



2023 Global Digital Trust Insights Survey – China report

Chinese companies gearing up for a cyber-ready future





Contents

02 / Introduction

03 /

- 03 Section 1**
Cybersecurity maturity and threat from competitors
- 07 Section 2**
Cybersecurity disclosure plays a critical role in organisations' approach
- 12 Section 3**
Cybersecurity resilience needs to be fortified
- 18 Section 4**
Taking ownership of cybersecurity transformation

26 / Closing remarks based on the findings

27 / Contact us



Introduction

The business world as we know it saw a paradigm shift as the COVID-19 pandemic had people working from home throughout lockdowns and quarantines. The pandemic was a catalyst for accelerated digital transformation, growing the digital economy.

As we continue to see the global migration towards a more digital economy, China is reinforcing its strength in cybersecurity as the country maintained its position as the world's second-largest digital economy for several years. By June 2022, China had 1.05bn Internet users, with a penetration rate of 74.4%. The country also boasts the world's largest 5G network, and is a leader in 5G technology and standards ⁱ.

The country has taken steps to significantly shore up data security across major industries ranging from finance to telecommunications. The Ministry of Industry and Information Technology (MIIT) and Cyberspace Administration of China (CAC), among 16 governmental bodies, jointly issued an important guideline in January 2023, which set a target for China to grow its data security industry by 30% each year, to over RMB150bn (USD22.4bn) by 2025 ⁱⁱ.

Organisations and governments are leveraging the development of the digital economy and new technologies to remain competitive and relevant in the post-pandemic New Normal. With widespread digitalisation, institutions need to further develop their cybersecurity capabilities to reduce their cyber vulnerabilities while preventing or mitigating cyber risks. At the same time, organisations need to stay ahead of technological developments to avoid the hefty costs of inactions or non-compliance in the event of a crisis.

As organisations navigate both new technologies and stricter regulations, there is a heightened focus on cybersecurity. Companies can't afford to be at the centre of a data breach scandal and lose their goodwill. The results of our 2023 Digital Trust Insights Survey lay out how organisations are addressing the need for more comprehensive cybersecurity to satisfy both customers and regulators.

This China report represents the views of 133 executives based in Mainland China and Hong Kong SAR. For the purpose of this report, 'China' refers to the People's Republic of China, including Hong Kong. Where there is a statistically significant difference in the survey results between Hong Kong SAR and Mainland China, results are presented separately.



Cybersecurity maturity and threat from competitors

As China and countries across the globe further develop their digital economy, both digital and non-digital businesses alike are exposed to cyber threats. The accelerated spread of technology at an unprecedented rate means that cybersecurity has never been more important. With the rise in the number of tech companies, regulations often end up playing catch up ⁱⁱⁱ. Businesses need to take the initiative to understand their risk exposure and develop their cybersecurity in line with industry developments rather than regulations.

Considering the context of the survey period, a smaller proportion of global executives (25%) saw a decrease in their organisation’s revenue over the last six to nine months compared to Chinese executives (40%). The converse was also true – a larger proportion of global executives (59%) saw an increase in their organisation’s revenue in the same time frame compared to Chinese executives (49%). Despite historical data, executives everywhere expect an increase in their organisation’s revenue over the next 12 months (China: 77%; Global: 72%). This is likely due to economies opening up following the pandemic, as well as technological developments and adoption that will drive revenue.

Figure 1. Please indicate the actual and expected change in your organisation’s revenue.

Over the next 12 months

	Global	China	Mainland China	Hong Kong
NET: Decrease	13%	14%	10%	27%
NET: Increase	72%	77%	80%	67%



Technological developments will transform all industries, and governments, especially the Chinese government, are cracking down on cybersecurity. Following its implementation in 2017, China's Cybersecurity Law has been strictly enforced. As China deliberates updates to the law, further tightening of the law with higher penalties for violations and more responsibility for critical information infrastructure operators can be anticipated^{iv}.

In order to reinforce its national strength in cybersecurity, China has also established a national strategy on cybersecurity, bringing a number of laws and regulations in this area into effect. China's Data Security law came into effect in September 2021, requiring localisation of data collected on Chinese citizens by foreign and domestic entities. It was soon followed by the implementation of the Personal Information Protection Law (PIPL), the first of its kind, in November 2021, and Chinese organisations have had to ensure compliance with the new regulations.

With increased exposure to technology and a stricter regulatory environment, we can see a higher proportion of Chinese executives plan for an increase in their organisation's cyber budget for 2023 compared to executives globally (China: 73%; Global: 65%). A mere 11% of Chinese executives anticipate a decrease in their budget (Global: 17%). 31% of Chinese companies will have their cyber budget increase by 6-10%, while only 23% of global organisations will see the same. 9% of Chinese organisations will see an increase of 15% or more.



Figure 2: How is your organisation's cyber budget changing in 2023?

Changes to organisation's cyber budget in 2023

	Global	China	Mainland China	Hong Kong
NET: Decrease	17%	11%	10%	17%
NET: Increase	65%	73%	76%	63%
Decrease by 15% or more	2%	1%	0%	3%
Decrease by 11-14%	3%	1%	1%	0%
Decrease by 6-10%	5%	5%	5%	7%
Decrease by 5% or less	6%	5%	4%	7%
Unchanged	13%	10%	9%	13%
Increase by 5% or less	23%	21%	17%	33%
Increase by 6-10%	23%	31%	35%	17%
Increase by 11%-14%	11%	12%	15%	3%
Increase by 15% or more	8%	9%	9%	10%

In terms of the characteristics of their budget allocation for cybersecurity activities over the next 12 months, the vast majority of Chinese CEOs say their cyber budget is informed by the quantification of cyber risks, reflects on their cyber priorities, and is adequate to help create value for their organisation, to a greater extent than their global counterparts.

Figure 3: Considering the following statements, to what extent do they accurately represent your organisation's cyber budget over the next 12 months?

Respondents who stated 'To a great / some extent'

	Global	China	Mainland China	Hong Kong
Is aligned with the business strategy	91%	93%	95%	87%
Reflects our cyber priorities	92%	96%	96%	97%
Is adequate for cybersecurity to help create value for my organisation	91%	96%	96%	97%
Is balanced between our current and long-term needs	91%	95%	96%	90%
Is informed by quantification of cyber risks	91%	97%	97%	97%
Considers the risk appetite of the organisation	91%	92%	92%	93%
Is allocated well against the risks that our organisation faces	92%	95%	94%	100%

Chinese and international organisations alike were impacted by an increase in their exposure to cyberattacks due to the acceleration of digitisation since 2020, whether it be from cloud migration, the move to e-commerce and digital service delivery methods, the convergence of IT and operational technology, or the use of digital currencies for other global organisations, among others. Mainland China perceives an increase in external demand for disclosures of cyber incidents and practices, especially as the current law calls for disclosure and transparency in cyber incident response and breach management by domestic corporations. At the same time, Hong Kong and global executives saw more challenges in the quality of internal reporting for their organisation's cyber exposure.

Figure 4: Which of the following has your organisation experienced since 2020?

Impacts experienced by organisations since 2020 (Ranked index)

	Global	China	Mainland China	Hong Kong
Increase in the organisation's exposure to cyber attacks due to increased digitisation (e.g. migration to cloud, move to e-commerce and digital service delivery methods, use of digital currencies, convergence of IT and operational technology etc.)	1st	1st	1st	1st
Challenges in the quality of internal reporting on the organisation's cyber exposure	2nd	3rd	3rd	2nd
Increase in external demand for disclosures of cyber incidents and practices	3rd	2nd	2nd	3rd
Increase in cyber breaches into our systems	4th	4th	4th	4th
Changes in the geopolitical environment that have made our organisation a target	5th	5th	5th	5th
Heightened regulatory investigations or enforcement action or litigation	6th	6th	6th	6th



Cybersecurity disclosure plays a critical role in organisations' approach

As the digital economy grows further, governments across the world are constantly trying to keep up with new developments and implement regulations to protect the public. Regulations such as the US' Cybersecurity Incident Reporting for Critical Infrastructures Act of 2022 requires companies to report significant cyber incidents while providing incentives for reporting. China also has its own Cybersecurity Law which includes mandatory reporting for breaches as well as penalties for compliance failures^v.

Following the COVID-19 outbreak, the world saw a drastic pivot towards the digital economy, partly as a result of people spending more time with their mobile devices and more companies migrating to hybrid work model. Between that and the tightening regulatory environment, since 2020, Chinese organisations experienced numerous challenges. Among the top were challenges in the quality of their internal reporting on cyber exposure, and an increase in external demand for disclosures of cyber incidents and practices. On one hand, some likely adopted a 'prevention is better than cure' mindset as they attempt to establish a comprehensive set of policies to ensure extensive internal reporting that both stay ahead of regulations and prevent cyber incidents that would require disclosure, potentially tarnishing their reputation. On the other, some organisations likely struggled to keep up with the latest regulations and ensure their processes are compliant.

Organisations have reinforced their cybersecurity and maintained a cautious attitude since 2020. Among impacts that Chinese and global organisations have experienced, heightened regulatory investigations or enforcement action or litigation was ranked last.

When it comes to stakeholder prioritisation for Chinese organisations, while the CEO and the board take up the first two spots, government agencies responsible for cybersecurity responses and regulators for consumer protection are third and fourth. This aligns with the heightened disclosure requirements Chinese organisations are facing since regulations like the Cybersecurity Law, Data Security Law and PIPL have come into effect.

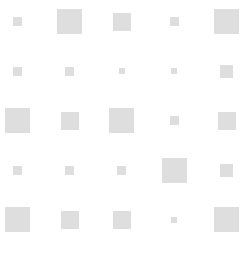
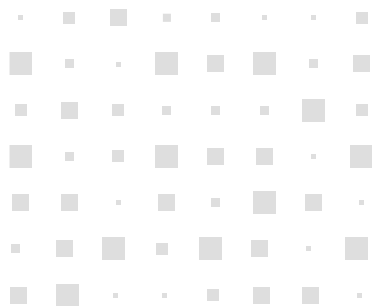


Figure 5: Thinking about reporting to each of the following stakeholders, please rank these stakeholders in order of priority for your organisation to address over the next 12 months.

Organisation priority in terms of addressing stakeholders (Ranked index)

	Global	China	Mainland China	Hong Kong
Board	1st	2nd	2nd	1st
CEO	2nd	1st	1st	2nd
Value chain participants	3rd	8th	8th	8th
Regulators for consumer protection	4th	4th	4th	3rd
Agencies responsible for national or federal cybersecurity responses	5th	3rd	3rd	7th
Industry regulators	6th	6th	5th	5th
Consumer and other private advocacy groups	7th	7th	6th	10th
Regulators of financial reporting	8th	5th	6th	4th
Agencies responsible for local cybersecurity responses	9th	10th	6th	6th
Law enforcement agencies	10th	9th	6th	9th

Chinese organisations tend to have a stronger response to regulatory changes with a closer adherence to regulations. A larger proportion of Chinese executives agree, or strongly agree, that their organisation has the ability to disclose cyber practices, strategy and incidents externally, when compared to their global counterparts. In particular, 86% of Chinese organisations can provide the required information about a material or significant incident within the required reporting period after the incident and 88% can effectively assess the materiality of a cyber incident for the purposes of reporting.

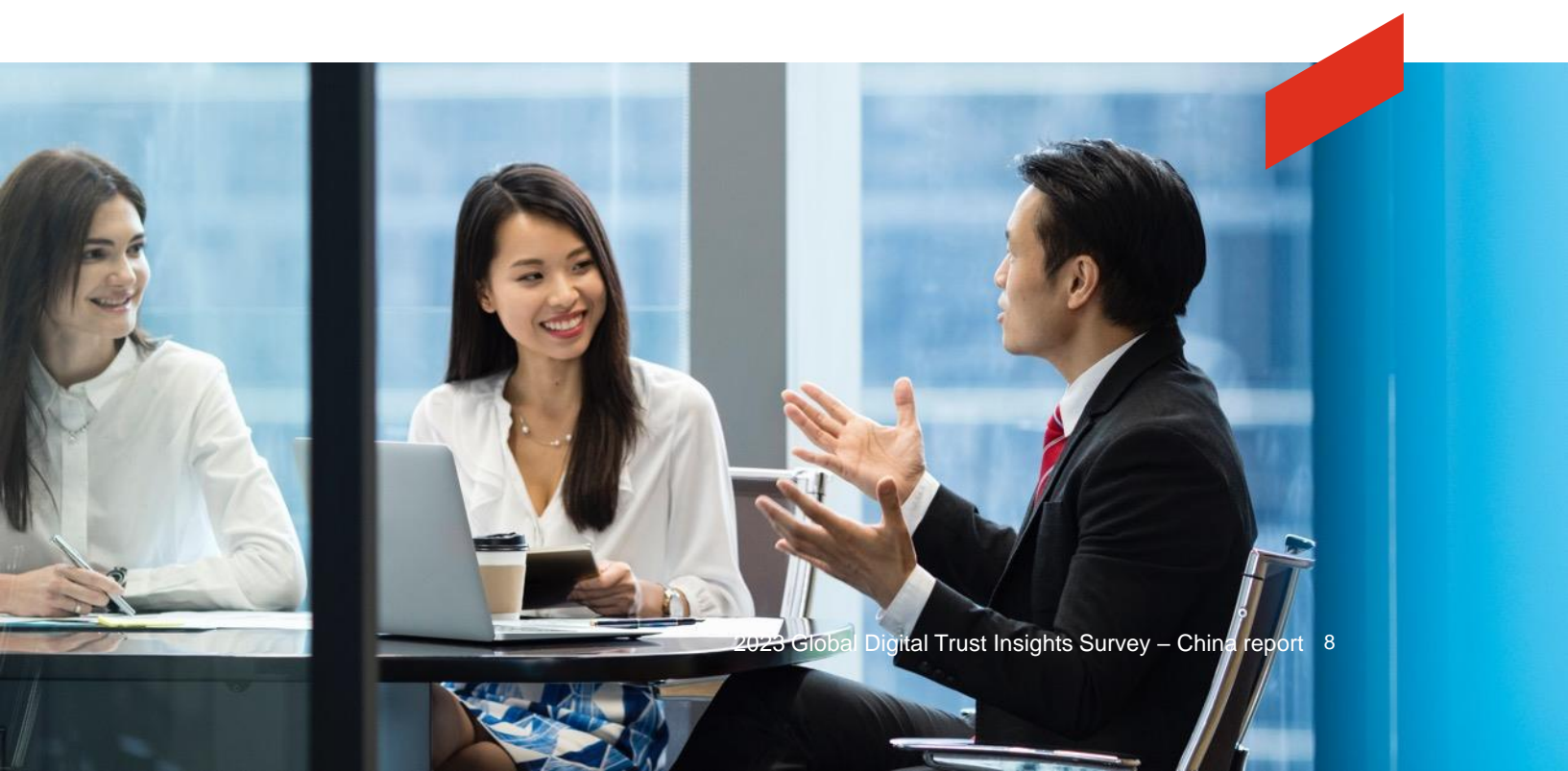


Figure 6: To what extent do you agree or disagree with the following statements regarding your organisation's ability to disclose cyber practices, strategy and incidents externally?

**Organisation's ability to disclose cyber practices, strategy and incidents externally
Respondents who stated 'Strongly agree / Agree'**

	Global	China	Mainland China	Hong Kong
My organisation can provide the required information about a material or significant incident within the required reporting period after the incident.	81%	86%	85%	87%
My organisation can effectively assess the materiality of a cyber incident for the purposes of reporting.	80%	88%	88%	87%
My organisation can describe the relevant cyber expertise on our board for the purposes of reporting.	78%	82%	82%	83%
My organisation has a policy stating which information can or cannot be disclosed regarding cyber incidents.	76%	84%	87%	73%
My organisation can provide information about third-party cyber risk management.	75%	85%	85%	83%

While looking at how organisations manage and disclose internal risks, with the growing popularity of managed services, it's critical for organisations to understand the scope of their risk exposure beyond the primary level. With the focus on risk increasing globally, we can see there is a clearer picture on risk transparency across organisations and along the value chain where third-party entities are involved. 85% of Chinese executives say that their organisation can provide information about third-party cyber risk management – 10 percentage points more than that of global executives. This is critical as 41% of Chinese organisations expect third-party breaches to significantly increase in 2023 when compared to 2022.



Figure 7: For each of the pathways by which adversaries can gain access to your systems, please select those that you expect to significantly affect your organisation in 2023 compared to 2022.

Pathways that adversaries will significantly affect organisations

	Global	China	Mainland China	Hong Kong
Mobile devices	41%	32%	33%	27%
Email	40%	27%	25%	33%
Cloud-based pathways	38%	44%	43%	47%
Web applications	37%	45%	43%	53%
Humans or user (insider or social engineering)	37%	37%	39%	30%
Third-party / nth party	34%	41%	38%	53%
Endpoints (desktops, laptops)	33%	42%	44%	37%
Software supply chain or access	32%	37%	35%	43%
Remote access portals	32%	34%	33%	37%
Internet of Things	29%	34%	36%	27%
Operational technology	26%	44%	45%	43%



In this increasingly digital economy, Chief Information Security Officers (CISOs) have been designated the responsibility of managing third-party risks. As organisations manage sensitive customer data, it’s comforting to know that they have policies in place to manage and govern customer data. Among these practices, the majority of organisations vet third parties and partners with whom they share customer data; however, a larger proportion of Chinese organisations do so more frequently (China: 82%; Global: 78%). Considering the recent implementation of the PIPL, such behaviour is expected to continue as data privacy will be at the forefront for all CISOs.

Figure 8: To what extent does your organisation implement the following policies and practices related to the management and governance of customer data?

Respondents who stated ‘Always / Frequently implement’

	Global	China	Mainland China	Hong Kong
We only use customer data when we have express consent	79%	78%	83%	60%
We vet all the third parties and partners with whom we share customer data	78%	82%	83%	77%
New products and services go through a data security and privacy evaluation before launch	79%	83%	83%	80%
We apply an ethical framework to guide our use of customer data for various use cases	77%	74%	75%	70%
We have a specific timeframe to respond to customers' requests related to the information we keep on them	77%	74%	76%	70%
Where regulations do not exist, we self-regulate through policies, guiding principles, and values	77%	77%	82%	63%
We follow an opt-in, privacy-first strategy in our marketing efforts	77%	80%	83%	73%
We limit, anonymise, and redact data collected through IoT / sensors / smart devices	70%	73%	75%	67%
We use the newest techniques (e.g. differential privacy) to pseudonymise our customers' data	72%	73%	76%	63%
We check for dark patterns in the way we design our customer-facing applications	68%	76%	82%	57%



Cybersecurity resilience needs to be fortified

Over the years, cybersecurity has become a dynamic field – rapidly shifting to keep pace with innovative business practices. As an integral part of operations, businesses need to ensure they have enough cybersecurity resilience to manage unexpected problems. Without resilience, cyber incidents can derail most, if not all, plans for business success, leading to financial losses, reputational damage and loss of trust.

Assessing and preparing for risks in 2023 tests executives' ability to work together, and lay out a plan that mitigates large-scale crises and avoids business disruption. Among the range of threats anticipated and accounted for in resilience plans, global organisations ranked a catastrophic cyberattack as the top. Chinese executives, on the other hand, at the time of the survey, ranked this third, after a resurgence of COVID-19 or a new health crisis and a looming global recession. Although this might have changed following Mainland China's economic re-opening in December 2022 and the elimination of the majority of the country's restrictive COVID-19 control measures.

It's no surprise that Chinese respondents are prioritising plans for a new health crisis as the COVID-19 pandemic drastically affected the country's economic landscape and shaped its path to digital transformation in the past three years. To navigate the short-term domestic challenges after China's COVID-19 policy adjustment and economic reopening, Chinese organisations not only need to account for anticipated events in their risk plans, but they also need to build resilience through these plans, including their capacity to withstand unanticipated cyberattacks.



Figure 9: Thinking about overall risks to your organisation over the next 12-24 months, please rank the top five scenarios that you are formally incorporating into your organisational resilience plans.

Top five scenarios formally incorporated into organisation's resilience plans (Ranked index)

	Global	China	Mainland China	Hong Kong
A catastrophic cyber attack	1st	3rd	3rd	2nd
Global recession	2nd	2nd	1st	8th
A resurgence of COVID-19 or a new health crisis	3rd	1st	2nd	1st
Inflationary environment	4th	5th	5th	4th
Supply chain bottlenecks	5th	6th	6th	3rd
A new geopolitical conflict	6th	8th	11th	5th
Commodity market volatility	7th	4th	4th	9th
Credit crunch / significantly reduced access to capital	8th	12th	9th	13th
Significant churn in our workforce	9th	9th	8th	10th
Social instability	10th	7th	7th	12th
A natural disaster or extreme weather event	11th	10th	10th	10th
Sanctions enforcement	12th	11th	12th	6th
A food crisis	13th	13th	13th	6th

The good news is businesses are already building cybersecurity resilience – their continuous effort, as guided by China’s cybersecurity regulations, are paying off. Cybersecurity has progressed on many fronts in the past 12 months. In that time frame, in line with their global counterparts, Chinese executives agree, or strongly agree, that their cybersecurity teams have achieved numerous accomplishments that reinforce their cybersecurity resilience in areas such as improved operational technology security (86%), increased value and efficiency of cyber resources (84%), and orchestrated cross-functional effort to comply with new regulations (84%). Over 77% of Chinese organisations saw these accomplishments, higher than the global level.

Figure 10: Please indicate whether or not your organisation’s cybersecurity team has accomplished the following in the past 12 months.

Cybersecurity team accomplishments in the past 12 months (Respondents who stated ‘Yes’)

	Global	China	Mainland China	Hong Kong
Improved operational technology security	79%	86%	90%	73%
Improved our ability to defend against ransomware	77%	82%	83%	77%
Helped the business design “security and privacy” into new products and services	75%	83%	83%	80%
Increased the value and efficiency of cyber resources	75%	84%	83%	87%
Improved collaboration with OT / engineering	73%	83%	85%	77%
Responded effectively to a breach or attack while ensuring no significant disruption and/or harm to our operations	72%	83%	89%	63%
Anticipated a new cyber risk related to digital initiatives that allowed us to manage it before it affected our partners or customers	71%	83%	86%	73%
Improved supply chain risk management	70%	77%	81%	63%
Orchestrated cross-functional effort to comply with new regulation	70%	84%	87%	73%
Detected a significant cyber threat to our business and prevented it from affecting our operations	70%	81%	83%	77%

In an interconnected world with growing complexity, risks can arise from any area. As it is impossible to completely safeguard against cyber risk^{vi}, taking an ‘all hazards’ approach for identifying sources of disruption is necessary for every organisation. More than seven in ten Chinese organisations surveyed (73%) have developed a broad understanding of the risks they face, while 65% have formally co-ordinated and integrated business continuity and recovery, a larger proportion than the global average of 62% and 52%, respectively. Nevertheless, organisations need more flexibility, beyond what is currently employed, to further enable cybersecurity resilience.

In a fast-paced digital world, speed and adaptability are essential for enterprises to achieve their objectives. With tougher and increasingly unconventional cyber challenges ahead, businesses need to maintain a level of agility to enable quick and appropriate responses. Only 44% of Chinese organisations are promoting an integrated and agile operating model that can respond to a diverse set of disruptive events. This means the majority are using individual, pre-defined plans and tactical processes designed for responding to specific disruptions that may not account for large-scale unexpected disruptions in a holistic manner.

There’s still room to further improve cybersecurity resilience. Chinese organisations need to accelerate the development of anticipatory plans that will enable businesses to tackle incidents proactively rather than reactively, while considering risks beyond high-priority critical systems. Similar to their global counterparts, only about half of Chinese organisations (52%; Global: 53%) take an anticipatory and preventative approach by assuming that incidents will occur and embedding resilience capabilities, including threat intelligence, to anticipate and withstand an occurring disruption. Less than half of the Chinese organisations (47%; Global 44%) consider secondary and tertiary dependencies.

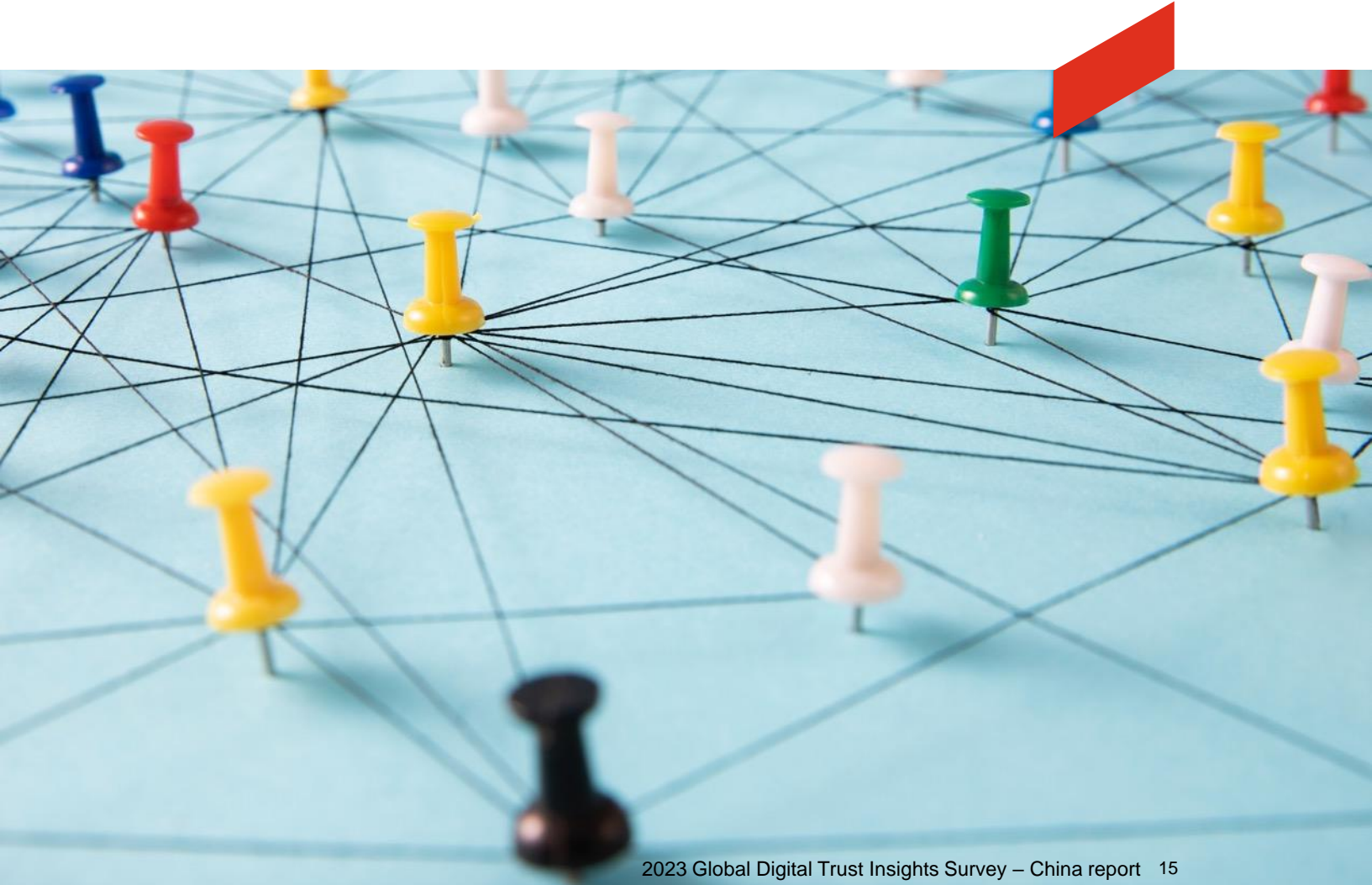
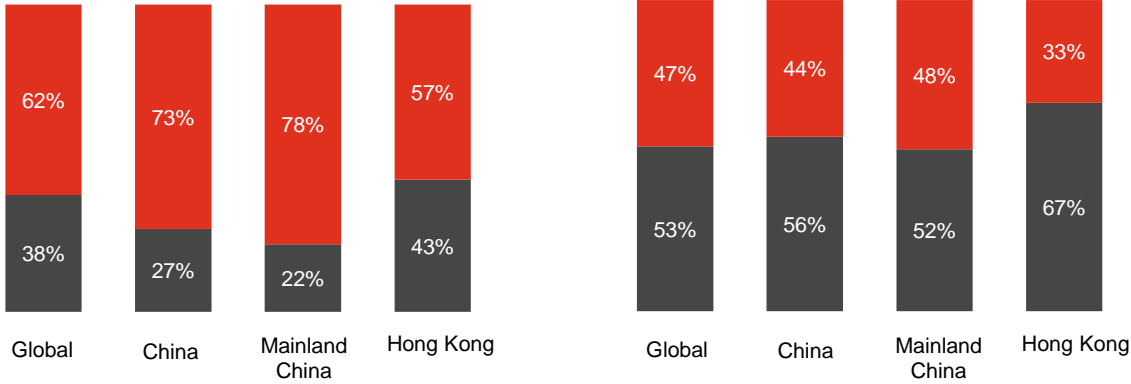


Figure 11: More than six in ten organisations develop a broad understanding of the risks they face, but there's more still to do to promote an integrated, agile operating model and to consider more than just high priority critical systems in cyber resilience.

Current cyber resilience approach and capability

- Develops a broad understanding of risks that corporations now face, and how to continue operations amid simultaneous risks across the entire organisation
- Promotes an integrated and agile operating model that can respond to a diverse set of disruptive events
- Focuses on isolated risk scenarios and how to address recovery for that specific disruption
- Uses individual, pre-defined plans and processes designed for responding to specific disruptions



- Takes an anticipatory and preventative approach by assuming that incidents will occur, and embedding resilience capabilities to withstand an occurring disruption
- Considers secondary and tertiary dependencies, not only high-priority critical systems and processes, that the organisation relies upon
- Reacts to a disruption by invoking plans after an incident, and focusing on recovery to return to business operations after a failure or incident
- Considers high-priority critical systems and operations required for continued operations

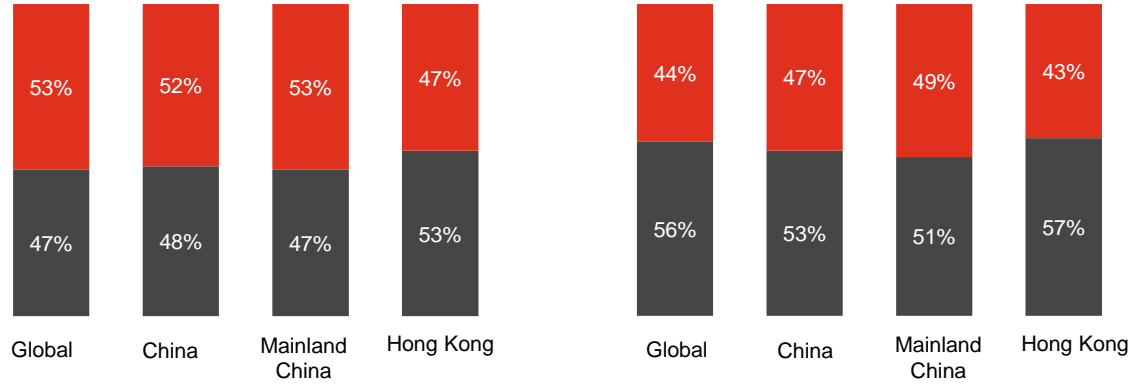
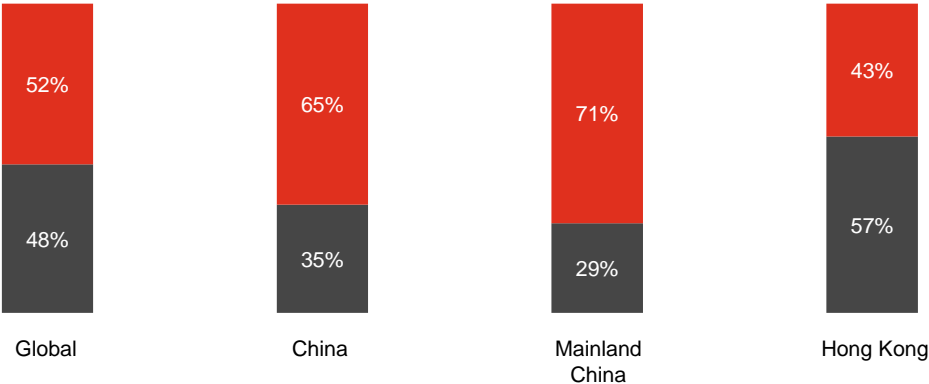


Figure 11: More than six in ten organisations develop a broad understanding of the risks they face, but there's more still to do to promote an integrated, agile operating model and to consider more than just high priority critical systems in cyber resilience.

Current cyber resilience approach and capability

- Formally coordinates and integrates business continuity / disaster recovery, crisis management, incident preparedness / response, and threat intelligence
- Addresses recovery and business continuity in an independent manner with individual platform and service teams





Taking ownership of cybersecurity transformation

Cybersecurity transformation involves numerous moving parts and various stakeholders, among which, the CEO and the board are prioritised. As employees are answerable to the CEO and the CEO is answerable to the board, it is critical for cybersecurity teams to involve the board and senior management in discussions about the company's cyber risk strategy.

China's Cybersecurity Law reinforces the importance of corporate leaders maintaining accountability and responsibility for cybersecurity within their respective organisations. Corporate leaders identified as directly responsible for serious network security incidents can be held personally liable for such breaches and would need to settle fines imposed out of pocket.

The survey indicates that senior executives are held accountable for various cybersecurity issues. Globally, while CEOs are involved in cyber matters, CISOs wield the most influence over several areas of cybersecurity. In terms of responsibilities, while the trend in China mostly aligns with that across the world, Hong Kong is seeing a different story play out.

In global and Mainland Chinese organisations, CISOs are primarily responsible for numerous cyber activities, namely: reporting on cyber and privacy risks to the board and senior management (Hong Kong: CIO); coordination on cyber incident response (Hong Kong: CDO); deciding on purchases of security solutions and technologies (Hong Kong: CIO); communicating with external stakeholders on cyber matters (Hong Kong: CEO); managing third-party risks (Hong Kong: CIO); evaluating the cyber risks associated with business decisions (Hong Kong: CIO); cyber due diligence of M&A targets (Hong Kong: CIO); cyber insurance coverage and policies (Hong Kong: CIO); and securing operational technology/ industrial internet of things (Hong Kong: CIO).

Compared to their global and Mainland Chinese counterparts, Hong Kong CIOs head up more areas of cybersecurity. We also see that global and Mainland Chinese CISOs are more empowered to advocate, collaborate, and orchestrate a better cyber future.

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

*** Top three responses shown**

Reporting on cyber and privacy risks to the board and senior management

Global	China	Mainland China	Hong Kong
CISO 21%	CISO 30%	CISO 34%	CIO 27%
CIO 16%	CIO 14%	CDO 13%	CEO 17%
CEO 13%	CEO 12%	CEO 11%	CISO 17%
CFO 7%	CDO 11%	CIO 11%	CDO/CPO 7%

Securing software development operations (DevOps secured by DevSecOps)

CIO 19%	CISO 29%	CISO 29%	CIO 30%
CISO 17%	CIO 19%	CIO 16%	CISO 27%
CTO 11%	CTO 13%	CTO 14%	CTO 10%
CEO 10%	CEO 8%	CEO 9%	CFO/Head of Engineering / Operations 7%

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

*** Top three responses shown**

Coordination on cyber incident response

Global	China	Mainland China	Hong Kong
CISO 25%	CISO 32%	CISO 37%	CDO 17%
CIO 17%	CIO 17%	CIO 17%	CIO 17%
CEO 11%	CEO 12%	CEO 12%	CISO 17%
CDO 8%	CDO 9%	CDO 7%	CEO 13%

Deciding on cyber budget

CFO 20%	CFO 26%	CFO 28%	CIO 20%
CEO 17%	CISO 23%	CISO 24%	CISO 20%
CIO 14%	CIO 11%	CEO 10%	CFO 17%
CISO 14%	CEO 10%	CIO 9%	CTO 13%

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

*** Top three responses shown**

Managing data governance and privacy

Global	China	Mainland China	Hong Kong
CIO 16%	CIO 21%	CDO 20%	CIO 30%
CDO 15%	CISO 18%	CISO 19%	CISO 13%
CISO 15%	CDO 17%	CIO 18%	CEO 10%
CEO 12%	CPO 11%	CPO 12%	CPO 10%

Deciding on purchases of security solutions and technologies

CISO 20%	CISO 27%	CISO 30%	CIO 27%
CIO 17%	CIO 15%	CFO 16%	CTO 20%
CEO 13%	CFO 14%	CIO 12%	CISO 17%
CFO 11%	CTO 11%	CEO 10%	CFO/COO/CRO 7%

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

* Top three responses shown

Communicating with external stakeholders on cyber matters

Global	China	Mainland China	Hong Kong
CISO 19%	CISO 20%	CISO 21%	CEO 27%
CIO 17%	CIO 16%	COO 16%	CIO 23%
CEO 16%	CEO/COO 14%	CIO 14%	CISO 13%
CDO 8%		CDO 11%	CFO 10%

Managing third-party risks

CISO 18%	CISO 20%	CISO 24%	CIO 30%
CIO 15%	CIO 17%	CEO 14%	CRO 17%
CEO 12%	CEO 13%	CIO 14%	CDO 10%
CRO 10%	CDO/CRO 11%	CDO 11%	CEO 10%

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

* Top three responses shown

Evaluating the cyber risks associated with business decisions

Global	China	Mainland China	Hong Kong
CISO 23%	CISO 30%	CISO 34%	CIO 27%
CIO 15%	CIO 17%	CEO 15%	CISO 17%
CEO 12%	CEO 12%	CIO 15%	CRO 13%
CRO 8%	CDO 10%	CDO 11%	CDO/CIRO/GC 7%

Cyber due diligence of M&A targets

CISO 17%	CISO 23%	CISO 27%	CIO 27%
CIO 17%	CIO 18%	CIO 16%	CDO 10%
CEO 13%	CEO 11%	CEO 13%	CFO 10%
CFO 8%	CDO/CFO 8%	CDO/CFO 7%	CAE/No single responsible executive/CCO/CEO/CISO 7%

Figure 12: Who is primarily responsible for each of the following areas of cybersecurity within your organisation?

* Top three responses shown

Cyber insurance coverage and policies

Global	China	Mainland China	Hong Kong
CISO 17%	CISO 28%	CISO 32%	CIO 23%
CIO 14%	CIO 18%	CIO 17%	CFO 17%
CFO 14%	CFO 11%	CFO 10%	CISO 13%
CEO 13%	CDO/CRO 7%	CDO 7%	CRO 13%

Securing operational technology (OT) / industrial internet of things (IIoT)

CISO 18%	CISO 29%	CISO 31%	CIO 30%
CIO 17%	CIO 15%	COO 12%	CISO 20%
CEO 10%	COO 11%	CIO 11%	CTO 10%
CTO 9%	CDO/CFO 8%	CDO 9%	CFO/COO/CRO/Head of Engineering / Operations 7%

Business leaders have an important role to play in ensuring their organisation adopts a heightened security position ^{vii}. In an ever-changing world, senior executives need to take ownership of their cybersecurity transformation, enabling organisations to rapidly identify and reduce cyber risk while confidently adopting new digital technologies that support their strategic goals ^{viii}.

In terms of what will make the most difference in transforming cybersecurity across the organisation in the next 12-18 months, China’s top three initiatives vary from those indicated by their global counterparts. Globally, ensuring all non-cybersecurity employees understand the potential cyber implications of their actions is the priority. While in China, strengthening the organisation’s data analytics capabilities on cyber and privacy activities (Global: 2nd) is believed to be the key driver of transformation, followed by consolidating enterprise technology solutions for a simpler tech stack/ infrastructure. Chinese respondents also acknowledge the importance of leadership that drives cybersecurity throughout the organisation.

China	Global
1 Strengthening our data analytics capabilities on cyber and privacy activities	Ensuring all non-cybersecurity employees understand the potential cyber implications of their actions
2 Consolidating enterprise technology solutions for a simpler tech stack / infrastructure	Strengthening our data analytics capabilities on cyber and privacy activities
3 Leadership that drives cybersecurity throughout the organisation	Leadership that drives cybersecurity throughout the organisation






Closing remarks based on the findings

Looking forward, China's cybersecurity market is poised for further growth in tandem with its proliferating digital economy, driven by: the increasing adoption of cloud-based services; the growing demand for advanced security solutions; the heightened awareness of cyber security threats; and the need to localise, and ringfence, systems, technology infrastructure and data in Mainland China. Additionally, the government's initiatives to increase the use of digital technology and enhance the institutional opening-up of key sectors are expected to present more opportunities to businesses who are cyber-ready for the future.

Given the current dynamic environment, Chinese organisations must develop an integrated and agile operating model that is capable of responding to a variety of disruptive events. Such models should be built with the flexibility for quick and effective responses, instead of relying on static plans and processes that may not account for unforeseen disruptions. Moreover, it is essential for organisations to adopt an 'all hazards' approach when identifying potential sources of disruption, including gathering threat intelligence information and formulating actions in response to identified threats, in order to remain resilient to cyber risk. In a fast-paced digital world, businesses must strive to maintain a level of agility, and develop and test anticipatory plans that can help them handle incidents proactively. To successfully achieve these objectives, senior executives must integrate cybersecurity transformation initiatives into their business strategy and enable organisations to confidently adopt new digital technologies.



ⁱ http://english.scio.gov.cn/tm/pressroom/2022-11/07/content_78506468.htm

ⁱⁱ <https://www.scmp.com/tech/policy/article/3206997/china-unveils-plan-boost-data-security-key-industries-bet-data-driven-economic-growth>

ⁱⁱⁱ <https://pro.bloomberglaw.com/brief/regulation-and-legislation-lag-behind-technology/>

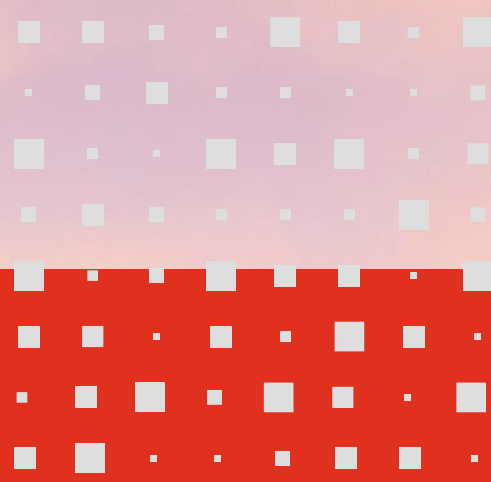
^{iv} <https://www.pwccn.com/en/issues/cybersecurity-and-privacy/china-cybersecurity-data-legal-developments-implications-businesses-oct2022.html#:~:text=October%202022&text=The%20Cybersecurity%20Law%20has%20been,at%20the%20end%20of%202021.>

^v <https://www.tiangandpartners.com/en/news-and-activity/china-cybersecurity-law-mandatory-breach-notification.pdf>

^{vi} <https://www.globalgovernmentforum.com/on-the-front-line-how-can-governments-safeguard-against-cyberattacks/>

^{vii} <http://www.cisa.gov/shields-up>

^{viii} <https://www.pwc.com/m1/en/services/consulting/technology/cyber-security/transformation.html>



Contact us

Kenneth Wong

Mainland China and Hong Kong Digital Trust & Risk –
Cybersecurity and Privacy Leader, PwC Hong Kong
+852 2289 2719
kenneth.ks.wong@hk.pwc.com

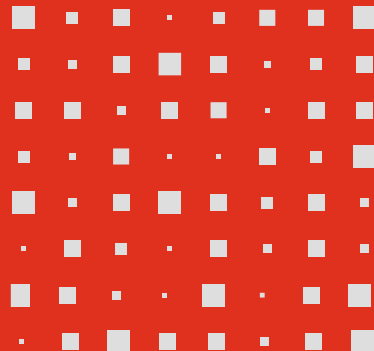
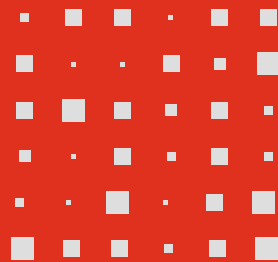
Lisa Li

Mainland China Digital Trust & Risk –
Cybersecurity and Privacy Leader, PwC China
+86 (10) 6533 2312
lisa.ra.li@cn.pwc.com



Editorial and writing

Shivia Ganglani
Terrance Lui
Julie Wu



© 2023 PwC. 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.