Russell Reynolds ASSOCIATES

Guardians of Trust: EMEA Boards Take Ownership of Cybersecurity

This article is available on russellreynolds.com

Boards and CEOs consistently rank cybersecurity as one of the most significant risks facing their organizations. It's indeed often "the defining risk of the moment," one chair told us, particularly given the rise of AI deployment.

Large organizations face hundreds of attacks each year, with consequences that can have enterprise-wide implications far beyond IT. The recent news surrounding Anthropic's Claude Mythos 5 and Fable 5 models serves as a reminder that AI is lowering barriers to sophisticated cyber activity, potentially amplifying both the frequency and severity of attacks.

The regulatory environment also is raising expectations, with frameworks such as the Network and Information Security 2 Directive introducing elements of personal accountability at the board level. In this context, several directors described the board as the last line of defense on cybersecurity.

"Cybersecurity is top-of-the-agenda right now in all the boards I sit on," said one director with multiple affiliations across several sectors.

This raises fundamental questions: How are boards of EMEA publicly listed companies governing cyber risks today, and what gaps remain?

To understand how boards are approaching the issue, we interviewed a dozen board chairs, audit committee members and non-executive directors from publicly listed companies across EMEA. Here's what we learned.

01 "Informed challengers" and the cyber capability question

In prior research from this series, we explored how boards have begun adding directors with tech experience as a core component of board effectiveness. While this capability is crucial for today's environment, chairs broadly reject the idea that boards should include solely technical specialists. "You cannot have a specialist for every topic," one said.

While cybersecurity expertise remains a management responsibility, truly effective boards must have:

- A baseline understanding of cybersecurity concepts and risks.
- The ability to assess management's policies and decisions.
- The confidence to ask relevant and probing questions.
- One or two experts with meaningful technology and cyber risk knowledge.

This informal model of "informed challengers" enables all directors to elevate the discussion. Without this, "we can't challenge what we're told," one director said.

Board members with CEO experience bring a valuable perspective on trade-offs, cost and acceptable risk. This translates into a growing demand on boards to add sitting CEOs who bring a current, operational perspective on these issues.

"Chairs are often retired executives who may be further from day-to-day cybersecurity considerations, so it's key that the board includes sitting executives with this more up-to-date exposure to cyber threats," one director said.

Other "informed challengers" may include executives from technology businesses, where cybersecurity is embedded by design; audit committee chairs with experience in cyber crises; or executives from highly regulated industries.

On cybersecurity, the consensus is that high-performing boards require a diversified and complementary makeup. Regular assessment of the board's skills helps ensure that governance can effectively oversee the company's cybersecurity preparedness.

---

02 Prior safety strategies don't equate to future security

Board members broadly agreed that one of the most significant transformations is from simply addressing prevention to making sure the organization can withstand an attack.

Cybersecurity discussions historically focused on how to avoid breaches, with prevailing wisdom suggesting that a lack visible incidents meant the organization was protected. The general belief was often, as one director put it, "since we've never been attacked, we must be well protected."

Today, this mindset leaves organizations underprepared to handle emerging risks. For example, information manipulation is increasingly seen as a corporate threat, whether through "deepfake" content, fabricated executive communications, or coordinated disinformation campaigns.

Directors now recognize the limits of over-relying on prior protections. Breaches are no longer hypothetical—they're inevitable. As a result, boards and audit committees are putting more emphasis on crisis preparedness along with recovery capabilities and business continuity mechanisms. Several directors emphasized that the key questions now center on resilience:

What is the recovery plan? What happens if our defenses are breached tomorrow? What stops immediately, what keeps on working, what do we lose access to?

In some organizations, audit committees are developing cyber crisis scenarios to review with the board. Indeed, several directors we interviewed said that often the real differentiator in a crisis is the extent to which such scenarios have been practiced.

"If a cyberattack occurs, the board must be ready: all hands on deck, roles have been rehearsed, the board reacts fast and efficiently," said one audit chair.

03 Regulation is a catalyst

Regulation is accelerating cybersecurity transformation. In Europe, the NIS2 Directive represents a significant shift from collective responsibility to collective and personal accountability. "Cybersecurity is no longer a data point that boards review, but a set of decisions they are accountable for," one board chair said.

In this context, many directors see NIS2 as an opportunity and a catalyst to strengthen cybersecurity governance more broadly. It's prompting boards to reassess their governance frameworks, clarify responsibilities and elevate oversight quality. "Board members become personallyresponsible — this is a real wakeup call," said one director.

04 Cybersecurity governance falls on the entire board

Cybersecurity is typically anchored in a board's audit committee, which monitors the issue as part of its review of enterprise risk management. Ad-hoc third-party counsel can prove useful. "An external audit [helps us] understand our maturity relative to others," said one audit committee member.

Still, ultimate accountability remains with the full board, with cybersecurity usually reviewed at least annually. "Risk management is really the full board's responsibility," said one audit committee member. "We mustn't shy away from it under the pretense that 'cybersecurity is too complex.'"

In a major cyberattack, the entire board focuses on crisis governance, stakeholder communication and key financial decisions, such as ransom considerations. Yet several directors we interviewed questioned whether boards are sufficiently prepared for such a situation. While governance structures are generally well established, many directors acknowledged that cyber crises place unique demands on boards: Decisions must be made quickly, often with incomplete information and under intense operational, regulatory and media scrutiny.

05 The education gap — and how to close it

Many directors are concerned that board training remains too limited, often amounting to little more than basic awareness sessions. "Training is critical, in that it allows you to ask the right questions and understand the answers," one director said.

Useful areas of focus include supplier requirements and dependencies, high-level systems architecture, the organization's ability to compartmentalize risk, and cybersecurity budgets relative to industry benchmarks.

Directors also emphasized that the most effective training often comes from inside the organization. "In reality, no one is better positioned than our own CIO or CISO to offer an accurate view on where we are," said an audit committee chair. Several said CISOs are often willing to speak candidly about their biggest concerns. Optional workshops or Q&A sessions, rather than formal annual reviews, may help boards cut through jargon and technical complexity.

Several directors and audit committee members insisted that cyber topics must be translated into decision-relevant insights that boards can act on. This highlights the need for best-in-class cybersecurity leaders to ensure boards can lean on them.

External training also helps, particularly on regulatory topics such as NIS2, where legal expertise is required. Some directors also highlighted the value of boards sharing their experiences with each other : "Regulations like DORA (the Digital Operational Resilience Act) and NIS2 have pushed for mandatory disclosure of cyberattacks and incident response, which we should leverage to foster awareness and education, said a Risk Committee member.

What's next? Cybersecurity as a test case for board effectiveness

Cybersecurity is a test of how boards adapt to a new category of risk: one that's dynamic, technical, and deeply interconnected with strategy, operations and reputation.

The evolution observed across boards reflects a broader shift:

- **From technical risk to enterprise risk.**
- **From protection to resilience.**
- **From collective responsibility to increasing individual liability.**
- **From delegated oversight to board accountability.**

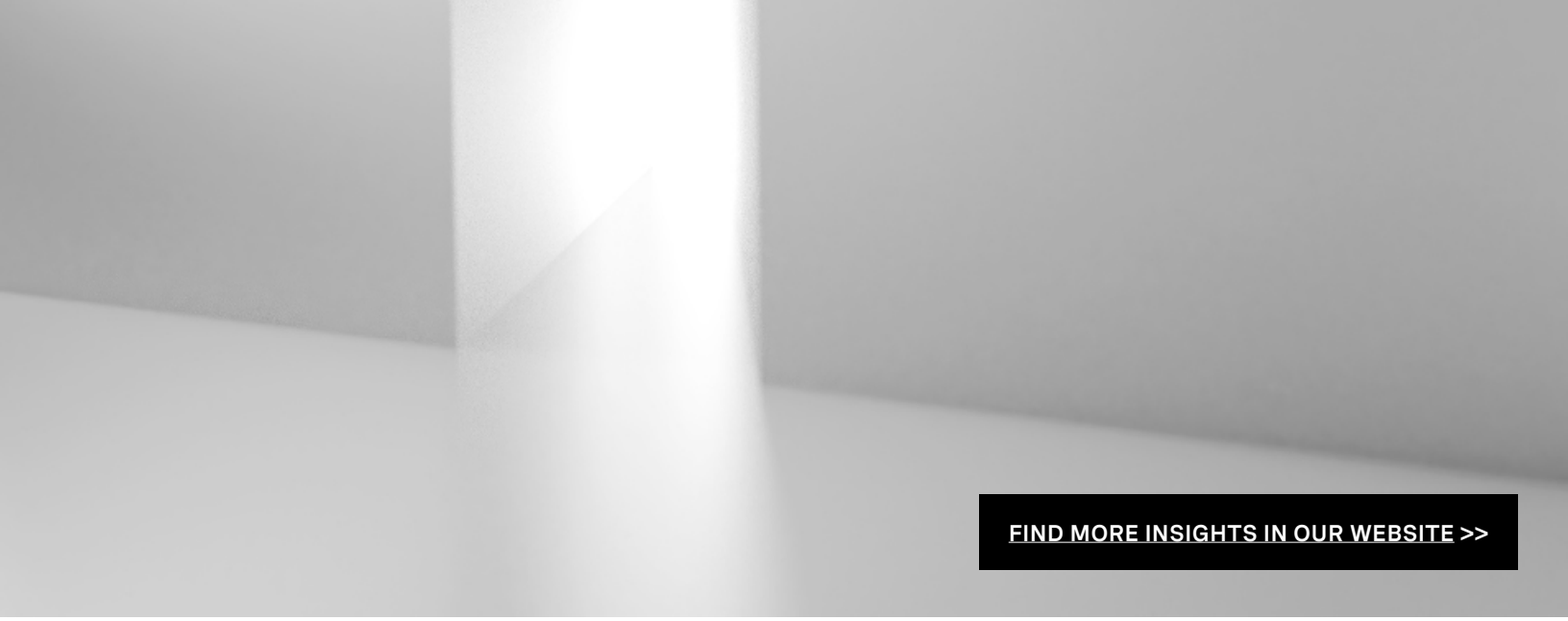
There's no one-size-fits-all governance model. The appropriate approach depends on sector, scale and exposure. However, a set of common principles is emerging:

- **Integration of cybersecurity within enterprise risk frameworks.**
- **Clear allocation of responsibilities among the board, committees and management.**
- **Focus on resilience, preparedness and testing.**
- **Continuous development of board capability — training of the full board and appointment of "informed challengers" with cybersecurity experience/savvy.**

Effective cybersecurity governance won't come from turning directors into technical experts or by appointing a swath of new experts to the board. Rather, boards must be equipped to understand the issues, ask the right questions, challenge management and make informed decisions when it matters most. As cyber threats evolve, so too must the boardroom.

List of interviewiees

- **Jacques Aschenbroich**, Board roles: Orange, TotalEnergies, BNP Paribas
- **Yannick Assouad**, Board roles: Vinci, Arkema
- **Valérie Beaulieu**, Board roles: Orange, ISS A/S
- **Anne Bouverot**, Board roles: Safran, Cellnex, Technicolor Creative Studios, Thomson Reuters
- **Fabienne Dulac**, Board roles: L'Oréal, FDJ United
- **Catherine Guillouard**, Board roles: Airbus, Lottomotica, Air Liquide, Ingenico, Arrive
- **Dominique d'Hinnin**, Board roles: Kering, Cellnex, Edenred, Vantiva, Eutelsat
- **Guillaume Poupard**, Board role: BNP Paribas
- **Katleen Vanderweyer**, Board roles: Vantiva, Euroclear, Ageas, AG Insurance
- **Nathalie Wright**, Board roles: Keolis, Quadient, Amundi



FIND MORE INSIGHTS IN OUR WEBSITE >>

Authors

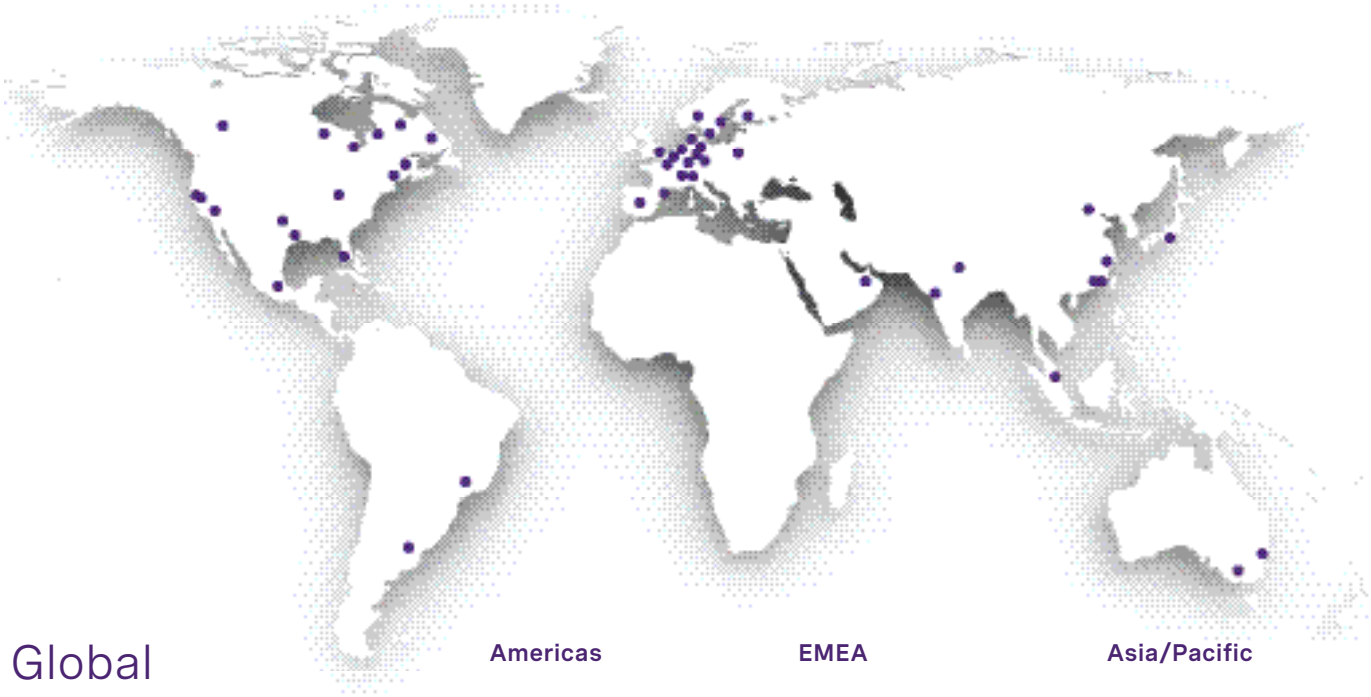
Agathe Martin-Gougenheim, is a senior member of Russell Reynolds Associates' Board & CEO Advisory practice and Technology Practice. She is based in Paris.

Yuelu He, is a member of the Russell Reynolds Associates' Commercial Strategy & Insights Board & CEO Advisory team. She is based in Munich.

About Russell Reynolds Associates

Russell Reynolds Associates is a global leadership advisory firm. Our 500+ consultants in 47 offices work with public, private, and nonprofit organizations across all industries and regions. We help our clients build teams of transformational leaders who can meet today's challenges and anticipate the digital, economic, sustainability, and political trends that are reshaping the global business environment. From helping boards with their structure, culture, and effectiveness to identifying, assessing and defining the best leadership for organizations, our teams bring their decades of expertise to help clients address their most complex leadership issues. We exist to improve the way the world is led

www.russellreynolds.com



Global offices

Americas

- Atlanta
- Boston
- Buenos Aires
- Calgary
- Chicago
- Dallas
- Houston
- Los Angeles
- Mexico City
- Miami
- Minneapolis/St.Paul
- Montreal
- New York
- Palo Alto
- San Francisco
- São Paulo
- Stamford
- Toronto
- Washington, D.C.

EMEA

- Amsterdam
- Barcelona
- Berlin
- Brussels
- Copenhagen
- Dubai
- Frankfurt
- Hamburg
- Helsinki
- London
- Madrid
- Milan
- Munich
- Oslo
- Paris
- Stockholm
- Warsaw
- Zürich

Asia/Pacific

- Beijing
- Hong Kong
- Melbourne
- Mumbai
- New Delhi
- Shanghai
- Shenzhen
- Singapore
- Sydney
- Tokyo