# Cybersecurity awakening

## A call to businesses

PwC Ghana is scheduled to host a thought leadership forum on the theme "Leadership strategies for cyber resilience and growth" on Wednesday, 30 October 2024.

The event will bring together cyber experts and business leaders as well as other stakeholders, such as regulatory institutions, with significant interests in particularly vulnerable industries, such as financial services, telecommunication, and energy to discuss the cybersecurity risks plaguing these industries and explore strategies for enhancing organisational resilience. PwC's cyber forum would also present the key findings from its 2025 Global Digital Trust Insights Report.

The article below outlines a few of the insights carried in the report, and actions to be taken by business leaders to build cyber resilience.

### Insights from PwC's 2025 Global Digital Trust Report

As businesses enter a future defined by digital transformation and increasing cyber threats, PwC's 2025 Global Digital Trust Insights report reveal alarming gaps in cyber resilience and preparedness. The report, based on a survey of over 4,000 business and technology executives across 77 countries, paints a sobering picture: while executives acknowledge the growing cyber risks, very few organisations have taken the necessary steps to safeguard their operations

One of the most striking findings is that only 2% of organisations have fully implemented cyber resilience measures across their entire business. What does this mean for business? Definitively, this means that despite widespread awareness, most companies remain vulnerable to cyber threats which could severely disrupt operations and compromise data. The report's message is clear: cybersecurity needs to be treated as an integral part of business strategy, not as a reactive afterthought.

### The expanding cyber threat landscape

The report highlights a rapidly expanding attack surface, driven by modern technologies such as Generative AI (GenAI) and the proliferation of connected devices. Notably, 67% of security executives reported that GenAI has increased their organisation's vulnerabilities over the past year. GenAI is not just a tool for innovation - it is also being exploited by cybercriminals, enabling them to launch sophisticated phishing attacks and deepfakes at a rapid pace and an unprecedented scale.

This development underscores the need for businesses to stay ahead of the curve by investing in advanced defence mechanisms and AI governance.

Yet, even as these risks grow, companies remain ill-prepared. Executives ranked cloud-related threats, third-party breaches, and attacks on connected products among their top concerns, but these are also the areas where they feel least capable of mounting a defence. The gap between recognising cyber risks and being ready to address them suggests that businesses are still not investing strategically in the right areas.

### Leadership gaps and misalignment

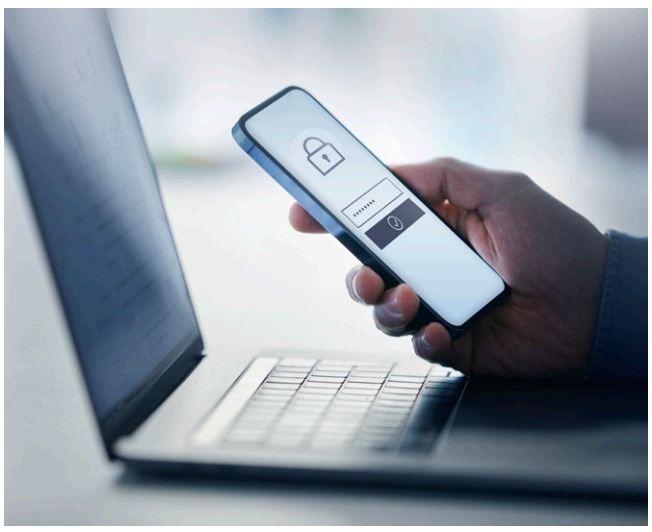
Leadership's vital role in in cybersecurity is another critical area of concern. 46% of Chief Information Security Officers (CISOs) indicated their involvement in major business decisions "to a large extent", such as strategic planning and board reporting. Their absence at such levels of decision making and organisational steering creates a disconnect between those responsible for safeguarding the organisation and those setting its strategic direction.

The report emphasises the need for C-suite alignment and urges leaders to better integrate cybersecurity into their overall business strategy. As David Bruyea, CISO at Moneris[1], states, "It's the CISO's job to contextualise and connect the threats that exist to the vulnerabilities within the organisation." In other words, unless security leaders have a seat at the decision-making table, businesses will continue to face blind spots in their resilience strategies.

### Regulatory pressure and missed opportunities

Regulatory compliance is another driving force behind cybersecurity investment, and 96% of executives acknowledge that new regulations have spurred them on to enhance their security measures. Yet, there remains a significant confidence gap between CEOs and CISOs regarding their organisations' ability to meet these regulatory demands, particularly when it comes to AI and resilience regulations. This gap highlights a deeper issue: the need for better communication and collaboration between business leaders and security experts.

One area where organisations are falling short of is in cyber risk quantification, i.e. the process of measuring the financial impact of cyber risks. Despite its importance, only 15% of businesses are doing this effectively. This is a missed opportunity to better prioritise resources and align investments with the most pressing risks. As the report points out, "The gap between recognition and implementation is a missed opportunity that can no longer be ignored."



### Calls to action

Throughout the report, PwC issues a series of calls to action to business leaders, urging immediate action to close the gaps in cyber resilience. The most urgent calls include:

Aligning business and cyber priorities:
Business and tech executives often prioritise different risks, creating a misalignment that leaves organisations exposed. The report stresses the importance of regular cross-functional assessments to keep strategies in sync and ensure cyber risks are adequately addressed.

Empowering CISOs:
Organisations must involve CISOs in strategic planning to ensure cybersecurity measures are proactive rather than reactive. Giving security leaders a seat at the table can bridge the gap between recognising threats and being ready to tackle them.

Investing in resilience:
Despite increasing cyber budgets, many organisations are still behind in implementing enterprise-wide resilience measures. Only 2% have fully integrated these actions, leaving most companies dangerously exposed to cyber threats. Businesses must take a holistic approach, integrate people, processes, and technology to build resilience.

Cybersecurity as a competitive advantage:
In a world where 57% of executives believe cybersecurity influences customer trust, failure to close the gaps in cyber resilience and leadership alignment could lead to devastating operational, financial and reputational consequences. PwC's 2025 Global Digital Trust Insights report is a stark reminder that cybersecurity is no longer just a technical requirement but a cornerstone of operational survival and competitive advantage.

The report also offers a clear path forward. Companies that prioritise cybersecurity, integrate CISOs into the overall strategic conversation and proactively invest in resilience are positioning themselves to not just survive but thrive. Cybersecurity is a critical differentiator; those who treat it as a foundation of trust and innovation stand to gain a clear edge in a competitive, trust-driven market.

The time for half measures has passed, as Dr. Georg Stamatelopoulos, CEO of EnBW AG2[2], succinctly puts it, "We need to be prepared at every level with our business continuity and resilience programs." The threats will only intensify, and organisations that fail to build resilience today are risking their tomorrow.

Now is the time for the Boards, CEOs, CISOs, CROs, CIOs, CTO and all leaders to step up and align on priorities and make cybersecurity a strategic imperative.

Source: PwC's 2025 Global Digital Trust Insights Report.

[1] Moneris is a Canadian financial technology company that specialises in payment processing. https://www.moneris.com/
[2] EnBW is an energy producer and energy supplier in Baden-Württemberg and beyond. https://www.enbw.com/company/


**Talk to us: gh_hello_cyber@pwc.com**

Winfred King
Partner
+233 (30) 2761500
winfred.king@pwc.com

Clement Yayra Tettey
Senior Manager
+233 (30) 2761500
clement.tettey@pwc.com