Global Digital Trust Insights Survey

Vietnam Report

PwC Research

Februrary 2022

Table of content

2022 Digital Trust Insights

Global Reach

3,602
business, technology, and security executives including 633 from Asia Pacific

33%
Female executives

20+
consecutive years

62%
companies US$1B+

33%
companies US$10B+

Signs of a worsening global threat landscape

Globally 69% of organisations predict a rise in cyber spending in 2022 compared to 55% last year. This is even more pronounced in the Asia Pacific region where 77% of organisations expect an increase in their cyber budget.

Investments continue to pour into cybersecurity because organisations know that risks are increasing. In our 2022 Global Digital Trust Insights Survey, more than 50% of surveyed respondents worldwide and in Asia Pacific expect reportable incidents this year will surge above 2021 levels. This finding is consistent with PwC's 25th Annual Global CEO Survey where cyber threat was cited as number-one risk to business prospect by global CEOs and as number-two by Asia Pacific CEOs - topped only by health risk.

2021 had shaped up to be one of the worst on record for cybersecurity. According to the recent Global Cybersecurity Outlook 2022 Insight Report, global ransomware attack volume increased by 151% within the first half of 2021. Similarly in Vietnam, the Vietnam National Cyber Security Centre (NCSC) recorded 1,383 cyber attacks in the first month of 2022, a steep increase of 10.29% from December 2021.

What is clear is that sophisticated attackers are seizing every opportunity to exploit vulnerabilities against people, organisation as well as critical infrastructure through technology. And this trend is expected to continue in the near future.

The consequences for an attack rise as our systems' interdependencies grow more and more complex. Critical infrastructures are especially vulnerable. And yet, many of the breaches we're seeing are still preventable with sound cyber practices and strong controls.

To better fit the needs of the local market environment, this Vietnam report extracts relevant points from PwC's 2022 Global Digital Trust Insights Survey, published in November 2021. It offers a guide to simplifying cyber with intention to address concerns that organisations have become too complex to secure and worry that too much avoidable, unnecessary complexity poses 'concerning' cyber and privacy risks.

Cybersecurity remains a national priority for Vietnam

Vietnam's digital economy is projected to exceed US$43 billion by 2025 as the country continues to pursue projects in e-government, internet of things, smart cities, financial technology, artificial intelligence etc. With cyberspace blurring regional and national boundaries, Vietnam will likely face an increase in cyber threats, and sophisticated attacks.

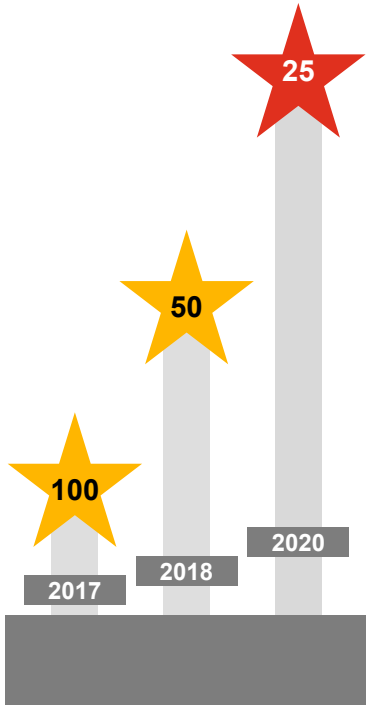
In recent years, the Vietnam government had issued numerous regulations in its effort to strengthen the local cybersecurity landscape, including:

- Directive No. 22/CT-BTTTT issued in May 2021 by the Ministry of Information and Communications focused on strengthening the prevention and combat of law violations and crimes on the Internet.
- Decision 1907/QD-TTg issued in 2020 which approves the Ministry of Information and Communications raise awareness and disseminate knowledge about information security for 2021-2025.
- Prime Minister's Directive No.14/CT-TTg in June 2019 enhanced safety measures on cybersecurity of the public sector whereby at least cybersecurity spend must account for 10% of an organisation's total annual IT expenditure in 2020-2025.
- Personal Data Protection Draft Decree, once enacted is set to be the first comprehensive legislation on personal data.

These efforts have yielded positive results given in 2020, Vietnam ranked 25th out of 194 countries in Global Cybersecurity Index (GCI). This ranking is a significant improvement from 2018 and 2017 when Vietnam was placed in the 50th and 100th positions respectively. In addition, this result exceeded Vietnam's target to enter the GCI's top 30 countries in 2030 as per the Prime Minister's Decision No. 749/QD-TTg dated 3 June 2020.

Vietnam's GCI* ranking

Source:GCI International Telecommunication Union



Simplifying cyber with intention

This 2022 Global Digital Trust Insights Survey provides a guide for organisations to streamline their operations and processes consciously and deliberately. It focuses on four key questions, starting at the top with the CEO, to establish a unified approach to cybersecurity. These questions are often overlooked but, if properly considered, can yield significant results.

1. How can CEOs make a difference to your organisation?
2. Is your organisation too complex to secure?
3. How do you know if you're securing your organisation against the most important risks to your business?
4. How well do you know your third-party and supply chain risks?

The following pages highlight our findings.

The top 10% reporting significant progress toward meeting important cyber goals[1] — the most improved — are many times more likely to be doing the right things. Below illustrates the multiplier effect of simplifying cyber.

12x more likely to say their CEOs give them the support they need

5x more likely to have streamlined operations enterprise wide

10x more likely to have a formal process fully implemented for data trust practices

11x more likely to have high levels of understanding of cyber and privacy risks from third parties

[1] Cyber goals covers instilling a culture of cybersecurity, managing cyber risk, enhancing communication between boards and management, and coordinating cyber strategy with business strategy

How can CEOs make a difference to your organisation?

How involved are CEOs in cyber?

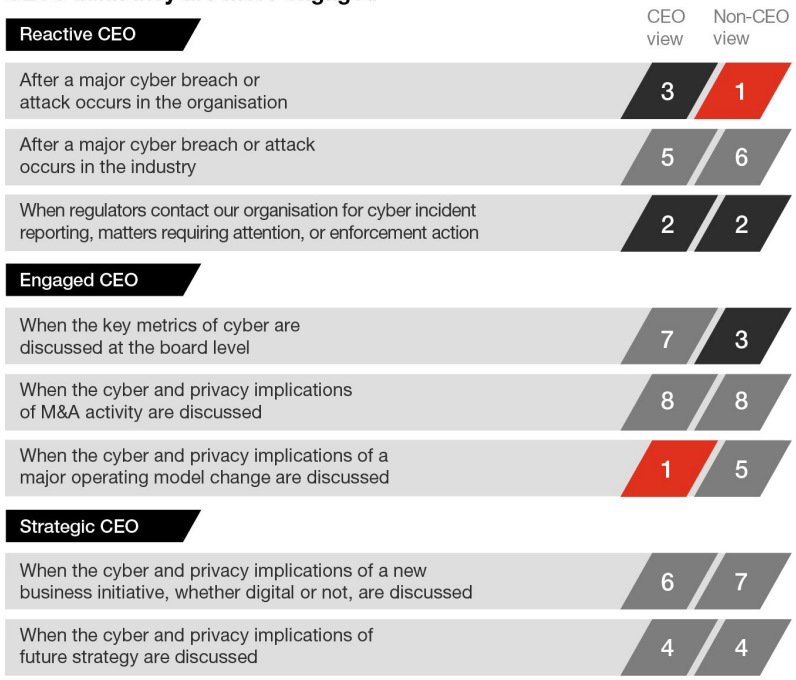
Our findings from the 2022 Global Digital Trust Insights Survey suggest an “expectations gap” for cyber:

- Executives see CEOs getting involved in cyber when a crisis strikes. CEOs see themselves as more engaged.
- CEOs believe they give ‘significant’ cyber support, but only 3 in 10 non-CEOs agree.

It’s time to close this gap between the chief executives and the others in the C-suite regarding the level of CEO involvement and support of cybersecurity. Unchecked, this gap can spell disaster if it instills a false sense of security company-wide, given the CEO’s leading role in defining an organisation’s culture.

CEOs have the power and potential to wield important cyber-related changes. In the “most improved” group of companies (those with the best cybersecurity outcomes the last two years), CEOs are **14x** more likely to provide considerable support across all areas. The survey further points out executives in most regions and industries say the most important act for a more secure digital society by 2030 is educating CEOs and boards so they can better fulfill their cyber duties and responsibilities.

Executives see CEOs getting involved in cyber when a crisis strikes. CEOs think they are more engaged



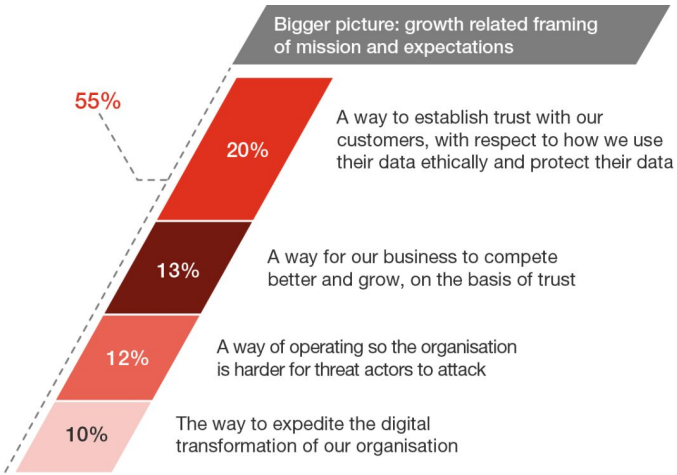
Question: On which of the following cyber & privacy matters, would you/your CEO become personally involved? Rank them in order.
Base: Non-CEO Respondents: 2,929; CEO Respondents: 673
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Changing cyber mission: Developing trust and business growth

Cybersecurity's mission is shifting to developing trust and business growth, with 54% framing it beyond cyber defense and controls.

In both CEOs and non-CEOs groups, "a way to establish trust with our customers with respect to how we use their data ethically and protect their data" was the number-one cyber mission choice. All agreed with prevention as the baseline, or most important; resilience coming next; followed by trust (including consumer trust: "improved customer experience" and "higher customer loyalty" rank further down the list).

Goals	Global	Asia Pacific
Increased prevention of successful attacks	No. 1	No. 2
Faster response times to incidents and disruptions	No. 2	No. 3
Improved confidence of leaders in our ability to manage present and future threats	No. 3	No. 1



Key takeaways

Top cyber-ready goals for the next 3 years are:

- Increased prevention of successful attacks (this ranks number three in the energy and utilities sector)
- Faster response times to incidents and disruptions
- Improved confidence of leaders in the organisation's ability to manage present and future threats (number one in energy, utilities, and resources)

CEOs:

- Frame cybersecurity as important to business growth and customer trust — not just defense and controls — to create a security mindset organisation-wide
- Demonstrate your trust in and steadfast support for your CISO
- Come to grips with the problems and risks in your business models and change what needs to be changed. You'll have lots of opportunities to follow Peter Drucker's advice: "Management is doing things right; leadership is doing the right things."

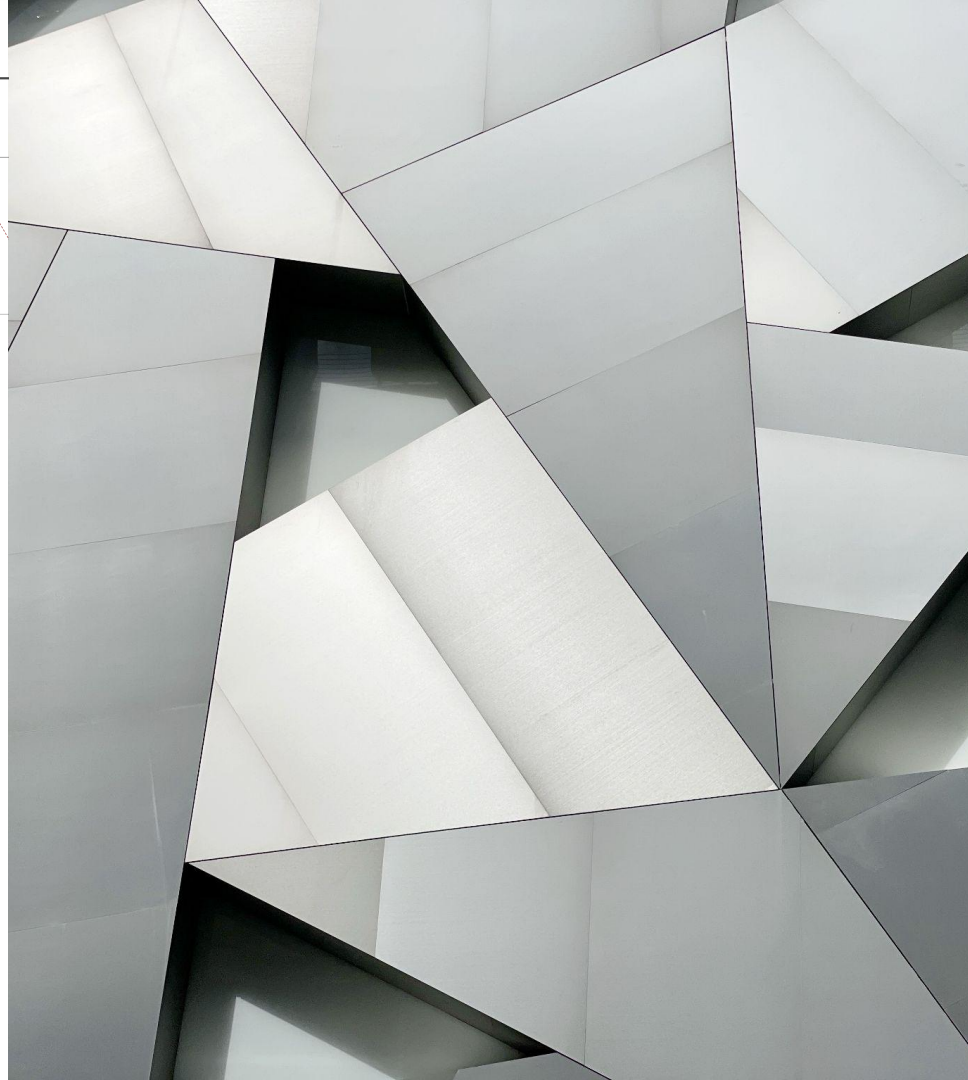
CISOs:

- Familiarise yourself with your organisation's business strategy
- Build a stronger relationship with your CEO, and keep the dialogue going to help your CEO clear the way for simply secure practices
- Equip yourself with the skills you need to thrive in the evolving, expanding role for cyber in business. And reorient your teams, if you haven't already, towards business value and customer trust.

“

Each organisation's cybersecurity starts and ends at the highest level of management. 70% of surveyed executives agreed that the 2022 budget will be increased for cybersecurity. In face of heightened risks, cybersecurity should no longer be defined as just a matter of “internal controls”, but also a pivotal instrument to help organisations build trust with customers and support sustainable business growth.

Nguyen Phi Lan
Partner, Risk Assurance Services Leader
PwC Vietnam




Is your organisation
too complex to secure?

Are organisations today too complex?

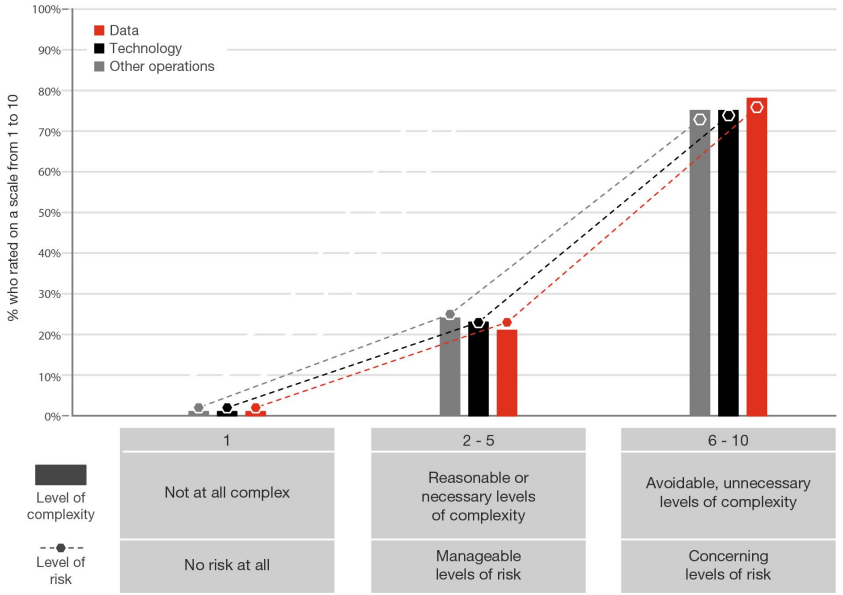
The most worried about all this complexity are CEOs having assigned a complexity level of 10 to seven of 11 areas in their organisations. Other findings include:

- 75% of executives report too much avoidable and unnecessary complexity in their organisations, in their technology, data, and operating environments.
- About as many believe that complexity leads to ‘concerning’ levels of cyber and privacy risks.

Simplification takes time and effort but is highly rewarding.

- The “most improved” companies are **5x** more likely to have streamlined operations enterprise-wide, with focuses on:
  - consolidating tech vendors (62%),
  - defining/realigning the mix of in-house and managed services (60%),
  - and reorganising functions and ways of working (59%).
- Simplifying cybersecurity, mainly cloud transformations, can help streamline business processes and IT architecture, provide flexibility and accelerate innovation.

75% of executives report too much complexity in their organisations, leading to ‘concerning’ cyber and privacy risks



Questions: In your view, how complex are the following operations in your organisation, on a scale of 1 to 10? How significant are the cyber and privacy risks posed by complexity in these areas in your organisation?
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Key takeaways

Streamlined operations in the past 2 years covered:

- Consolidating tech vendors (62%),
- Defining/realigning the mix of in-house and managed services (60%),
- Reorganising functions and ways of working (59%) and
- Creating an integrated data governance framework (58%).

COOs and transformation leaders: Ask: what's the cyber plan for that? You can ignite major changes — operational and cultural — simply by asking this one question of every business executive in charge of a transformation or new business initiative. By placing cybersecurity front-row-center, you'll avoid the unnecessary and costly complexities you may see now, when it's an afterthought.

Include the CISO and security teams early in cloud migration and adoption, mergers and acquisitions, and other organisational initiatives.

CISOs and CIOs: Dare to subtract. Left on their own, technology and data tend to multiply, divide, and conquer efficiency and security. You could unwittingly add complexity with the amount of security tools you add. Instead, whittle down excess with security goals in mind: assess your data stores and eliminate everything you don't need now; move your disparate apps and solutions into a cloud environment for easier management; and consolidate, liquidate, standardise, and automate where you can.

Also, rethink your tech and cyber investment processes. Focus first on simplifying where benefits are greatest for the whole organisation.

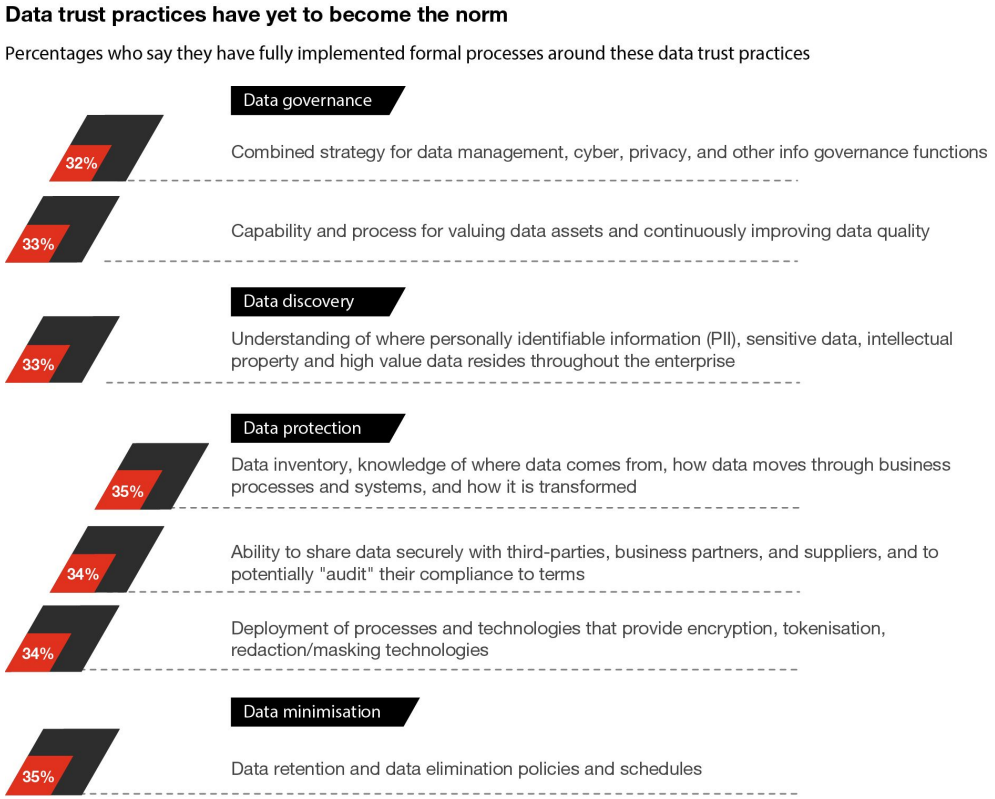

Are you securing against
the most important risks
to your business?

How are you sizing your important risks today and tomorrow?

Although organisations leaders recognise the value of verifying and safeguarding business data, data and intelligence are often overlooked in the decision-making process.

- < 33% of respondents say they've integrated analytics and business intelligence tools into their operating model.
- Only 35% have mapped all their data, meaning they know where it comes from and where it goes. The same goes for those who have mature data minimisation processes.

Data trust practices have yet to become the norm. Data is the asset attackers covet most. Your companies can minimise that risk by minimising the target. Organisations first need to set up that good foundation we call data trust: making sure your data is accurate and verified and secure so you can rely on them for business decisions. However, only about a third of respondents report having mature, fully implemented data-trust processes in four key areas: governance, discovery, protection and minimisation.



Question: For each of the following, please rate how mature your organisation's data trust practices are. Percentages are for the response 'formal process, fully implemented'
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Use data or lose out

This year's findings show that executives underutilise data and intel for better decisions and risk management.

- Only 30% consider real-time threat intelligence integral to their operating model.
- Only 26% turn data into insights for cyber risk quantification, threat modeling, scenario building and predictive analysis — all critical technologies for smart cybersecurity decisions.
- Fewer than 30% to benefit from today's advanced intelligence tools and approaches such as information sharing platforms with industry, etc.

Businesses predicting an increase next year in their cybersecurity spending are often the same enterprises whose operational models use business intelligence and data analytics. Data cannot only help you spend your cyber budget wisely, it can also help you get more to work with. The most improved (top 10% in cyber outcomes) are **18x** more likely to state that these advanced approaches are integral to their operating model.

Executives underutilise data and intel for better decisions and risk management

Percentage who say these are critical to their operating model today

Questions: To what extent does your organisation use the following tools and approaches when making decisions about cyber investments and responding to cyber risk? What best describes your organisation's plans for using the following tools and approaches for better operational intelligence?
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Key takeaways

Threat outlook for 2022

Top list of anticipated targets:
- Mobile,
- Internet of Things, and
- Cloud

Types of attack most likely to see significant increases
- Cloud service attacks (22%)
- Ransomware (21%)
- Cryptomining (21%)

CFOs:

- Work with the CISO in using risk-based, growth-oriented approach to cyber budgeting.
- Get visibility from the CISO into the cost of breaches and incidents, as well as potential costs of exposure.

CISOs:

- Build a strong data trust foundation: an enterprise-wide approach to data governance, discovery, protection and minimisation.
- Create a roadmap from cyber risk quantification to real-time cyber risk reporting.
- Don’t stop at cyber risks. Tie the cyber risks to overall enterprise risks and, ultimately, to effects on the business.
- With a fuller accounting of cyber risks, identify what works in your business model and where you might need to simplify.

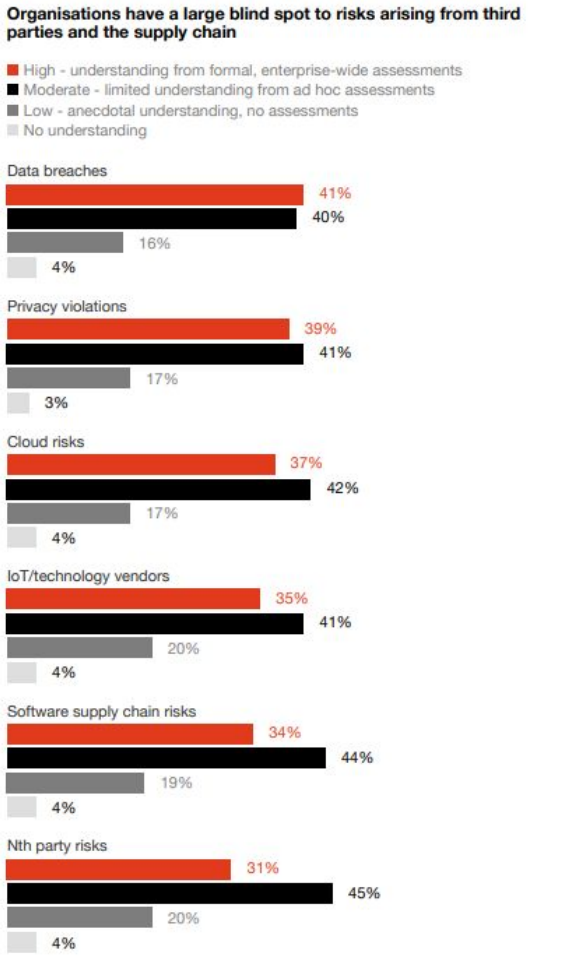

How well do you know
your third-party and supply chain risks?

How well do you know your third-party and supply chain risks?

Most of our respondents have trouble spotting third-party risks - risks obscured by the complexities of their business partnerships and vendor/supplier networks. Our survey highlights that **third-party cyber risks are a glaring blind spot:**

- Only **40%** of survey respondents say they thoroughly understand the risk of data breaches through third parties, and only **37%** profess an understanding of cloud risks based on formal assessments.
- 56% expect an increase in reportable incidents in 2022 from attacks on the software supply chain, but only 34% have formally assessed their enterprise's exposure to this risk.

Today's trending cyber-attack target may come from your supply chain of trusted vendors, suppliers and contractors. An organisation could be vulnerable to a supply chain attack even when its own cyber defences are good, with attackers simply finding new pathways into the organisation through its suppliers. The weapon? A process many have taken completely for granted: the software update. The organisations that had the best cyber outcomes over the past two years have consolidated tech vendors as a simplification move. Paring the number of tech and other third parties reduces complexity and increases your ability to know how secure they are.



Question: What is the level of understanding within your organisation of the cyber and privacy risks arising from your third parties or suppliers across the following areas?
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Key takeaways

Good practices to mitigate these risks include:

- Reducing the number of third-party relationships,
- Increasing the monitoring process
- Deepening assessments of third parties

COO and the supply chain executive:

- Map your system, especially your most critical relationships, and use a third-party tracker to find the weakest links in your supply chain
- Scrutinise your software vendors against the performance standards you expect. Software and applications that your company uses should undergo the same level of scrutiny and testing that your network devices and users do.
- After a fuller accounting of your third-party and supply chain risks, identify ways to simplify your business relationships and supply chain. Should you pare down? Combine?

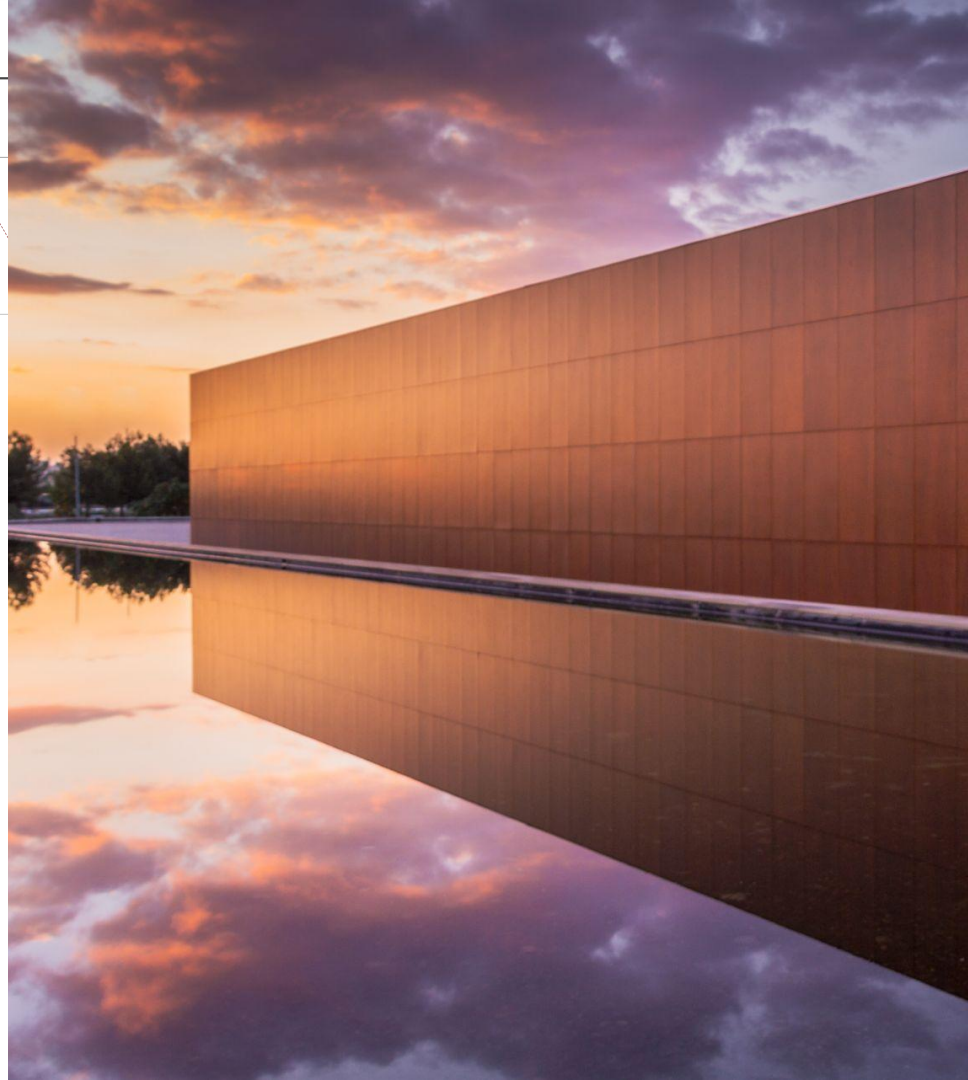
CRO and CISO:

- Build up your technological ability to detect, resist and respond to cyber attacks via your software, and integrate your applications so you can manage and secure them in unison.
- Establish a third-party risk management office to coordinate the activities of all functions that manage your third-party risk areas.
- Strengthen your data trust processes. Data is the target for most attacks on the supply chain.
- Educate your board on the cyber and business risks from your third parties and supply chain.

“

In Vietnam, few companies are able to comply with the requirements related to digital transformation, particularly those concerning the management of third-party cyber and privacy risks. Hence, the adoption of international standards and good practices are imperative for organisations to improve the effectiveness of supply chain management and minimize third-party risks.

Pho Duc Giang
Director
PwC Vietnam Cybersecurity Ltd.



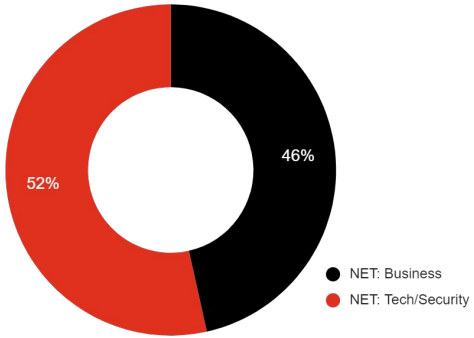
Appendix

Demographic

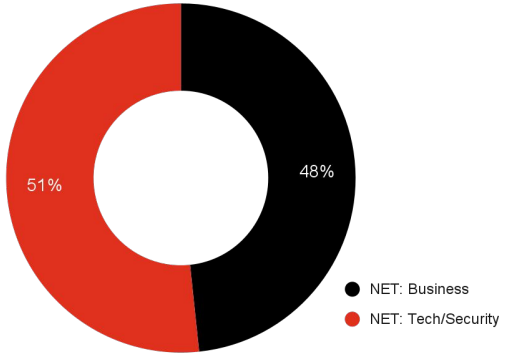
Demographics

Job Title

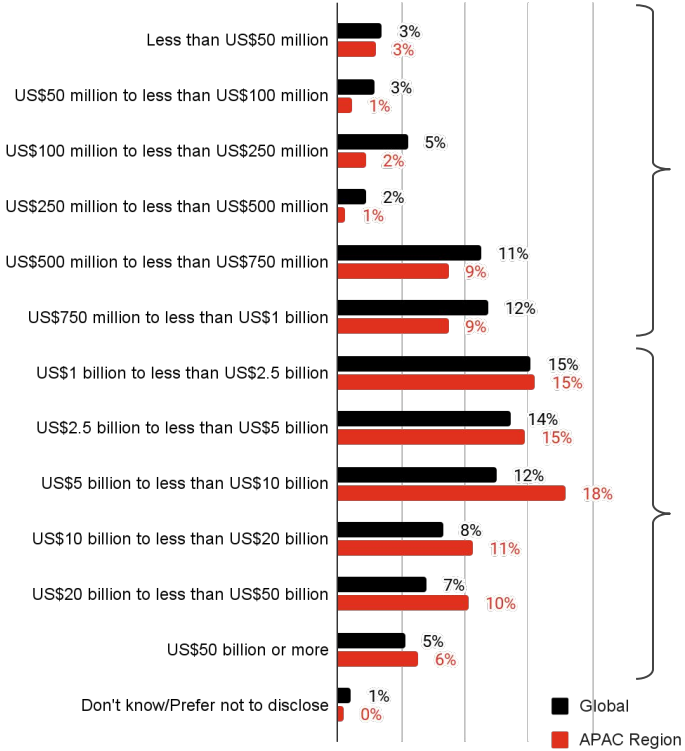
Global



Asia Pacific



Revenue



NET: Less than US$1 billion

Global: 37%

Asia Pacific: 24%

NET: Greater than US$1 billion

Global: 62%

Asia Pacific: 75%

Source: PwC's Global Digital Trust Insights Survey 2021, September 2021. Base: Global=3602, Asia Pacific=633

Cyber security landscape in Vietnam

Current statistics

Vietnam was ranked 25th out of 194 countries and 7th in the Asia Pacific region in Global Cybersecurity Index (GCI) 2020 by the International Telecommunication Union, up from the 50th in 2018. This leap exceeded Vietnam's target to enter the GCI's top 30 countries in 2030, and demonstrates its determination and performance in assuring cybersecurity and tackling cybercrimes.

Regulatory developments

- Directive No. 22/CT-BTTTT: issued by The Minister of Information and Communications and dated May 26, 2021, focused on strengthening the prevention and combat of law violations and crimes on the Internet.
- Personal Data Protection Decree: The Ministry of Public Security released on its website Vietnam's Draft Decree on Personal Data Protection for the public to submit their opinions. If passed, it would establish the first comprehensive framework on data protection and privacy law in Vietnam.

Future goals

Vietnam's digital economy will exceed $43 billion by 2025 as the country pursues projects in e-government, internet of things, smart cities, financial technology, artificial intelligence. With the rapid growth for digital transformation throughout the country, Vietnam faces an increase in cyber threats, and sophisticated attacks.

In an effort to improve the cybersecurity capabilities, in 2020 the Government of Vietnam issued a decision 1907/QD-TTg on the approval of cyber awareness strengthening master plan for the period 2021-2025. Besides, the Prime Minister's Directive No.14/CT-TTg issued on June 7, 2019 on enhancing safety measures on cybersecurity stated that the public sector must spend at least 10% of their organization's total annual IT expenditure on cybersecurity in 2020-2025.

The Vietnam Cybersecurity Market stood at USD142.12 million in 2020 and is forecast to grow at a CAGR of 16.52% until 2026. Growth in the Vietnam Cybersecurity Market is driven by the increasing digital economy.

Demographics

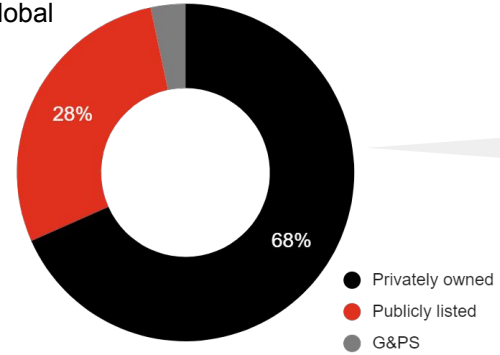
Gender

Female
Global: 33%
Asia Pacific: 27%

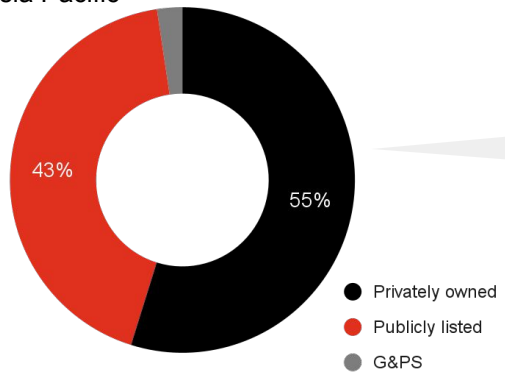
Male
Global: 66%
Asia Pacific: 62%

Organisation ownership

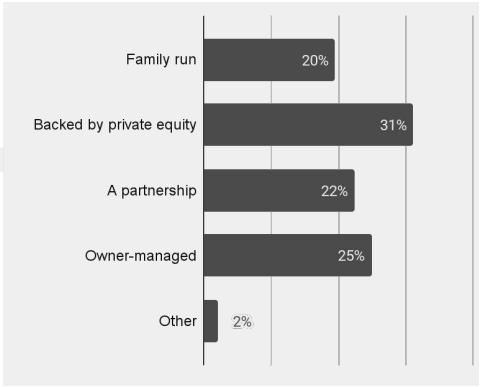
Global

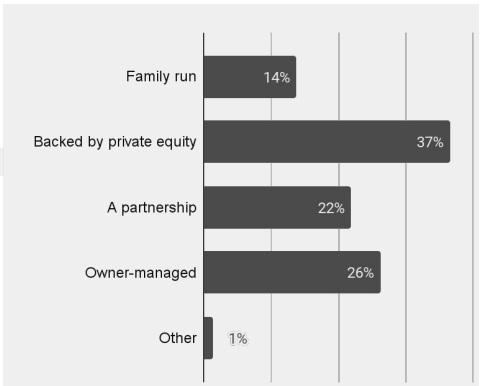


Asia Pacific



Privately owned organisations





Source: PwC's Global Digital Trust Insights Survey 2021, September 2021. Base: Global=3602, Asia Pacific=633. Privately owned organisation base: Global=2462, Asia Pacific=347

Contact us

Nguyen Phi Lan
Partner / Risk
Assurance Leader
PwC Vietnam

Pho Duc Giang
Director
PwC Vietnam
Cybersecurity Ltd.

Thank you

pwc.com/vn