Press Release

Date	13 February 2026
Contacts	Nguyen Phuong Khanh, PwC Vietnam, Marketing & Communications
	Email: nguyen.phuong.khanh@pwc.com
	Tel: (+84) 28 3823 0796; Mobile: (+84) 933 270 366
Pages	5 pages

AI Tops Cybersecurity Investment Priorities Globally and in Vietnam Amid Rising Threats and Regulatory Shifts

Vietnam, 13 February 2026 – AI tops the agenda for cybersecurity and business leaders when it comes to cyber budget allocations, addressing cyber talent shortages, and bolstering cyber defence capabilities over the next 12 months, according to PwC's 2026 Global Digital Trust Insights survey.

The survey, which includes perspectives from 3,887 executives across 72 countries, reveals that only 6% of organisations feel very capable of defending against cyber threats across all vectors.

Vietnam's cybersecurity landscape is evolving in parallel with these global trends. In October 2025, Vietnam hosted the signing of the United Nations Convention against Cybercrime, commonly referred to as the Hanoi Convention. Vietnam played a leading role in shaping the treaty, advocating for capacity-building for developing nations and ensuring respect for national sovereignty. This international development complements Vietnam's domestic regulatory momentum. The 2025 Cybersecurity Law, set to take effect in July 2026, introduces stricter obligations for service providers, including mandatory user identity verification, 24-hour breach reporting, and enhanced data protection compliance. Alongside this, the Personal Data Protection Law, effective from January 2026, aligns with global standards like the EU's GDPR. Together, these changes signal a decisive shift toward international best practices and increased regulatory maturity, at a time when businesses are under growing pressure to demonstrate digital trust to customers, partners, and regulators.

PwC (Vietnam) Limited
No. 29, Le Duan Street, Saigon Ward, Ho Chi Minh City, Vietnam

“Vietnam is entering a transformative era in cybersecurity governance. New and emerging technologies and a digitally interconnected ecosystem have brought us to a tipping point that demands executive alignment. The most successful organisations give CISOs a seat at the table and weave cyber into every business decision. The leaders of tomorrow will invest in cyber not just to respond, but to anticipate because resilience not only comes from hindsight but also strategic foresight. For Vietnamese businesses, this is the moment to align with international standards, strengthen compliance frameworks, and prioritise AI and cyber skills, upskilling and reskilling their teams to proactively map and manage the risks they face.” said **Pho Duc Giang, Partner, Digital Trust and Cybersecurity Services, PwC Vietnam**.

AI emerges as top-of-mind for cyber security leaders and budgets

Consistent with last year, nearly eight-in-ten (78%) organisations say their cyber budget will increase over the coming year, highlighting the continuing importance organisations are placing in bolstering their cyber security capabilities as the risk landscape continues to evolve. Nearly one-third (32%) of these said their budgets would likely increase 6-10%.

Looking within cyber budget priorities, investment in AI (36%) was the top priority over the next 12 months, ahead of cloud security (34%), network security (28%) and data protection (26%), as AI’s rapid advance continues to transform the digital landscape.

When looking at the AI security capabilities organisations are prioritising over the next 12 months, nearly half (48%) of security leaders are prioritising AI threat hunting capabilities, with more than one-third prioritising other capabilities such as agentic AI (35%).

PwC Vietnam’s Expert View: " Vietnamese firms are increasingly shifting from a reactive to a predictive cybersecurity mindset. Recent advances in AI enable businesses to detect and respond to threats faster and more effectively. Most organisations remain in the “co-pilot” phase, focusing more on use cases that deliver clear business values. However, building trust in autonomous AI systems requires even stronger attention to AI governance practices." said **Tran Minh Quan, AI & Cyber Risk Senior Manager, PwC Vietnam**.

More organisations are now quantifying cyber risk

As organisations contend with a rising array of cyber risks – they are also increasingly putting a number behind it. Half now report using cyber risk quantification to measure financial impact to a significant or large extent, up from 44% last year.

This comes as more than a quarter (27%) of businesses say their most damaging data breach in the past three years cost their organisation at least US $1 million, consistent with last year's responses. The most exposed include enterprises with US $5 billion or more in revenue (41%), US-based companies (37%), and TMT sector companies (33%).

In Vietnam, this practice is still emerging but gaining traction, especially in the banking and fintech sectors. The 2025 CIC data breach, which exposed 160 million records, has accelerated interest in cyber risk modelling.

PwC Vietnam's Expert View: "In Vietnam, there's a growing demand from regulators and businesses for clear metrics on cyber risk. This shift is essential for aligning cybersecurity with business goals and investment decisions, moving from a technical countermeasures focus to adopting a measurable, risk-based management approach." said **Ton That Tuong, Cyber & Data Privacy Senior Manager, PwC Vietnam**.

Skills gaps weigh on bolstering AI and cyber defence capabilities

Cyber security workforce shortages continue to impede progress as organisations operationalise AI, secure complex environments and prepare for the next generation of threats.

Half (50%) of global respondents said a lack of knowledge in the application of AI for cyber defence, or lack of relevant skills (41%), were the biggest internal challenges to implementing AI for cyber defence over the last 12 months. Vietnam also faces a severe cyber talent gap, with an estimated shortfall of 700,000 professionals in the coming years[i].

Globally, while talent shortages persist, businesses are responding by prioritising areas such as AI and machine learning tools (53%), security automation tools (48%), cyber tool consolidation (47%) and upskilling or reskilling (47%).

The cyber skills deficit challenge runs deeper beyond preparation for AI. Nearly half (47%) of leaders cite a lack of qualified personnel as a top challenge when securing operational technology (OT) and the industrial internet of things (IIoT) systems.

At the same time, as quantum technologies are advancing and represent one of the top-ranked threats organisations are least prepared to address (after cloud-related threats, 33%; attacks on connected products, 28%; third-party data breach, 27%; quantum computing threats, 26%), almost half (49%)

PwC (Vietnam) Limited
No. 29, Le Duan Street, Saigon Ward, Ho Chi Minh City, Vietnam

haven't considered or started implementing any quantum-resistant security measures due to a lack of understanding about post-quantum risks, limited internal resources and competing.

Read the full survey findings here: https://pwc.to/US-QR-mlhj5z34

Ends.

Note to editors

About PwC's 2026 Global Digital Trust Insights survey

The 2026 Global Digital Trust Insights survey captures the views of 3,887 business and technology executives between May-July 2025. One-third of the executives (33%) are from large companies with US$5 billion or more in revenues. Respondents operate in a range of industries, including financial services (21%); industrial manufacturing and automotive (21%); tech, media and telecom (19%); retail and consumer markets (16%); healthcare (10%); energy, utilities and resources (9%); and government and public services (4%). Respondents are based across 72 countries. The regional breakdown of responses is Western Europe (32%), North America (27%), Asia Pacific (18%), Latin America (11%), Central and Eastern Europe (6%), Africa (4%) and the Middle East (3%). Now in its 28th year, it's the longest-running annual survey on cybersecurity trends. It's also the largest survey in the cybersecurity industry and the only one that draws participation from senior business executives, not just security and technology executives.

About PwC

At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 360,000 people in 136 countries. Across audit and assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

About PwC Vietnam

PwC Vietnam established offices in Hanoi and HCMC in 1994. With strong industry knowledge, our team of more than 1,000 local and expatriate professionals bring a breadth of skills and depth of resources to effectively address and solve issues that matter to our clients, wherever they do business.

[i] https://en.vietnamplus.vn/vietnam-faces-severe-cybersecurity-workforce-shortage-post319739.vnp

PwC (Vietnam) Limited
No. 29, Le Duan Street, Saigon Ward, Ho Chi Minh City, Vietnam