**Title:** Security leaders in urgent need to reformulate cyber strategies
**Author:** PwC Vietnam | **Vietnam Investment Review** dated 24/08/20
**Link title:** https://www.vir.com.vn/security-leaders-in-urgent-need-to-reformulate-cyber-strategies-78732.html

Vietnam Investment Review

# Security leaders in urgent need to reformulate cyber strategies

*Businesses aspire to reap the benefits of the digital age. Going digital is not just a trend; it has become an integral part of the digital economy. In this increasingly digitised world, one could say that data is the new currency. And digital trust – the level of confidence in people, processes, and technology – is the backbone of the digital economy.*

Without a doubt, COVID-19 has accelerated digitalisation – including automation, virtual collaboration, distributed work, cloud adoption, telehealth, direct-to-consumer channels, and more. The pandemic's impact on the nature of the workplace, the market, and business processes has highlighted that digital transformation may be here for good.

As organisations adjust to different futures, the focus on fast-tracking technology development is exposing businesses to new and rapidly evolving security threats. According to PwC's Digital Trust Insights Pulse Survey launched in June, in which 141 security and information leaders in the United States took part, more than half of the chief information security officers (CISOs) surveyed saw cyber-attacks soar since February, and expect threats to remain elevated in the next 6-12 months.

The role of cybersecurity has been heightened and this poses the question of what companies can do differently in order to keep operations running smoothly and securely, as digital connections multiply.


*Based on what you have learned and experienced during the crisis, which of the following changes to your cybersecurity strategy, if any, are you planning to make? (Please rank up to three. Indexed score.), Source: PwC. Digital Trust Insights Pulse Survey. June 2020: base of 141*

In search of insights, PwC researchers in the same survey looked at how organisations in the US weathered this test of resilience during the COVID-19 pandemic, and how businesses are rethinking their strategy and investments going forward. Results from the Digital Trust Insights Pulse Survey that pertain to the Vietnam market revealed some notable insights.

Boards and C-suite executives, who in the past may have wondered about returns on investment in all their cybersecurity personnel, solutions, and architectures, no longer have to wonder. The value of their cybersecurity expenditures over the years – and of CISO leadership – became crystal clear during this crisis.

The investments in the past 2-3 years that paid off the most during the crisis were not one-off security solutions, but investments related to remote work, crisis management, and data-driven risk management.

"Vietnamese enterprises show similar investment trends in identifying and accessing management solutions, real-time threat intelligence capabilities, and cloud adoption to facilitate distributed work locations," said Pho Duc Giang, director of PwC Vietnam Cybersecurity Ltd. "Additionally, to address related risks, some key actions organisations can take are compliance enhancement or establishment of information governance for better data-driven decision-making, as well as better integration of cyber risks with overall enterprise risk management."

More than ever, cybersecurity leadership has become critical not only for risk control but also for value creation. CISOs and chief information officers (CIOs) will play a major role as businesses pursue twin goals in coming months: accelerating digital models and restoring organisations to financial health.

To emerge sustainably, it is important to rethink cyber strategy and investment priorities. There are several key actions for both CISOs and CIOs.

First, they must sustain improved collaboration between cyber, business, and risk leaders beyond the crisis. Also vital is to prioritise the identification and repair of any gaps or vulnerabilities that may have resulted from the crisis. The opportunity must be taken to modernise and simplify.

Third, they should anticipate and manage risks that emerge from accelerated digitalisation, cloud adoption, and shifts to digital business models. Finally, CISOs and CIOs should bring to the table imaginative ways to improve security, resilience, and trust, while helping to contain costs by being good stewards of the cybersecurity budget.

***Reporter: Hoang Anh***