO remains the enterprise security leader.

But leadership is exercised through a network, not only through direct reporting lines.

Model 2: CISO Under the Three Lines of Defence

In the Three Lines of Defence model, cybersecurity responsibilities are deliberately separated between operations, risk oversight and independent assurance.

The first line owns and operates cybersecurity controls.

These functions may report to the COO, CTO or another operational executive and commonly include:

Security operations

Security Operations Centre

Security engineering

Security architecture

Identity and access operations

Vulnerability management

Infrastructure and cloud security

Application security

The first line is responsible for implementing controls, managing daily cyber threats, responding to incidents and remediating security weaknesses.

The second line is led by the CISO, who reports to the Chief Risk Officer.

In this model, the CISO leads cybersecurity from a governance, risk and compliance perspective.

The role is not to operate security technologies or directly manage the SOC, architecture and engineering teams.

The CISO’s responsibilities may include:

Establishing cybersecurity policies and standards

Defining the cyber risk framework

Setting risk appetite and tolerance measures

Conducting independent risk assessments

Challenging the adequacy of first-line controls

Monitoring cybersecurity risk exposure

Overseeing regulatory compliance

Reviewing security exceptions and risk acceptance

Reporting material cyber risks to the CRO, management and board

Escalating exposure that exceeds risk appetite

The third line is internal audit.

It provides independent assurance over both the first-line control environment and the effectiveness of second-line oversight.

A CISO moving into this structure from a full operational role must adapt carefully.

Previous experience managing a SOC, architecture or engineering function remains valuable. However, that experience should be used to improve governance, ask better questions and challenge whether controls are effective.

It should not be used to take over first-line responsibilities.

If the second-line CISO begins directing operational teams, designing detailed technical solutions or managing daily security activities, the separation between control ownership and risk oversight becomes unclear.

The CISO may unintentionally become both the reviewer and the operator of the same control.

At the same time, governance should not become a passive compliance exercise.

The CISO should not limit the role to issuing policies, collecting risk registers and reporting overdue findings.

Effective second-line leadership requires enough technical understanding to challenge whether controls genuinely reduce risk.

The leadership style in this model is governance-led, risk-based and independently challenging.

The CISO must remain close enough to understand operational realities, but sufficiently independent to assess whether the first line is managing cyber risk effectively.

In this model, the CISO does not own cybersecurity operations.

The CISO governs how cybersecurity risk is identified, assessed, treated, accepted, monitored and reported.

Model 3: Full CISO Reporting to the CEO

In the third model, the CISO reports directly to the CEO and leads the full cybersecurity organisation.

Security operations, SOC, engineering, architecture, governance, risk and compliance may all report to the CISO.

This gives the CISO broad authority and direct accountability for cybersecurity outcomes.

The CISO is not only responsible for identifying risk.

The CISO is responsible for reducing it.

This model requires a more integrated and execution-focused leadership style.

The CISO must balance:

Cybersecurity strategy

Security operations

Incident response

Architecture and engineering

Governance and compliance

Investment priorities

Talent and capability development

Operational resilience

Executive and board communication

A CISO coming from a second-line governance role may find this model challenging.

It is no longer enough to identify weaknesses, issue recommendations and escalate unresolved risks.

The CISO must make delivery decisions, allocate resources, manage operational performance and take accountability for implementation.

The leadership style must shift from oversight to execution.

However, the organisation must still preserve appropriate independence.

When operations, governance and assurance sit under the same leader, there is a risk that the cybersecurity function becomes responsible for evaluating its own effectiveness.

Independent testing, separation of duties, enterprise risk oversight and strong internal audit remain necessary.

Past Experience Is Context, Not a Template

Experienced CISOs naturally rely on lessons from previous roles.

That is valuable.

The problem begins when previous experience becomes the only reference point for how the new organisation should operate.

A model that worked in a technology company may not fit a regulated financial institution.

A highly centralised structure may not work in a federated organisation.

A second-line CISO should not behave like the operational head of cybersecurity.

A full-scope CISO should not behave only as an adviser.

The CISO must first understand:

The governance model

Regulatory expectations

Reporting lines

Decision rights

Control ownership

Risk ownership

Budget authority

Organisational maturity

Business culture

Technology operating model

Only then can the CISO determine which previous lessons remain relevant and which leadership behaviours must change.

The Wrong Leadership Style Creates New Risk

When a CISO fails to adapt, the operating model becomes weaker.

In a CISO, TISO and BISO structure, excessive central control may undermine local accountability and slow decision-making.

In a Three Lines of Defence model, operational interference by the second-line CISO may compromise independence and confuse control ownership.

In a full CISO model, remaining too distant from execution may result in weak delivery, unresolved operational risk and unclear priorities.

The problem is not always a lack of competence.

It is often a mismatch between leadership style and operating model.

A strong CISO in one structure may become ineffective in another unless they are willing to adapt.

A CISO Must Relearn the Role

Every new CISO appointment should begin with a review of the operating model.

Before trying to reshape the security organisation, the CISO should ask:

Which functions do I directly control?

Which functions do I independently oversee?

Where must I remain separate?

Who owns cybersecurity controls?

Who owns remediation?

Who accepts residual risk?

Who controls the cybersecurity budget?

Who has authority during a major incident?

How are disagreements escalated?

How does the board expect assurance to be provided?

These questions determine how leadership should be exercised.

The answer may require the CISO to lead through coordination, independent challenge or direct execution.

Sometimes it requires a combination of all three.

Adaptation Is a Leadership Capability

The most effective CISOs are not those who repeat the same model everywhere they go.

They are those who understand why different organisations require different approaches.

In a CISO, TISO and BISO model, the CISO must coordinate.

In a Three Lines of Defence model, the CISO must govern, challenge and oversee risk from the second line under the CRO.

In a full CISO model, the CISO must execute and deliver.

Past experience remains important.

But it must be adapted to the organisation’s structure, mandate and maturity.

A CISO should not enter a new organisation asking how to recreate the previous one.

The better question is:

What type of cybersecurity leadership does this operating model require from me?

The title may be the same.

The leadership cannot be.

Question assumptions. Share knowledge. Build trust.