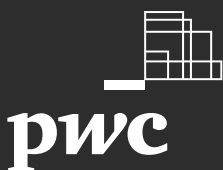




2022 Global Digital Trust Insights

The C-suite guide to simplifying for cyber readiness, today and tomorrow



2022 Global Digital Trust Insights

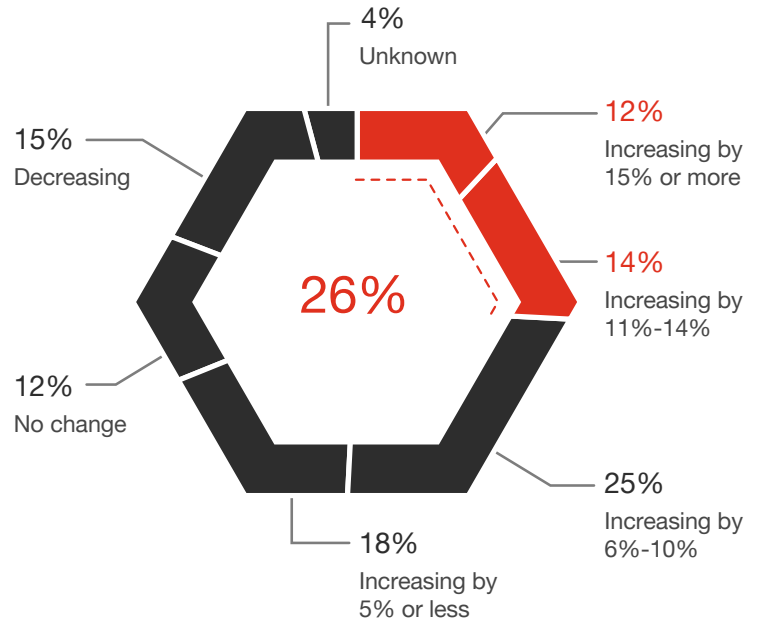
Investments continue to pour into cybersecurity. Sixty-nine percent of organisations predict a rise in cyber spending in 2022 compared to 55% last year. More than a quarter (26%) predict cyber spending hikes of 10% or more; only 8% percent said that last year.

Organisations know that risks are increasing. More than 50% expect a surge in reportable incidents next year above 2021 levels.

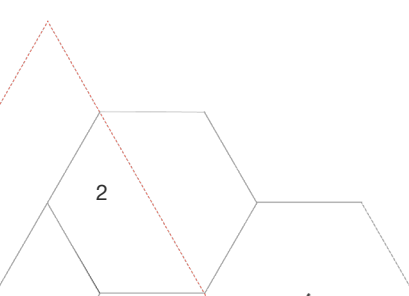
Already, 2021 is shaping up to be one of the worst on record for cybersecurity. Ever more sophisticated attackers are plumbing the dark corners of our systems and networks, seeking — and finding — vulnerabilities. Whatever the nature of an organisation's digital Achilles' heel — an unprotected server containing 50 million records, for example, or a flaw in the code controlling access to crypto wallets — attackers will use every means at their disposal, traditional as well as ultra-sophisticated, to exploit it.

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.

More than 25% expect double-digit growth in cyber budgets in 2022



Question: How is your cyber budget changing in 2022?
Base: 1,638 technology and security executives
Source: PwC, 2022 Global Digital Trust Insights, October 2021.



Few have realised benefits to-date, raising the question of what could be done better for future cyber investments

- Realising benefits from implementation
- Implemented at scale
- Started implementing / Planning to do in the future



Question: To what extent is your organisation prioritising investments in the following?
 Base: 3,602 respondents
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Simplifying cyber

As digital connections multiply, they form increasingly complex webs that grow more intricate with each new technology. Having a smart phone enables us to carry a variety of “devices” — telephone, camera, calendar, TV, health tracker, an entire library of books, and so much more — in our pocket, simplifying our lives in many ways and letting us work on the go. The Internet of Things lets us perform myriad tasks by uttering a simple command, enables factories to all but run themselves, and lets our healthcare providers monitor our health from a distance.

But the processes needed to manage and maintain all these connections — including cybersecurity — are getting more complicated, too. Runaway complexity evokes the Lernaean Hydra from Greek mythology: cut off one head, and two grow in its place.

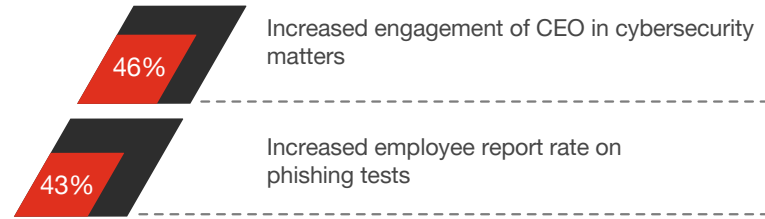
Is the business world now too complex to secure? Leaders are sounding the alarm. Some 75% of respondents to our 2022 Global Digital Trust Insights Survey say that too much avoidable, unnecessary organisational complexity poses “concerning” cyber and privacy risks.

But because some complexities are necessary, your enterprise shouldn’t streamline and simplify its operations and processes thoughtlessly, but consciously and deliberately.

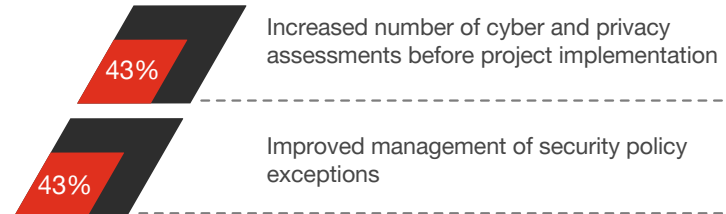
This 2022 Global Digital Trust Insights Survey offers the C-suite a guide to simplifying cyber with intention. It focuses on four questions that tend to get short shrift but, if properly considered, can yield significant dividends.

Cybersecurity scorecards: 4 out of 10 organisations report significant progress in the past two years on four fronts

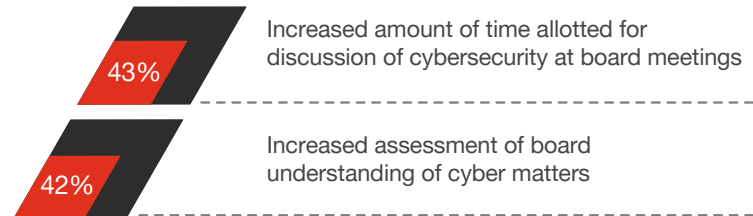
Instilling a culture of cybersecurity



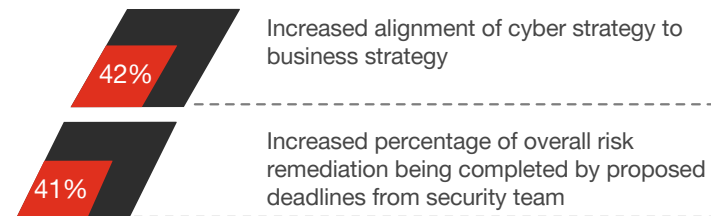
Cyber risk management



Communications between management and board



Aligning cyber with overall business goals



Question: How much progress has your organisation made in the past two years? Only the top two metrics are reported under each category.
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

These questions may surprise and even challenge you because, in a survey about data trust, they aren't technology-centered. Tech, in itself, is not the answer to simplified security.

Our focus, instead, is on working together as a unified whole, from the tech stack to the board room — starting at the top with the CEO. Security is a concern for the entire business, in every function and for every employee.

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?

Based on respondents' answers to these questions, we determined the top 10% of organisations that are **most advanced** in their practices. These **most advanced are twice as likely to report significant progress on important cyber goals**: instilling a culture of cybersecurity, managing cyber risk, enhancing communication between boards and management, and coordinating cyber strategy with business strategy.

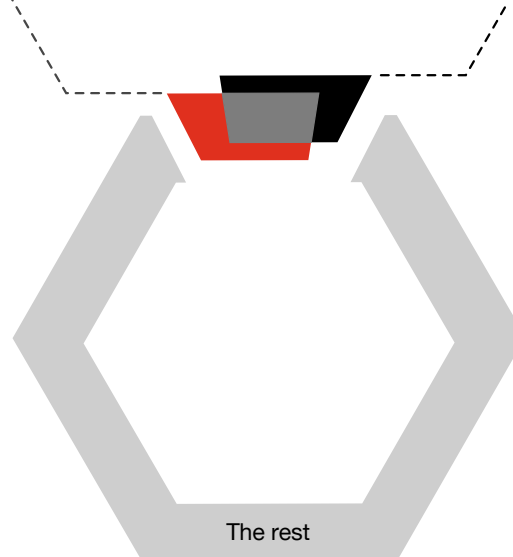
Organisations with the most advanced practices are twice as likely to have made significant progress in cybersecurity over the past two years

Top 10%

Most advanced
in four areas: engaged CEO, streamlined organisation, data trust, secure ecosystems

Top 10%

Most improved
report significant progress in four outcomes: cyber risk management, culture, alignment with business, communication between board and management



PwC analyses of data based on 3,602 survey respondents. Source: PwC, 2022 Global Digital Trust Insights, October 2021.

The top 10% reporting significant progress toward meeting these goals — the most improved — are many times more likely to be doing the right things.

- 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
- 12x**
more likely to say their CEOs give them the support they need
- 18x**
more likely to state data and intel tools and approaches are integral to their operating model
- 34x**
more likely to say they have achieved public-private sector collaboration goals 'very effectively'



Multiplying the effect: simplifying moves that get you 5x or more results

Strategists and technologists have touted the potential of digital business models to boost business 10x — a Holy Grail promise of exponential returns on digital investments. Likewise, the Survey reveals how simplifying business processes and operations can have a “multiplier” effect on security and privacy.

Here are the four Ps to realising your full cyber potential, as exemplified by most advanced and most improved organisations, who employ them all.

Principle. The CEO must articulate an explicit, unambiguous foundational principle establishing security and privacy as a business imperative.

People. Hire the right leader, and let CISO and security teams connect with the business teams. Your people can be vanguards of simplification even as you build “good complexity” in the business.

Prioritisation. Your risks continually change as your digital ambitions rise. Use data and intelligence to measure your risks continually, as well.

Perception. You can’t secure what you can’t see. Uncover blind spots in your relationships and supply chains.

As common-sense as these precepts and practices might seem, they’re not commonplace. Only the top 10% have adopted them and they also report making significant progress toward their cyber objectives during the past two years.

On the other hand, many enterprises continue to struggle amid risky, runaway, befuddling complexity. Bad habits are often why: Using many tech solutions that, too often, don’t even work together. Not coordinating the work of various functions on resilience or third-party risk management. Not creating and adhering to processes for dealing with data (governance). Not speaking in the language of business when talking about cyber.

Businesses develop these bad habits in the name of speed, or they accept and assimilate them out of resistance to change. The good thing, however, is that bad habits can be broken. And C-suite champions can help develop new habits of coordination and collaboration among all functions, business and tech, for an organisation that’s simply secure.

Can the CEO make a difference to your organisation's cybersecurity?

Chief executives at companies that had the best cybersecurity outcomes over the past two years are 14x more likely to provide significant and broad support to cybersecurity.

Make 'simply secure' your business mantra

Cyber has got CEOs' attention, but are they taking action?

Chief executives cited cyber threats as the number-two risk to business prospects in PwC's 24th Annual Global CEO Survey — topped only by pandemics and other health crises. In North America and Western Europe, cyber was number one.

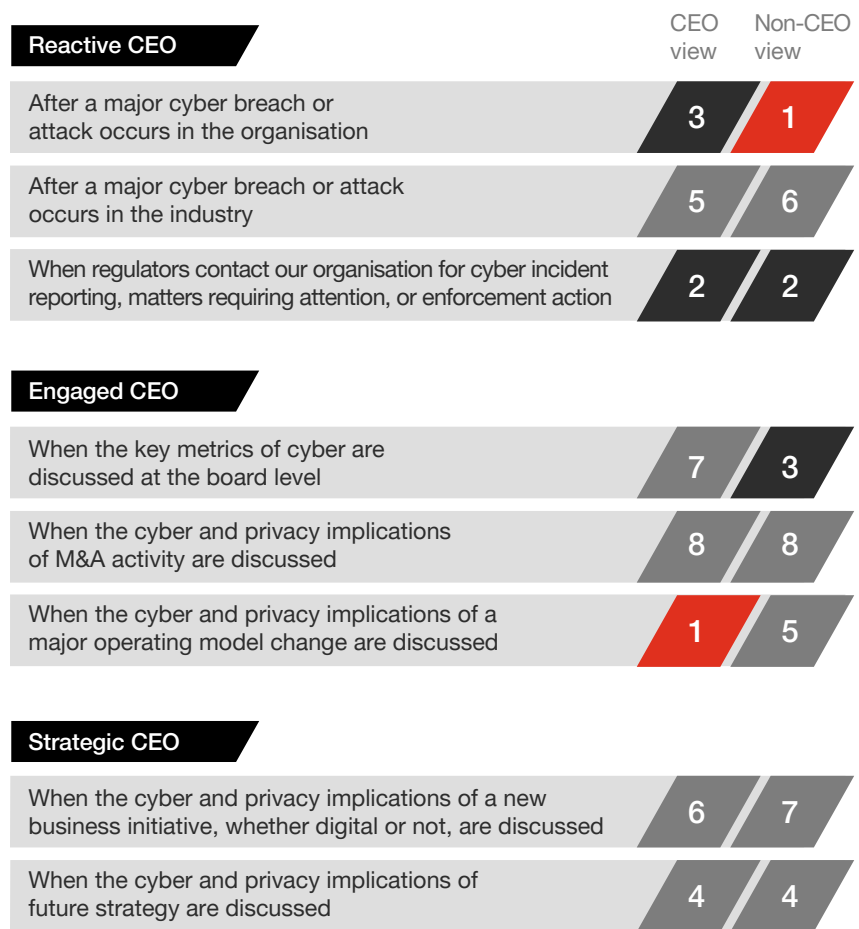
Our findings from the 2022 Global Digital Trust Insights Survey suggest an "expectations gap" for cyber, with CEOs perceiving that they are more involved in, and supportive of, setting and achieving cyber goals than their teams do. A persistent gap can spell disaster if it instills a false sense of security company-wide, given the CEO's leading role in defining an organisation's culture.

How involved are CEOs in cyber? We asked nearly 700 CEOs and 2,900 other C-suite execs. Among our respondents, CEOs tend to see themselves as more involved in cybersecurity than others in the organisation do.

Many CEOs self-identify as *engaged* and *strategic* in their approaches to cyber. Our CEO respondents indicate that they participate in discussions about the cyber and privacy implications of mergers and acquisitions, future changes to their operating model, and future strategy.

Other executives don't view things in quite the same way. Non-CEOs rated their CEOs as more reactive than proactive regarding cybersecurity. They say the chief executive is most likely to take part in cyber and privacy matters *after* a company breach or when contacted by regulators — not before.

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.

How much support does the CEO provide CISO leadership?

CEOs were more likely than non-CEOs to rate as “significant” their level of support in six areas. For instance, 37% of CEOs said they provide significant support for “ensuring adequate resources, funding and sufficient priority” to cyber, while only 30% of non-CEOs agreed that their CEOs do so.

And 34% of CEOs say they provide significant help to cyber leadership with “reducing investors’ uncertainty regarding organisational cyber risks” — while just 29% of non-CEOs agree. Thirty-six percent of CEOs say they empower their cyber leadership to connect with customers and business partners, while only 30% of non-CEOs say cyber gets that kind of support.

CEOs matter. CEOs in our “most improved” group (those with the best cybersecurity outcomes over the past two years) are **14x** more likely to provide significant support across all categories. Similarly, the non-CEOs in the most improved group are **12x** more likely to say their CEOs provide that significant boost.

The CEO’s engagement and support wield long-term importance. 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.

It’s time to close the expectations gap between the chief executives and the others in the C-suite regarding the level of CEO involvement and support of cybersecurity. Things seem headed in the right direction: Interactions with the CEO on cyber matters have increased significantly in the past two years, according to 46% of our survey respondents.

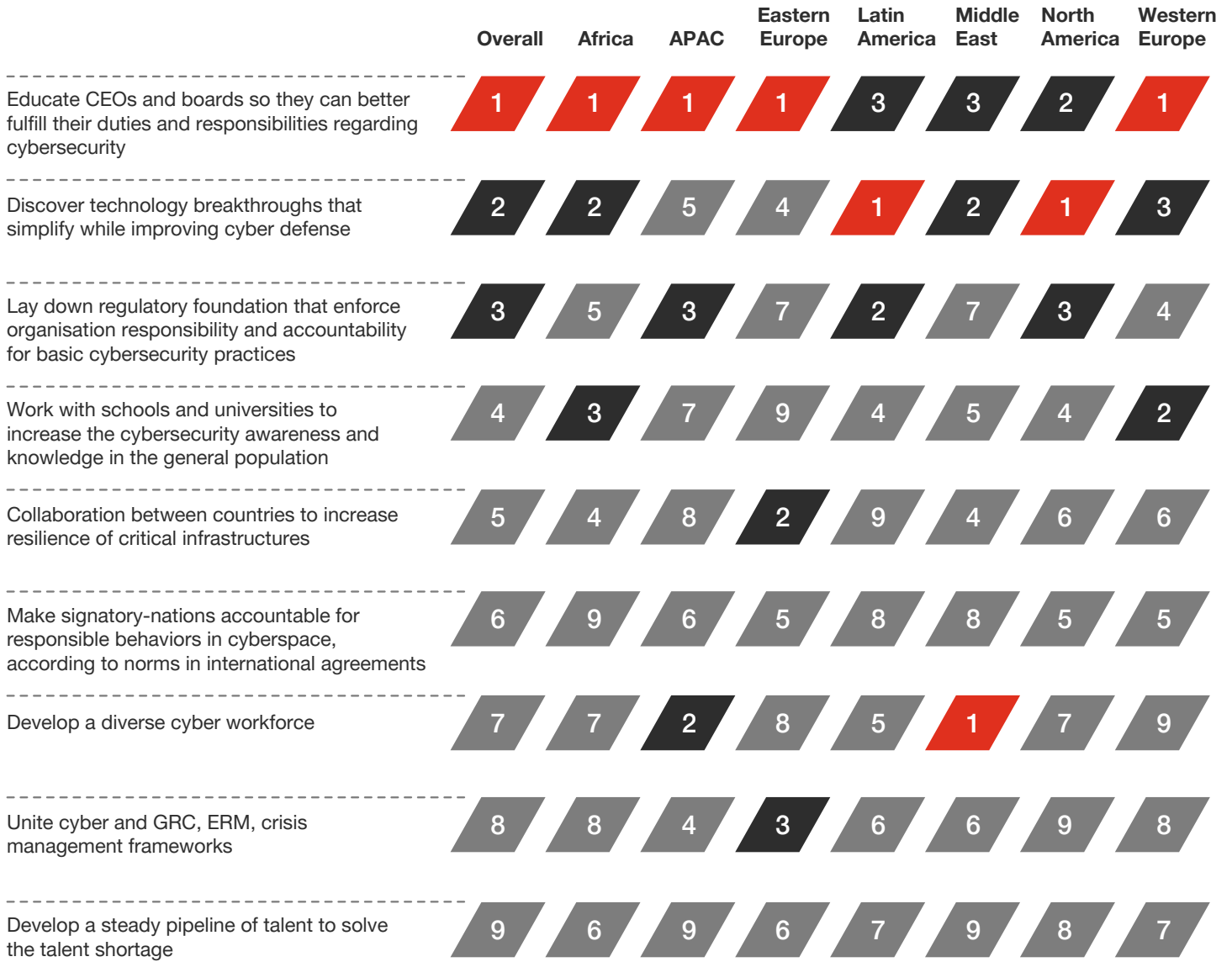
CEOs believe they give ‘significant’ cyber support, but only 3 in 10 executives agree

■ CEO ■ Non-CEO



Question: What level of support do you/does your CEO provide your cyber leadership to accomplish the following?
 Base: Non-CEO Respondents: 2,929; CEO Respondents: 673
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Executives around the world put a lot of stock in cyber-savvy and engaged CEOs and boards – and tech breakthroughs that simplify cyber defense – for a more secure digital society by 2030



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

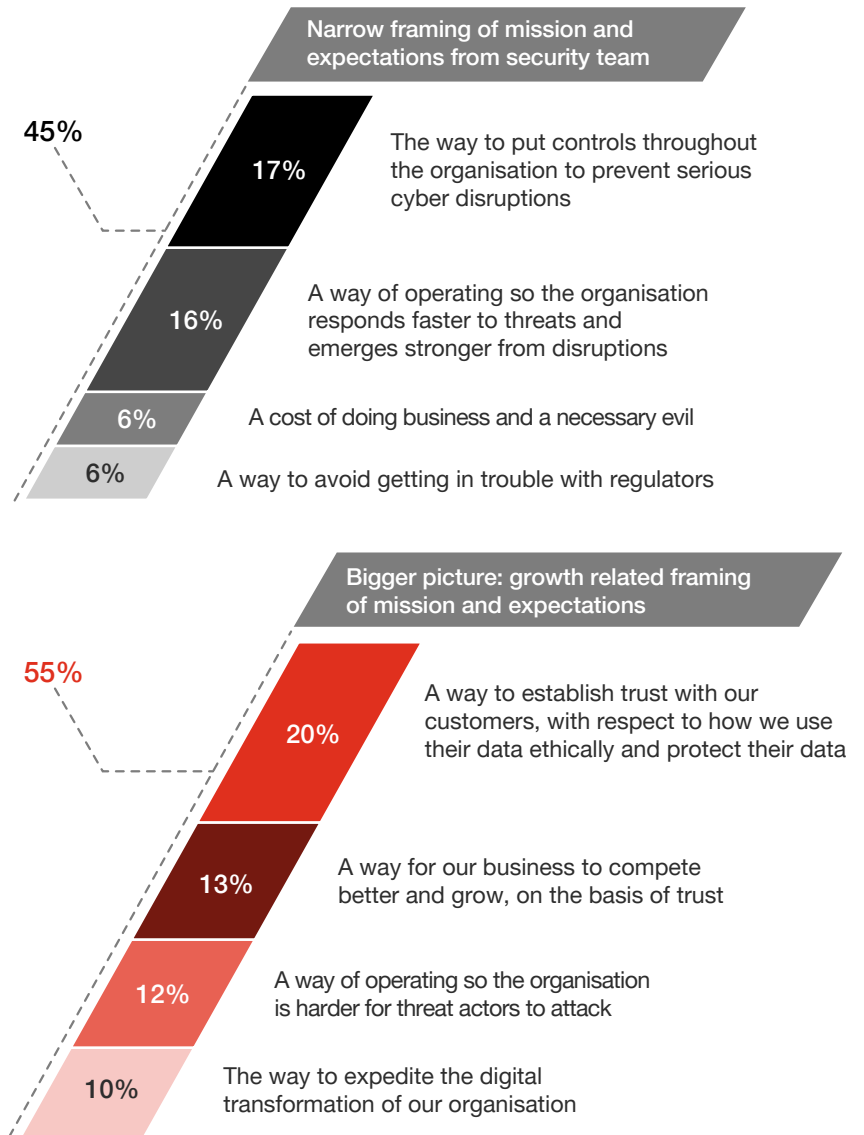
CEOs and other executives agree on the changing cyber mission

Asked how CEOs frame the cyber mission in their organisation, more than half (54%) of the CEOs chose bigger-picture, growth-related objectives from their security team, as opposed to narrower, shorter-term expectations.

Non-CEOs echoed this mindset. In both 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. CEOs really do set the tone for the rest of the organisation.

CEOs and non-CEOs name similar top goals for cyber in the next three years. These objectives mirror the famous Maslow’s hierarchy of needs, 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 fifth and seventh, respectively). Protection, resilience and trust comprise the three legs of the cybersecurity stool, each important for the security of the business overall.

Cybersecurity’s mission is shifting to developing trust and business growth

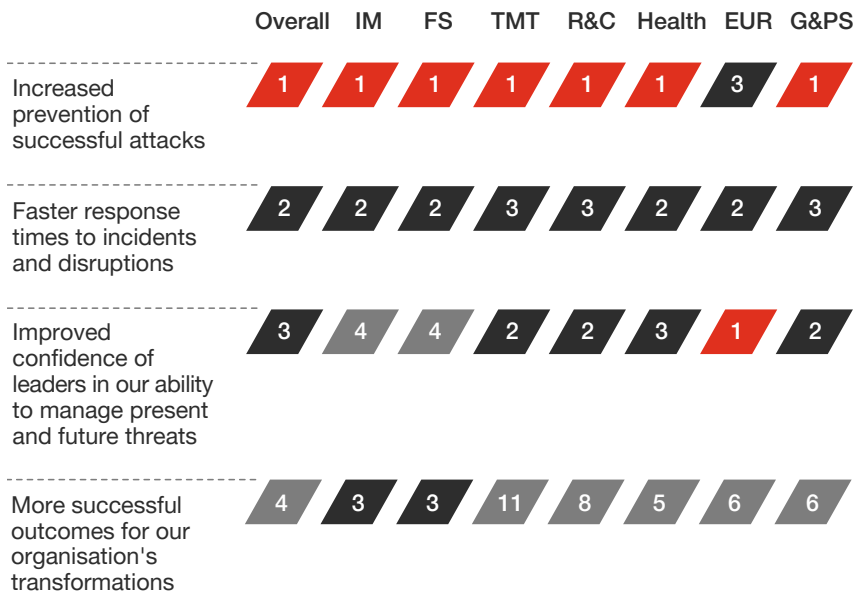


Question: Which of the following best describes how you/your CEO frames the cybersecurity mission to your organisation?
 Base: 3,602 respondents
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Top goals 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)

Cyber-ready for today and tomorrow: goals for the next three years



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?
 Respondents: Industrial manufacturing=789, technology, media & telecommunications=824, financial services=724, retail and consumer=581, energy, utilities and resources=299, healthcare=255, government/ public services=126
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.





How can CEOs make a difference to their organisation's cybersecurity?

The top 10% that are “most advanced” in cyber practices or “most improved” on cyber outcomes are in a good position. But the majority overall — 63% of organisations — don't get the kind of support they need from their CEO. The fact is, both the CEO and CISO need to work together better to benefit the company.

CEO: How much should you be involved in your organisation's cybersecurity — without taking on undue burden?


A powerful CEO move: making an explicit statement establishing an imperative for security and privacy organisation-wide. In some cases, the organisation's mission statement is already implicitly supportive, such as Liberty Mutual's mission statement to “help people live safer, more secure lives.” Red Bull's dedication to distinguished products and services gives its CISO the mandate to make security an integral part of the product and service quality delivered to customers.

A related CEO imperative: empowering your CISO to carry out the cybersecurity mission, voicing support and providing resources for secure-by-design, secure-by-default processes.

Some may add the CISO to the C-suite. Others may help the CISO communicate more with the board or revamp the enterprise's structure to embed security staff on business teams. Empowering CISOs may also mean giving them the platform to speak outside the organisation to customers about its security and privacy initiatives, as a trust officer would.

This period of great complexity in the business world demands a third CEO imperative. The CEO must modify certain elements of the company's business and/or operating models to make the company “simply secure” when the security team identifies wasteful habits. For example, in the name of speed, a “get to market first, fix security later” mindset prevails. Companies aren't fully mitigating remote work risks. Business units often buy technologies and contract with third parties autonomously. Cybersecurity is too often an afterthought in cloud adoption or transformation.

By taking action, the CEO reinforces a zero-tolerance mentality for complexity that gets in the way of security.



CISO: How well do you understand the business?
How connected are you with leaders on the
business side?

For an organisation that's simply secure, **CISOs must move out of the technology trenches and broaden their outreach** — learning from the CFO how to talk about the financial implications of risk, for example, in a language the board understands, or working with the product manager to devise developer-friendly ways to secure applications.

This change may require a mindset shift for many CISOs. CISOs interact most frequently with the CIO and chief technology officer, our survey shows, and least frequently with the chief marketing officer and product management leader. The CFO also ranks low on the interactions list. CISO will need to spend more time with these business partners to begin to speak their language and better understand their business imperatives.

More than 21% placed the CEO among the three positions with whom they least come in contact; some 10% placed the CEO at the very bottom of the list. The CEO-CISO divide is widest in Europe: 27% of CISOs in western Europe and 28% in eastern Europe placed their chief executive among the bottom three with whom they interact, followed by Asia Pacific (21%) and North America (19%).

Takeaways

For the CEO

- 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."

For the CISO

- 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.



Is your organisation too complex to secure?

75% say their organisations are too complex. But those that had the best cybersecurity outcomes over the past two years are 5x more likely to have streamlined operations enterprise-wide.

Be deliberate about simplicity and simplification

In an overly complex organisation, it's easy for the left hand not to know what the right hand is doing — and the consequences for cybersecurity and privacy can be dire. Seventy-five percent of C-suite respondents to our survey, including CISOs, say their companies are too complex, *avoidably* and *unnecessarily* so, and nearly as many say complexity poses “concerning” cyber and privacy risks to their organisations in 11 key areas.

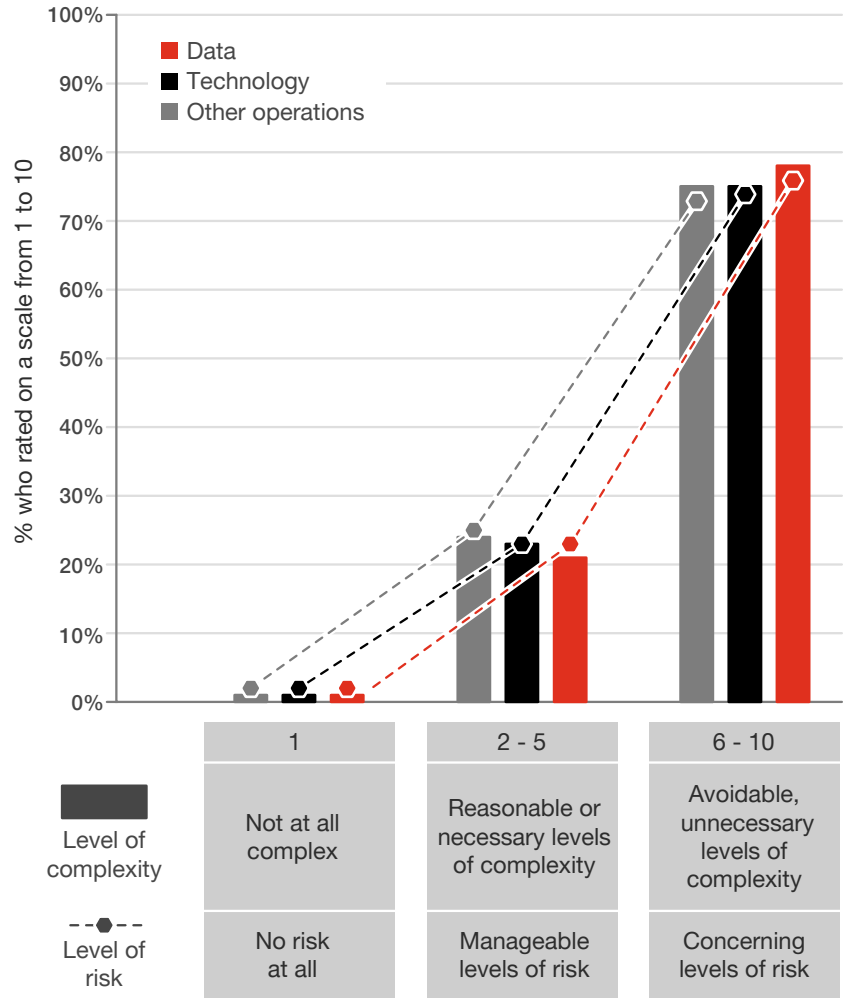
Data seems to be a chief point of concern, especially among large companies (revenues of \$1 billion or more). Data governance (77%) and the data infrastructure (77%) ranked highest among areas of “unnecessary and avoidable” complexity.

Technology networks and devices are also highly complex, particularly in large companies and North American companies. Digital-native companies — those that exist entirely online — tend to use the newest technologies, which are designed to connect and operate together. Most other companies' technology architectures, which include legacy systems, are more complicated. Mergers with other entities may multiply risks by connecting already complex networks and systems.

The most worried about all this complexity are CEOs. They assign a complexity level of 10 to seven of 11 areas in their organisations. CEOs tend to be more concerned about cyber and privacy risks arising from complexities in the cloud environment, governance of tech investments, and crossover from IT to operational technology (OT).

Executives in large organisations and in North America are more likely to be concerned about risks from complexities in the cloud environment and the crossover from IT to OT.

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.

The costs of complexity

Complexity isn't bad in and of itself. Often, it's a by-product of business growth. The larger an organisation, the more complex it will naturally be, needing more people and technologies to serve a growing customer base.

The costs of creating unnecessary complexity are not obvious, and it's hard to create urgency around combatting complexity — that is, until an attack occurs.

One company needlessly kept the sensitive data of people it no longer did business with, making that data available for hackers to steal.

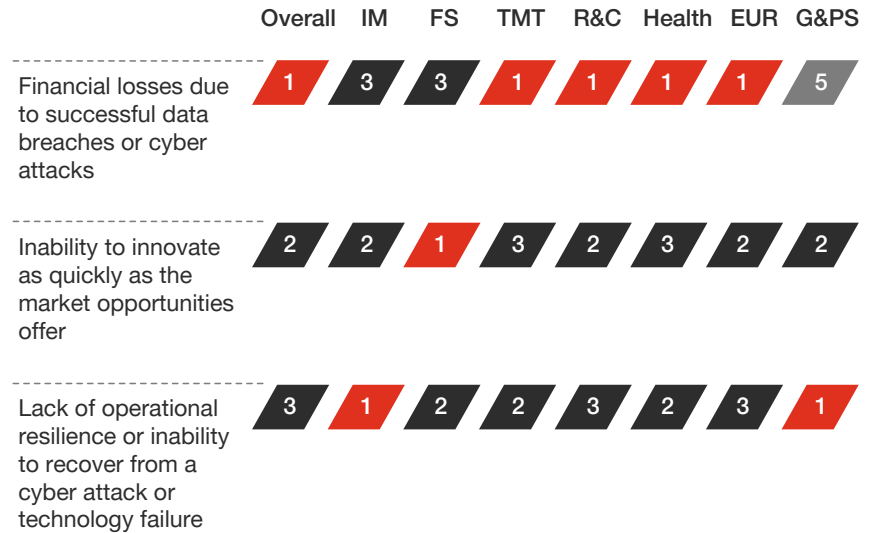
In our article Simplifying cyber, we give examples of how simplification can improve security. At a global retail organisation, six vendors managed customer contacts. Two of those vendors' systems had been breached in the past. After consulting with the CEO and board, the new operations director whittled the vendor list to two. This simplification improved security: Monitoring two vendors is easier than keeping tabs on six, making information access easier to control, and the retailer could more readily back up the smaller cache of customer data.

Asked to name the top consequences of operational complexity, our respondents named:

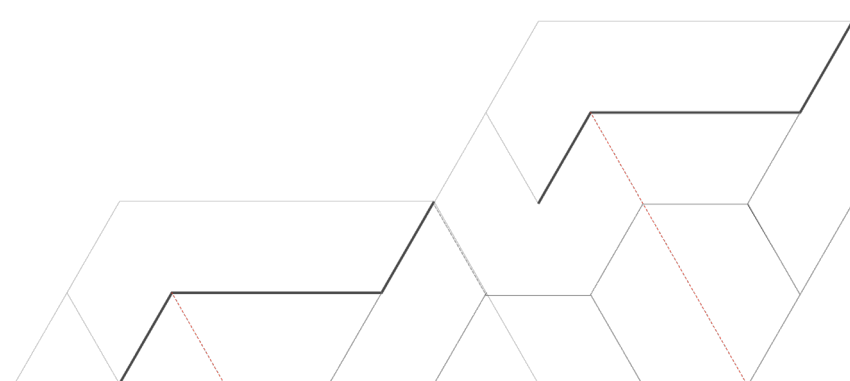
1. Financial losses due to successful data breaches or cyber attacks.
2. Inability to innovate as quickly as the market opportunities allow.
3. Lack of operational resilience, or the ability to recover from a cyber attack or technology failure.

Complexity not only threatens today's fortunes, in the view of executives. It also prevents organisations from creating new opportunities quickly and pursuing future ones.

In all industries, top consequences of complexity are financial losses, inability to innovate, and lack of resilience



Question: In your view, What are the most important consequences of complexity on your business?
 Respondents: Industrial manufacturing=789, technology, media & telecommunications=824, financial services=724, retail and consumer=581, energy, utilities & resources=299, healthcare=255, government/public services=126
 For government/public services, the third most important consequence is 'inability to retain top talent.'
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.



The move to simplification

Businesses know the risks of complexity, yet only 35% of our respondents have performed any streamlining of their operations and a quarter say they've done nothing at all or are just getting started. But a shift appears to be underway.

Simplifying an organisation takes time, requiring changes in viewpoints and company culture. That's not easy to achieve, but the payoffs are mighty. The companies that had the best cybersecurity outcomes over the past two years (most improved) are **5x** more likely to have streamlined operations enterprise-wide. They've focused on 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%).

More and more CISOs and CIOs are taking a hard look at their tech investments, no longer just entertaining or chasing the latest products from tech vendors. We're seeing consolidation of tech vendors and applications to reverse the hard-to-manage and risky tangle of disparate and vulnerable software and tech stack.

Simplification in organisations: 3 in 10 have streamlined over the last two years

Defined a new mix of remote/virtual and onsite work



Reorganised functions and ways of working



Consolidated technology vendors



Created an integrated data governance framework



Automated standard, repetitive processes



Created an integrated dashboard for key metrics



Defined or re-aligned the mix of in-house resources and managed services



Rationalised technologies, including decommissioning legacy technologies



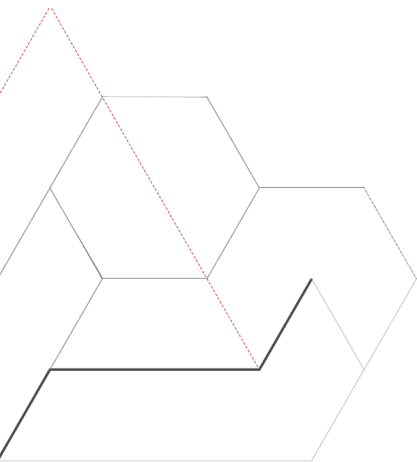
Removed redundancies in processes



Question: In the last two years, to what extent has your organisation streamlined operations in the following ways? Percentage responding 'completed enterprise-wide'. Other potential responses were 'partially completed,' 'just started,' or 'not at all.'

Base: 3,602 respondents

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



Simplification of cyber. To be fair, simplifying cybersecurity can be challenging. Even knowing where to begin can be difficult, especially given the attacks hitting businesses on every front. Asked to prioritise among nine initiatives aimed at simplifying cyber programs and processes, respondents couldn't choose, allotting near-equal importance to all of them. CISOs who are building layers of control, for defense in depth, are well-intentioned but must guard against introducing more complexity and cost. More controls don't always make a company more secure.

Moving to the **cloud** can help simplify business processes and IT architecture, provide flexibility and accelerate innovation. Yet companies typically waste an average of 35% of their cloud budgets on inefficiencies. Runaway complexity can quickly result from extensive technology options, new architectural approaches, complicated service plans, unused capacity and confusing billing and pricing, especially when the technologies offered are constantly changing.

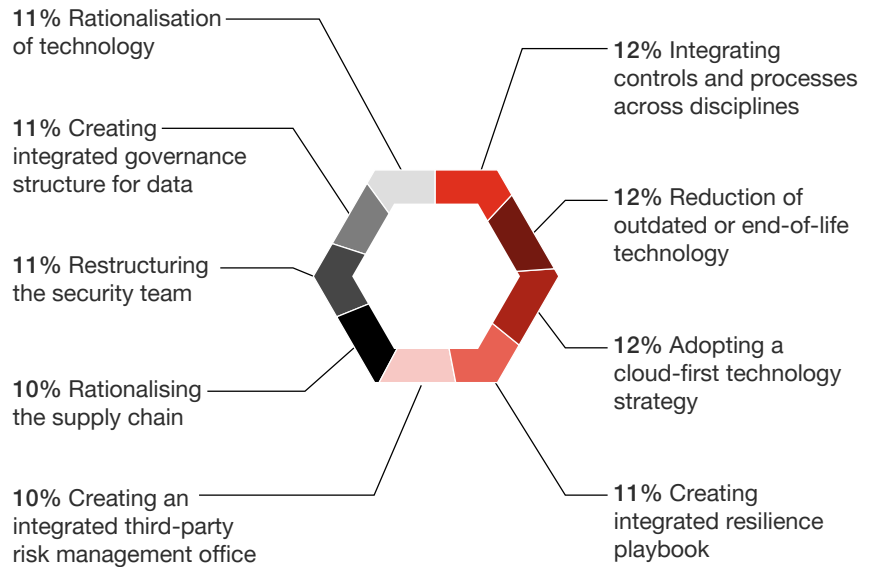
Done right, however, cloud transformations can be secure, efficient, and successful. Cloud security is the top investment priority of our survey respondents, as well as in our June US-specific survey. That's encouraging — but only 16% report realising benefits from these investments. Thirty-five percent haven't fully benefited from cloud security investments and 45% are just starting or planning theirs.

Whether or not you're using the cloud to simplify, minimising and combining your tech stack and processes may feel like a bold move. Doing so requires asking hard questions and maintaining a keep-it-simple mindset. To get there, your organisation will need security-minded leadership starting at the very top.

Don't overlook moves that can have a significant impact. For example, two moves — deploying two-factor authentication and putting your remote desktop protocol (RDP) behind the firewall — can vastly reduce the risks from phishing, which remains a popular tactic, by itself, and in tandem with malware and ransomware attacks.

Simplification of cyber: spending is spread across several initiatives

Average share of total spending on cyber simplification



Question: In the next two years, what proportion of your cybersecurity spend will your organisation allocate to each of the following initiatives to simplify cybersecurity?
 Base: 3,602 respondents
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Across different areas...

- Cloud migration or adoption
- IT development operations
- Product development and design
- Supply chain
- Hybrid work arrangements

...How difficult is it to build cyber and privacy into operations?

Minimally or not at all difficult

51%

...How much of an impact would it make?

Significant impact

25%

Question: In your view, how difficult will it be to make the changes needed to build a cybersecurity 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: 3,602 respondents

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

Takeaways

For Operations 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 can 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. That way, every executive at the helm of a major business initiative will be able to readily answer the cyber-plan question.

For the CISO and CIO

Dare to subtract. Left on their own, technology and data tend to multiply, divide, and conquer efficiency and security. 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, 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 today and tomorrow?

Fewer than 1 in 3 organisations use available data and intelligence when making decisions. But those that had the best cybersecurity outcomes over the past two years are **18x** more likely to say data and threat intel are integral to their operating model.

Size up your risks — using data you can trust — to realise opportunities

Organisational leaders recognise the importance of verifying and safeguarding their business information. Asked to frame the cybersecurity mission, the number-one response was, “A way to establish trust with our customers with respect to how we use their data ethically and protect their data.” Eighteen percent of CEOs and 20% of non-CEOs selected customer trust as the way the CEO frames the cyber mission in their organisation.

Data infrastructure and data governance rank as the two most needlessly complex aspects of business operations in PwC’s 2022 Global Data Trust Insights Survey: 77% say both have “avoidable, unnecessary” levels of complexity. About three-quarters say complexity in these areas poses “concerning” risks to cybersecurity and privacy. Complexity of data can stymie any organisation’s ability to effectively use the information it collects and generates.

A foundation for data you can trust for better business decisions

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. (And when it comes to customer data, you want to make sure customers know they can trust you to keep their information safe from unauthorised eyes.)

But only about a third of respondents report having mature, fully implemented data-trust processes in four key areas: governance, discovery, protection and minimisation. Nearly a quarter of our respondents say they have no formal data-trust processes in place at all.

Only about one-third of organisations report having a full, formal data governance program — a surprisingly low number. Once you’ve crafted your data strategy, governance — the policies, procedures and processes for fulfilling the strategy — should follow immediately.

Securing your data from tampering as well as theft is also critical to success, yet only about one-third of respondents report having in place fully implemented, formal data security processes including encryption and secure data-sharing (34%). Verifying and protecting the integrity of your data is essential as well. Not doing so is like hiring workers without fact-checking their resumes. You can’t be certain of the quality of the information.

And 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 is the asset attackers covet most. Your companies can minimise that risk by minimising the target. You must govern, discover and protect *only* the data you need — and eliminate the rest. Drafts, duplicates, superseded data, legacy data and employee personal data are common candidates for elimination. Low-value data not only creates unnecessary risk, it also crowds out or buries your high-value data.

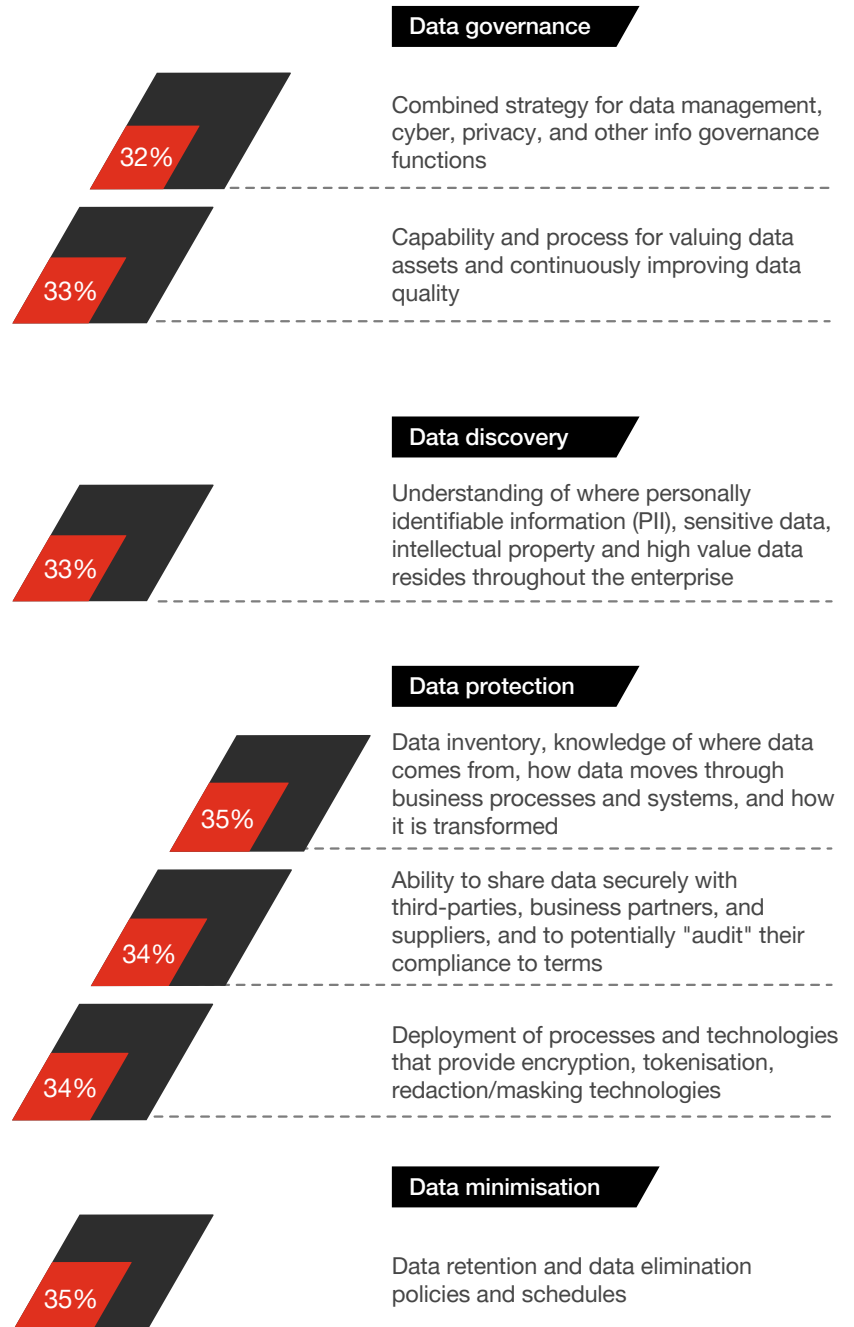
The two-thirds of organisations that haven't formally implemented data trust practices may be at risk in more ways than one. Effective data governance is important not only for operational resilience but also for compliance with regulations such as the European Union's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA). New, more stringent regulations loom on the horizon as well. When someone asks for information about their data — what you're keeping and what you're doing with it — you'd better be able to answer quickly and accurately. If it's a regulator doing the asking, the wrong answer could bring heavy fines.

Turning data into true assets that can increase your revenues is one benefit of good data security — as some leading businesses are discovering. Our "most improved" are more than **10x** more likely to have a formal process fully in place for *all* data trust practices.

According to our Trust in Data Survey, companies with more mature data trust practices tend to be ahead in many respects. They earn revenues from data monetisation by personalising services, operating more efficiently and better serving their customers. They strongly agree that higher customer trust leads to demonstrably higher revenue. They've made significant moves in the past year to improve customer and investor trust. And they're more confident in their third-party risk management program because they monitor their third parties more.

Data trust practices have yet to become the norm

Percentages who say they have fully implemented formal processes around these data trust practices



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 it or lose out

Chances are good that neither you nor your competitors are letting data inform your cyber risk management. Fewer than one in three of survey respondents say they've integrated analytics and business intelligence tools into their operating model.


These respondents scored lowest in their ability to turn data into insights for cyber risk quantification, threat modeling, scenario building and predictive analysis — all critical technologies for smart cybersecurity decisions.

So many entities fail to benefit from 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, but only about a quarter of respondents say they're reaping benefits from these tools.

The other three quarters are missing out. 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 can not 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


Real-time threat intelligence
 30%


Use of generally accepted standards and frameworks in assessment and diagnostic tools
 29%

Autonomous threat detection, including cognitive security
 29%

Common industry metrics and dashboards
 27%


Policy and regulatory strategic intelligence platform
 26%

Cyber risk quantification, using FAIR or other methods
 26%


Threat modeling, scenario building, and predictive analysis
 26%


Percentage who report realising benefits from these tools and approaches

Information sharing platforms with industry
 27%

Information sharing platforms with government agencies
 26%

New types of internal data we've not traditionally used
 25%

New data partnerships to complement and enrich our first-party data sources
 24%

New external sources of information we've not traditionally used
 24%

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.

Sizing up risks — and opportunities

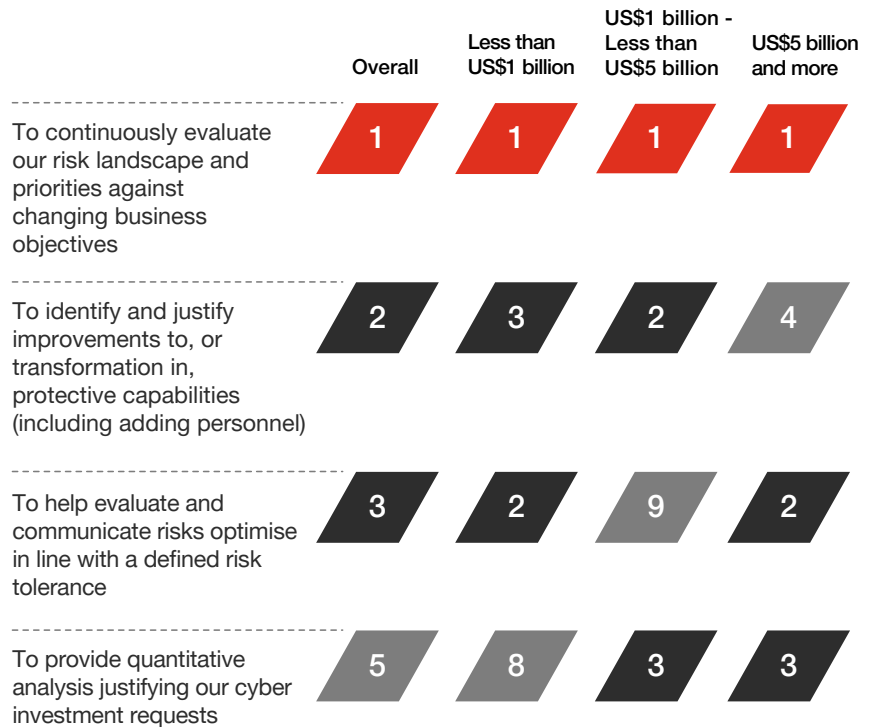
“In today’s system-of-systems world, cybersecurity can no longer be treated as a ‘too-hard-to-measure’ problem,” the US Cybersecurity and Infrastructure Security Agency argues. Still, as we saw above, only 26% quantify cyber risks today.

The data you use to spot and understand threats, put a dollar figure on risks and prioritise them, and predict cybercrime trends can be a powerful tool for convincing boards and the CEO to invest in your cyber program. On the other hand, if you’re having trouble getting the funding you need for cyber, you may need to do a better job of quantifying your cybersecurity risk.

By the same token, data can help you stay apprised of real-time risks, and adjust security tactics and strategies as the business shifts. Respondents in five business sectors said the most important reason to quantify cyber risk is “to continuously evaluate our risk landscape and priorities against changing business objectives.” Enterprise leaders recognise that risks are always in a state of flux and that data is the tool that lets them monitor and measure changes.

Sizing up risks is also important for sizing up opportunities and linking cyber-threat narratives to business narratives that the C-suite and boards can understand. A growing number of organisations recognise the importance of cybersecurity to business — but many still have a long way to go. Between 37% and 42% claim “significant progress” linking the two, while 16% to 18% say they’ve made little or no progress aligning cyber and business goals.

Executives want to size up cyber risks in continually changing risk landscape



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

The 2022 threat outlook

Our respondents do make predictions about the next 12 months. Sixty percent expect an increase in cybercrime; 53% say nation-state attacks are likely to grow. Mobile, the Internet of Things, and cloud top the list of anticipated targets. But the type of attack could take almost any form, in our respondents' minds. Cloud service attacks (22%) narrowly edged out ransomware (21%) and cryptomining (21%) as most likely to see significant increases, and a long line of other attack types scored at 20% and 19%. Notably, 56% expect a rise in breaches via their software supply chain, with 19% eyeing significant increases — a number that grows to 25% among North American respondents.

The 2022 threat outlook: Executives expect a surge in attacks and reportable incidents

■ Increase significantly ■ Increase

Reportable incidents

Attack on cloud services

22% 36%

Ransomware

21% 36%

Cryptomining

21% 33%

Malware via software update

20% 36%

State-sponsored attack on critical infrastructure

20% 33%

Business email compromise

20% 35%

Disinformation

19% 33%

Attack on software supply chain

19% 36%

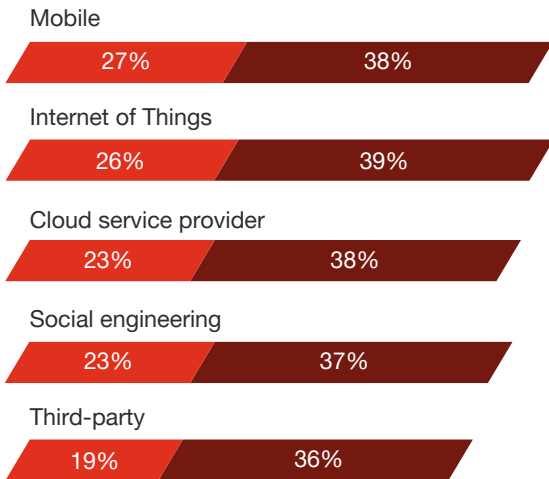
Foreign influence in research and development

19% 34%

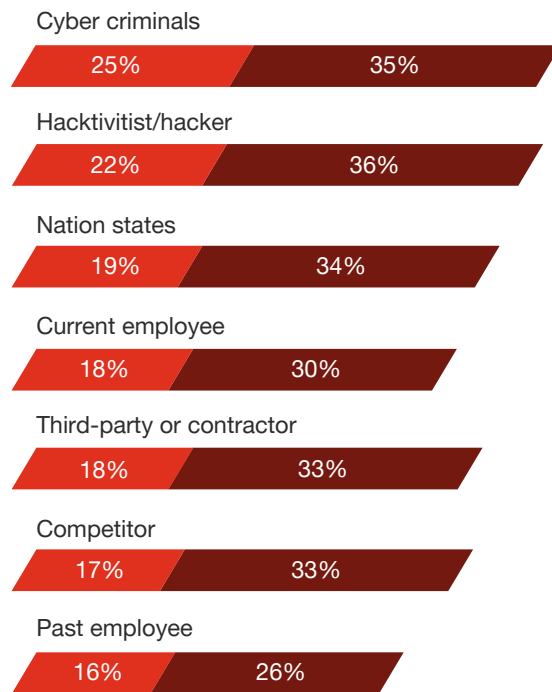
Attack on hardware supply chain

16% 34%

Threats via vectors



Threats via actors



Questions: How do you expect a change in reportable incidents for these events in your organisation? How do you expect threats via these vectors/actors to change in 2022 compared to 2021?
Base: 3,602 respondents
Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Takeaways

For the CFO

- Work with the CISO in taking a risk-based approach to cyber budgeting that ties to business objectives.

For the CISO

- 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 the risks posed by your third parties and supply chain?

At best, only 40% say they thoroughly understand their third-party cyber and privacy risks. But those that had the best cybersecurity outcomes over the past two years are **11x** more likely to say they do.

Shrink the large blind spot hiding the risks in your business relationships

You can't secure what you can't see, and most respondents to the PwC 2022 Global Digital Trust Insights Survey seem to have trouble seeing their third-party risks — risks obscured by the complexities of their business partnerships and vendor/supplier networks.

Only 40% of survey respondents say they thoroughly understand the risk of data breaches through third parties, using formal enterprise-wide assessments. Nearly a quarter have little or no understanding at all of these risks — a major blind spot of which cyber attackers are well aware and willing to exploit.

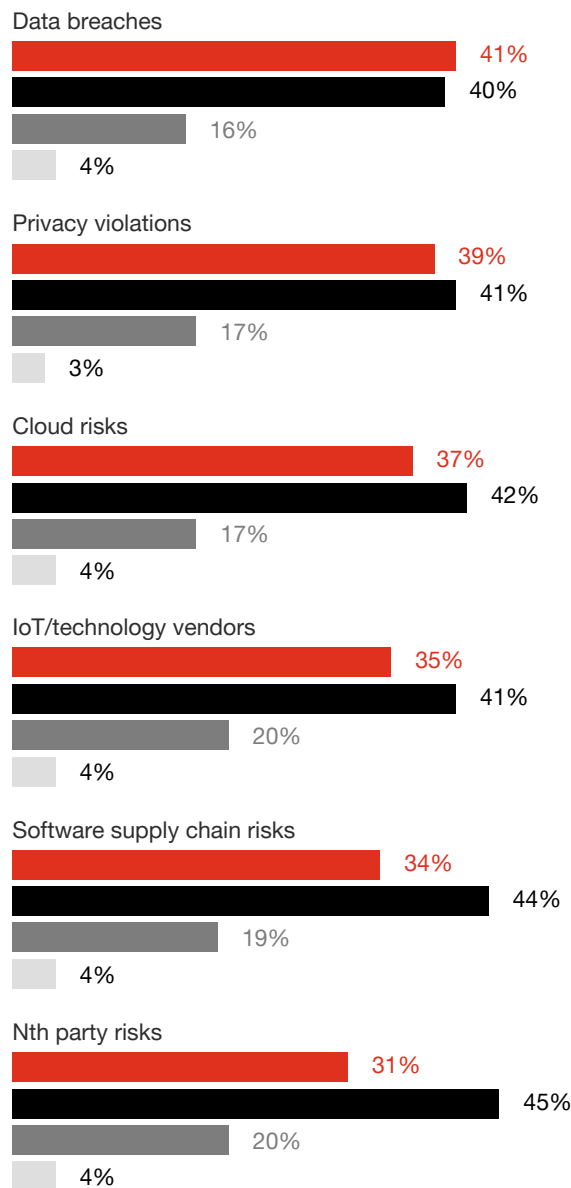
Among our respondents, 56% expect an increase in reportable incidents in 2022 from attacks on the software supply chain, but only 34% have formally assessed their enterprise's exposure to this risk. Fifty-seven percent expect a jump in attacks on cloud services, but only 37% profess an understanding of cloud risks based on formal assessments.

The "most improved" organisations, on the other hand, have taken note and taken action. They are **11x** more likely to report a high understanding of their third-party risks. Some three-quarters say they're highly knowledgeable about third-party dangers in five of six areas.


Only in their knowledge of "nth-party" risks — those posed by their suppliers' suppliers and so on, down the line — does the number dip: 69% of the "most improved," 31% for the rest. The more complex the connection, the harder it becomes to see the risks buried within.

Organisations have a large blind spot to risks arising from third parties and the supply chain

- High - understanding from formal, enterprise-wide assessments
- Moderate - limited understanding from ad hoc assessments
- Low - anecdotal understanding, no assessments
- No understanding



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.



Fewer than half of all respondents — 30% to 46% — say they've responded to the escalating threats that complex business ecosystems pose. The ones that have responded seem to be focusing their efforts primarily on today, perhaps at the expense of tomorrow. Asked how they're minimising their third-party risks, they gave largely reactionary answers: auditing or verifying their suppliers' compliance (46%), sharing information with third parties or helping them in some other way to improve their cyber stance (42%), and addressing cost- or time-related challenges to cyber resilience (40%).

Only one top response — that they are refining criteria for onboarding and ongoing assessments (42%) — could be considered proactive, offering benefits over the long term. Publicly listed organisations (47%) were significantly more likely to claim this step.

Still, more than half have taken *no* actions that promise a more lasting impact on their third-party risk management. They've not refined their third-party criteria (58%), not rewritten contracts (60%), not increased the rigor of their due diligence (62%). Meanwhile, the “most improved” are five times more likely to have taken all seven actions listed.

Simplifying the chain

Dependence on third parties continues to rise. The “transaction” costs within the enterprise of establishing multiple nodes of partnerships (where risks are hidden) have gone down, thanks to the ubiquity and lower cost of digital interactions via APIs.

Today's trending cyber-attack target may be the most nefarious one yet: your supply chain of trusted vendors, suppliers and contractors. The weapon? A process many have taken completely for granted: the software update. The payoff? Ransom payments to cybercriminals, valuable intelligence to nation-states or training data sets for AI models to competitors. Over the past decade, vendors and hijacked updates accounted for 60% of software supply chain attacks and disclosures, according to The Atlantic Council. The European Union Agency for Cybersecurity (ENISA) predicted in a July 21, 2021 report that supply chain attacks would quadruple in 2021 over the number of 2020 attacks.

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. Detecting and stopping a software-based attack can be very difficult, and complex to unravel. That's because every component of any given software depends on other components such as code libraries, packages and modules that integrate into the software and are necessary for its operation.



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. One benefit is that different functions (procurement, risk managers, fraud team, legal, security) can better understand their roles in protecting their supply chains from cyber disruptions. And with fewer vendors to monitor, your organisation can more efficiently keep an eye on their security practices.

Gaining visibility into the web of third-party relationships and dependencies is a must. Top cybersecurity companies integrate solutions (real-time threat intelligence, threat hunting, security analytics, vulnerability management, intrusion detection and response) on broad platforms.

Finally, good habits go together. In our US Digital Trust Insights Survey, respondents with more advanced data trust practices stood out in multiple ways. They significantly reduced their number of third-party relationships, increased their monitoring, deepened their assessments of third parties and felt confident that their third-party risk management program had shown tangible benefits in the last two years — including increased cost savings, faster implementation of business initiatives, greater customer confidence and enhanced market power.

More than half have taken *none* of three actions that promise a more lasting impact on their third-party risk management

Audited or verified the security posture and compliance of third parties or suppliers



Refined our criteria for onboarding and ongoing assessments of third parties



Provided knowledge-sharing or assistance to third parties shore up their cybersecurity postures



Addressed challenges, cost-related or time-related, that affect your ability to be cyber resilient



Rewritten contracts with certain third parties to mitigate our risks



Performed more rigorous due diligence



Exited relationships with certain third parties



None of the above

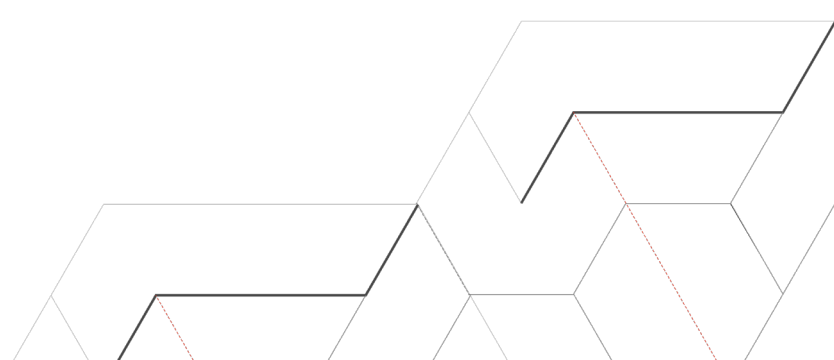


Question: Has your organisation done any of the following actions in the past 12 months to minimise third-party or supplier risks in your ecosystem? Check all that apply.

The three lasting actions are: refining criteria for third-party assessments, rewriting contracts, and performing more rigorous due diligence.

Base: 3,602 respondents

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



Public-private collaboration

Visibility also means seeing which challenges others face and what they are doing to meet them. Collaborators can be an important part of your cyber-business ecosystem. Just ask the companies and federal agencies that benefited from the public-private partnership and government responses to significant cyber incidents early in 2021. Timely sharing of information matters for cybersecurity in general, critical infrastructure or not.

But fewer than one-third of survey respondents said their public-private collaboration efforts are “very effectively” helping them achieve their cyber goals. Those who’ve had the best cybersecurity outcomes over the past two years, however, were **34x** more likely to have achieved their public-private collaboration goals “very effectively.”

Organisations increasing their cyber budgets in 2022 were significantly likely to say they have achieved these goals “very effectively”:

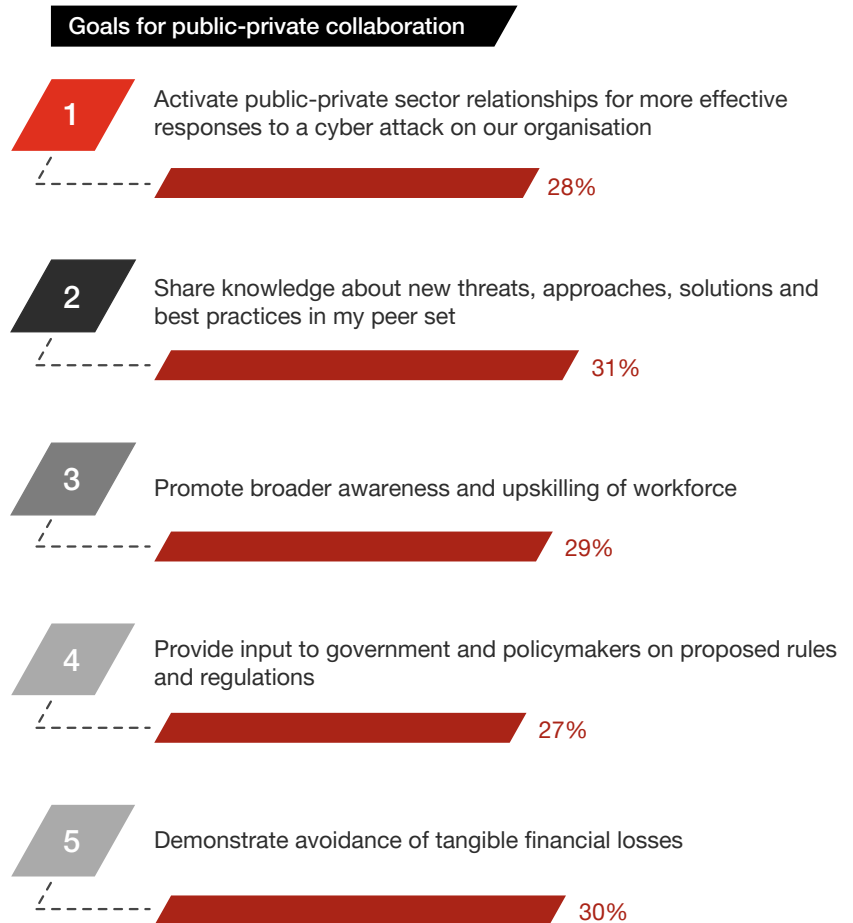
- Share knowledge about new threats, approaches, and solutions in my peer set (38%)
- Demonstrate avoidance of tangible financial losses (36%)
- Activate public-private sector relationships for more effective responses to a cyber attack on our organisation (33%)
- Promote broader awareness and upskilling of workforce (32%)

“Very effective” collaborators also include those in technology, media and telecommunications; those with more than \$5 billion in yearly revenues; and, in terms of promoting broader cyber awareness and upskilling the workforce, female respondents.

For influencing governments and policymakers on proposed rules and regulations, smaller companies perceive that they are less effective than larger ones. Respondents from organisations with yearly revenues under \$1 billion were significantly more likely to say they are “not very effective” at wielding this influence (7%), as opposed to 4% of those with revenues greater than \$1 billion and 3% of those with \$5 billion yearly revenues or higher.

Collaborators are an important part of secure ecosystems. More effective public-private collaboration is needed before, not just after, attacks.

■ Percentage who say that the goal was achieved ‘very effectively’



Questions: Thinking about your most significant public-private collaboration mechanism, what are your organisation’s goals with public-private collaboration? And in the past year, how well has your organisation achieved each of those goals you mentioned?
 Base: 3,602 respondents
 Source: PwC, 2022 Global Digital Trust Insights, October 2021.

Takeaways

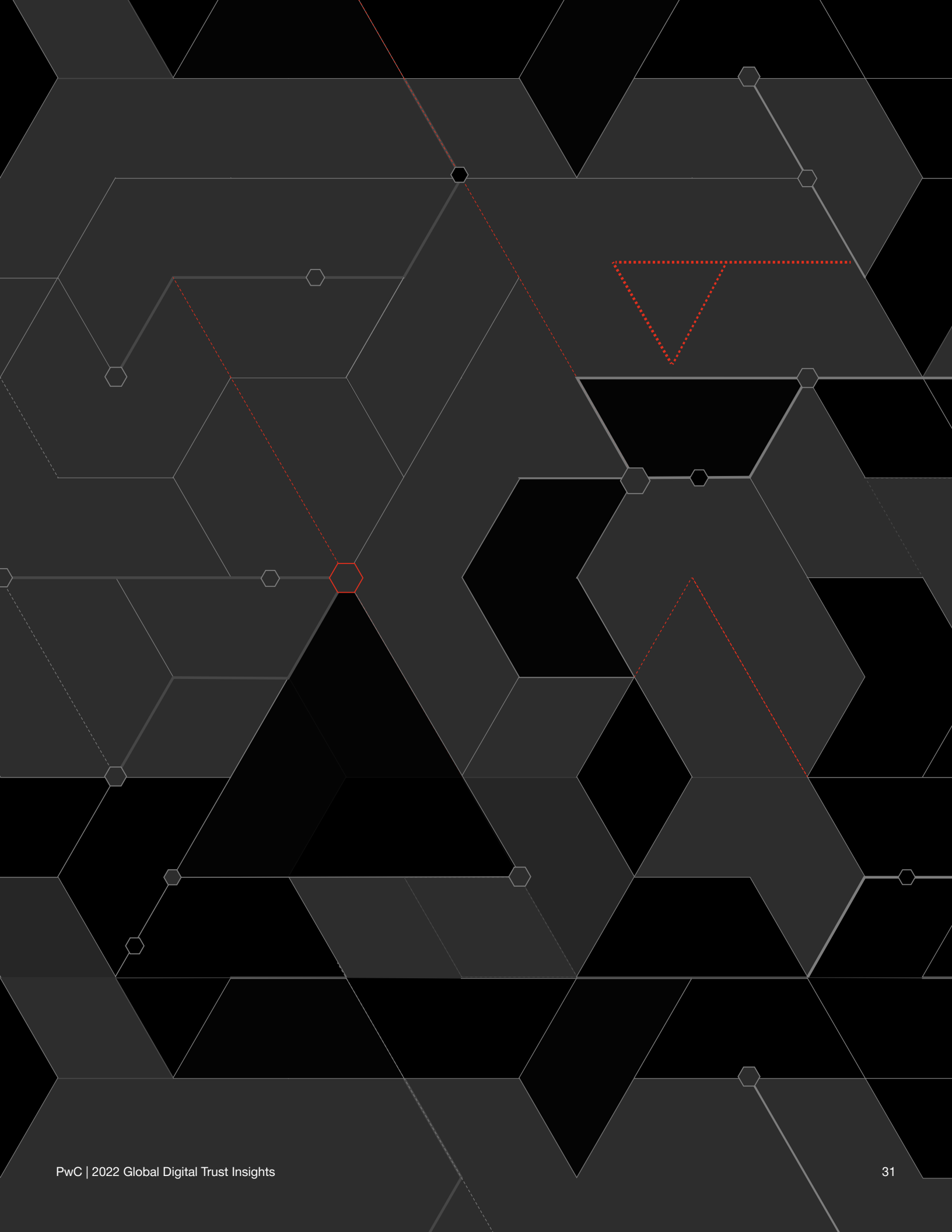
For the COO and the supply chain executive

- 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. The National Institute for Standards and Technology published minimum standards for software testing in July 2021.
- 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?

For the 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. Data trust and good third-party risk management go hand in hand.
- Educate your board on the cyber and business risks from your third parties and supply chain.





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) conducted in July and August 2021. Female executives make up 33% of the sample.

Sixty-two percent of respondents are executives in large companies (\$1 billion and above in revenues); 33% are in companies with \$10 billion or more in revenues.

Respondents operate in a range of industries: Tech, media, telecom (23%), Industrial manufacturing (22%), Financial services (20%), Retail and consumer markets (16%), Energy, utilities, and resources (8%), Health (7%), and Government and public services (3%).

Respondents are based in various regions: Western Europe (33%), North America (26%), Asia Pacific (18%), Latin America (10%), Eastern Europe (4%), Middle East (4%), and Africa (4%).

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

Sean Joyce

Global Cybersecurity and
Privacy Leader, PwC US

sean.joyce@pwc.com