The CRO cyber risk agenda: what boards should be asking

Building a better working world

Cybersecurity has been a top priority for bank board directors for years. The 12th annual global bank risk management survey, conducted by Ernst & Young LLP (EY US) and the Institute of International Finance (IIF) surveyed 88 chief risk officers (CROs) from banks around the world.

This survey confirms just how complex the cyber risk landscape has become and where CROs think boards should engage.

CROs told us that cybersecurity risk is their No. 1 priority for the next 12 months, and they also see it as the top risk priority for boards. This may seem surprising given the billions invested to safeguard core systems and vital data assets. However, in the eyes of CROs, cyber risks are ubiquitous and originate from various external sources, including criminal groups and state-sponsored organizations; plus stem from lenient internal breaches as well. In addition, cyber risks evolve constantly as bad actors seek vulnerabilities and adopt increasingly sophisticated techniques.

The pervasive connectivity at the heart of the global banking system presents significant risks. Technology ecosystems and partnership-driven strategies amplify cyber risk. So does geopolitical turbulence. Collectively, these factors explain why CROs see cyber as the risk most likely to result in a crisis or major operational disruption — even when they perceive their own internal systems as largely secure.

Board members in financial services and other sectors can glean a lot from looking at the survey results and better understanding front-line risk.

Five key takeaways for boards:

1

Cyber risk was the top risk priority for bank CROs, ahead of credit risk.

World events and economic forces from the past few years have complicated traditional risk management, boosting the role of cyber risks on CRO agendas. CROs rated cyber risk on average as their most significant immediate-term risk priority. That's no surprise given the war in Ukraine, which has potentially significant implications for cybersecurity and for banks with major operations or outsourcing relationships in Eastern Europe. Credit risk concerns are no doubt on the rise in the wake of the March 2023 banking crisis and are likely to escalate board oversight.

Top CRO risk priorities for the next 12 months

Questions for the board to consider

- How does the board maintain its focus on cyber risk if macroeconomic conditions place new emphasis on credit risk?
- How should cyber risk fit within board priorities?

2

Cyber poses both near-term operational risks and longer-term strategic risks.

While directors and CROs are justifiably focused on the immediate impacts of cyber attacks, they aren't overlooking the longer-term implications. CROs ranked cybersecurity risk as their top long-term strategic risk by a significant margin. Environmental, social and governance (ESG) and technology risk generate lots of attention, but cyber risk dominates the strategic agenda in the eyes of CROs. Boards must keep that perspective in mind as they help business leaders prioritize investments and activities. Here again, the connections between cyber threats and other types of risks cannot be overlooked.

The top strategic risks that concern CROs over the next three years

The inability to manage:

Questions for the board to consider

- How does the company's risk management framework balance near-term concerns with longer-term strategic risks?
- What practices might improve the company's ability to manage cyber risk?

3

CROs believe boards are aligned to their view of cyber risk as a top priority.

CROs believe they are largely aligned to board-level views of risk priorities, with cyber at the top, followed by credit risk. That ranking could change if macroeconomic conditions worsen or if we see more bank defaults. For boards, a complex risk landscape requires a deep understanding of both individual risks and the relationships between them — and regularly challenging the organization's risk appetite in the context of cyber risk prevention, detection and remediation.

Top board risk priorities for the next 12 months (according to CROs)

Questions for the board to consider

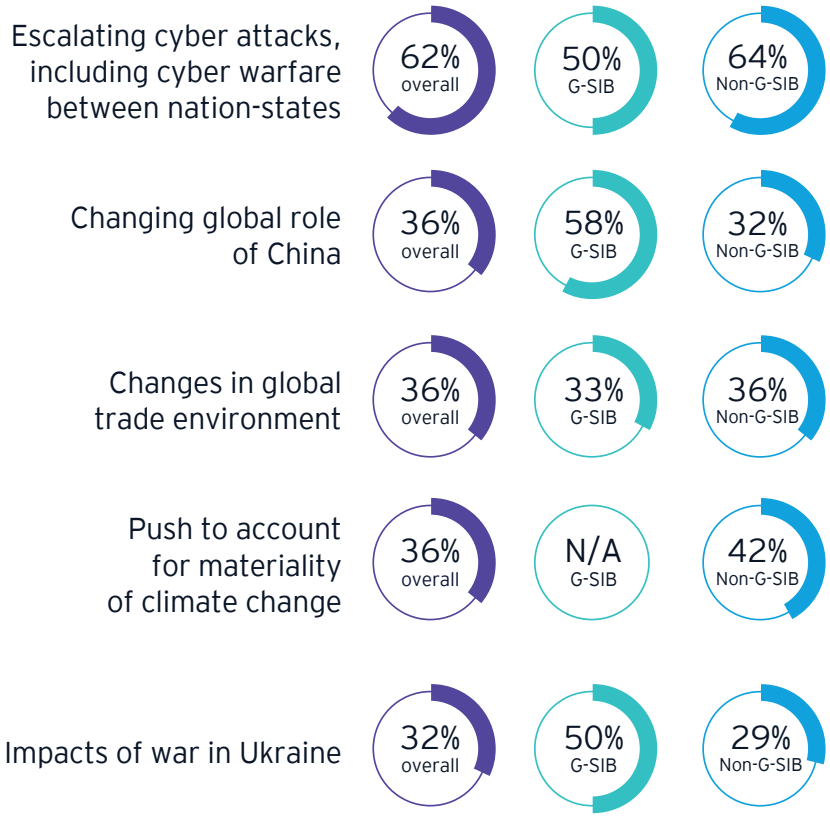
- Are the board's risk priorities aligned with those of CROs and business leaders?
- Does the board understand the relationships between cyber risk and other top-priority risks?
- Do board meeting agendas allow ample time to address organizational cyber risk through the three lines of defense —CRO, chief information security officer (CISO) and internal audit director?

4

Geopolitical risk amplifies cyber risk.

The link between cyber and geopolitical risk illustrates the complex interrelatedness of different risk categories. CROs at different types of banks have differing views of the threats. For instance, 58% of CROs at G-SIBs view China's changing global role as a significant risk, versus only 32% of CROs at non-G-SIBs. Such gaps highlight how every bank must assess its cyber risk profile based on its unique operational and geographic footprint.

What are the top geopolitical risks that will most affect our organization over the next year?



Questions for the board to consider

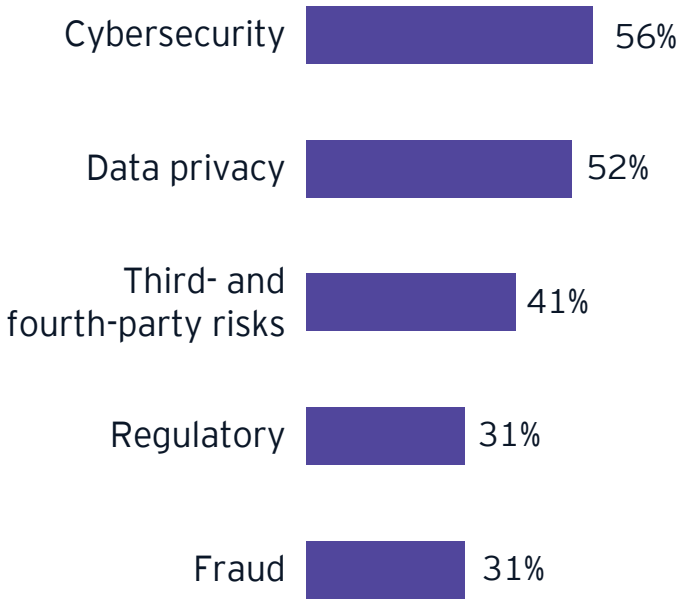
- What role do geographic footprint and use of outsourcing and offshore partners play in tracking cyber risks?
- How often should the board evaluate the organization's risk profile to reflect geopolitical trends?

5

Business transformation and innovation strategies can create vulnerabilities.

CROs are paying more attention to growth and innovation strategies, including digital product development, new business models and ecosystem plays. Digital transformation programs that rely heavily on AI and machine learning are also on CROs' radars. All of these present potential cyber risks, often through connections to third parties. The overall objective must be to de-risk information technology wherever possible, which is why boards may feel a need to keep informed on both cyber risks and digital transformation trends. These are especially critical considerations when formulating and executing ecosystem strategies.

Ecosystem and alliance risks that will require the most CRO attention in the next three years



Questions for the board to consider

- How can leading cybersecurity practices be embedded into business transformation programs and technology deployments?
- What processes are in place to manage third-party ecosystem and alliance risks?

Effective board leadership on cybersecurity: supporting CROs in managing risk

CROs and board members must work together to lead and govern effective cyber risk management. Specifically, boards must support CROs — and the entire business — in protecting critical systems and assets from cyber threats. That process starts with asking the right questions to challenge senior management and business leaders to drive accountability for current cybersecurity practices and outcomes.

Beyond the questions already outlined, directors may also ask:

- Is the board hearing from the CRO and CISO often enough?
- How can the board stay attuned to unanticipated risks?
- Does the board have the data and tools it needs to understand and monitor vulnerability?
- What are the most credible sources of information on the latest cyber threats?
- How is the organization positioned to comply with new regulation relative to cybersecurity?

About the survey

The global EY organization, in conjunction with the IIF, surveyed CROs or other senior risk executives from 88 banks in 30 countries around the world from June 2022 through October 2022. Participants were interviewed, completed a survey or both. Participating banks were headquartered in Asia-Pacific (11%), Europe (16%), Latin America (18%), the Middle East and Africa (19%), and North America (36%), and 14% were G-SIBs.

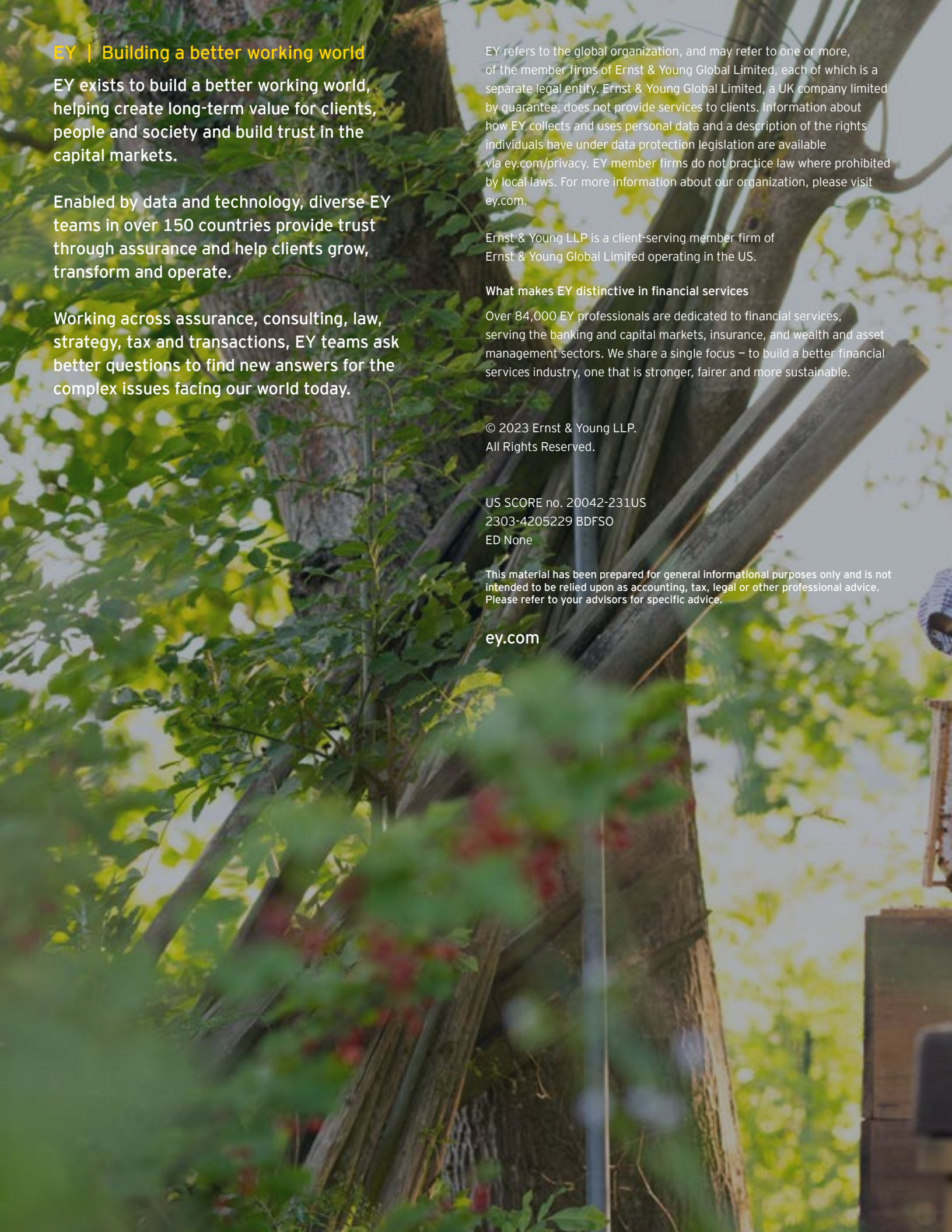
Related content:

12th annual global bank risk management survey

Looking for more information and insights relative to cyber risk?

Contact EY professionals to learn more about the resources we offer board directors in banking and financial services:

Cybersecurity, strategy, risk, compliance and resilience



EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

What makes EY distinctive in financial services

Over 84,000 EY professionals are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. We share a single focus – to build a better financial services industry, one that is stronger, fairer and more sustainable.

US SCORE no. 20042-231US
2303-4205229 BDFSO
ED None

ey.com