2022 Digital Trust Insights Survey: India edition

Changing mindset of India's C-suite towards cyber readiness

pwc

Changing investment priorities: Rethinking cyber strategy to maximise benefits

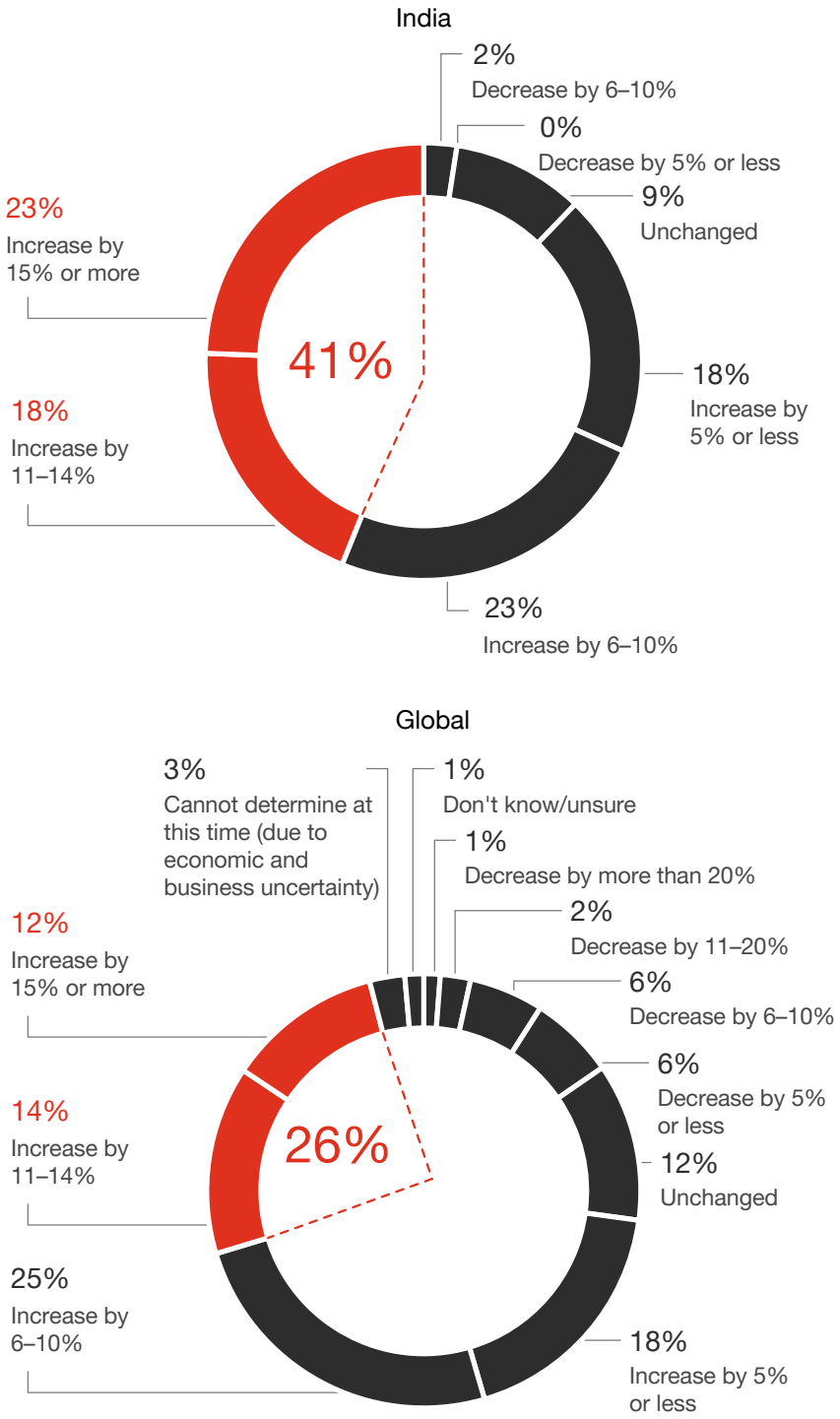
In the digital age, organisations with the highest level of digital trust have become the consumer's first choice. However, with an ever-increasing focus on digitisation and the utilisation of enormous amounts of data, organisations have become heavily reliant on complex, deeply rooted and interdependent technologies.

This has created a playground for attackers as the number of reported attacks has surged over the years. Armed with highly sophisticated methods, attackers today are seeking and exploiting vulnerabilities and compromising systems and networks. Organisations are aware that the risk landscape is continuously evolving and are investing more than ever in cyber security to manage their risks.

As the business environment turns more complex due to the interconnectedness of systems and information, the impact of a risk event is not limited, but rather has a domino effect with high consequences. Organisations are therefore gearing up to implement robust cyber security practices and controls to manage these risks.

As per PwC's 2022 Digital Trust Insights Survey, **82%** of the Indian respondents have **predicted an increase in their cyber security budget in 2022. Moreover, 41% of organisations in India** predict **double-digit growth in their cyber budgets in 2022,** as against **26% organisations globally.**

Changing cyber budgets in 2022



Question: How is your cyber budget changing in 2022?
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

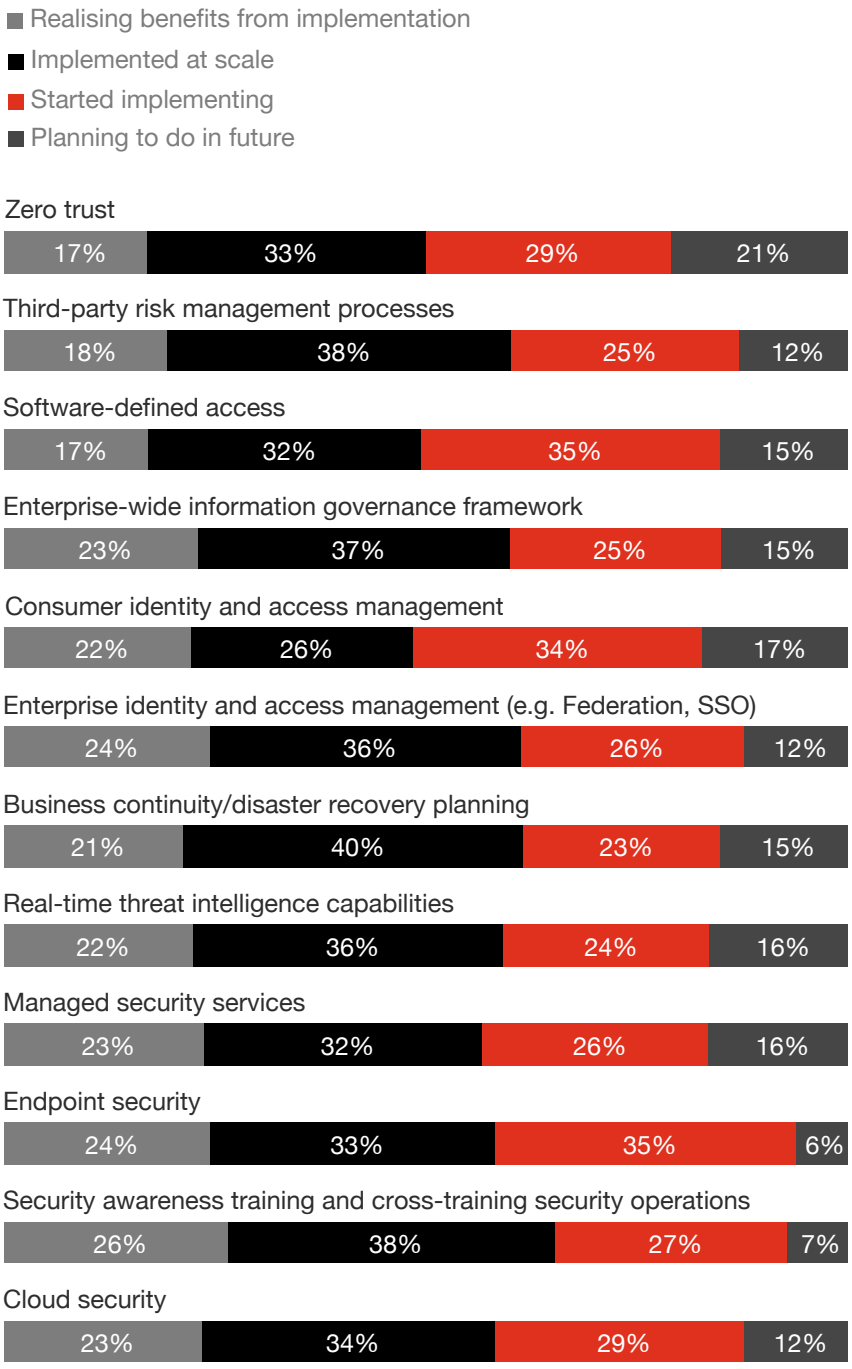
While technology has brought in greater convenience and efficiency, it has also increased the risk of security threats. The investments and efforts required to manage and prevent these threats have increased simultaneously. Organisations that have understood and acted upon the importance of cyber security are reaping the benefits of their investments. However, as per our survey, to date, **only 25% of respondents in India have realised the benefits of their cyber investments. So, how can companies achieve better returns from future cyber investments?**

The 2022 Digital Trust Insights Survey reveals that four out of ten organisations in India have initiated, or are planning to initiate, investment in cyber security by focusing on areas such as customer identity and access management, zero trust architecture, managed security services, cloud security and endpoint security. How can they derive maximum value from each dollar spent on strengthening their cyber security posture?

With the impetus for digitisation having only increased during the pandemic, organisations have reinvented their business models to reach out to their consumers. We have seen considerable growth in digital health, industrial automation, enhanced e-commerce, FinTech and other areas. However, with rising digitisation, businesses have been compelled to rethink and reconfigure their cyber security objectives, which have become more complex. The processes needed to manage and maintain the guardrails around services and information have become complicated and, in some instances, challenging.

More than 75% of the Indian respondents to our Global Digital Trust Insights Survey say that too much avoidable and **unnecessary organisational complexity poses 'concerning' cyber and privacy risks.**

Investment priorities for organisations



Question: To what extent is your organisation prioritising investments in the following?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

How can organisations improve their investment returns by simplifying their cyber security programme? Our survey offers some vital insights. **A security focus that cuts across** the entire business – from top leadership to every department and across all employees – is key to achieving this goal. Our survey results indicate that organisations that have made significant progress with these cyber goals – **instilling a culture of cyber security, managing cyber risks, enhancing communication between boards and management, and aligning their cyber strategy with their business strategy** – are more likely to simplify their cyber security practices and reap dividends on their cyber investments.

In order to achieve their full cyber potential, organisations need to build capabilities in the following areas:

1. Security-first leadership: Organisations need to have a dedicated leadership group that understands the significance of cyber security and treats security as a priority.

2. Reducing complexity in cyber security: Organisations are operating in a complex cyber security ecosystem and often find it difficult to manage their risks due to underlying complexities. Simplifying cyber security and prioritising their investments in the right areas is the need of the hour.

3. Securing against the critical risks of today and tomorrow: Organisations need to manage cyber risks effectively, including the blind spots emerging from their extended ecosystems, so that they can realise the value of their investments and operate risk free.

Cyber security scorecard: Five out of ten organisations in India reported significant progress on the following four fronts in the past two years

Question: How much progress in cyber risk management has your organisation made in the past two years?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Security-first leadership: Can the CEO make a difference to your organisation's cyber security?

Cyber security has traditionally been the sole responsibility of the IT department. But those in IT have long acknowledged the fact that keeping a company cyber secure is really everyone's job. Involvement of the C-suite has a big role to play in creating a security-conscious culture. The well-known saying 'culture eats strategy for breakfast' basically implies that no matter how good the strategy, it will not work unless the workforce buys into it.

Senior leaders have a significant role to play in their organisation's cyber security posture. Leaders should understand cyber security best practices well enough to enable sound decision making. They do not need to become technical experts themselves — these roles are generally delegated or outsourced — but they do need to have a fundamental understanding of the field, much as they must understand their business operations.

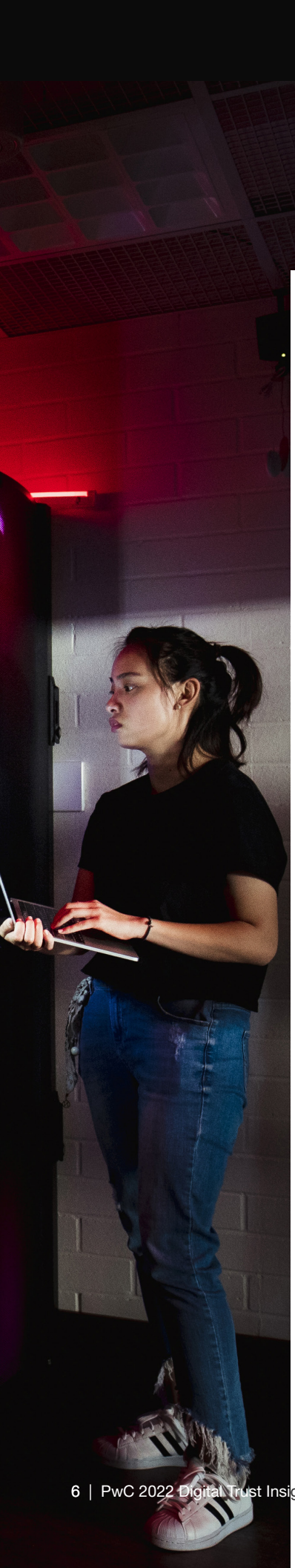
In this digitised world, cyberattacks are a constant threat and business leaders understand their dire consequences. Considering the number of successful cyberattacks in corporate and government spaces over the last few years, everyone from the C-suite down to an IT analyst is aware that a single security breach can cost a fortune. While most CEOs recognise these risks, the mountain of responsibilities on their plate often means they can't make cyber security an immediate priority. So, how involved are CEOs in cyber security initiatives?

Our findings from the 2022 Global Digital Trust Insights Survey suggest that CEOs tend to be disconnected from cyber security, and many leaders still fail to realise the seriousness of the issue. Our survey indicates that many CEOs in India self-identify as r**eactive, engaged and strategic** in their approach towards cyber security. However, others view their involvement to be more **reactive and strategic, but not engaged**. Often, cyber security becomes a concern for CEOs only when they are contacted by regulators or during discussions on the cyber and privacy implications of a new initiative or future strategy.

Executives believe that CEOs are proactively engaged in cyber security only when a crisis arises

	India		Global	
	CEO view	Non-CEO view	CEO view	Non-CEO view
Reactive CEO				
After a major cyber breach or attack occurs in the organisation	2	5	3	1
After a major cyber breach or attack occurs in the industry	7	4	5	2
When regulators contact our organisation for cyber incident reporting, matters requiring attention or enforcement action	4	1	2	8
Engaged CEO				
When the key metrics of cyber are discussed at the board level	8	7	7	5
When the cyber and privacy implications of M&A activity are discussed	1	6	8	6
When the cyber and privacy implications of a major operating model change are discussed	5	8	1	7
Strategic CEO				
When the cyber and privacy implications of a new business initiative, whether digital or not, are discussed	6	2	6	3
When the cyber and privacy implications of future strategy are discussed	3	3	4	4

Question: On which of the following cyber and privacy matters, would you/your CEO become personally involved? Rank them in order.
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021



Moving towards a more secure digital society by 2030

When asked about the ways in which the cyber security field has to evolve to create a more secure digital society by 2030, a majority of the respondents in India chose "develop a diverse cyber workforce" and "educate CEOs and boards so they can better fulfil their duties and responsibilities regarding cyber security" as their top choices.

Global respondents, however, had a different perspective on the matter, and they ranked "discover technology breakthroughs that simplify while improving cyber defence" along with "educate CEOs and boards so that they can better fulfil their duties and responsibilities regarding cyber security" as the most important areas.

Cyber security scorecard: Executives in India are looking at developing a diverse cyber workforce and educating CEOs regarding cyber security as key change drivers for moving towards more a secure digital society by 2030

	India	Global
Develop a diverse cyber workforce	1	7
Educate CEOs and boards so they can better fulfill their duties and responsibilities regarding cyber security	2	1
Work with schools and universities to increase the cyber security awareness and knowledge in the general population	3	4
Make signatory-nations accountable for responsible behaviours in cyberspace, according to norms in international agreements	4	6
Lay down regulatory foundation that enforces organsiational responsibility and accountability for basic cyber security practices	5	3
Collaboration between countries to increase resilience of critical infrastructure	6	5
Discover technology breakthroughs that simplify while improving cyber defence	7	2

Question: In what ways does the cyber security field have to change so there is a more secure digital society by 2030?
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

The cyber mission is changing – CEOs and other executives agree

Not so long ago, business leaders could discuss technological enhancements without even mentioning security. This is definitely not the case today!

With technology evolving at a rapid speed, the adoption of remote working and the increase in customer expectations regarding their personal data, **board members and senior executives acknowledge the need for and importance of cyber security**. However, in our survey, this recognition was higher among India's **non-CEO respondents** (69%) than it was among CEOs (51%). When asked about their organisation's cyber security mission, "a way to establish trust with our customers, with respect to how we use their data ethically and protect their data" was the top choice for non-CEO executives and CEOs. **However, 49% of CEOs still relate to a narrow definition of mission and expectations from the security team.** For these CEOs, cyber security represents a way to implement controls throughout the organisation for preventing serious cyber disruptions and responding faster to threats. It is a cost of doing business and a necessary evil.

CEOs around the globe now understand the gravity and magnitude of the threat that cyberattacks pose to their business. In the last year or so, we witnessed the unprecedented adoption of remote working. CEOs prioritised the adoption of digital transformation initiatives as a means to sustain themselves the pandemic era. Taking into consideration the extraordinary changes in technology, corporate culture and the mindset of business leaders, the question that needs to be asked is, '**What should be the CEO's focus and goals with respect to cyber security for the next three years**

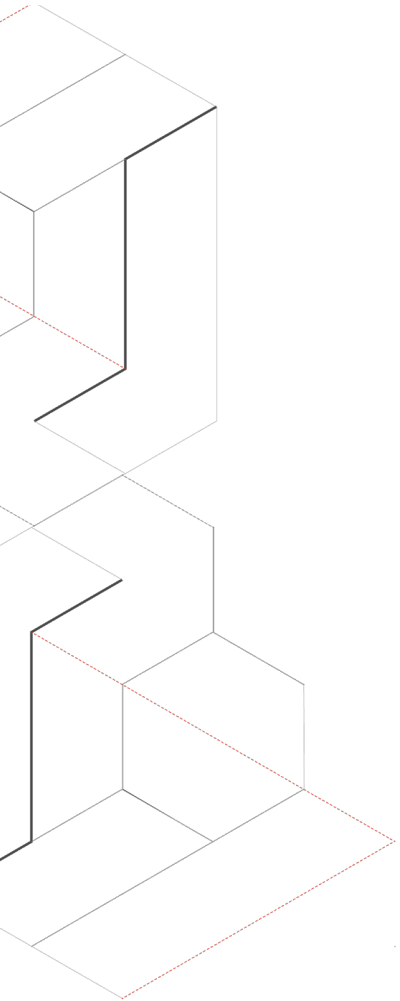
Bigger picture: Growth-related framing of mission and expectations

Narrow framing of mission and expectations from the security team

Question: Which of the following best describes how your CEO frames the cyber security mission of your organisation?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Amongst India respondents, “improved confidence of leaders in our ability to manage present and future threats” was the number one choice with regard to goals and changes in cyber strategy, people and investments over the next three years. However, globally, “increased prevention of successful attacks” was the top choice.

Additionally, in India, the cyber security strategy of CEOs for the next three years is driven by regulatory compliance. A compliance-based approach to security is fundamentally weak and focused on the here and now of risks. Instead, organisations need to focus on a risk-driven approach to manage current and future threats.



Cyber security goals for the next three years

Global

Increased prevention of successful attacks	1
Faster response time to incidents and disruptions	2
Improved confidence of leaders in our ability to manage present and future threats	3
More successful outcomes for our organisation’s transformations	4

India

Improved confidence of leaders in our ability to manage present and future threats	1
Greater compliance with regulations	2
More successful outcomes for our organisation’s transformations	3
Faster response times to incidents and disruptions	4

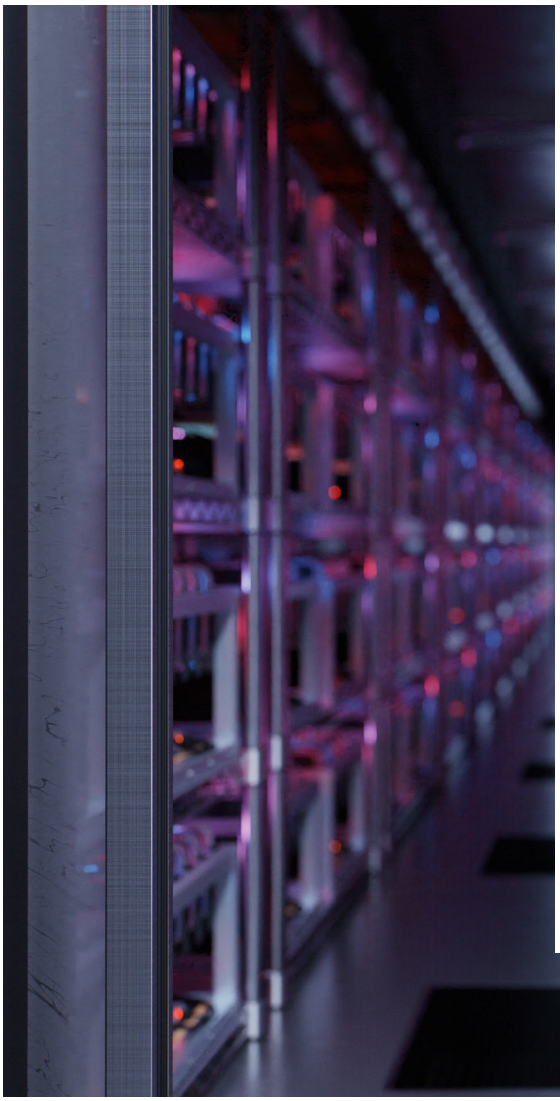
Question: In the next three years, what goals will you be focused on, in relation to the changes you will be making in cyber strategy, people and investments?
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Reducing complexity in cyber security

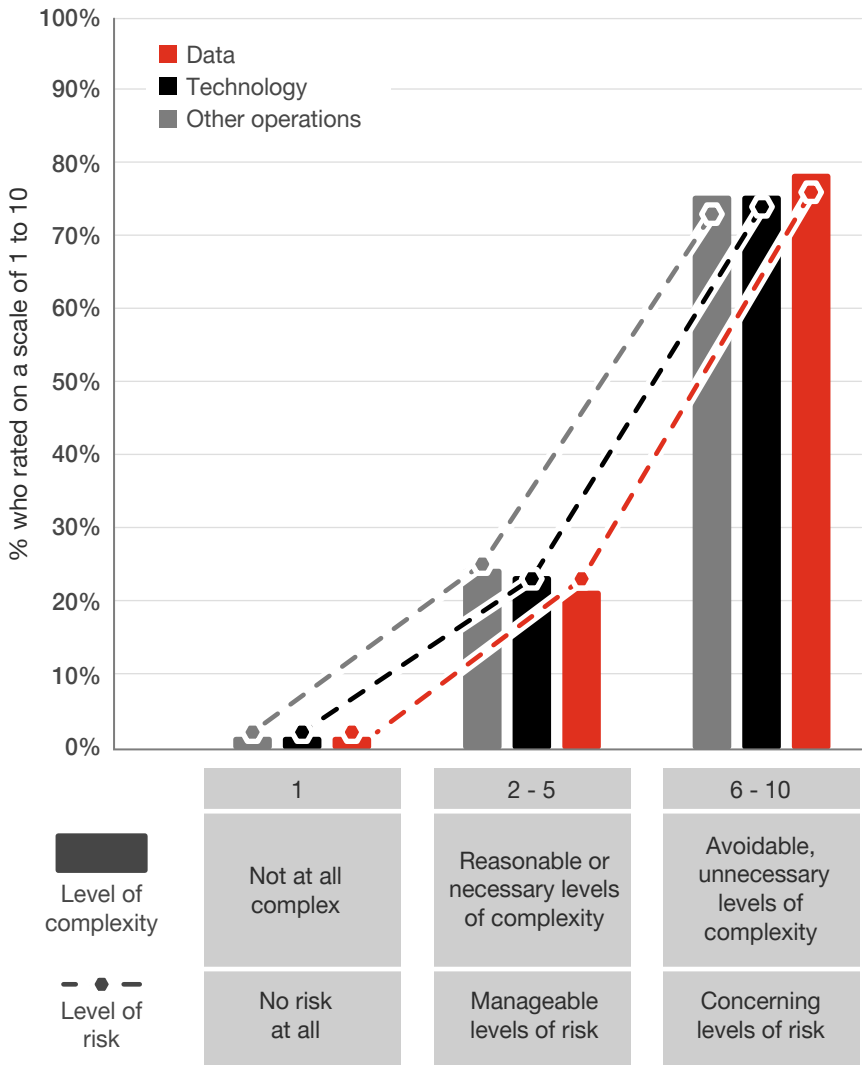
With data, technology and operations functioning in silos, the cyber ecosystem is highly complex to manage, thus increasing the risk of cyber security breaches.

The 2022 Global Digital Trust Insights Survey offers insights into this complexity and how Indian organisations can simplify their cyber security programme by streamlining data, technology and operations.

The current situation is an opportunity for industry leaders to set the right cyber security roadmap for their organisations by empowering and placing greater trust in people, technology and customers.



Rise through complexity by levelling up on simplicity



Question: 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: 109 Indian respondents

Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

The complexity crisis in cyber security

Complexity by itself isn't a bad thing, and it typically accompanies growth. As the revenues, customer base and workforce of organisations grow and they add more processes and generate more data, the level of complexity of operations increases. The right approach and proactive measures to combat cyber security threats can lead to new growth avenues in a secured environment.

The cost of complexity varies: **financial losses** due to cyberattacks, **inability to innovate** with a shift in industry trends, lack of operational resilience or failure to recover from a cyberattack, **inability to achieve near-term goals**, and lack of ability to sustain long-term growth in a dynamic environment, among others.

Our survey findings indicate that the cost of complexity arises not just from the internal ecosystem of an organisation but also from the external ecosystem, such as the vendor ecosystem or a business function completely run by third parties. Building more resilience and simplicity through a proactive approach rather than reacting to situations will help in managing both cost and complexity.

The first move – today not tomorrow

Organisations need to streamline not to fix but to grow. The India findings of the Digital Trust Insights Survey reflect a change in mindset among major Indian organisations and leadership towards streamlining company operations through increased investments in technology and talent. At the same time, some businesses are finding it difficult to manage operational complexities.

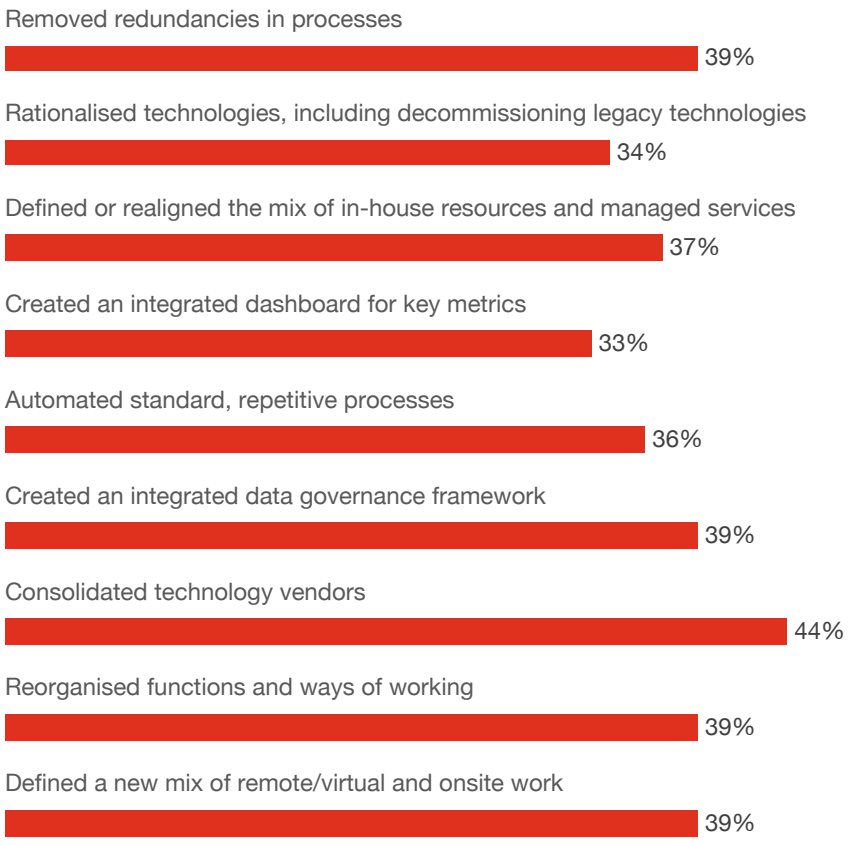
Around four out of ten Indian survey respondents are implementing focused strategies to streamline operations with initiatives like vendor consolidation for tech sourcing (44%), reorganising the functions and ways of working (39%), creating an integrated data governance framework (39%), removing redundancies in processes (39%), creating a hybrid working environment (39%), automating repetitive tasks (36%), creating an integrated dashboard for key metrics (33%), defining or realigning the mix of in-house resources and managed services (37%), and moving to next-gen technologies from legacy systems (34%).

In India, the consequences of complexity are financial losses, lack of resilience and inability to sustain growth in the long term

	India	Global
Financial losses due to successful data breaches or cyberattacks	01	01
Lack of operational resilience or inability to recover from a cyberattacks or technology failure	02	03
Inability to sustain growth for the long term	03	05
Inability to innovate as quickly as the market opportunities offer	04	02
Inability to retain top talent	05	06
Inability to achieve near-term growth goals	06	04

Question: What are the most important consequences of complexity on your business?
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Strategies for streamlining operations



Question: In the last two years, to what extent has your organisation streamlined operations in the following ways?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

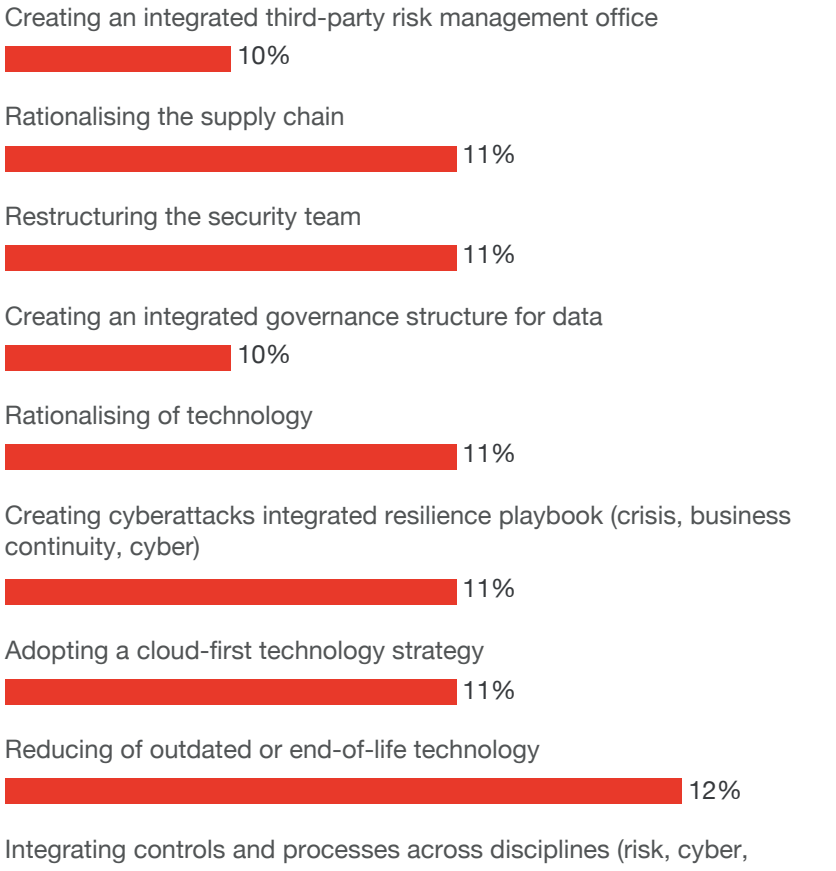
Spend today to grow tomorrow with simplification

Simplification is challenging: Where does one start, when and how? In a situation where cyberattackers can strike from any corner, organisations find it challenging to prioritise costs and investments.

A majority of organisations are seeking to streamline operations by integrating relevant controls and processes in their focus areas (12%) and migrating from outdated tech platforms to next-gen technology (12%).

Another common approach among India companies is adopting cloud services (11%). Many organisations have set this as their top priority, which will give them more space to control and manage operations. Other areas in which organisations are spending are creating an integrated resilience playbook (11%), rationalising technology (11%), restructuring the security team (11%) and rationalising the supply chain (11%).

Spending is spread across several initiatives for cyber simplification

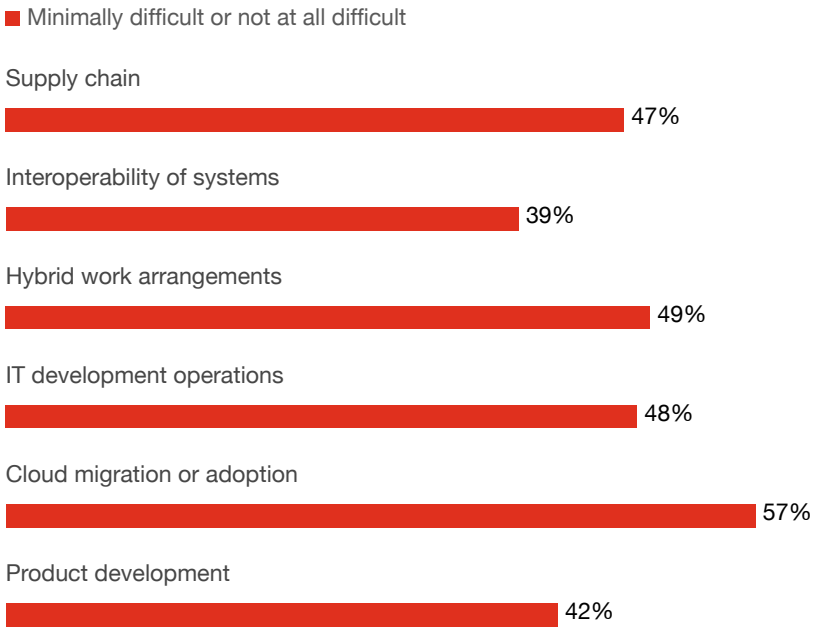


Question: In the next two years, what proportion of your cyber security spend will your organisation allocate to each of the following initiatives to simplify cyber security?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

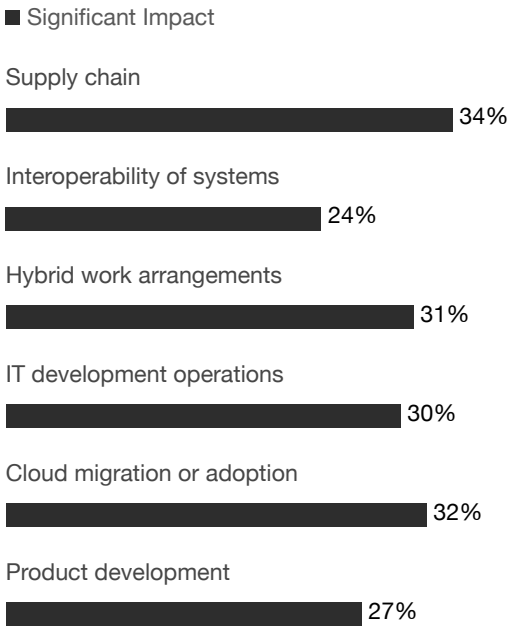
When asked about the areas that would pose a challenge with respect to building a cyber security and privacy programme into their organisation, many respondents chose “cloud migration or adoption” (32%) and “supply chain” (34%).

Additionally, we inquired about the level of impact that building security and privacy into the following operations would have on the organisation.

How difficult will it be to make the changes needed to build a cyber security and privacy programme into the following operations in your organisation?



What level of impact would building security and privacy into the following operations have on your organisation?



Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Threat outlook in India

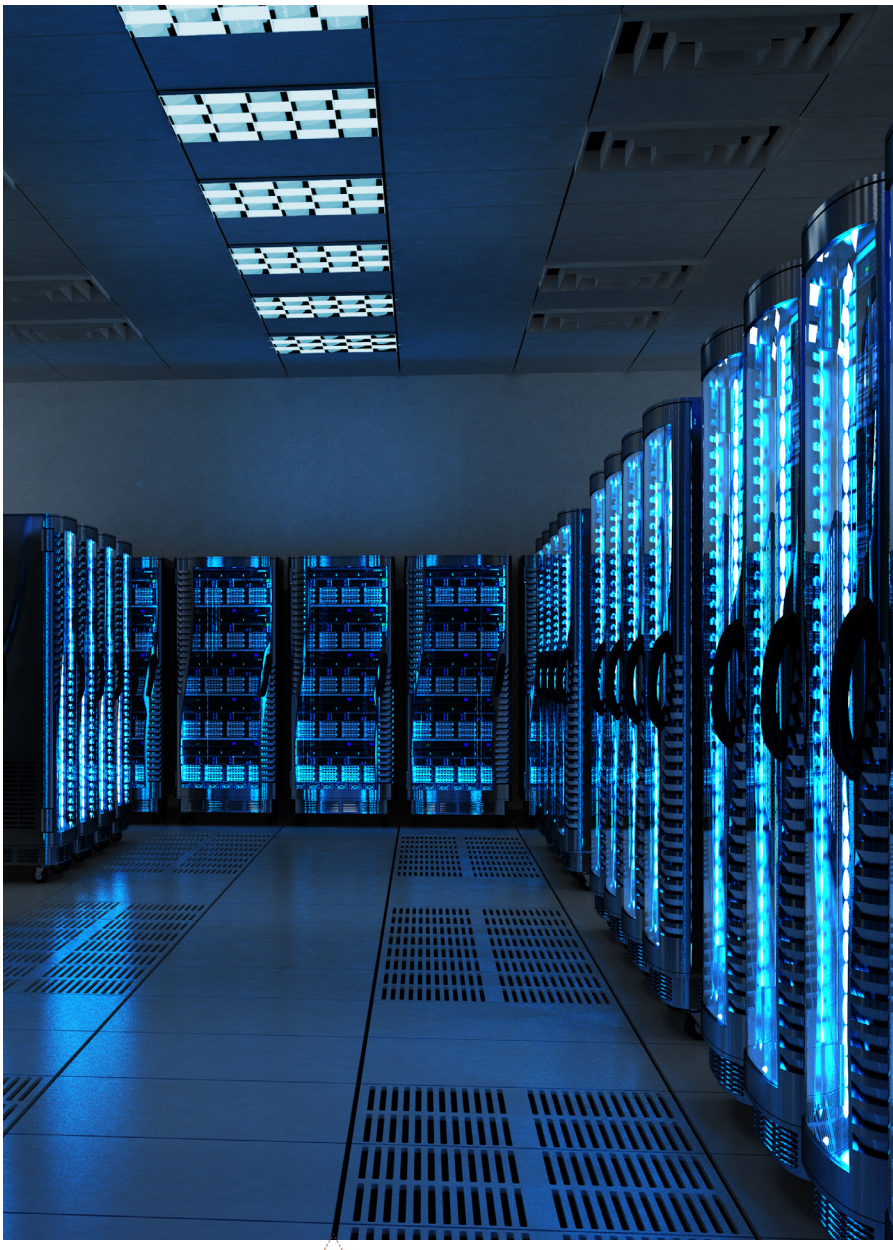
The exponential growth in the digitalisation of services, both public and private, has increased the overall attack surface of organisations. India's cyber environment is going through a rapid transition which is further exposing vulnerabilities across the system. Organisations across the world are witnessing an increase in both the scope and frequency of cyberthreats.

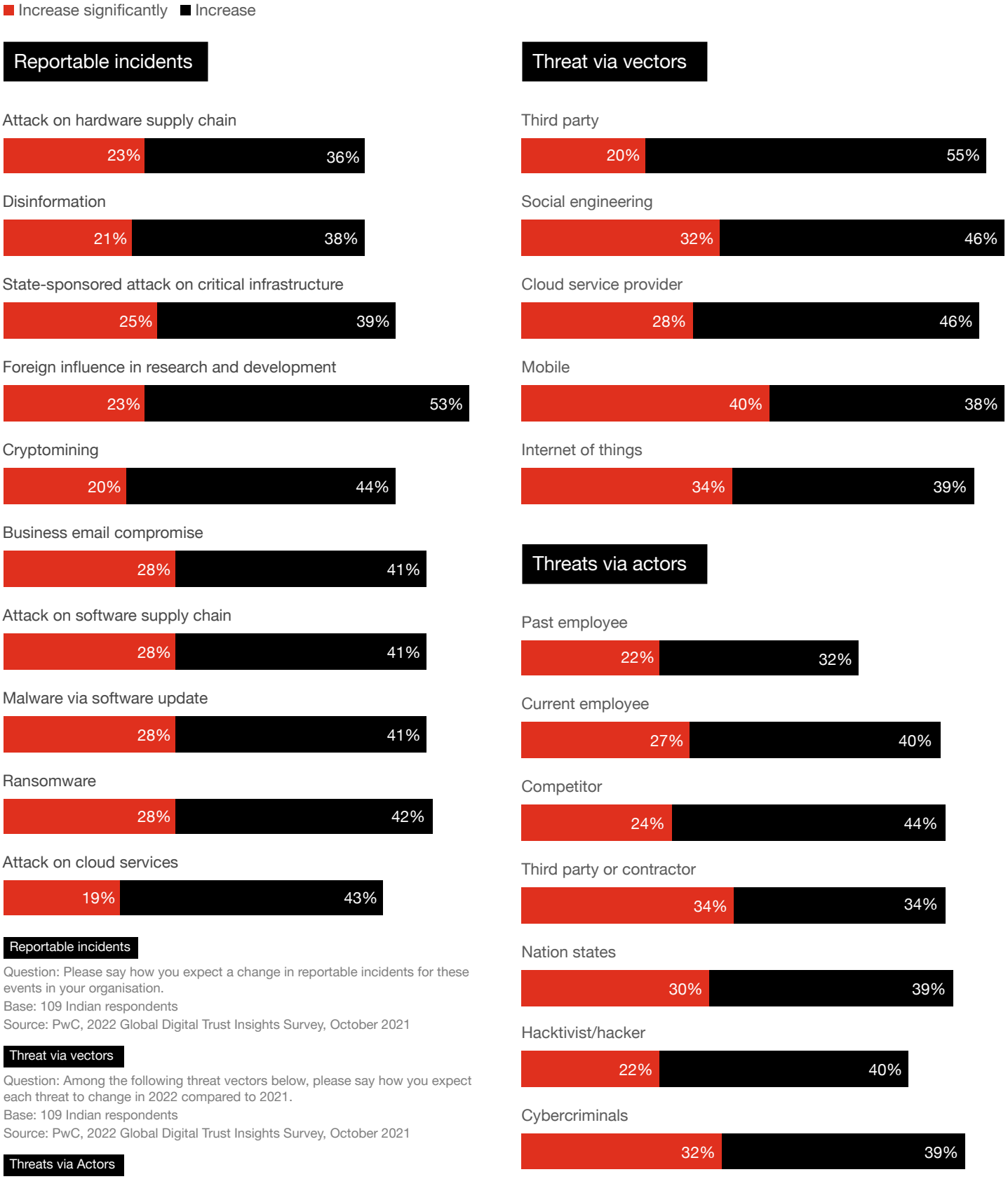
Our respondents in India have predicted that in the next 12 months, "foreign influence in research and development" (76%) and "ransomware" (70%) are among the reportable incidents that are likely to increase the most. Other incidents which are likely to increase significantly are "attack on software supply chain" (28%), "malware via software update" (28%) and "business email compromise" (28%).

Our survey respondents in India believe that mobile (78%) and social engineering attacks (78%) are likely to increase the most compared to threats via a cloud service provider, third party or the internet of things (IoT).

Indian respondents also believe that threats actors like cybercriminals (71%), nation states (69%) and third parties or contractors (68%) could pose a greater threat in future than hackers or past employees.

Thus, respondents understand that as their organisations continue to adapt to the rapidly changing cyber landscape, their systems are likely to become more vulnerable to attacks, which may result in huge financial, operational and reputational losses.





Reportable incidents

Question: Please say how you expect a change in reportable incidents for these events in your organisation.
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Threat via vectors

Question: Among the following threat vectors below, please say how you expect each threat to change in 2022 compared to 2021.
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Threats via Actors

Question: Among the following threat actors below, please say how you expect each threat to change in 2022 compared to 2021.
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Securing organisations against the most important risks of today and tomorrow

Organisation leaders have realised the significance of business information and the need to safeguard it. They have shifted the focus of their risk management efforts to not only mitigating risks but also seeking opportunities by building greater trust with customers. Today's data environment is characterised by structural power imbalances. Those with access to large pools of data – often data about customers – can leverage the value of aggregated data to create products and services that help in better business decision making.

In a world where data is constantly accumulating, organisations must implement sound security practices, making sure that data is accurate and secure so that it can be relied upon for making business decisions. At the same time, they need to reassure customers that their data is safeguarded at all times.

When asked about the foundations of a data trust, only four out of ten respondents said that they have implemented formal and mature data trust practices in four key areas – governance, discovery, protection and minimisation.

Further, 40% of the respondents in India say that formal data governance mechanisms have been implemented in their organisation, whereas only 35% have complete visibility into where their data comes from, how it moves through their business processes and systems, and how it is transformed. This is a surprisingly low number, as without an understanding of the data landscape, an organisation cannot select an appropriate cyber risk management strategy.

Today, when methods of breaking into networks and systems have become more sophisticated, it is imperative for organisations to assure their customers and investors of the safety of their data. However, only 41 % of the respondents have in place fully implemented, formal data protection processes and technologies such as encryption, tokenisation and ability to share data securely (44%) with third parties, business partners and suppliers.

Question: For each of the following, please rate how mature your organisation's data trust practices are.
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Data is the vital resource that is fuelling the digital economy. Deploying cyber risk management processes and technologies is becoming a challenge for organisations as the amount of data they collect and process is enormous. Organisations need to rethink their strategy on data minimisation and retention, as efficient data governance practices would help them not only better protect their crown jewels but also comply with data protection regulations which have much larger implications today. However, only 35% of respondents in India say they have fully implemented formal data retention and elimination policies and procedures.

Clearly, data trust practices are yet to become the standard. Governance, discovery and protection of 'valuable' business data are critical, as this would not only increase customer and investor trust, but also boost an organisation's top line, as some of the mature businesses have learned over the years. As per our survey, organisations that implement the most advanced data trust practices are more likely to report significant progress in their cyber risk management goals.

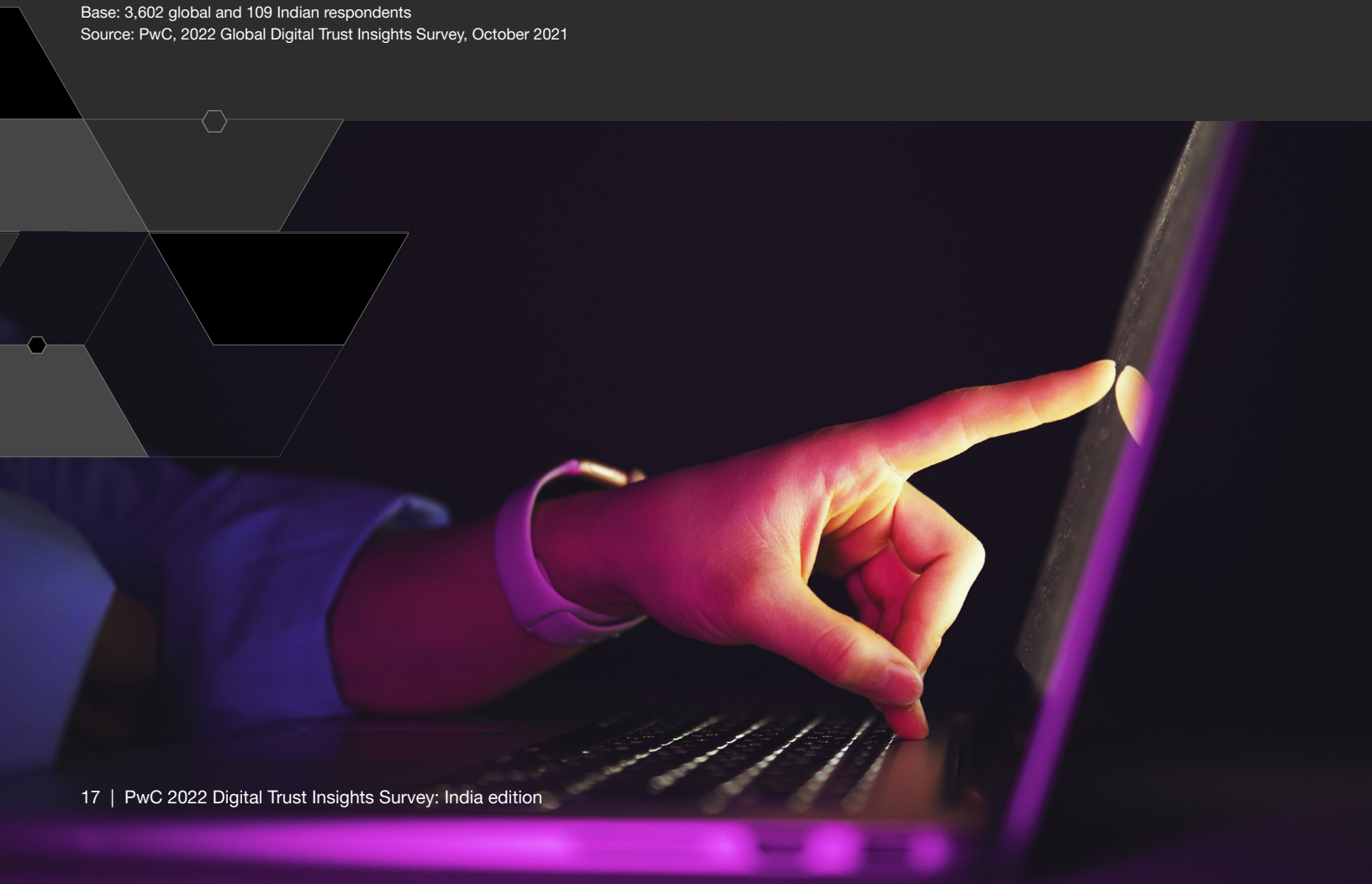
Manage downsides and seize upside opportunities by knowing evolving risks

For our survey respondents in India, the most important reasons to quantify cyber risk are “to respond to stakeholder demands to support risk management decisions and performance” and “to measure the contribution of our security capabilities to risk mitigation”. Indian organisations tend to adopt a reactive approach that focuses on managing risks in the here and now. In contrast, globally, organisations take a more strategic approach towards continuously evaluating the risk landscape and priorities against changing business objectives.

Most important reasons to quantify cyber risk

	Global	India
1	To continuously evaluate the risk landscape and priorities against changing business objectives	To respond to stakeholder demands to support risk management decisions and performance
2	To identify and justify improvements to, or transformation in, protective capabilities (including adding personnel)	To measure the contribution of the organisation’s security capabilities to risk mitigation
3	To help evaluate and communicate risks optimise in line with defined risk tolerance	To identify and justify improvements to, or transformation in, protective capabilities (including adding personnel)

Question: What are your organisation’s most important reasons to quantify cyber risk?
Base: 3,602 global and 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021



Cyber security is currently undergoing a huge shift, with data science helping organisations make informed cyber risk management decisions.

An intelligence-driven approach for cyber security risk management

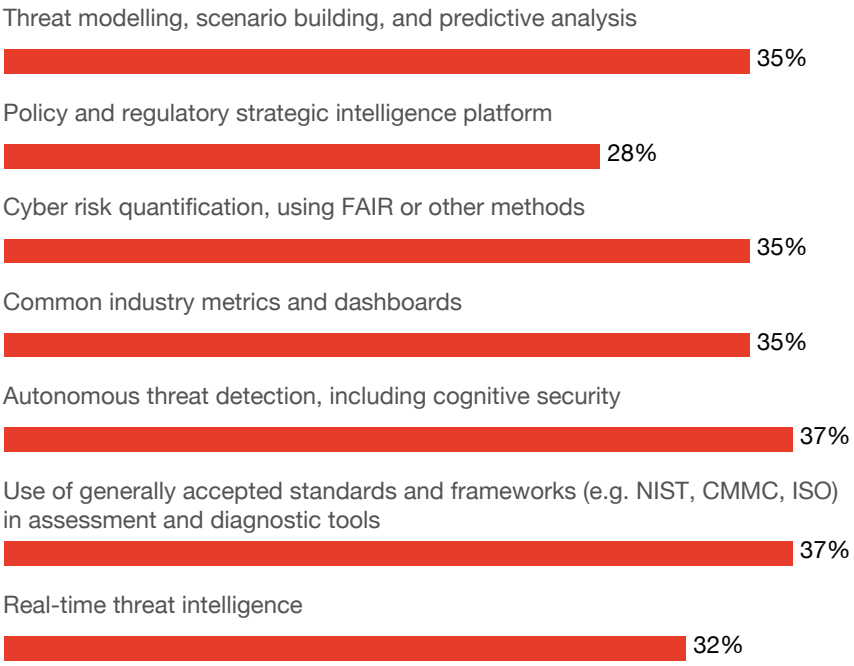
In the past few years, organisations have invested in a multitude of cyber security tools and technologies to manage their cyber risks. However, their ability to fully utilise the potential of these technologies to gain data-driven insights and make intelligent and informed decisions for cyber risk management is uncertain.

Fewer than four out of ten survey respondents say that they have integrated analytics and business intelligence tools into their operating model. These data insights can not only help organisations firm up their cyber defence but also strategise and plan their cyber budget spends in the right areas to maximise their investment returns.

Unlike their global counterparts, a majority of the organisations in India are relying on autonomous threat detection, including cognitive security and generally accepted standards and frameworks in assessment and diagnostic tools. Globally, on the other hand, organisations have realised that real-time threat intelligence tools are critical to their operating models today.

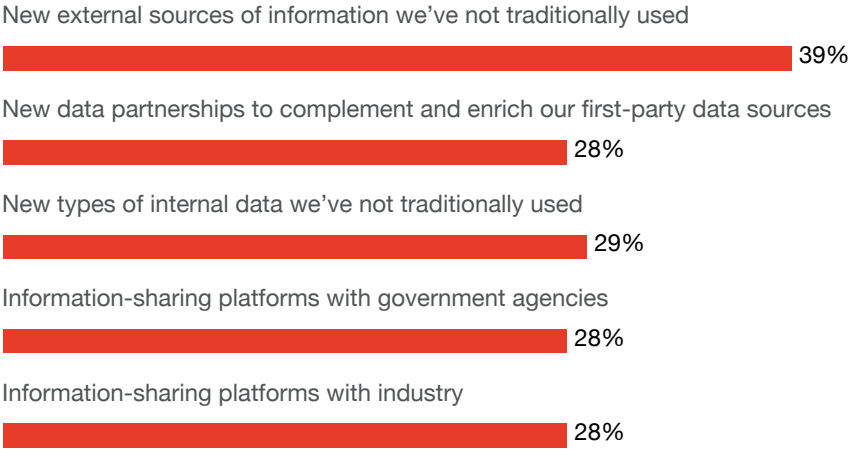
Many organisations fail to realise the benefits of today's advanced intelligence tools and approaches. New types of internal data, data from new external sources, new data partnerships and information-sharing platforms can be important sources of business intelligence. However, only about 30% of our survey respondents in India say that they are reaping the benefits of these tools.

Tools and approaches that are critical to an organisation's operating model today



Question: To what extent does your organisation use the following tools and approaches when making decisions about cyber investments and responding to cyber risk?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Percentage of organisations realising the benefits of these tools and approaches



Question: What best describes your organisation's plans for using the following tools and approaches for better operational intelligence?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Securing your ecosystem: Managing the risks posed by third parties and the supply chain

In this globally interconnected era, organisations have complex ecosystems with substantial dependence on third parties to help manage daily operations and satisfy customer needs. Unfortunately, dependence on these third parties exposes organisations to critical cyber security risks which should be continually managed.

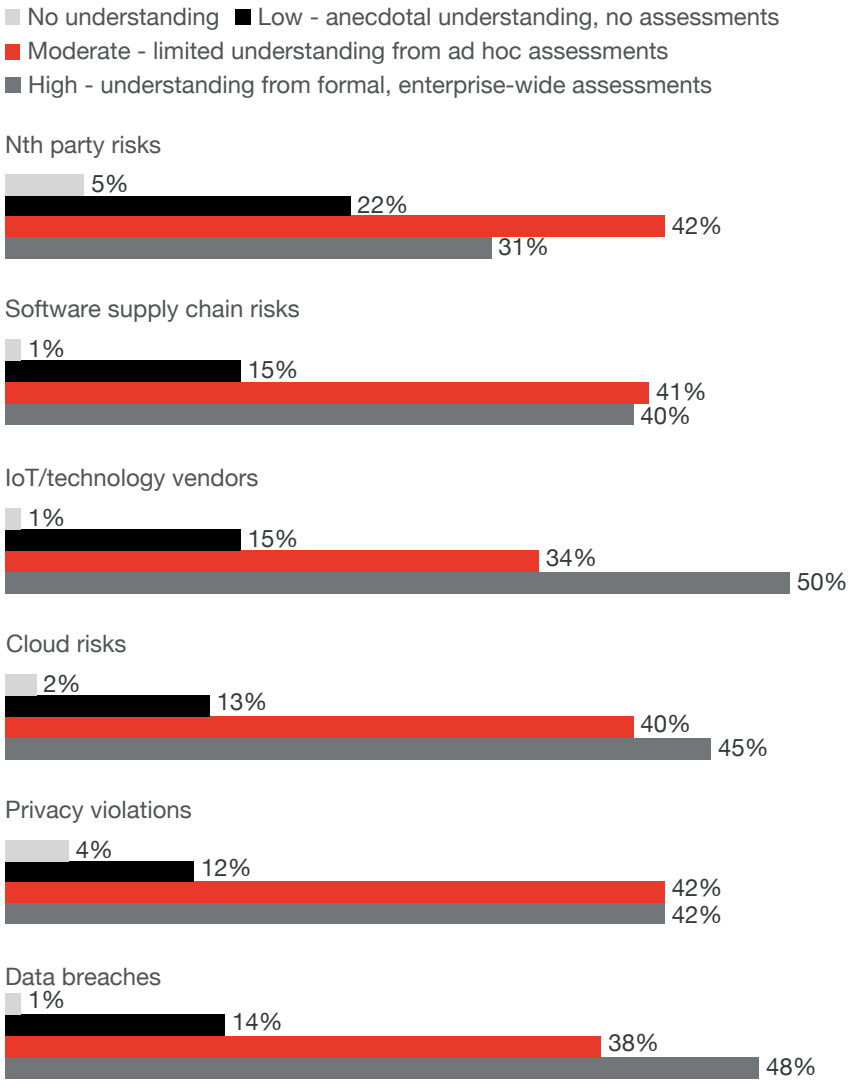
On the other hand, cyberattackers are using sophisticated techniques to identify weak links in the third-party ecosystem, target an organisation's critical assets and compromise their business-sensitive data. Despite all their investments in cyber security, organisations might be left vulnerable if they fail to secure the threats arising from third parties and the supply chain.

Our survey revealed that more than 50% of Indian respondents do not understand the risks posed by their third parties.

Only 48% of survey respondents in India say they thoroughly understand the risk of data breaches through third parties, using formal enterprise-wide assessments. Among our respondents in India, 68% expect an increase in reportable incidents in India due to attacks on the software supply chain. However, only 40% have formally assessed their software supply chain risk.

Around 30% of the survey respondents have knowledge of their Nth party risks and have formally assessed them, which essentially indicates that more complexity in the third-party chain would result in blind spots which are difficult to identify and mitigate.

Understanding within organisations of the cyber and privacy risks arising from third parties and suppliers

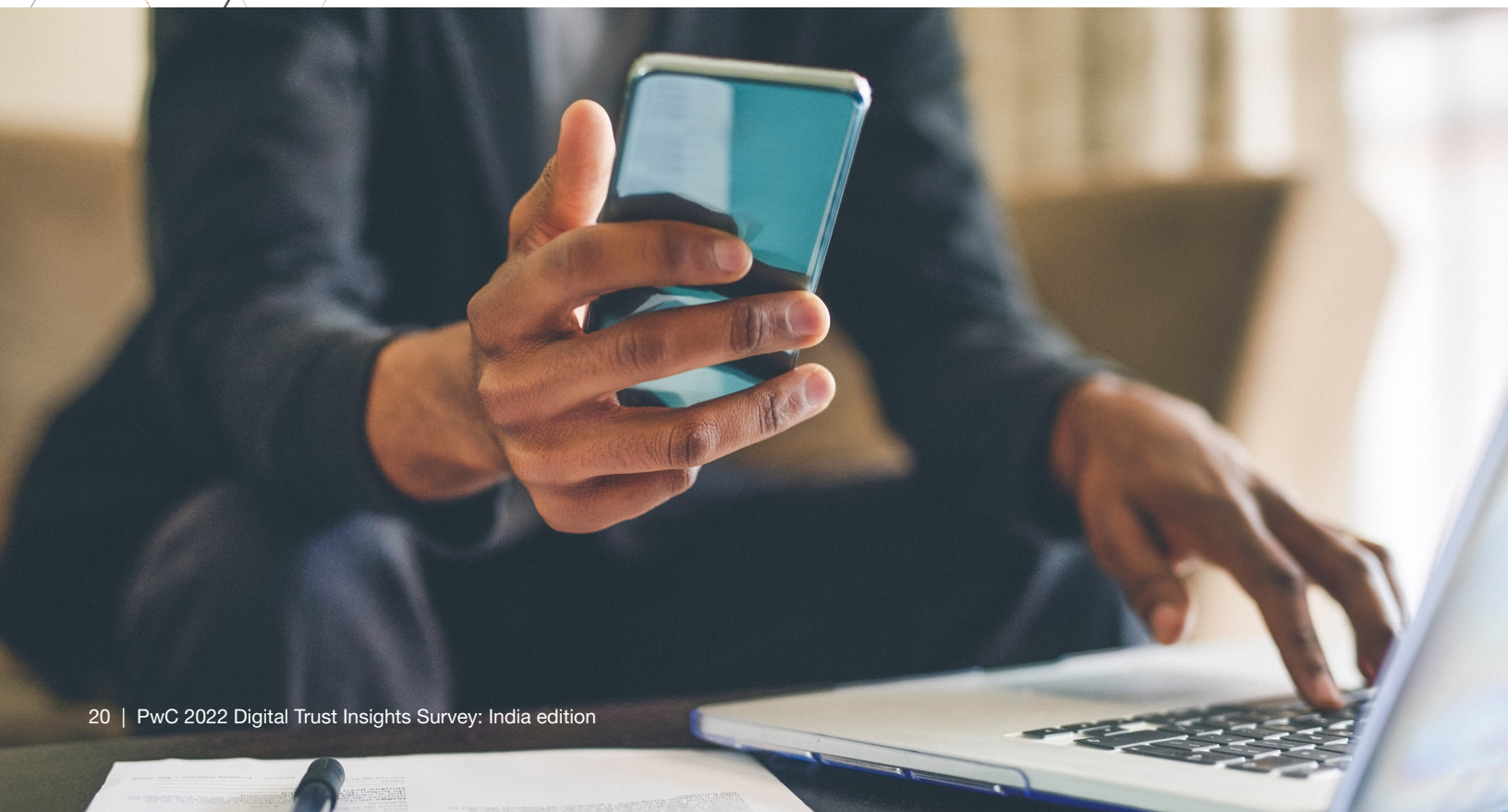


Question: What is the level of understanding within your organisation of the cyber and privacy risks arising from your third parties or suppliers across the following areas?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021

Understanding the third-party ecosystem is an absolute must. In an effort to simplify their cyber strategy, most organisations have started consolidating their vendor landscape. However, there is still a long way to go in terms of security. Indeed, 40% of our survey respondents have taken no substantial action to manage their third-party risk. Other actions are more reactive – auditing or verifying their suppliers' compliance (56%), sharing information and helping third parties in cyber defence (62%), and addressing cost-related or time-related challenges to cyber resilience – rather than proactive – refined criteria for on-boarding or off-boarding assessments of third parties (51%).

Actions taken by organisations in the last 12 months to minimise third-party and supplier risks

Question: Has your organisation done any of the following actions in the past 12 months to minimise third-party or supplier risks in your ecosystem?
Base: 109 Indian respondents
Source: PwC, 2022 Global Digital Trust Insights Survey, October 2021



About the survey

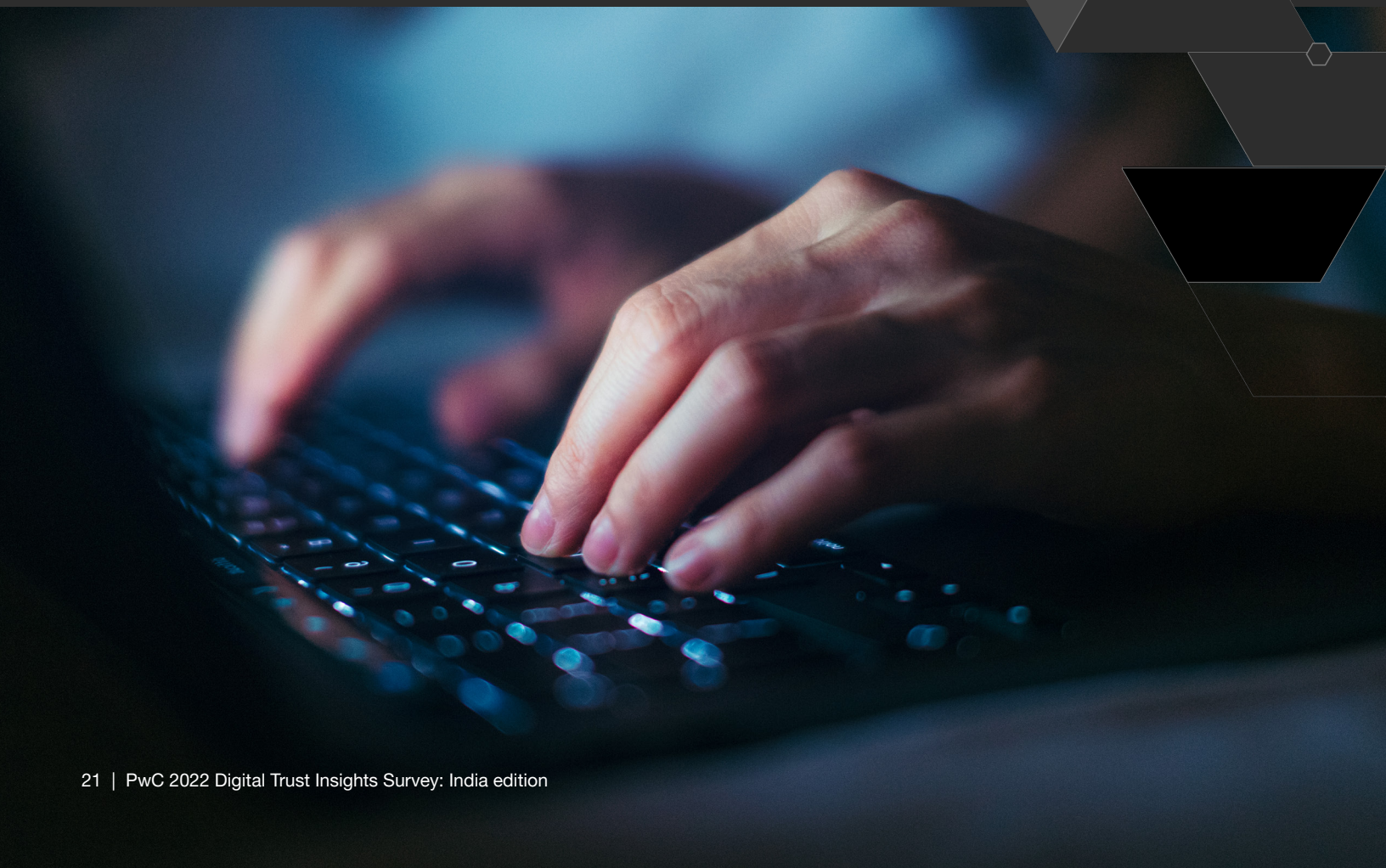
The 2022 Global Digital Trust Insights is a survey of 3,602 business, technology and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-suite officers) based in various regions. The survey was conducted in July and August 2021. The India edition of the global survey report focuses on the responses of the executives of 109 Indian business.

Seventy-six percent of the respondents are executives in large companies (USD 1 billion and above in revenues); 47% are in companies with USD 10 billion or more in revenues.

The respondents who participated in our survey belong to a range of industries: tech, media and telecom (32%); industrial manufacturing (24%); financial services (15%); retail and consumer markets (14%) and healthcare (6%).

The Global Digital Trust Insights Survey is formally known as the Global State of Information Security Survey (GSISS).

PwC Research, PwC's Global Centre of Excellence for market research and insight, conducted this survey.



Contact us

Sivarama Krishnan
Partner and Leader – APAC Cyber and India Risk Leader
PwC India
sivarama.krishnan@pwc.com

Anirban Senupta
Partner, Cyber Security
PwC India
anirban.sengupta@pwc.com

Dinesh Chowbey
Partner, Cyber Security
PwC India
dinesh.chowbey@pwc.com

Murali Talasila
Partner, Cyber Security
PwC India
murali.talasila@pwc.com

Ram Periyagaram
Partner, Cyber Security
PwC India
ram.periyagaram@pwc.com

Sangram Gayal
Partner, Cyber Security
PwC India
sangram.gayal@pwc.com

Unnikrishnan Padinjyaroot
Partner, Cyber Security
PwC India
unnikrishnan.padinjyaroot@pwc.com

Amanjit Makesh
Executive Director, Cyber Security
PwC India
amanjit.makesh@pwc.com

Rajesh Huddar
Executive Director, Cyber Security
PwC India
rajesh.huddar@pwc.com

Siddharth Vishwanath
Partner and Leader, Cyber Security
PwC India
siddharth.vishwanath@pwc.com

Amol Bhat
Partner, Cyber Security
PwC India
amol.bhat@pwc.com

Manu Dwivedi
Partner, Cyber Security
PwC India
manu.dwivedi@pwc.com

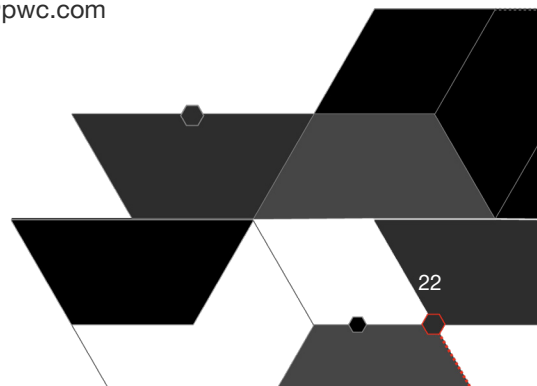
Rahul Aggarwal
Partner, Cyber Security
PwC India
rahul2.aggarwal@pwc.com

Raviraja Rao
Partner, Cyber Security
PwC India
raviraja.rao@pwc.com

Sundareshwar Krishnamurthy
Partner, Cyber Security
PwC India
sundareshwar.krishnamurthy@pwc.com

Venkateshwar Nippani
Partner, Cyber Security
PwC India
venkat.nippani@pwc.com

Prashant Mehendru
Executive Director, Cyber Security
PwC India
prashant.mehendru@pwc.com



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with over 295,000 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.

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.

Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

KS/October2021-M&C 15621