



Empowering our clients with data and insights  
to make diverse, inclusive and impactful hires

# 2025 Beyond the Breach: What Today's CISOs See on the Horizon

# Introduction

The conversation silences. The room is quiet just before the board meeting begins. A stack of reports sits ready, risk dashboards glow on the screens, a question about AI looms, and at the head of the table is a Chief Information Security Officer (CISO) whose career began in a totally different world of security. It's a familiar scene. Despite being across different industries, the people in these seats often share strikingly similar backgrounds: highly technical and as resilient as they come.

As security becomes core to business resilience and in turn, resilience becomes a key driver of profitability, the transformation of the CISO role is still underway. It's no longer a question of whether the CISO has a seat at the boardroom table, but how regularly they're there and how deeply the board understands the technology risks that shape strategic decisions.

Marlin Hawk has been mapping this evolution for the past five years, tracing the meteoric rise of the CISO from technical expert to board-level executive. Today, the challenge isn't just keeping pace with threats but preparing for the future of cybersecurity leadership. To understand what the next-generation CISO looks like

(and how to get there) we spoke with leading CISOs across multiple industries and locations. These are individuals not only navigating the unfamiliar AI-fuelled threat landscapes and tightening regulatory frameworks but also questioning how future-proofed security leadership pipelines should be built.

**What we heard was clear:** The next generation of CISOs must be as comfortable being at the apex of innovation, side-by-side with the Chief Data Officer who is becoming data defence, and the Chief AI Officer as they look at AI company wide. Getting there, however, means addressing the current roadblocks: limited diversity, skills shortages, and a tendency to hire externally rather than invest in internal potential. On top of all these bottlenecks, the cyber budget to protect the enterprises continues to grow.

The solution lies in long-term thinking - building succession plans, investing in skills-based hiring, and creating internal programs that genuinely develop future-ready talent. The organisations that succeed will be those that stop retrofitting the CISO role and start designing it for what's next.





# Cybersecurity Steps Into the Boardroom – and Stays There

Once regarded as a solely technical and risk concern, cybersecurity has established itself as a strategic imperative in the boardrooms of leading organisations. Increasingly, CISOs are briefing boards on the threat landscape, aligning security with enterprise strategy, and influencing how companies engage with clients, manage reputational risk, and build long-term resilience. Karl Schimmeck, Chief Information Security Officer at Synchrony noted that there has been a clear shift with cybersecurity now being viewed as a core strategic pillar, shaping how customer bases are engaged with across multiple industries. This evolution marks a profound change. Cyber is no longer a backroom function – it's a topic tied directly to client trust, operational resilience, and long-term growth.

Looking ahead, this role is set to become more prominent as a competitive advantage in a digital-first world. The organisations that succeed will be those that embed security leadership into their governance frameworks and treat risk as a daily leadership concern, not just a quarterly check-in.

## The Case for CISO Visibility at the Top

The strongest signals of progress come from organisations that treat cyber risk as essential. At a global energy company, cybersecurity is listed among the company's top strategic risks, and the CISO has a mandatory, top of agenda portion of the board presentation twice a year, and even more frequently to the audit and risk committee. This level of visibility reflects a governance model that sees cybersecurity as central to enterprise resilience.

The leading voices from within the industry underscore the growing case and need for CISO representation at the board level. Audit and risk committees now rely on CISO expertise several times a year, often supported by premeeting briefings tailored to elevate discussion and sharpen decision-making. Some companies have even experimented with dedicated cybersecurity subcommittees, allowing more time for in-depth sessions, rather than 15-minute briefings at quarterly board updates. Experts commented that both approaches can be effective when supported by early preparation and clear communication.

Many CISOs that connect at clients and vendors still lack board access entirely, leaving companies dangerously exposed to digital threats.

Echoed across our interviews is the notion that it should be mandatory for CISOs to meet quarterly with CEOs and boards, with regular engagement across the C-suite to ensure alignment.

“Before every audit committee meeting, I have a one-on-one meeting with the audit committee chair where I do a dry run of the material that's going to be presented. It is the most valuable hour because they know the questions that are going to be asked.”

- Brian Tschinkel, VP, Chief Information Security Officer, HSS

## Bridging the Knowledge Gap

The path to more exposure is far from straightforward. A persistent obstacle is the limited technical literacy within many boards and executive committees, where fundamental concepts like cloud infrastructure or Kubernetes often require translation into accessible business language. Few directors have hands-on cybersecurity, or even general technology experience, and many don't know what questions to ask.

**As one CISO put it:** “Most boards lack cyber expertise; without it, organisations are blindsided to one of their biggest risks. If you haven't got expertise on the board, then they need to learn.”

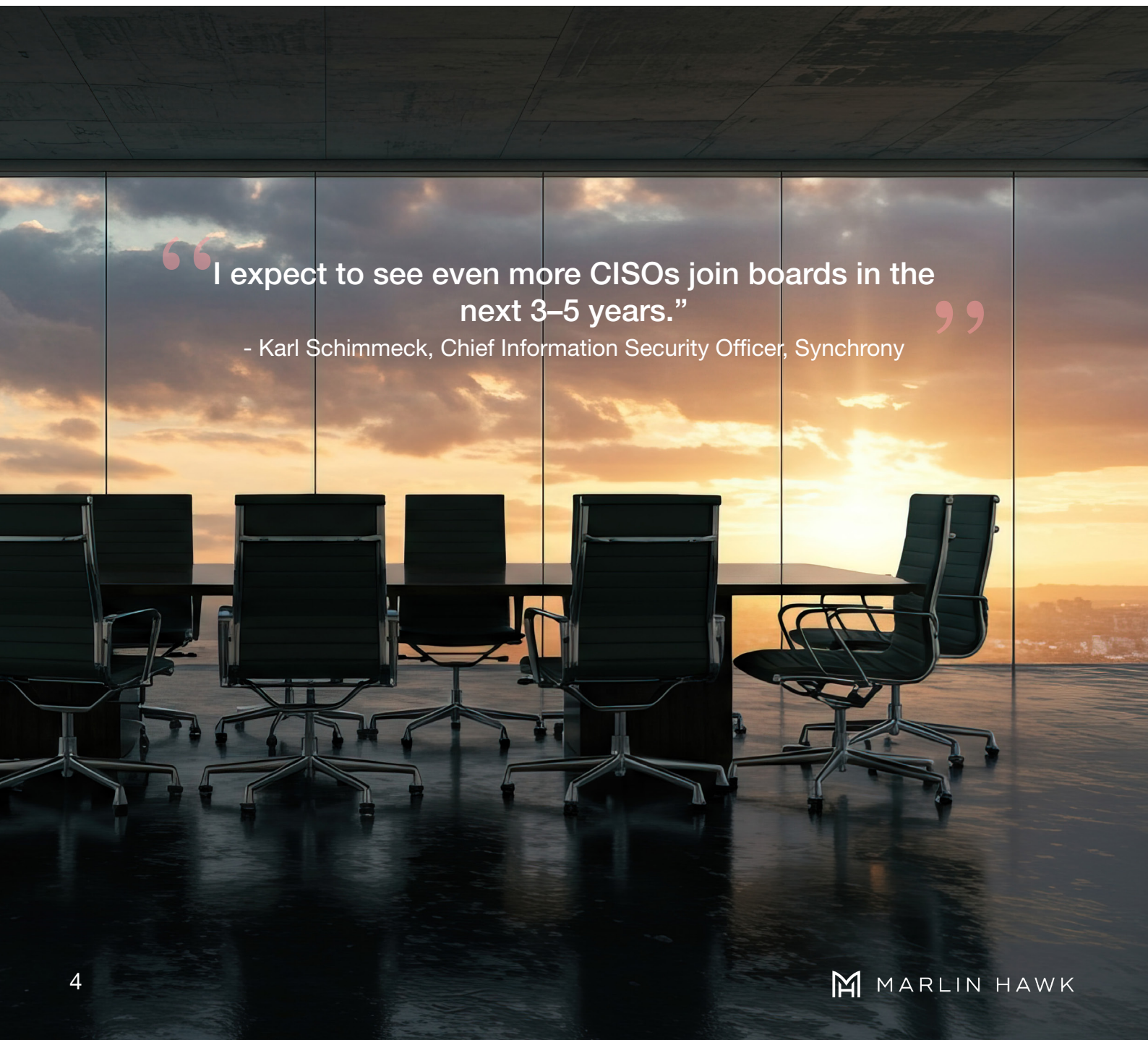
This lack of cyber literacy represents a blind spot. In some cases, boards may include a token ex-CIO, but experts warn that's often insufficient. Many CISOs also pointed out that, while demand for their expertise is growing, formal board seats dedicated to cybersecurity professionals remain scarce, with advisory roles often being the point of entry.

### An Assortment of Roles and Preferences

Even among seasoned security leaders, there is a diversity of appetite for boardroom involvement. Some relish the opportunity to shape high-level strategy, while others prefer to remain one step removed, focusing on operational transformation and the hands-on work. For CISOs eyeing board roles, the appeal is clear – but so are the risks. Today's regulatory environment places a heavy burden of personal accountability, making some hesitant to step in. Many, however, are finding a middle ground by serving on nonprofit or industry boards, gaining influence and experience without the same level of highly critical exposure.

### Looking Ahead to the Room Where it Happens

Nonetheless, the trajectory is clear: over the next three to five years, more CISOs are expected to take up board positions as organisations seek to embed cyber expertise into their governance structures. In parallel, there is a louder call to improve technical literacy across boards, ensuring that tomorrow's board members are better prepared to navigate the relationship between technology, risk, and strategy. For now, CISOs who can bridge the gap of translating technical realities into actionable business insights are emerging as some of the most valuable voices in the modern boardroom as governance must catch up to risk.



“I expect to see even more CISOs join boards in the next 3–5 years.”

- Karl Schimmeck, Chief Information Security Officer, Synchrony



# AI in Cybersecurity: The Tool, the Threat and the Test of Leadership

Artificial intelligence is rapidly reshaping the cybersecurity landscape, emerging as both an accelerator of defence and an amplifier of threat. In every conversation we had with today's CISOs, one truth rang clear: if your defences aren't AI-powered, they will not keep up with AI-driven attackers.

CISOs now face an adversary armed with deepfakes and polymorphic malware. Yet attackers are evolving just as quickly, using generative AI to craft convincing phishing emails and deploy large language models to evade detection.

**"The speed at which attackers are evolving is outpacing traditional defences,"** Allan Cockriel, current Group Chief Information and Data Officer at ASML and previous CISO for Shell, warned. **"Without automation on our side, it will be increasingly difficult to keep up."**

To stay ahead, organisations are investing in AI specific threat modelling and refining defences to identify AI generated content, while building governance frameworks that prioritise transparency and compliance. However, adopting AI is proving more complex than previous technology shifts. Companies face a fast changing vendor landscape, high costs and the need for agility. Security teams feel mounting pressure as evaluation cycles shorten, but the upside is clear. AI is already improving network defence and vulnerability management, even as the market searches for skills and leaders in AI security solutions. The future of cyber defence, CISOs agree, will rely on real-time augmentation – systems that can detect in seconds, respond in minutes, and continuously learn.

## Strategic Integration and Cultural Change

The early corporate reflex to ban generative AI (blocking tools like ChatGPT) proved unsustainable. Now, many organisations are embracing AI to boost productivity under strict oversight, with controls to prevent data leakage and policies informed by user feedback. Enterprise grade Co-pilots, such as Microsoft Copilot, are underway, while security assessments now include AI specific criteria like model training and data handling.

As Tony Jowett, Group Chief Information Security Officer at ITV put it: **"Generative AI is both an incredible opportunity and a serious risk. In production, it's opening doors to creativity and efficiency, but we also must protect our IP – we don't want our programming sucked into a platform that lets anyone spin up their own Coronation Street. We treat AI tools like any other SaaS application, with the same checks and balances, and we've even seen it being used in conjunction with traditional programme making to enhance rather than replace what people do. It's an exciting time, and while we don't want to make mistakes, we know we must embrace it to stay competitive."**

AI is also embedded in creative workflows and compliance, with generative tools replacing time-intensive reviews and enabling cost-effective content creation. Risks such as intellectual property leakage, however, continue, demanding a balance between innovation and protection. Vendors like Adobe Firefly and Runway are helping teams experiment, even as governance remains central.

## The New Risk Perimeter

AI today is a test of enterprise governance. CISOs report the growing overlap between cybersecurity, data protection and ethics functions, as AI risk has become a multidimensional issue. Tools like Microsoft Purview are becoming key to oversight, however a lot of the AI risk is still unknown, particularly as SaaS vendors frantically embed AI functionality into their products with minimal security. At industry conferences and in vendor collaborations, AI consistently dominates discussions, reflecting both hesitant excitement and unanswered questions about its future.

The weaponisation of AI has made cyber attackers more creative and more dangerous. Attackers are now using malware that continuously rewrites itself to dodge traditional defences. Deepfakes have already enabled multi-million-pound fraud. Phishing campaigns can now be launched by those with minimal technical skill. The barrier to launching sophisticated attacks is lower than ever.

“With all the recent cyber attacks in the UK, its been unsettling as a consumer. As we were focused on AI, there were always geopolitical risks, but everything is now converging. The entire threat landscape is becoming increasingly complex.”

### The Focus on Cyber Resilience, not just Cybersecurity

Threat actors are leveraging AI to automate and amplify attacks, while regulations and systems struggle to keep pace as attacks become more sophisticated. Governments are scrambling to catch up. The EU AI Act is setting the tone globally, while other states lag. CISOs are now being expected to build AI risk into existing control frameworks, not create more, parallel processes. What that looks like is prioritising augmentation over autonomy, and explainability over experimentation.

**There is growing demand for regulators to focus on resilience and supply chain standards, not just risk identification.**

Some regions are moving faster. For example, the United Arab Emirates (UAE) has built collaborative AI governance through its National Cybersecurity Council. Meanwhile, most enterprises continue to integrate AI into operations, from alert automation to anomaly detection. For now, AI remains both a game changer and a new risk frontier, despite the complex regulatory landscape.



# A Shifting Landscape of Security and Regulation

## Untangling a Web of Global Rules

Across industries, regulatory compliance has become more than a box-ticking exercise. Organisations now face fragmented requirements, spanning from cyber risk disclosure and third-party oversight to operational resilience and now AI ethics. The challenge is not the rules themselves, but the velocity and volume of change: more than 20 GDPR-scale regulations are in play, across 70+ jurisdictions, each with varying thresholds and obligations.

To keep up, leading firms are embedding compliance into the foundations of product development and SaaS procurement, leaning on enterprise risk. Yet many CISOs argue that without coordination and better enforcement, organisations are left in an unsustainable cycle of reactive compliance.

As Isabelle Theisen, Chief Information Security Officer at Nomura, summed up: **“Cybersecurity is regulation-heavy, and AI just adds another layer.”**

There is growing advocacy for global alignment of cyber standards, especially as AI has begun to disrupt how companies manage data, automate processes, and interact with third-party vendors. Leaders observed that clearer, enforceable regulation could not only ease complexity, but create the confidence needed to innovate without risk.

## A Call for Clarity and Resilience

Security executives have become increasingly vocal about the need for regulators to shift to resilience-building as opposed to risk identification. As AI becomes deeply embedded within supply chains – often through third-party vendors and SaaS platforms – traditional governance models are falling behind. Many believe that rules can encourage innovation rather than hinder it if designed with technical realism and consistent standards across regions. Current regulation focuses too narrowly on post-incident response or compliance, rather than future-looking safeguards that reflect today’s digital ecosystems.

CISOs are pushing for a mandate on secure-by-design principles, real vendor accountability, and cross-sector

“ There’s lots of new fintechs and emerging companies stepping into the market who may or may not be putting us all at risk. What’s needed is stiffer enforcement around the regulations that exist because we’re an ecosystem.”

- Phillip Westgarth, Chief Information Security Officer, Network International

oversight. The proposed EU Cyber Resilience Act is one example of the charge, extending regulatory expectations to service providers. True cyber resilience, especially in the age of AI, requires more than just frameworks. There is also a growing opinion for the CISO to report directly to a Chief Executive or Chief Operating Officer to avoid conflicting priorities and elevate security within corporate decision making.

## Broken Governance Models and Sector Disparities

Outside the financial services sector, which benefits from a more globally established framework, many industries continue to operate with weak or inconsistent cyber regulation. Standards like National Institute of Standards and Technology (NIST) exist, but in many cases, regulators lack enforcement power or intervene only once a breach has occurred. This results in a system where cybersecurity is neglected until a crisis forces attention.

Even internal governance structures mirror these external gaps. In many non-banking sectors, the “three lines of defence” model is poorly implemented. Enterprise risk teams often lack the influence needed to drive meaningful change, second-line functions act as first-line responders, and Chief Risk officers often report too far down the hierarchy to drive strategy. As Network International’s Group CISO Westgarth described: **“It’s a structure designed to satisfy auditors, not challenge the business.”**



## REGULATION

Meaningful change will require CISOs and cyber CROs to be where decisions are made, not buried in reporting lines that dilute their influence. Risk teams must be empowered to challenge, not just consult, and cybersecurity needs to be embedded into board-level governance. Without this recalibration, even the most well-intentioned regulations risk becoming shelfware.

### Industry Differences and the Supply Chain Challenge

Regulatory scrutiny remains uneven across sectors. While finance, healthcare, defence and some elements of energy face detailed oversight with sector-specific bodies and formal comment periods, industries like media, entertainment, and tech often operate with minimal constraints. This unevenness poses a significant threat in a world where digital supply chains connect nearly every sector to every other.

In addition, forms of customer verification that have become mainstays in regulated industries, such as

facial recognition and voice ID, become more and more vulnerable to AI-led attacks. Even the most regulated sectors are at risk.

As more AI capabilities are quietly embedded into third-party products, organisations are left increasingly dependent on vendor promises they cannot independently verify. Security leaders are asking regulators to step in—not just with more rules, but with smarter auditing methods, mandatory self-certification models, and stronger supply chain governance.

Regardless of the sector, the spotlight on supply chains is intensifying. The proposed Cyber Resilience Bill aims to extend standards to service providers. As another CISO flagged, it is driven by the belief that a chain is **“only as strong as its weakest link”**. Security leaders are asking for stronger enforcement of existing frameworks, smarter auditing methods, and self-certification models. Resilience demands ecosystem wide caution, especially as new players enter the market at speed. Regulation must move with innovation, not follow behind it.





# Breaking the Cyber Ceiling: The Push for Diversity in CISO Leadership

Despite years of conversation and small gains, cybersecurity leadership remains overwhelmingly like previous years. The CISO role is still male-dominated, and progress on gender and ethnic diversity is slow. A major blocker is the experience bottleneck. Many underrepresented candidates struggle to progress due to hiring criteria that over-prioritise technical tenure and board exposure.

The funnel narrows early. Limited exposure in schools, a lack of role models, and skewed university pathways all feed into a pipeline that still favours traditional profiles. Even when diversity policies exist, they're often undercut by bias and low application volume. The consensus is organisations keep looking externally to find talent they should have been growing themselves.

Phillip Westgarth, Group CISO at Network International, reflected on this missed opportunity: **“And that is a sadness in our industry – that we haven’t yet got to the point where we start to trust people who are within our organisation and grow them as future leaders.”**

## Building Talent from Within and the Missing Succession Plan

Mentorship has emerged as a powerful lever to support the development of diverse cybersecurity leaders. One CISO noted that experienced CISOs are stepping up to guide future leaders. Mentoring females that they themselves have crossed paths with, they offer insights into the day-to-day realities of the job, from navigating “bad news” board conversations to managing risk with limited resources. Mentorship doesn’t only build technical and strategic capabilities. It strengthens emotional resilience, especially for women who may face scepticism or pressure in high-stake leadership roles.

As they outlined, persistent misconceptions about leadership styles continue to influence diversity in cybersecurity leadership. Some still question whether women possess the assertive qualities to handle the

high-conflict, high-pressure demands of the CISO role. However, the reality is that female leaders often bring an empathetic, nuanced approach to leadership, balancing authority with collaboration and emotional intelligence. These qualities are increasingly necessary in managing complex, cross-functional teams and navigating organisational risk.

“There’s still a perception that women lead with a softer style and might not be cut out for tough conversations. But I see it differently. My approach isn’t less effective, it’s just different. In fact, leading with empathy can make security messages land better, not weaker.”

Role models and representation play a vital role in transforming these perceptions. Many aspiring female leaders look for someone who looks like them in a position of power before envisioning themselves there. Highlighting diverse success stories is essential to normalise a broader range of leadership styles in cybersecurity. Practical mentorship, paired with a higher effort of encouragement, is essential, as many women don’t pursue advancement unless explicitly told they have potential or the right attributes.

Yet, a critical blind spot remains – internal succession planning. Diversity must also go beyond gender. Several CISOs noted the value of professionals from non-traditional backgrounds (psychologists, lawyers, even artists) who thrive in security roles when supported. Without structured succession planning, however, these individuals rarely rise to leadership. Most CISOs are still hired externally. A shift toward intentional internal pipelines is urgently needed.



### Intentional Inclusion: Rethinking Hiring to Build a Smarter Function

Some companies are using deliberate hiring mandates – not quotas, but tactics to widen the talent lens and counter systemic bias. At one large oil and gas company, 42% of leadership is female, driven by a policy requiring 50% diverse candidate slates. Despite hesitation at first, this ultimately improved hiring outcomes and team performance.

Another multinational information technology company applies the same 50% mandate for women in all leadership pools. It is about merit, but better decisions come from broader pools. One CISO shared a key insight: **“There’s growing evidence that female leaders often bring strengths we overlook: integrity, long-term thinking, and collaboration.”**

Several leaders referenced Tomas Chamorro-Premuzic’s TED Talk, *“Why So Many Incompetent Men Become Leaders”*, as a reminder to challenge how leadership potential is defined. Overconfidence still gets overvalued – a quality that may be a liability in future-focused security teams.

### Embedding Inclusion into the Security DNA

Organisations making real progress are embedding inclusion into every layer, from early education to executive hiring. Schimmeck (Chief Information Security Officer at Synchrony) and Tschinkel (VP, Chief Information Security Officer at HSS) both highlighted inclusive early-career programs focused on potential, not just credentials. Crucially, their efforts are backed by data to ensure progress is measurable and meaningful.

Culture change however, still takes time. Diversity must be designed into how teams are hired, led, and sustained, from STEM education in schools to junior hires and training. That includes better succession planning, stronger feedback loops, and training paths that recognise talent beyond the usual profiles. With cybersecurity threats growing in at an alarming rate of sophistication and scope, leveraging the full spectrum of human talent is not just the right thing to do, but the smart thing to do.



# The Next Generation CISO Leads Beyond Protection

## Beyond “Shiny New”

As organisations race toward digital transformation and new technology, a cautionary note is emerging from security leaders: resist the allure of short term adoption of **“shiny new”** technologies without sustainable planning. Investments must be made with an eye on legacy systems, operational realities, and the future-readiness of the enterprise.

This approach requires discipline to ensure new capabilities integrate seamlessly with existing ecosystems, while positioning the organisation to pivot and scale securely in the years ahead.

## Human Centred Leadership for an AI-Driven Future

Technology alone will not define the next generation of CISOs. Future leaders will need emotional resilience, humility, and intellectual curiosity to thrive in a high stakes, rapidly changing environment. Humility is crucial for effective leadership. It opens the door to honest feedback.

Success in these roles often hinges on creating win-win scenarios, handling adversity, and learning from challenges. CISOs who excel in change management and stakeholder engagement are already finding their way into broader, advisory or non-executive director positions.

## The Shift to Data Centric Cyber Leadership

The CISO's role is moving well beyond checklists and audits. Protecting data – wherever it travels – has become the organising principle, with security leaders forging deeper partnerships with data analytics teams.

The next wave of leaders will master AI-driven tools to follow and safeguard data in motion, harnessing analytics not just for security insights but for shaping business decisions. As Operational Technology (OT) and Information Technology (IT) converge, protecting 40-year-old industrial assets now shares the same urgency as defending cloud workloads – requiring integrated processes, unified reporting, and cross-domain expertise.

“Shiny new tools look great now, but the challenge is we might not be able to support that in five years' time. Decisions control that speed, making sure investments are made with a five-year view.”

- Phillip Westgarth, Group Chief Information Security Officer, Network International

“One of the people I'm working most closely with is our Chief Data & Analytics Officer. I think we will expand our partnership working with data teams, especially as AI gets introduced. It's becoming more of a natural progression that way.”

- Brian Tschinkel, VP, Chief Information Security Officer, HSS

### Varied Expectations and Career Pathways

Organisations continue to vary in how they define the role. Some see the CISO as a governance focused advisor, while others demand operational oversight and hands on leadership. In this context, frequent job hopping (common in the industry) can undermine the long term impact and growth that comes from embedding deeply in an organisation's culture and strategy.

At the same time, the scope is widening. CISOs are finding themselves responsible for securing global OT, deploying dedicated OT Security Operations Centres, and ensuring parity between operational and IT security. The work is as much about enabling operational forecasting and planning as it is about defence. For manufacturers, defence and medical device companies, they are also being pulled into product safety – ensuring things are designed un-hackable from birth, rather than assessed after they have been created.

---

“**The days of the engineering-focused CISO are becoming numbered.**”  
- Tony Jowett, Group Chief Information Security Officer, ITV

---

### The CISO's Place in the Room That Matters

As Karl Schimmeck, Chief Information Security Officer, Synchrony said: **“The future CISO is a translator, a strategist, and most importantly a manager of risk.”** They will balance operational, technological, and third party risks while translating security concepts into business results.

At some companies, this evolution is already underway. Cybersecurity is being embedded into digital transformation initiatives, with business units taking ownership of risk in partnership with security teams. In five to ten years, success will be measured not by whether a project is considered too risky, but by how confidently and securely the enterprise can deliver on its goals.

---

“**We'll know we've arrived when the question isn't 'what's the risk?' but 'how can we do this securely and create real value for the enterprise?'**”  
- Karl Schimmeck, Chief Information Security Officer, Synchrony

---



# Acknowledgements

We would like to thank all of those who contributed to the content of this article, some of whom have graciously consented to be listed below:

- **Brian Tschinkel**, Vice President, Chief Information Security Officer, Hospital for Special Surgery
- **Karl Schimmeck**, Chief Information Security Officer, Synchrony
- **Isabelle Theisen**, Chief Information Security Officer, Nomura
- **Tony Jowett**, Group Chief Information Security Officer, ITV
- **Allan Cockriel**, Group Chief Information and Data Officer, ASML
- **Phillip Westgarth**, Group Chief Information Security Officer, Network International







MARLIN HAWK

**Empowering our clients with data and insights to make diverse,  
inclusive and impactful hires**

[marlinhawk.com](https://marlinhawk.com)