University of Pisa

Department of Information Engineering

Master's Degree in Cybersecurity

Organizational Sciences Module

Academic Year 2024 -25

The evolving role of CISO – Cybersecurity as a competitive advantage

Insights from Harvard Business Review

In the age of the 4th Industrial Revolution, businesses are more connected than ever, both within the enterprise itself and with other parts of the digital ecosystem.

As their technology investment mounts and they analyze larger caches of digital data, they become **ever more dependent** on data for growth and innovation.

Cybersecurity becomes a **strategic concern**. For every costly, headline-making data breach and procedural lapse, there are a multitude of threats that could have been just as destructive.

Source: Harvard Business Review (2019, October 4). Evolving the CISO Role to Make Cybersecurity a Competitive Advantage. Available at: https://hbr.org/sponsored/2019/10/evolving-the-ciso-role-to-make-cybersecurity-a-competitive-advantage

The new CISO role

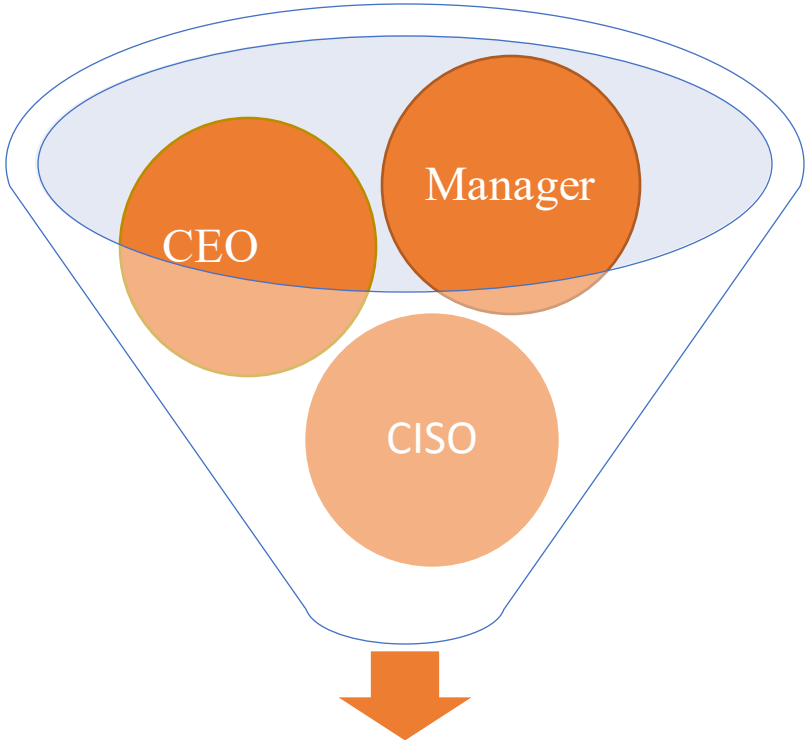
The CISO role must **shift from a mostly technical role to one centered on providing leadership and partnership across the business**—connecting to business and transformation strategies and driving initiatives and solutions that enable the organization to realize its goals.

The right CISO…

Is **fluent in business strategy** as well as technology, and knows how to effectively **collaborate** on new strategies with others in the C-suite, as well as on the board.

Steers an organization through the tricky terrain of **complex policy and regulatory challenges** tied to new technologies and rising concern over privacy and use of consumer data.

Helps nurture a **shared-risk view** alongside leaders in risk management, internal audit, compliance, business unit leaders, and the C-suite.



CEOs and board members can make a difference by fulfilling the “other side of the bargain” by giving the position a seat at the leadership and decision-making table, **empowering the CISO to drive change, and committing to manage cyber risk strategically across the business.**

Some insights

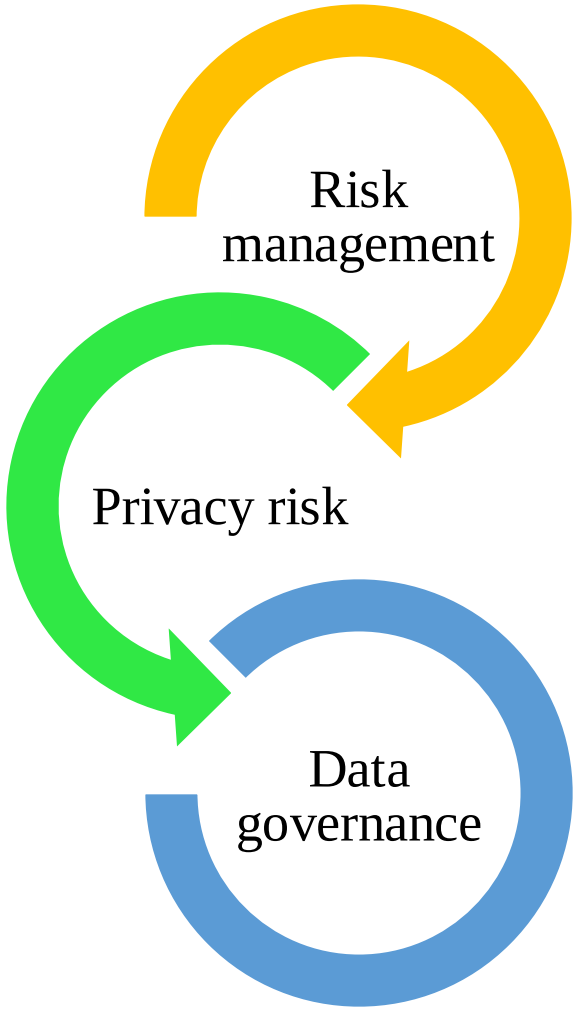
Large majorities of respondents say strong **leadership (76%), collaboration (84%), and communication skills (82%)** are very important for a successful CISO.

But there's a disconnect when it comes to developing and applying cybersecurity risk metrics.

Only 26% name it as being among the CISO's principal responsibilities today, and only 31% expect it to be a principal responsibility three years from now.

Not only an IT department matter

This finding suggests that,
at least conceptually,
organizations **no longer see cybersecurity as a matter that can be siloed within the IT desk**,
but as being closely linked
to their overall risk management efforts,
privacy risk, and approach to data governance.



Recruiting

Most organizations appear to have recruited their CISO **externally**, through either **human resources** (40%) or a **professional recruiting firm** (34%).

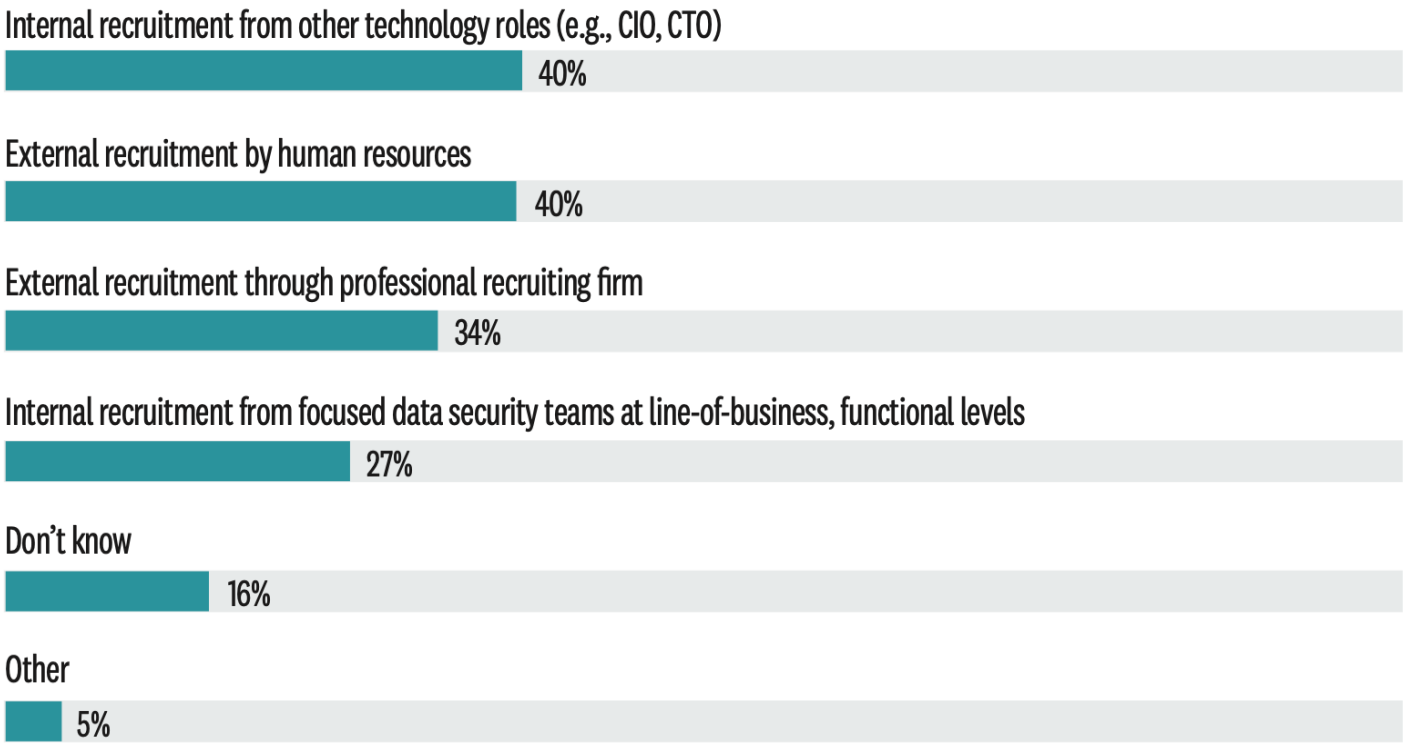
Thus, the profile of a cybersecurity leader is becoming better defined and organizations are becoming more **intent on filling the role with the best possible people.**

FIGURE 2

LEADERSHIP SEARCH

External recruitment is the preferred method for identifying future cybersecurity leaders.

What are the elements of your organization's strategy for identifying future CISO/cybersecurity leader candidates?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, MAY 2019

Insights

At York Risk, Bilger says about half the specialists in the CISO's office are recruited internally, typically from technology roles, and half from outside, generally from major accounting and consulting firms and from compliance backgrounds.

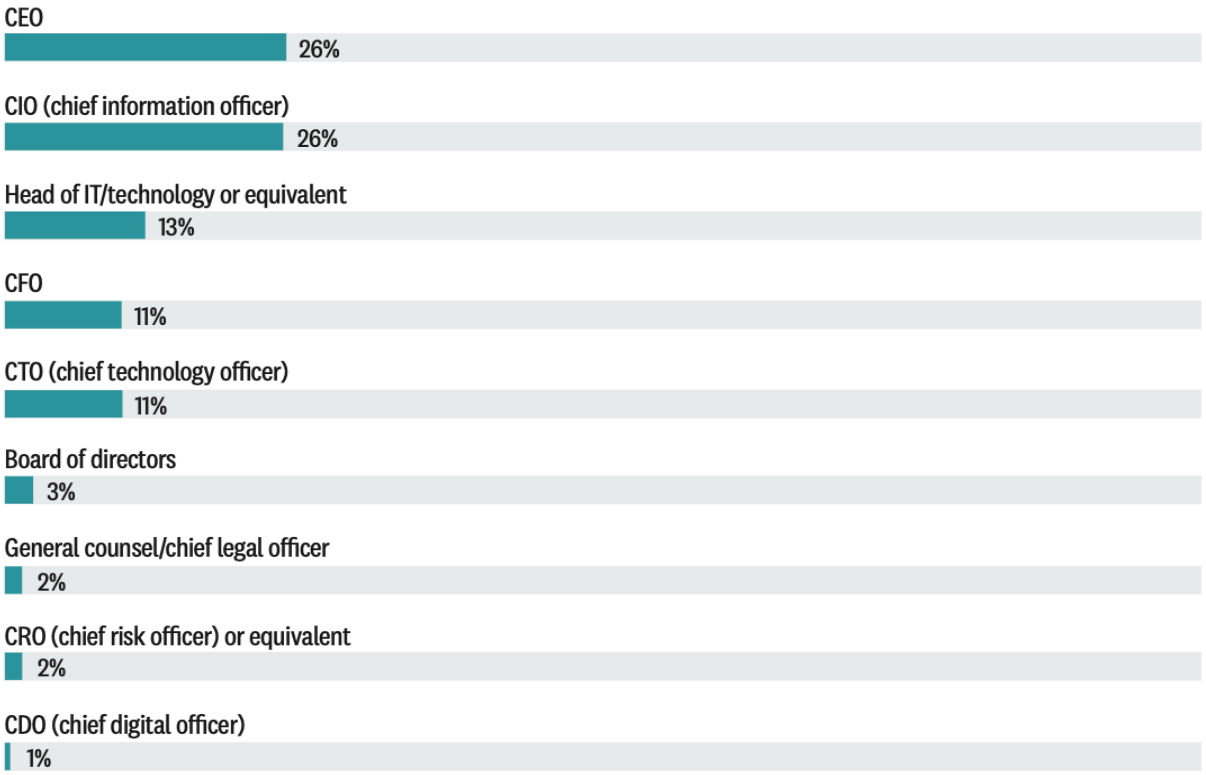
"If your people don't understand compliance policy, then you can have great tech controls, but you may not know how to enforce them in the right way"

FIGURE 4

LINES OF REPORTING

At most companies, the CISO reports to another data security or IT executive.

To whom does the CISO/cybersecurity leader directly report?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, MAY 2019

- CISO must have **access to and support from the board and the CEO.**
- Since cybersecurity **spans the whole company**, it needs support and buy-in from executive leadership

Examples

At SAP, the **CISO reports directly to the CIO and manages** all processes and policies related to data and broader cybersecurity, as well as some vendor relationships focusing on cybersecurity.

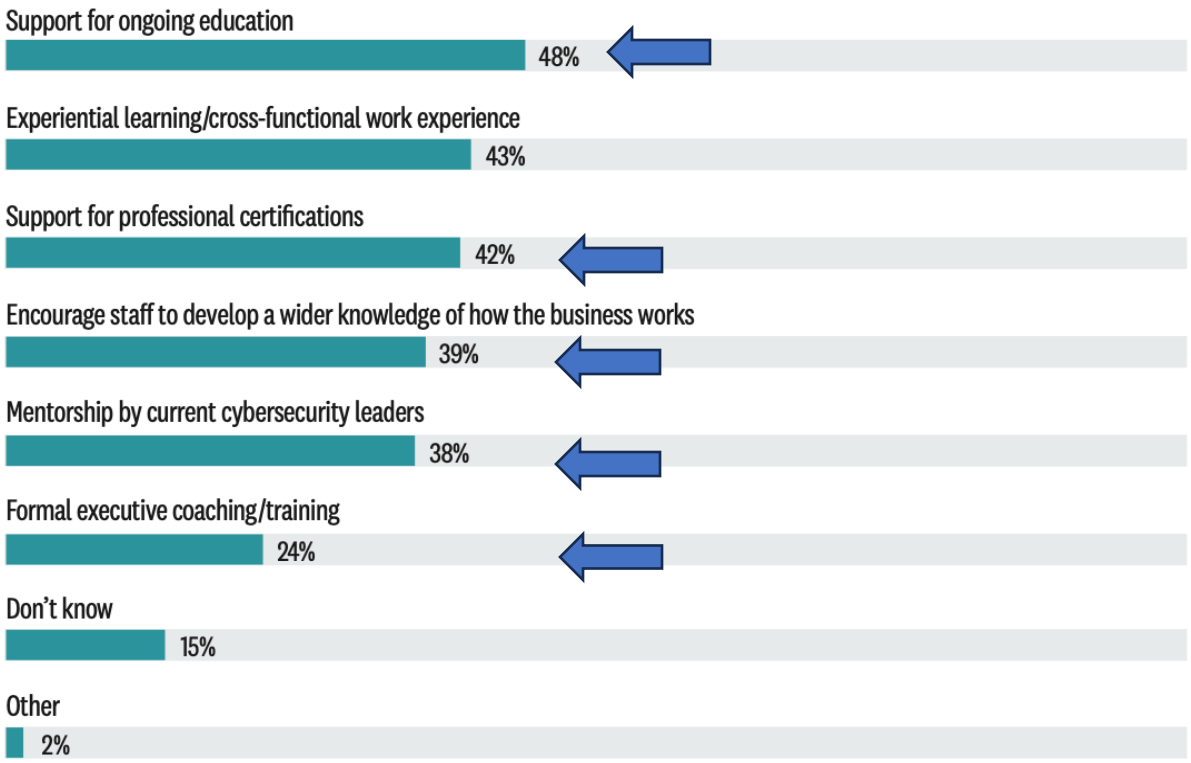
At York Risk, too, the **CISO reports to the CIO, who reports directly to the CEO**, underscoring the **importance attached to data and cybersecurity at the top levels of the organization.**

FIGURE 5

LEADERSHIP DEVELOPMENT

Few are encouraged to develop a wider knowledge of the business.

What are the elements of your organization's strategy for developing/mentoring future CISOs/cybersecurity leaders?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, MAY 2019

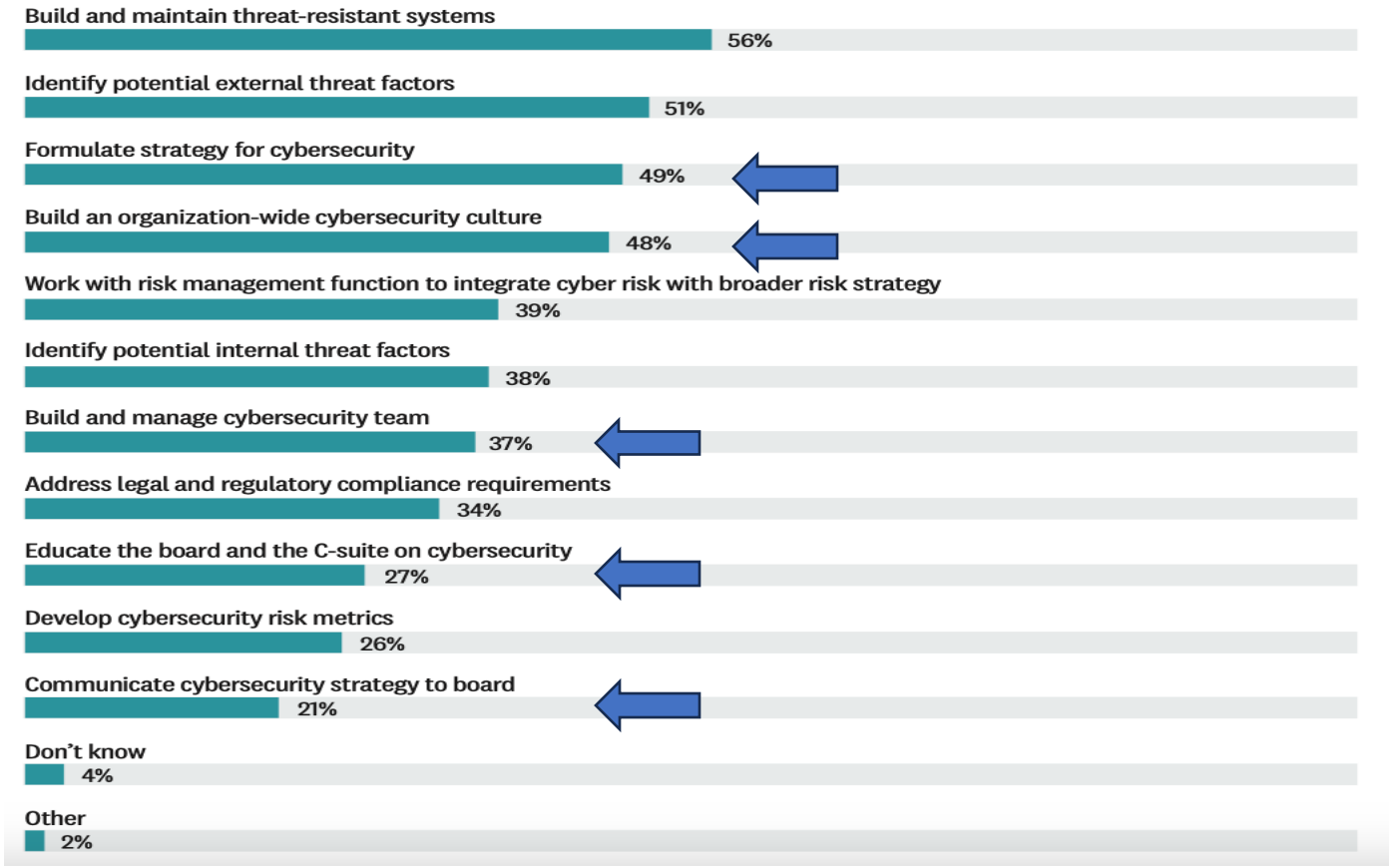
While developing and enforcing day-to-day data protections remain the CISO's most immediate tasks, **organizations that want to build a resilient cybersecurity culture will need to enlarge the role and make it more strategic.**

FIGURE 6

RESPONSIBILITIES TODAY ...

One key strategic task, developing cybersecurity risk metrics, ranks low.

What are the CISO's/cybersecurity leader's principal responsibilities today?



Responsibilities today

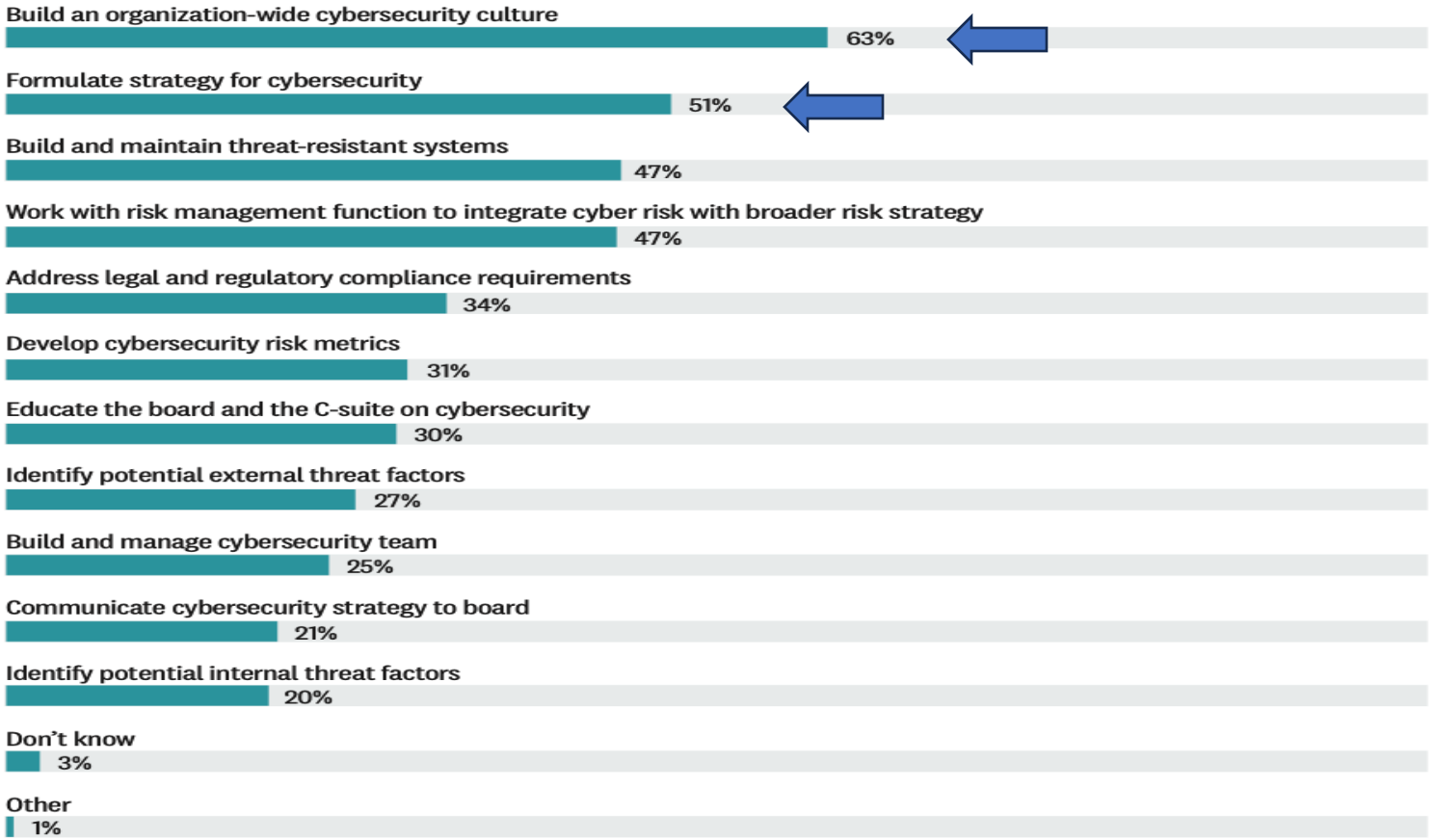
- The board and top management at most organizations are not as fully focused on cybersecurity as they need to be.
- For example, only 21% and 27% of respondents, respectively, say **communicating cybersecurity strategy to the board and educating the board and the C-suite on cybersecurity are top five responsibilities of the CISO**
- And **only 26% mention developing cybersecurity risk metrics**

FIGURE 7

... AND RESPONSIBILITIES IN 3 YEARS

Formulating strategy, building a cybersecurity culture will become more important.

What should be the CISO's/cybersecurity leader's principal responsibilities 3 years from now?



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, MAY 2019

Responsibilities in three years

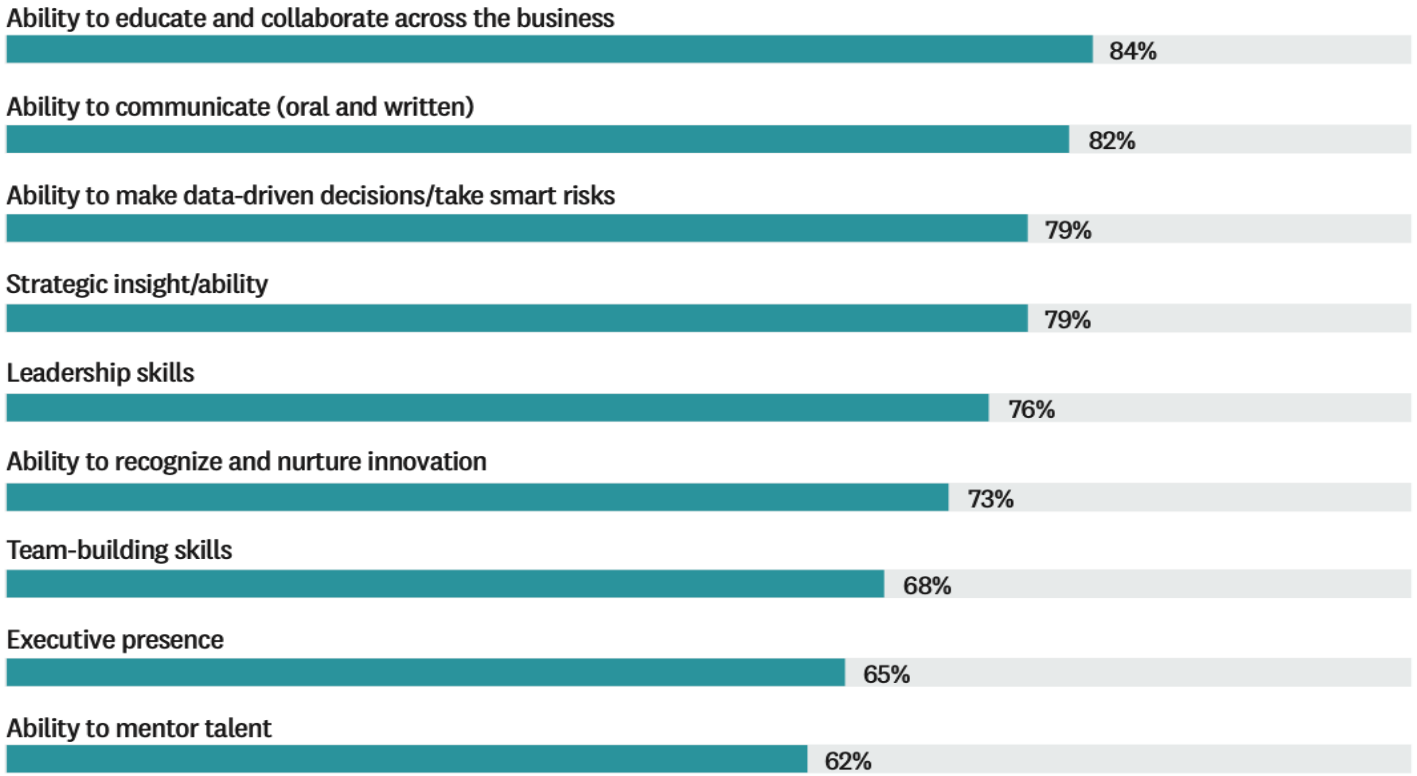
- The **strategic aspect** of the CISO's role is likely to grow.
- Building an organization-wide **cybersecurity culture takes the biggest leap in importance** with 63% of respondents saying it will be a top five responsibility.
- Formulating a **strategy for cybersecurity** rises slightly as well, to 51%.
- Less than half of respondents (47%) say that working with **the risk management function to integrate cyber risk** with the organization's broader risk strategy will be one of the CISO's top five duties.
- Basic CISO tasks like **threat identification and managing threat-resistant systems** are **expected to be less important**, possibly because respondents assume these tasks will become more routinized.

FIGURE 8

LEADERSHIP QUALITIES

The abilities to educate, communicate, and nurture innovation are prized.

How important are each of the following skills to being a successful CISO/cybersecurity leader?
[VERY IMPORTANT]



SOURCE: HARVARD BUSINESS REVIEW ANALYTIC SERVICES SURVEY, MAY 2019

The first three all pertain to the CISO's **ability to be a strategic player** alongside the organization's top executives; the fourth reflects the **capacity to take initiative within the cybersecurity space.**

Leadership abilities

- Communication moves in two directions. One important aspect of the CISO's leadership role is to **keep the board up to date and focused on cybersecurity** matters; another is to **convey management's and the board's business objectives to the organization's cybersecurity specialists and developers**.

- Once the CISO has that support they need to **create an environment where skills and expertise are shared.**

- **«The death spiral is when someone has all the keys and is not sharing them».**

Product development

- Because of the increasing need to **integrate security features into new designs from the start**, the CISO should play a key role in product and application development.
- At less than half does the CISO or cybersecurity leader participate in product testing (44%), development (42%), or strategy (42%), according to respondents, and in earlier stages—idea generation, idea screening, and evaluation—the CISO is even less present.
- Most businesses are **not taking full advantage of the expertise that the CISO** and the security team **can bring to these activities** that hold the key to their future.

Organizations should…

- Create a document setting out the business case for a strong, **organization-wide cybersecurity program.**
- Enable the CISO to devote more attention to formulating cybersecurity strategy and building an **organization-wide cybersecurity culture.**
- Decouple the CISO from the IT function and **promote more frequent engagement** between the CISO and both executive management and the board.
- Give the CISO an **earlier, stronger role in the product and application development** process.
- Devote more attention to **recruiting and training cybersecurity leaders.**
- Ensure the CISO has the **budget and resources** needed to do a job that is constantly expanding.

CISO task descrption

- Developing and implementing secure processes and systems used to prevent, detect, mitigate, and recover from cyberattacks
- Educating and managing technology risk in collaboration with business leaders
- Building and driving a cybersecurity strategy and framework, with initiatives to secure the organization's cyber and technology assets
- Continuously evaluating and managing the cyber and technology risk posture of the organization
- Implementing and managing the cyber governance, risk, and compliance (GRC) process
- Reporting to the most senior levels of the organization (the CEO and board of directors, or equivalent)
- Developing, justifying, and evaluating cybersecurity investments
- Developing and implementing ongoing security awareness training and education for users
- Leading cybersecurity operations and implementing disaster recovery protocols and business continuity plans with business resilience in mind

Source: CISCO. Available at: https://www.cisco.com/c/en/us/products/security/what-is-ciso.html#~ciso-role-explained

Job description

Public Company Accounting Oversight Board

- participate and contribute as an effective member of the **leadership team, working closely with and advising the CIO**, executive leadership.
- responsible for the implementation, optimization, and delivery of our **comprehensive information security strategy.**
- development and implementation of a **security program**, facilitate information security governance.
- continuously assess and develop the cybersecurity landscape, act as a **change agent**, and help to lead **information security resilience.**

Source: https://pcaobus.wd1.myworkdayjobs.com/en-US/PCAOB/details/Chief-Information-Security-Officer_R1093
https://www.linkedin.com/jobs/view/head-of-it-and-cyber-security-it-manager-ciso-at-techyon-4036804707/

Job description

Techyon

- Develops and implements an **IT strategy clearly aligned with the company strategy**
- Develops and implements cybersecurity policies that align with European regulations and Defense & Aerospace industry standards.
- Ensures that security practices are **integrated at all levels of the IT infrastructure.**
- Defines plans for **vulnerability assessments** and penetration tests to identify weaknesses in computer systems and devices.
- Develops **cybersecurity training programs to educate company employees** on best practices and cyber threats. Promotes a **culture of corporate IT security.**

Source: https://pcaobus.wd1.myworkdayjobs.com/en-US/PCAOB/details/Chief-Information-Security-Officer_R1093
https://www.linkedin.com/jobs/view/head-of-it-and-cyber-security-it-manager-ciso-at-techyon-4036804707/

To summarize

The CISO symphony

The CISO symphony


THE
END