

Press Release

Date 21 October 2020
Contacts Nguyễn Thu Hà
Tel: (+84) 24 3946 2246, Ext: 4692; Mobile: (+84) 979 893 020
Email: ha.nguyen@pwc.com
Pages 03

Cybersecurity coming of age

- 96% of executives have shifted their cybersecurity strategy due to COVID-19
- 40% of executives say they're accelerating digitisation
- 55% of respondents lack confidence that their cyber spending is allocated towards the most significant risks

Cybersecurity stands at a pivotal point for the industry, its organisations and people it serves and is becoming a key enabler of the business. This is highlighted in PwC's latest [Global Digital Trust Insights 2021: Cybersecurity comes of age](#). Gathered from a survey of over 3,000 business and technology executives from around the world, the report provides insights into the changing landscape of cybersecurity and what the future holds.

Amid the backdrop of COVID-19, organisations have seen recent shifts in business models and the acceleration of digital programme adoption. The report deep dives into five moves that Chief Information Security Officers (CISOs) need to make to get to the next level:

Five moves to get to the next level

	Reset your cyber strategy, evolve leadership for these new times Make the shift to business-driven cyber strategy and let your CISO take on the larger role you need
	Rethink your cyber budget to get more out of it Business wants budgets that directly tie to business growth and better risk management
	Invest in every advantage to level the playing field with attackers That new thinking in your cyber strategy? Carry it out in new approaches to boost odds of success
	Build resilience for any scenario What the threat outlook for 2021 means for your resilience strategy
	Future-proof your security team Hiring, training, and managed services to get the deep talent you need in this tight labour market

Source: PwC Vietnam

Sharing views on this report, Nguyen Phi Lan, PwC Vietnam Risk Assurance Leader, commented "Our survey of C-suite levels has indicated that 96% executives surveyed say they will adjust their cybersecurity due to COVID 19, while 50% (up from 25% last year) indicate they are likely to consider cybersecurity in every business decision. Hence, the evolving role of a CISOs and their importance to the organisation has never been more crucial. CEOs and boards are turning to their CISOs for help to increase business resilience and create business value. Many organisations are resetting their cybersecurity strategies."



Urgent need to update cyber strategy

New technologies and business models - and the fast pace of adoption - bring new risks. In the pandemic's first three months, CEOs reported that their organisations were accelerating digitisation at a surprising speed, advancing to year two or three of their five-year plans. Doing things faster and more efficiently is the top digital ambition for 29% of executives, while 31% are modernising with new capabilities.

Rethinking cyber budgets

Getting the most value for every cybersecurity dollar spent becomes more critical as organisations digitise: every new digital process and asset becomes a new vulnerability for cyber-attack. More than half of organisations (55%), state that their cyber budget will be increasing in 2021. While a larger budget for cybersecurity is good news, the industry should expect changes in the way they are being managed, going forward.

In the Vietnam context, Pho Duc Giang, director of PwC Vietnam Cybersecurity Ltd., commented: "Recently we have seen similar, increased investments in cyber security in terms of technical solutions, managed cyber services and human resources in Vietnam. However, from our observations, few companies are operating cyber risk quantification-related processes in practical ways; and local cyber leaders need more sufficient business planning information to raise confidence in budget estimation and decision-making."

Leveling the playing field against cyber attackers

Innovation and technology are changing the way organisations are leveling the playing field against cyber attackers, with 43% of executives saying they have improved customer experiences and are responding more quickly to incidents and disruptions. The top-ranked outcomes desired in the next two to three years are: increased prevention of successful attacks, faster response times to disruptions, improved confidence of leaders in their ability to manage threats, and improved customer experience.

Building resilience

Greater and faster digitisation means an increase in digital attack surface and potential harm to the business. 2020 has been a year full of "firsts": for economic, public health, and cyber organisations. There has been a surge in intrusions, ransomware, data breaches in health and educational institutions, and phishing. As a result, 40% of the executives surveyed said they plan to increase resilience testing to ensure critical business services will function even if a disruptive cyber event occurs.

"For the past few years, many local companies have been on the rise to develop and offer ecosystem services to their clients," said Pho Duc Giang. "One of the fastest ways for such companies to achieve this is to connect their core systems with those of other third parties or by using third parties to deliver value-added services to the clients. However, these practices via third or fourth parties have potential data leakage risks. Thus, it is vital for companies to plan for resilience testing and assessment as needed."

The threat outlook for 2021: Internet of Things (IoT) and cloud service providers top the list of 'very likely' threats (mentioned by 33%), while cyber-attacks on cloud services top the list of threats that will have a 'significantly negative impact' (reported by 24%).



Future-proofing cyber teams

With 3.5 million cyber security jobs to be filled in 2021, the one problem plaguing the cybersecurity industry is a lack of skilled workers. 51% of executives in the survey said they plan to add full-time cybersecurity personnel over the next year, with more than 22% saying they will increase staffing by 5% or more.

An alternative many organisations have used to fill job vacancies is 'hiring from within,' offering upskilling to increase existing workers' skills in the same areas they are hiring for: digital skills, business acumen, and social skills. A few organisations have started to rely on managed services to fill the acute need for deep talent and advanced technologies.

According to Pho Duc Giang, in Vietnam many companies are facing a similar issue. Having cybersecurity specialists with a proper understanding of the relevant business operations remains a challenge. "We believe that upskilling and training existing cybersecurity engineers can be one of the most effective ways for local enterprises to have good CISOs in the future. Those who understand the business operations and are capable of dealing with evolving cyber risks will help their organisation ride through the rapid digital changes." added Giang.

Next-gen security organisations have a three-fold mission: to build trust, build resilience and accelerate innovation. These findings suggest that investing in technologies, processes and capabilities, and people is critical to making meaningful headway against attackers – and they underscore the importance of a CISO who can play a transformational leadership role.

/END

Notes to editors

For full details of the Digital Trust Insights survey, including methodology, please access the report at <https://www.pwc.com/gx/en/issues/cybersecurity/digital-trust-insights.html>

About PwC Vietnam

At PwC Vietnam, our purpose is to build trust in society and solve important problems. We're a member of the PwC network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory, tax, and legal services. This means that you get the benefits of leveraging on our global network to effectively address and resolve your issues - when you need it.

PwC Vietnam established offices in Hanoi and HCMC in 1994. With strong industry knowledge, our team of more than 1,000 local and expatriate staff offers integrated services, bringing a breadth of skills and depth of resources to our clients wherever they do business, throughout Asia and across the world.

Visit our website for further information: www.pwc.com/vn.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We are a network of firms in 155 countries with over 284,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

©2020 PwC (Vietnam) Limited. All rights reserved.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.