27 MARCH 2025

THE FUTURE

GRC

5th EDITION

BE CONNECTED

CYBER SECURITY COALITION

Solvay Brussels School
Economics & Management

ISACA
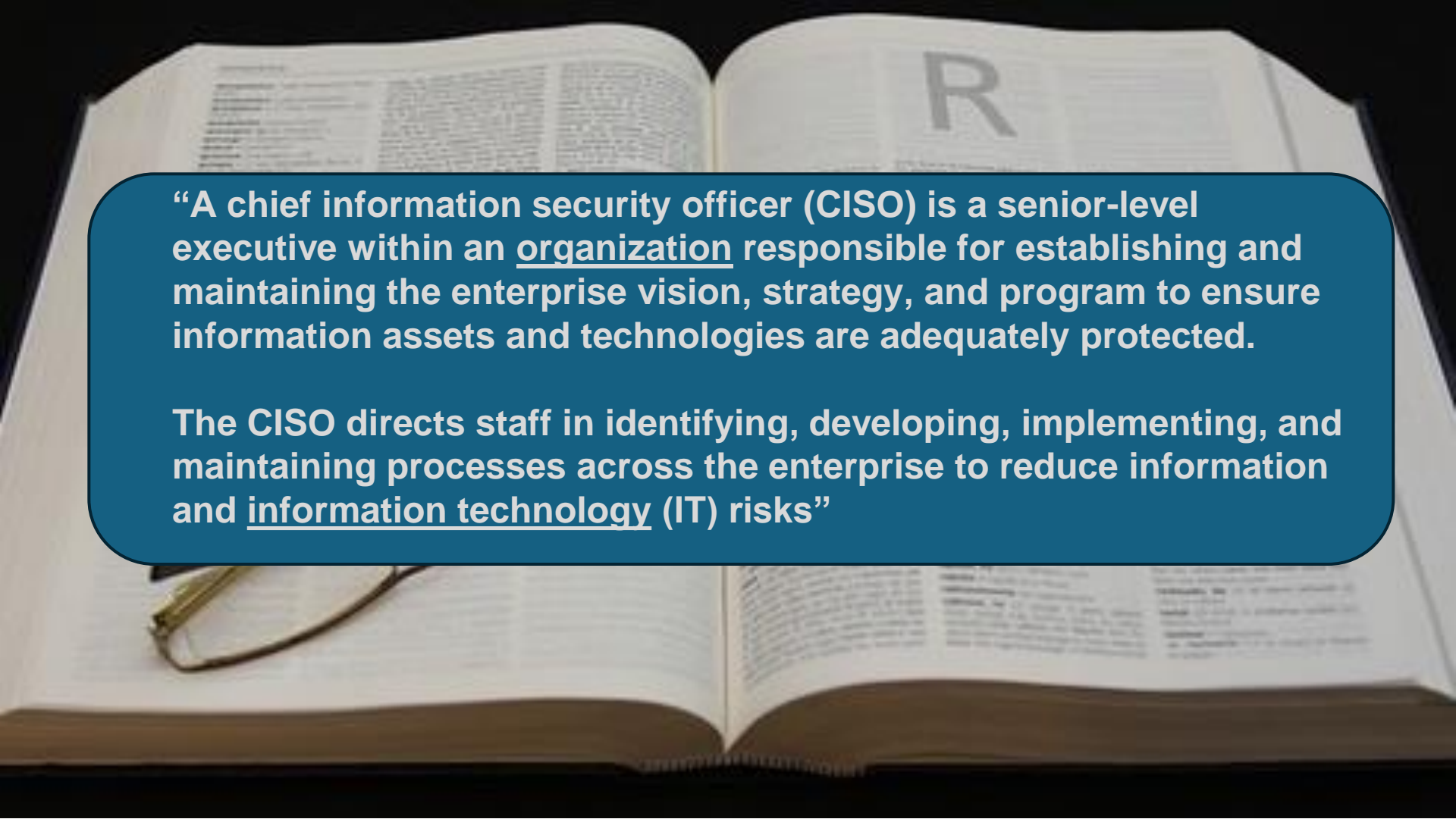Belgium Chapter

"A chief information security officer (CISO) is a senior-level executive within an <u>organization</u> responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and <u>information technology</u> (IT) risks"

How can CISO's work with the board to understand, plan for and mitigate risks in the organisation while continuing to encourage innovation for competitive advantage?

What's the Board's role?

Provide strategic direction

Provide governance and oversight

Enforce a Code of Ethics

70%

say cybersecurity is a beneficial topic for director development, training and education

Source: "Nominating/Governance Chair Survey 2024." n.d. https://www.spencerstuart.com/research-and-insight/nominating-governance-chair-survey Accessed July 16, 2024.

88%
of companies in the S&P 500 don't have cybersecurity professionals on their boards

Source: NightDragon, Securing our world for tomorrow. 2023. "NightDragon, Diligent Report Finds Gap in Cyber Experience in S&Amp;P500 Board Rooms." September 29, 2023. https://www.nightdragon.com/insights/nightdragon-diligent-report-cybersecurity-awareness-board-room/. Accessed July 16, 2024.
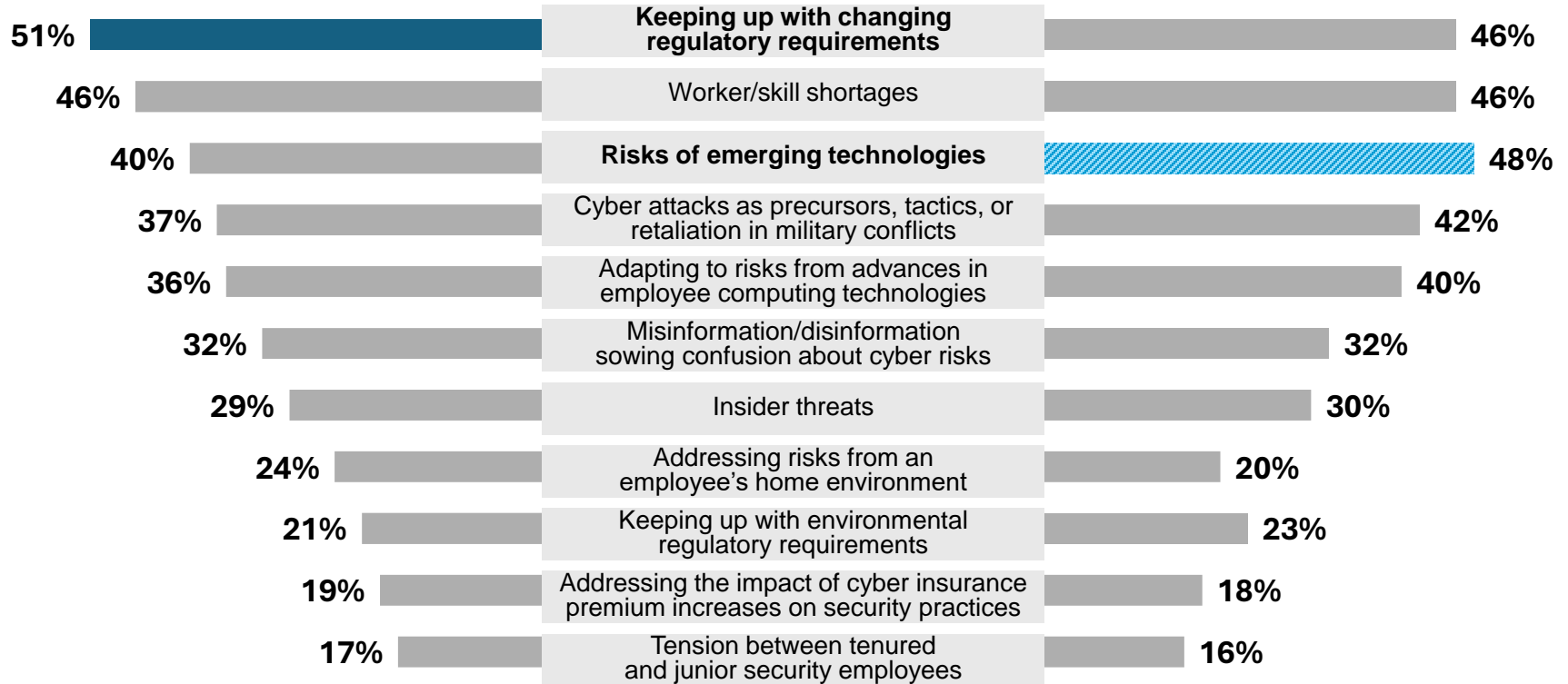
The Regulatory Landscape

Regulations, Laws and Acts
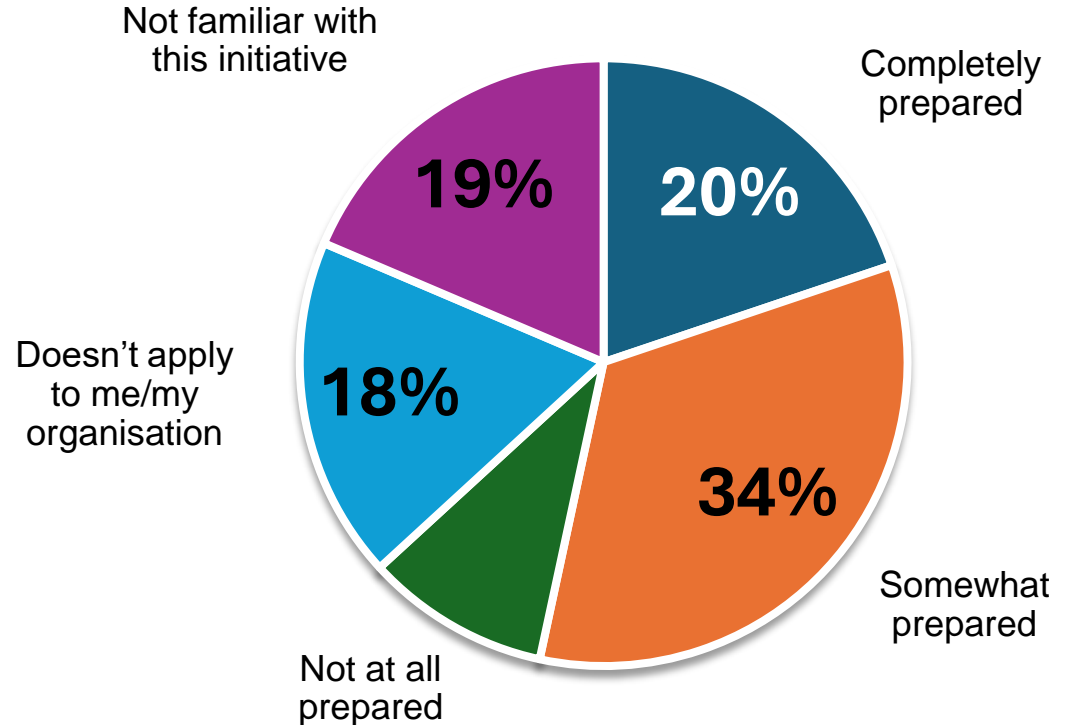
It's getting complex

Biggest challenges faced in the E.U. over the *past 12 months*

Biggest challenges to come in the E.U. in the *next two years*

Past 12 months	Challenge	Next two years
51%	**Keeping up with changing regulatory requirements**	**46%**
46%	Worker/skill shortages	**46%**
40%	**Risks of emerging technologies**	**48%**
37%	Cyber attacks as precursors, tactics, or retaliation in military conflicts	**42%**
36%	Adapting to risks from advances in employee computing technologies	**40%**
32%	Misinformation/disinformation sowing confusion about cyber risks	**32%**
29%	Insider threats	**30%**
24%	Addressing risks from an employee's home environment	**20%**
21%	Keeping up with environmental regulatory requirements	**23%**
19%	Addressing the impact of cyber insurance premium increases on security practices	**18%**
17%	Tension between tenured and junior security employees	**16%**

Source: 2024 ISC2 Cybersecurity Workforce Study.

54%
are prepared to implement CRA
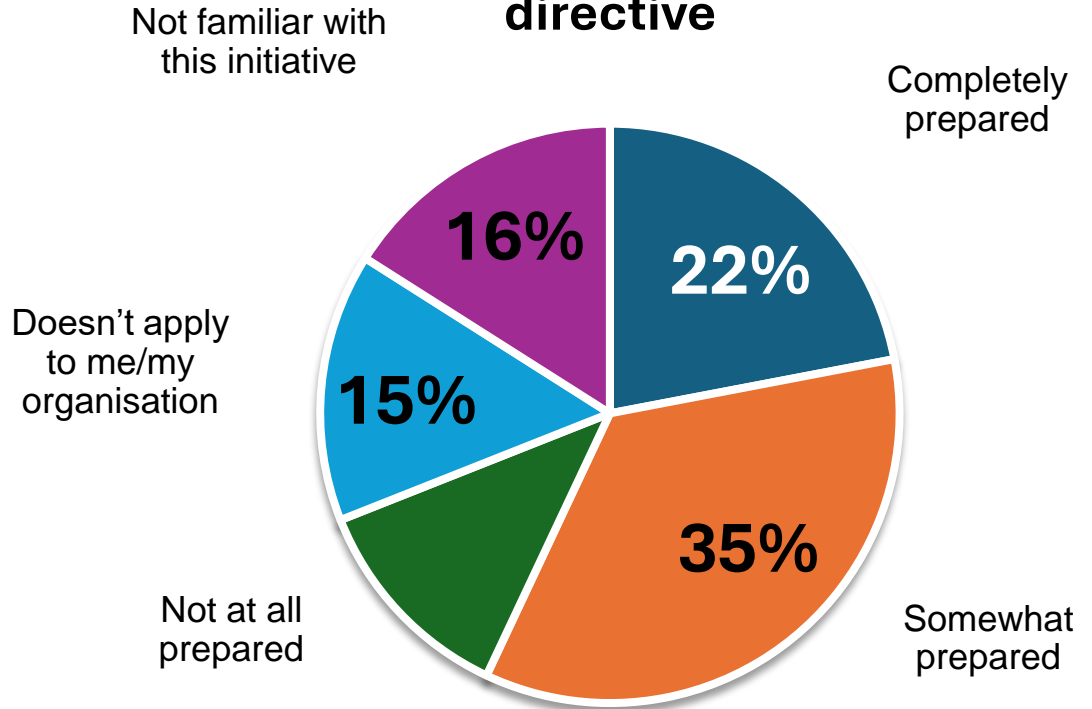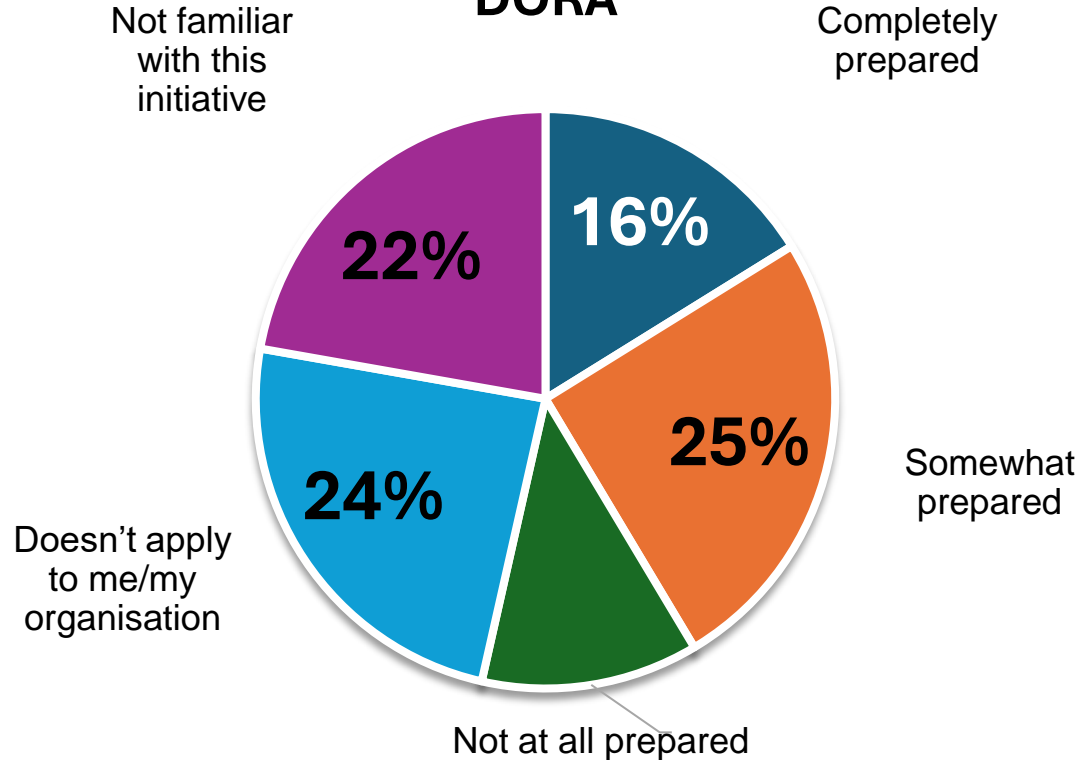
Level of preparedness to implement requirements of CRA

- Not familiar with this initiative — 19%
- Completely prepared — 20%
- Somewhat prepared — 34%
- Not at all prepared
- Doesn't apply to me/my organisation — 18%

57%
are prepared
to implement
NIS2

Level of preparedness to implement requirements of NIS2 directive

Not familiar with this initiative

Completely prepared

Doesn't apply to me/my organisation

Not at all prepared

Somewhat prepared

22%

35%

15%

16%

Source: 2024 ISC2 Cybersecurity Workforce Study.

41% are prepared to implement DORA

Level of preparedness to implement requirements of DORA

- Not familiar with this initiative — 22%
- Completely prepared — 16%
- Somewhat prepared — 25%
- Not at all prepared
- Doesn't apply to me/my organisation — 24%

The Tech Landscape

Communication

Typical organisation and leadership structure
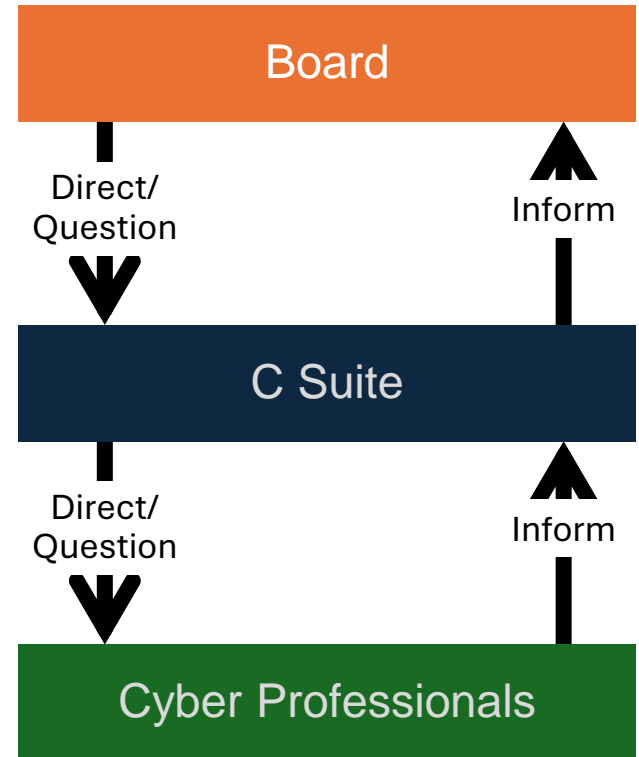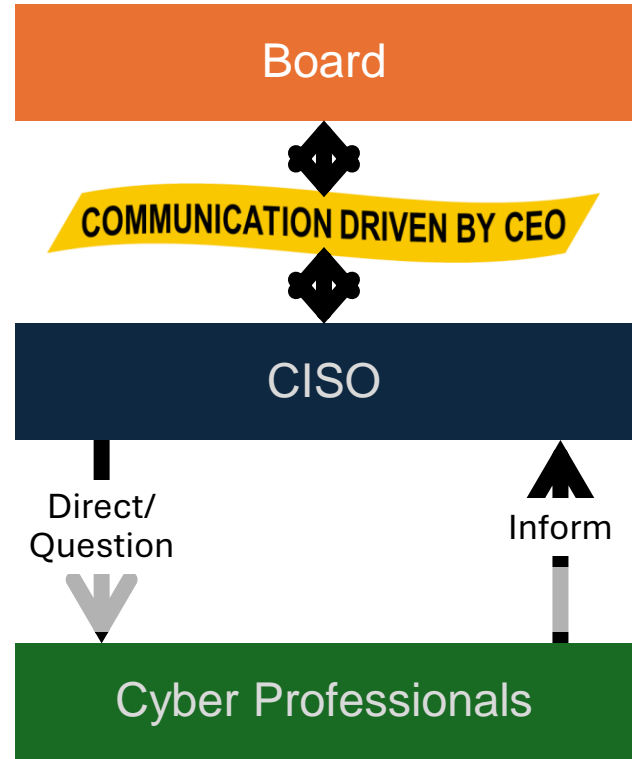
Board

Direct/Question — Inform

C Suite

Direct/Question — Inform

Cyber Professionals

CISO up front

Board

COMMUNICATION DRIVEN BY CEO

CISO

Direct/Question

Inform

Cyber Professionals

Communication Strategies:
Cyber Leaders to Board

Determine correct information level

Lead with business rationale, not cyber

Embrace the real world

Build trust by educating

Key Takeaways
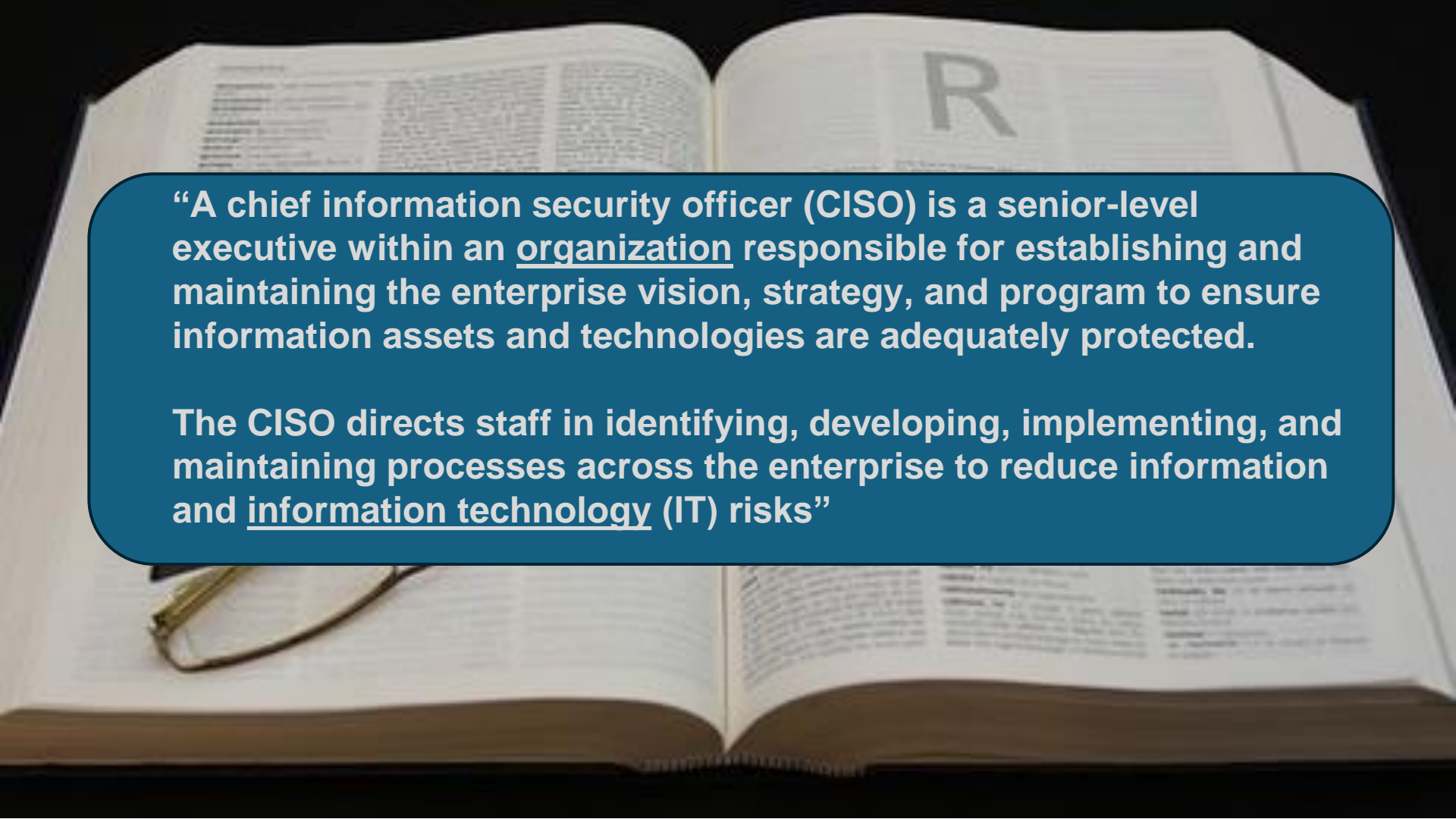
Understand what type of org you are in

Build a coalition

Translate technology to risk
(And enablement !)

Compliance is not enough

Compliance is not enough

Don't forget the 'day job'

"A chief information security officer (CISO) is a senior-level executive within an <u>organization</u> responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets and technologies are adequately protected.

The CISO directs staff in identifying, developing, implementing, and maintaining processes across the enterprise to reduce information and <u>information technology</u> (IT) risks"

A trusted leader that protects the organisation from threats to its information and operation through collaborative risk management.

As part of the wider leadership team enables business to take appropriate risks and embrace new opportunities