



C-suite playbook on cyber



C-suite playbook on cyber

Cybersecurity has become a dynamic field, rapidly adjusting and shifting to keep apace with business inventiveness.

Agility is what's needed for the tougher challenges ahead. How can you continue to make a difference? Where should CISOs and cyber teams wield influence for the greatest effect?

The C-suite playbook on cybersecurity, featuring our latest Global Digital Trust Insights, highlights what you've done, what you're doing now, and what you need to do to tackle the challenges of 2023 — with your fellow executives, all working together to build **cyber-ready futures**.

Cyber in the suite spot

CISO are seizing the initiative to truly *lead* — to step out of their independent cyber-specialist role and into one of partnering with not just with a few executives, but the entire C-suite. These collaborations have never been more critical.

Forty-two percent of senior executives say cyber breaches of their systems have increased since 2020. Executives and boards should ask again and again, “Are we affected?” and, if not, “Are we vulnerable?”

More than a quarter had a consequential data breach in the past three years that cost more than USD 1 million. Around 10% suffered costs of USD 10 million or more, CISOs and CFOs reported.

To CFOs, the most devastating consequences when a breach (other than a data breach) occurred were:

- Downtime or disruptions
- Damage to service and product quality
- Lost contracts and business opportunities

To privacy and data executives who work with the public, a breach's most dire effects were:

- Lost customers
- Costs to recover data (not counting ransom payments)
- Lost customer data (if not recovered)

These gut-wrenching moments can serve as a catalyst to collaboration, sharpening awareness of a single breach's ripple effects from shop floor to boardroom and calling the entire C-suite to act — together.

As a result, the C-suite has renewed its resolve to do better on cyber and privacy. To get there, top executives are starting to understand the need to work as a cohesive unit — the “suite” spot.

At the centre is the CISO, empowered by the CEO to advocate, collaborate, and orchestrate a better cyber future. Forty-six percent of CEOs — 49% at previously breached organisations — want to give the CISO more authority to drive collaboration on security next year.

A note:

Management teams are organised differently around the world, so we may refer to C-suite titles that might not exist in your organisation.

Consider the titles as shorthand for the executive tasked with cybersecurity in the organisation (CISO) who works with the executives responsible for the overall business (CEO), management oversight and governance (the board), technology infrastructure (CIO / CTO), cyber investments (CFO), operations and supply chain (COO), risk management (CRO), data (CDO / CPO) and human resources (CHRO).

CEOs take a more active stance on cybersecurity this year

More than half of CEOs say they'll demand a cyber risk management plan for each major business or operational change. And more than half say they'll spearhead major initiatives such as streamlining the supply chain and eliminating products that weaken the enterprise's cyber posture.

CEOs at companies that have suffered breaches in the past are even more determined to change how cyber gets done.

CEOs want more information to help them do a better job overseeing their organisations' cyber programmes. More than 35% prioritise three areas for better reporting:

- Cyber risk assessments and practices
- Business continuity plans, contingency, and recovery plans in the case of a cyber incident
- A dashboard on key cyber risks

CISOs are **learning** how to give their CEOs just the right information on their cyber programme and the risks their organisation faces.

Message to the CEO

Where can you, the CEO, make the most difference in cybersecurity? Big changes may be the most effective way to improve cyber posture — and only you can instigate them.

Are you tolerating avoidable, unnecessary complexities in your operations and technologies? This needs to change.

But so often, investigations after a major cyber breach reveal weaknesses more systemic than technological, caused by a lack of focus among enterprise leaders on addressing weaknesses that teams knew existed. Are you ready to support a dramatic turnaround? It could be the most effective fix.

Perhaps a disconnect among your senior executives or between your business and cyber functions is slowing your efforts at growth — an app for consumer use, perhaps; a new business line that uses artificial intelligence; expansion into a new market; or the use of the Industrial Internet of Things in your factory. Isn't it time you joined forces to secure it all?



CEOs forging ahead to tackle cyber insecurity — and win

4% say they plan to be involved in all 6 ways

% of CEOs who say they plan to personally be involved in cyber matters



Q: Which, if any, of the following actions do you intend to take over the next 12 months to be involved in cybersecurity matters in your organisation?
Base: 795 CEOs
Source: PwC 2023 Global Digital Trust Insights Survey

CALL TO ACTION: Speak out about your commitment to cyber. Use your influence to inspire sweeping changes and create a united front against attacks. Rally the C-suite around the notion that the secure way could truly be the easier way to business success.

Boards can spur better cyber reporting to improve oversight

Boards are more engaged in cyber as their companies face increasing risks. Fifty-four percent say their organisation has taken on more cyber risks as it pursues more digitisation, and 44% report an increase in cyber breaches into their system since 2020.



They recognise the challenge of keeping up with cyber. Today, less than half of board respondents say that their board governs cyber “very effectively” in six areas. Fewer than half, for instance, say they “very effectively” understand the causes and effects of cyber risks (37%) or oversee the alignment of cyber risk management to business needs (43%). Only 9% of board respondents say that their board governs cyber “very effectively” across all areas.

But the future of cyber oversight could be different. Corporate directors are willing to learn about cyber and devote time to it. They say these will help them do a better job governing cybersecurity in 2023:

- Internal board training by management (47%)
- Increased frequency of meetings focused on cyber (47%)
- Improved reporting on cyber incidents, practices, and improvements (44%)
- Adding a board member with cyber expertise (43%)

CISOs and the C-suite can help boards get savvy about the cybersecurity of their organisation, especially on these top improvements that boards would like to see in cyber reporting:

- A scorecard / dashboard that helps board members understand the key cyber risks to the organisation with relevant metrics
- The organisation’s cybersecurity strategy and how it is aligned with its overall strategy
- The business continuity, contingency and recovery plans in the event of a cyber incident

Boards are more engaged in cyber as their companies face increasing risks.

Boards know they need to be better cyber stewards

9% say their board governance is very effective on all 6 counts

Oversight of the alignment of cyber risk management to the business’ needs



Understanding the drivers and impacts of cyber risks to the organisation



Alignment of cyber investments against the most important risks



Overseeing the organisation’s collaboration with public sector on cyber matters



Monitoring the organisation’s systemic resilience to cyber threats



Understanding how the organisation’s design supports cybersecurity goals



Very effective Moderately effective
Slightly effective Not at all

Q: In your view, how well do you in your role as a board member exercise governance over the following areas of cybersecurity in your organisation today?
Base: 124 corporate directors
Source: PwC 2023 Global Digital Trust Insights Survey

Message to corporate directors

CALL TO ACTION: First, allot more time to the CISO and cyber matters on your agenda. Second, don't settle for board reporting that doesn't give you confidence and insights that the organisation is managing the cyber risks related to its strategic moves. Cybersecurity is not an end state, so monitor how the company is making progress in its cyber posture and ability to defend against emerging threats. Ask to take part in exercises that help you understand your organisation's cyber resilience.

The new era of cyber transparency

Stakeholders clamour for more information about how companies manage their cyber risk exposure.

Regulators want visibility into cyber practices because they want to protect citizens from fraud and loss of privacy, help investors make better decisions, and prevent industry- or system-wide disruptions. India has published [guidance](#) on cyber incident notification required under the Information Technology Act. The UK Financial Reporting Council has issued [guidance](#) about digital security risk disclosures after it found that current disclosures by some FTSE 350 companies are not meeting investor needs and are often 'boilerplate' and overly static. In addition to the rules pending with the Securities and Exchange Commission ([proposal](#)) and the Cybersecurity & Infrastructure Security Agency ([law](#)), the New York State Department of Financial Services is weighing a [proposal](#) that turns leading practices into regulatory requirements for covered entities.

Investors are looking for consistent and comparable disclosures so they can put their money in companies that fit their needs. Cyber incidents can affect shareholder value — temporarily or permanently.

Individuals know how their data and privacy are vulnerable to cyber breaches. **Business partners** want their data and other assets to be safe. These stakeholders want to understand how much they can trust in the ability of businesses and entire systems to withstand increasing cyber threats.

The C-suite sees an upside to all this transparency. Four-fifths of senior executives in our survey agree that mandatory disclosure of cyber incidents, with comparable and consistent formats, is necessary to gain stakeholder confidence and trust.

But fewer than 10% are confident that their enterprise can comply. More than half are [not confident](#) that they:

- Can provide required information about a material or significant incident within the required reporting period after the incident (58% not confident)
- Can assess the materiality of a cyber incident for purposes of reporting (58%)
- Can describe the relevant cyber expertise on the board for purposes of reporting (59%)
- Have a policy stating which information can or cannot be disclosed regarding cyber incidents (60%)
- Can provide information about third-party risk management (63%)

CALL TO ACTION: CISOs can position their teams to work with the CFO, general counsel and other senior executives to prepare to translate strategy and practices into an accurate, cohesive and compelling narrative on the company's cyber risk management practices. The new era of cyber transparency means that CISOs should become adept at presenting information in a way that the board, senior management and investors can understand and act upon. It requires a communication strategy that's different from the everyday jargon of cybersecurity.



CIOs, CTOs, and CISOs tackle cloud security



CISO



CIO/CTO

“Is our cloud security plan as agile as our business is, itself, in the cloud?” That’s the question CIOs and CISOs should be asking now.

Cloud-based threats are increasing at nearly 40% of organisations. Meanwhile, nearly two-thirds of senior executives say they haven’t fully mitigated the risks of cloud adoption.

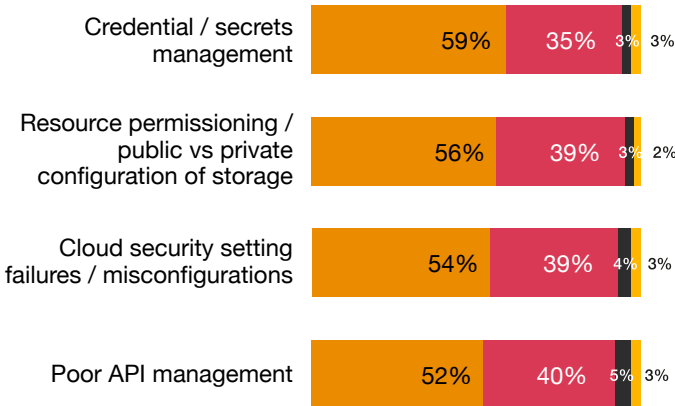
The news isn’t all negative. Half of CISOs, CIOs and CTOs say they’ve made progress in putting governance in place, credential management, resource permissioning, cloud security configurations and API management.

But only 19% are “very confident” that their organisation has adequately secured all these common cloud-breach pathways.

The CIO or CTO and their DevOps team may feel eager — or pressured — to take advantage of the agility, speed and collaboration working in the cloud affords.

Cloud security initiatives are paying off, but more work remains

Only 19% are very confident that their cloud environment is secured appropriately against all four



■ Very confident ■ Somewhat confident
■ Not at all confident ■ Don't know / Not applicable

Q: With regard to your cloud environment, how confident are you that your organisation is secured appropriately against the following reasons for cloud security breaches?
 Base: 1,253 CIOs, CISOs, CTOs and other senior IT and security executives
 Source: PwC 2023 Global Digital Trust Insights Survey

They may allow developers to stand up projects in a cloud environment before security is in place, or “lift and shift” existing systems into the cloud with plans to secure them later.

These personnel may sidestep the CISO to avoid the methodical, security-first approach the CISO would almost certainly advise. In the fast-paced digital world, the business side knows, enterprises need speed to achieve their objectives. When agility and speed are the goals, who needs brakes?

But cohesive governance is key, especially in a multi-cloud environment where each cloud service provider has different security abilities and requirements. Frequent releases of new features and updates means that, like the clouds in the sky, your enterprise cloud environment is continually changing.

In 2023, it's time to design an [overarching security architecture](#) that includes all the cloud platforms your enterprise is using.

Bring together all your enterprise security controls so you can secure them from one location, and with as much automation as possible.

Build infrastructure-as-code (IaC) and DevSecOps tooling to automatically set the right security checks on all your cloud platforms.

CISOs might provide developers with cloud security services that are easy to use and conform to the organisation's security policies. Building an encryption API for developer use, for instance, can help speed an application's time to market as well as confirm that encryption uses company-approved protocols.

Message to CIOs and CTOs

Form alliances with your CISO and DevSecOps team. Adopt the “shift left” paradigm and start putting in place cloud security mechanisms before cloud use begins — or, if it's too late for that, as soon as possible.

Fast development and strong controls can go hand-in-hand. Leading companies design and administer [controls](#) that operate not at the sluggish pace often associated with oversight, but at the quick and agile speed of DevOps. In these organisations, everyone wins.

CALL TO ACTION: To secure your back-end, front-end, IoT and operational technologies, work with the CISO to lock down your cloud environments.





CFOs and CISOs get serious about cyber investment risks vs. rewards

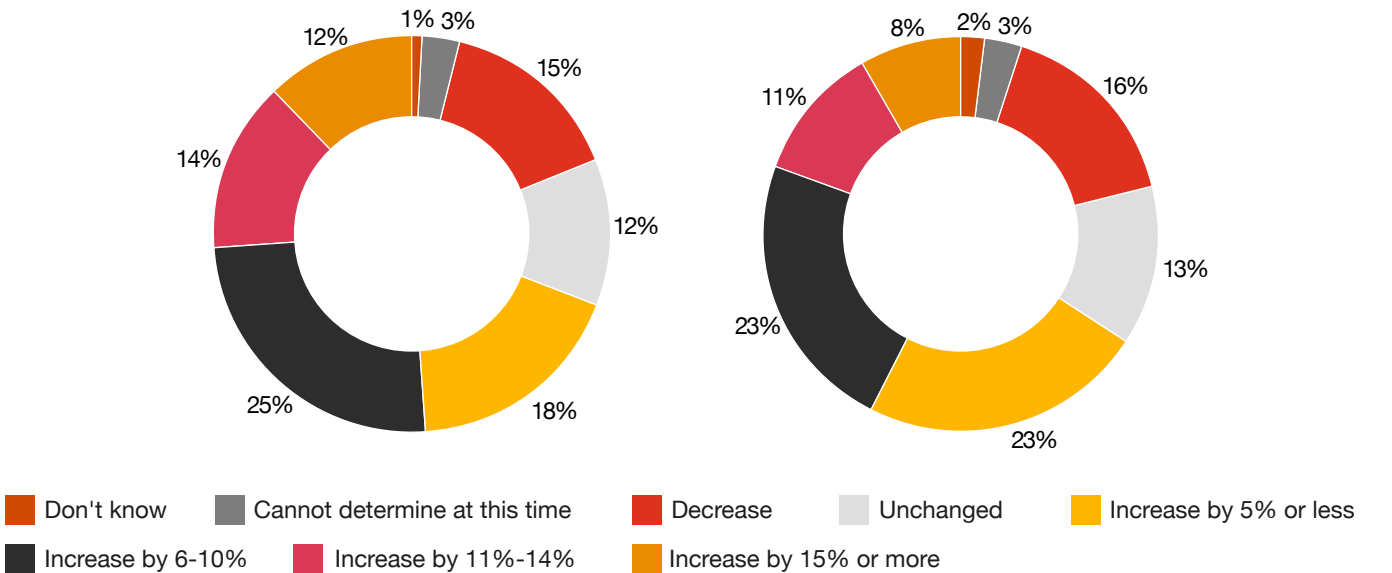


Companies continue to increase their spending on cybersecurity. Sixty-five percent of senior executives tell us they expect an increase in 2023, compared to 69% in 2022.

But they aren't increasing cyber budgets as much as they did for 2022. While more than a quarter of enterprises expected 2022 cyber outlays to rise by more than 10%, fewer than one-fifth expect that rate of escalation next year.

Not surprisingly, organisations that have been breached were significantly more likely to say that they would boost their 2023 cyber spending: 68% versus 55% that have not been breached. And among larger enterprises (with yearly revenues greater than USD 1 billion), 10% said their cyber outlays would rise by 15% or more.

Companies rein in cyber spending increases

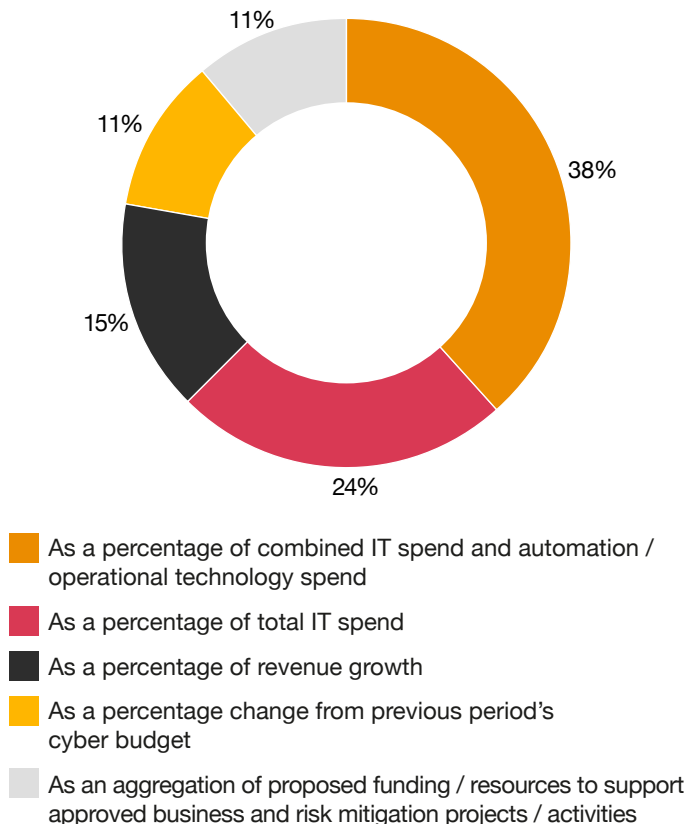


Q: How is your organisation's cyber budget changing in 2023?
Base: 3,522 business and technology executives in this survey; 1,638 security and technology executives in last year's survey
Source: PwC 2023 Global Digital Trust Insights Survey

Budgeting for cyber is changing

When they budget for cyber, enterprises are taking a more expansive approach. Nearly 4 out of 10 CEOs, CFOs, and CISOs tell us their companies now fund cybersecurity as a percentage of *all* tech spending, including OT and automation. Another 15% say they budget for cyber as a percentage of revenue.

How organisations set their cyber budgets



Q: How does your organisation set its cyber budget?

Base: 2,498 CEO, CFO, CISO, CIO, CTO and other executives in finance, security, IT roles

Source: PwC 2023 Global Digital Trust Insights Survey

Many have begun to shift their cyber investment strategy, as well. More than half say they're choosing "to a great extent" how to spend on cyber in line with seven key parameters, including:

- Aligned with the overall business strategy (55%)
- Reflecting cyber priorities (55%)
- Adding value to the organisation (52%)
- Balancing immediate and long-term needs (51%)
- Informed by risk quantification (51%)
- Considers the risk appetite of the organisation (51%)
- Allocated well against the risks that the organisation faces (51%)

We saw this shift coming in our [2021 survey](#), in which 50% of senior executives said they wanted to see budgets better reflecting business strategy, 44% wanted a better budgeting process and 44% wanted to quantify risks.

Fewer than 8%, however, indicated that they'd made this shift in every area. Respondents from the largest organisations were significantly more likely to say that they've evolved how they invest, with 60% saying their spending supports the business strategy, for example.

Modernisation of tech

Cyber tech solutions are at the top of the list of areas that CFOs see as key to improving their organisation's cyber posture.

Indeed, modernisation, especially of operational technology, is still a problem at many organisations. Outdated tech and managing its vulnerabilities are top barriers to improving security of operational technology, CISOs, CIOs, and CTOs say.

Complexity, too, remains a big concern. Simplifying and consolidating the software portfolio is a top 2023 priority among respondents that have been breached in the past three years. Our [2022 Global Digital Trust Insights report](#) foresaw this trend with 75% reporting that their data, technology and other operations were too complex, causing concerns about cyber risk.

It's telling that another major focus among the previously breached is the elimination of technical debt — the literal and figurative costs of cutting corners in development for the sake of speed. For the rest, however, it ranks near the bottom of the list of cyber transformation goals.

CFOs support more resources to improve their organisation's cyber posture

Percent who plan to increase these resources in the next 12 months



Q: In which areas do you plan to increase resources the most to improve the cybersecurity posture of the organisation in the next 12 months?

Base: 326 CFOs

Source: PwC 2023 Global Digital Trust Insights Survey

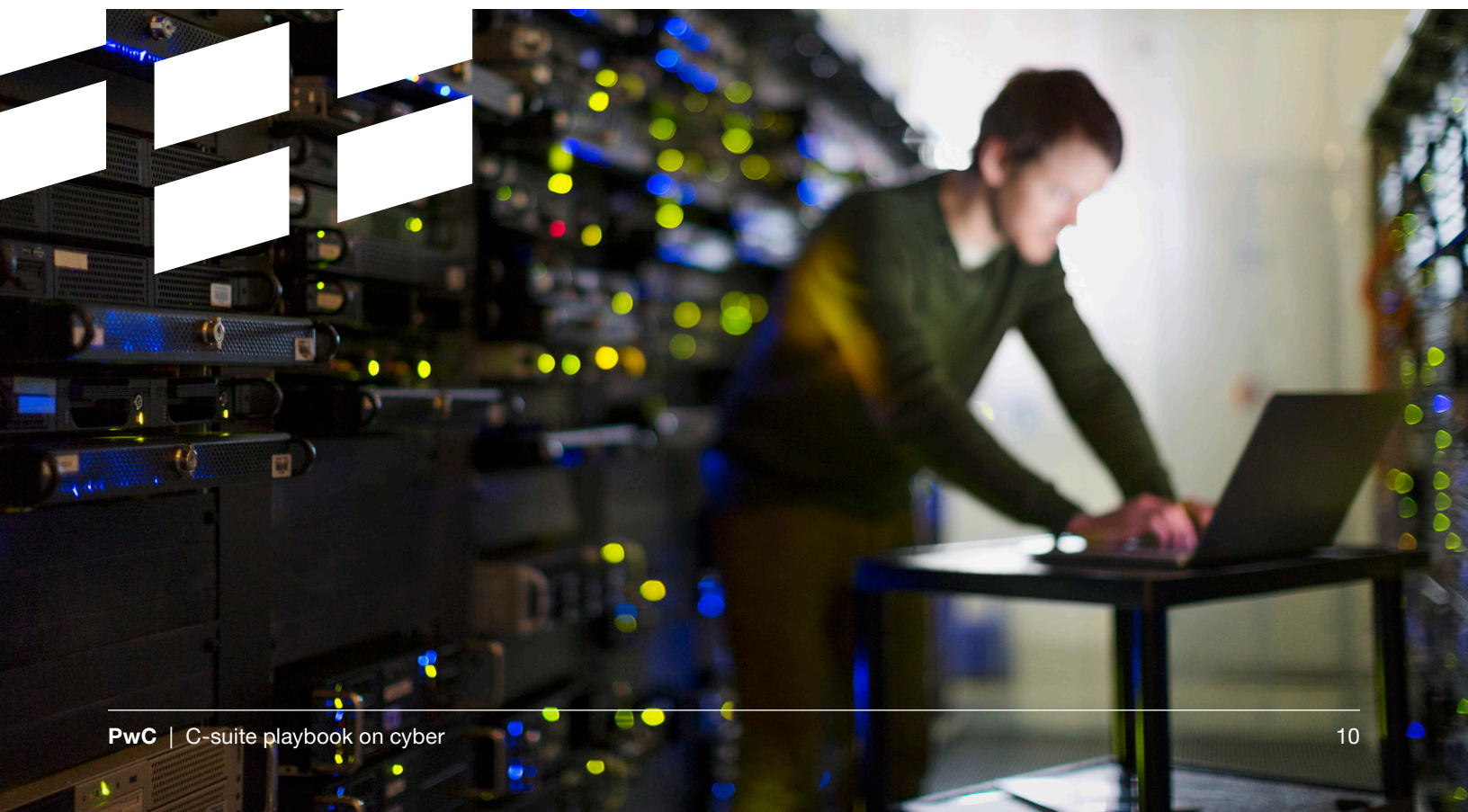
Message to CFOs


You're right to ask, "Are we spending enough and in the right areas? Are we getting the right amount of cyber risk reduction from our investments?"

As tech solutions proliferate, you'll need to work with the CISO to craft a [big-picture plan](#) to secure your organisation at multiple levels while also simplifying and streamlining all your company's software. Mind your early cloud deployment — the workloads that were "lifted and shifted" to the cloud. They, too, contribute to your technical debt.

The open nature of the cloud also requires organisations to tighten their trust parameters — to zero. You'll need a big-picture plan for your shift to [zero trust architectures](#). Thirty-six percent of CISOs say they have started to implement components of zero trust and another 25% will start in the next two years.

CALL TO ACTION: As you modernise and simplify IT, ask how each incremental amount you spend can reduce the most cyber risk. Companies that know the monetary costs of risk are more likely to secure by design — and save.





COOs and CISOs team up on plans to defend against rising attacks to the supply chain and OT



The supply chain is a focal point for cyber and other threats, competitive and macroeconomic pressures, and ESG concerns.

More than half (56%) of CROs and COOs tell us they're **extremely or very concerned** about their ability to withstand supply chain attacks.

Only about one-quarter strongly agree that their operations workforce has the needed digital skills, or that they have invested enough, to prevent cyber attacks from disrupting their supply chain.

And they worry that their ability to control these threats rests partly in the hands of third parties that are ill-equipped to protect them. Only one-fifth strongly agree that their third-party partners and suppliers have invested or are doing enough to prevent supply chain disruptions from cyber attacks; 13% disagree.

More than half (56%) of CROs and COOs tell us they're extremely or very concerned about their ability to withstand supply chain attacks.

Operational technologies: More, better solutions needed

Only about one-third of all survey respondents say they have fully mitigated the risks associated with the convergence of OT and IT or the risks from increased use of Internet of Things.

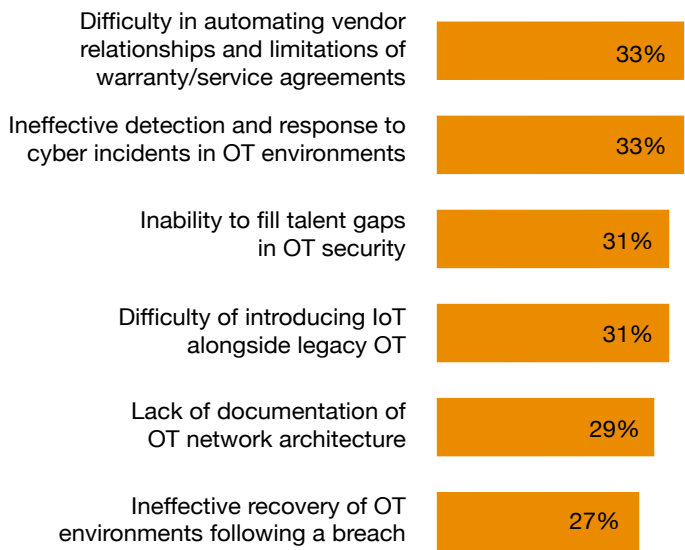
Another area of concern to COOs and CROs is operational technology (OT) security. As OT technologies and solutions grow more sophisticated — using artificial intelligence and machine learning to increase automation in manufacturing plants, for instance — organisations are struggling to keep up with making their operations secure and safe.

Not only CROs and COOs see these challenges. CISOs and CIOs are aware of them, too. Between them, however, lie differences in what each views as the greatest hindrance to modern and fully secure operations.

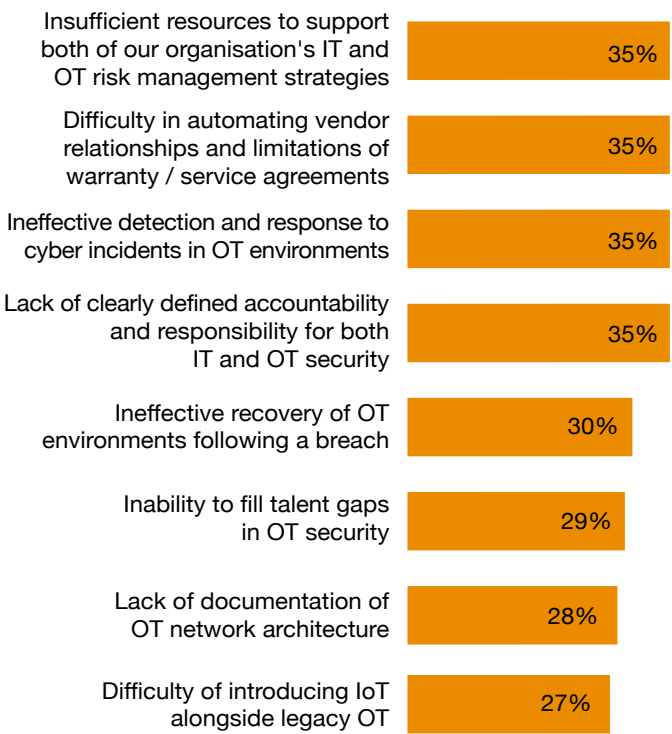
- Both groups say having inadequate tech solutions is a top hindrance to improving OT. They also want solutions that specifically address OT security.
- But for CISOs/CIOs, the number-one obstacle comes from using outdated software and vulnerability-management tools. Altogether, 27%, including CROs, say this is a problem.
- At the same time, CROs/COOs think a more expansive approach to OT cyber risk is in order — one that considers not only business and financial risks but also health, safety and environmental risks. That these concerns aren't getting equal consideration plays the number-one role in hampering OT improvements, they say.

While aware of these deficiencies, CISOs and CIOs also point out that their organisations lack a complete and accurate asset inventory of OT data, people, systems and facilities — critical to operational resilience.

CISO, CIO, CTO view



CRO, COO view



Q: What are your most significant challenges to improving operational technology (OT) in your organisation? Rank the top five.
Base: 1,253 CIOs, CISOs, CTOs and other senior IT and security executives; 711 CROs, COOs, and risk and operations executives
Source: PwC 2023 Global Digital Trust Insights Survey

Message to COOs

As your enterprise operations become increasingly digital, you recognise the importance of working with cybersecurity teams to keep it all secure — and to do more to make up for deficiencies among third-party partners and suppliers.

Your risk, internal audit and compliance teams may already be working with cybersecurity teams on a number of cyber tasks. Half of the CROs/COOs surveyed say these teams are jointly monitoring and prioritising risks consistently. Another one-third are doing so sometimes.

This teamwork is paying off. Nearly four-fifths (79%) of respondents say their cyber team has made progress in securing OT during the past year. Nearly three-quarters say they've seen better collaboration between cyber and OT teams — certainly no coincidence.

But supply-chain and OT attacks have not made it to the top of list in terms of likely threats, which may create complacency. Remain vigilant. We've already seen this year

what can happen when companies let their guard down regarding the software supply chain, and OT attacks are on the rise. Cyber-threat actors seeking a way into your systems often target the point of least resistance, so don't let your domain be that point.

CALL TO ACTION:

Work actively with your CISO to have your teams collaborate on OT and supply chain security from daily tasks such as monitoring to bigger-picture ones such as governance. Ask together how you can build your resilience to interruptions or delays in your supply chain as well as attacks on your OT systems. And work with your CIO and CISO to establish a process for creating cyber risk management plans whenever you're making a major change in your operations.

CROs and CISOs responding to risk with resilience



“Risk” is the word in cyber today. More and more, cybersecurity teams are working together with those in risk, internal audit and compliance, a sign that cyber is taking an important place as an enterprise risk-management priority.

A growing number of CROs, CAEs, and chief compliance officers recognise that cyber means business. Half of respondents say cyber teams are “consistently” monitoring and prioritising risks in tandem with these other functions. Roughly another third are doing so some of the time.

50%	Monitoring risks consistently
50%	Prioritising risks
49%	Have a common understanding of how cyber risks fit in enterprise risk management
49%	Reporting to the board
48%	Responding to cyber attacks and breaches together
45%	Applying a common data governance model
44%	Developing a common view of risks and threats across the ecosystem
44%	Quantifying risks
43%	Providing the business unit leaders (the risk owners) the tools to better manage the risks on the front lines/operations
41%	Applying a common digital governance model
40%	Following one operating model for the division of responsibilities among risk and cyber functions

Those with a breach in their enterprise’s history are much more likely to consistently respond in tandem to cyber intrusions — 50% as opposed to 38% of non-breached companies.

The “all for one, one for all” approach to cyber risk doesn’t happen as often as it might seem at first glance, however. Only 7% say cyber teams work consistently with other risk functions in all risk-related activities. CROs/COOs have work to do in this area.

CROs and COOs do tend to applaud the performance of their organisations’ cyber and privacy teams. Nearly half say these teams are meeting important goals exceptionally well, including putting controls in place to prevent serious disruptions — important for business resilience. However, only 5% of CROs/COOs think cyber and privacy meet all expectations “exceptionally.”

Tests of resilience in 2023

“Life is what happens while you’re making other plans,” the saying goes. It’s also true of business.

Resilience means being able to stay on track even when unexpected problems arise: A catastrophic cyber attack. A global recession. A new health crisis or resurgence of COVID-19. Rising inflation.

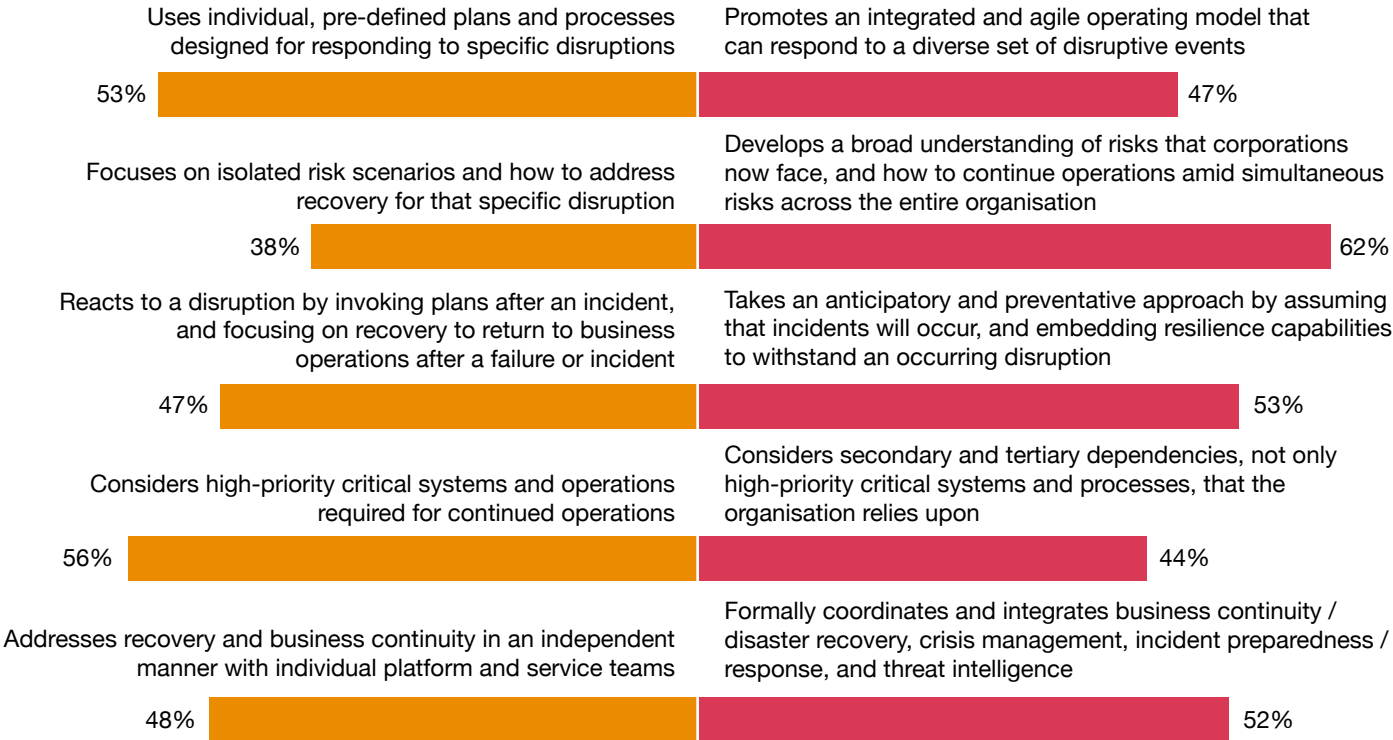
These are our respondents’ top concerns for the next 12-24 months. But few appear ready to handle them with grace.

Taking an “all hazards” approach to identifying sources of disruption is necessary for any organisation in light of today’s risk environment. Yet only 7% of senior executives say they’re taking truly integrated, holistic approaches to five key capabilities that define resilience.

The good news for CROs/COOs is that 62% are handling risk holistically. But in all other areas — incident response, business continuity, disaster recovery — roughly half of organisations appear to treat each breach as a one-off rather than integrating the lessons learned from the various resilience core competencies.

This approach, CROs/COOs are realising, is akin to patching leaks with duct tape rather than making permanent repairs, a much more effective approach.

Fragmented or expansive: What’s your approach to organisational resilience?



Q: For each of the following paired statements, which statement better describes your organisation’s current cyber resilience approach and capability?
Base: 3,522
Source: PwC 2023 Global Digital Trust Insights Survey

Message to CROs

The 2023 scenarios require the C-suite to work together. Breaches, it’s said, are inevitable. A graceful response — one that severely limits the damage bad actors can cause — is largely a function of the groundwork you’ve done to lay a strong, resilient cyber foundation.

Increasingly, financial authorities around the world are collaborating to test the resilience of financial institutions. And regulatory guidance and enforcement is beginning to spread beyond financial services.

You, in partnership with CISOs, should make a case to the CEO and board: true organisational resilience requires much coordination among the entire C-suite, and they need to lead the way.

CEOs may need the occasional nudge to get past their comfort zone, especially if they’re in a state of inertia. They may think they don’t need to act because the company already has crisis

management, business continuity or disaster recovery plans. But how coordinated are these plans? Has the organisation tested them? Can the organisation recover within the time objectives it has established?

CALL TO ACTION: Revisit your risk appetite so you know your resilience limits — the specific meaning of resilience depends partly on an organisation’s risk tolerance and appetite. Rework crisis, business continuity, and disaster recovery plans into a cohesive enterprise resilience plan. Remain in sync with senior executives so you can establish a coordinated approach that keeps the company on track if and when issues arise.



Collaboration on data security and privacy protection is urgent

Companies are becoming adept at using data to better understand what customers want and give it to them. Data is now part and parcel of their customer-centric digital transformation.

A third of CMOs, CDOs and CPOs say they always use data to monitor customer feedback and create personalised customer experiences. More than a quarter consistently use data to find underserved segments and grow their business.

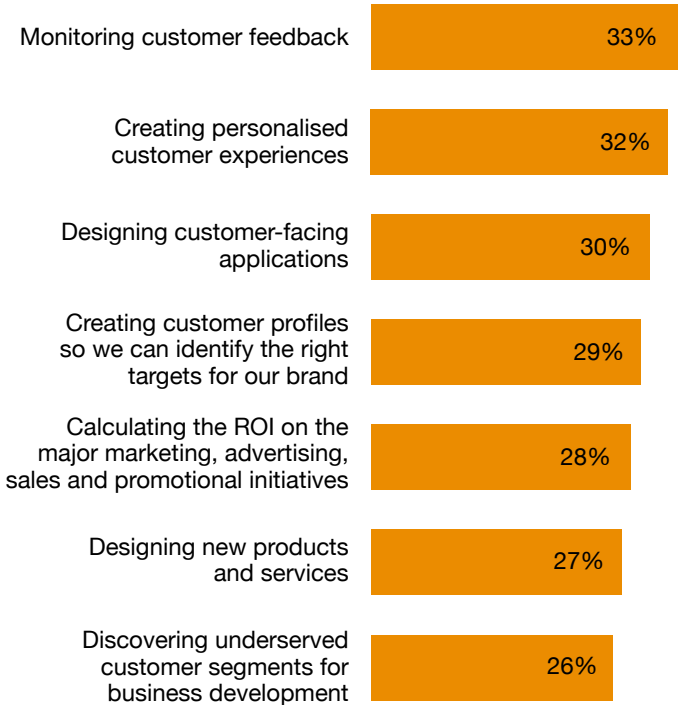
To capture lasting value from this transformation, companies need to process and manage data and algorithms intelligently and efficiently. At the same time, they should address public ethics and privacy concerns and comply with regulatory standards.

But how many really take customer consent and privacy seriously? The approaches to data management and governance that senior executives report is eye-opening — and at the same time, unsurprising.

A third of CMOs, CDOs and CPOs say they always use data to monitor customer feedback and create personalised customer experiences. More than a quarter consistently use data to find underserved segments and grow their business.

To serve customers, data is becoming a must-have tool

% whose organisations always collect and use customer data for the following purposes



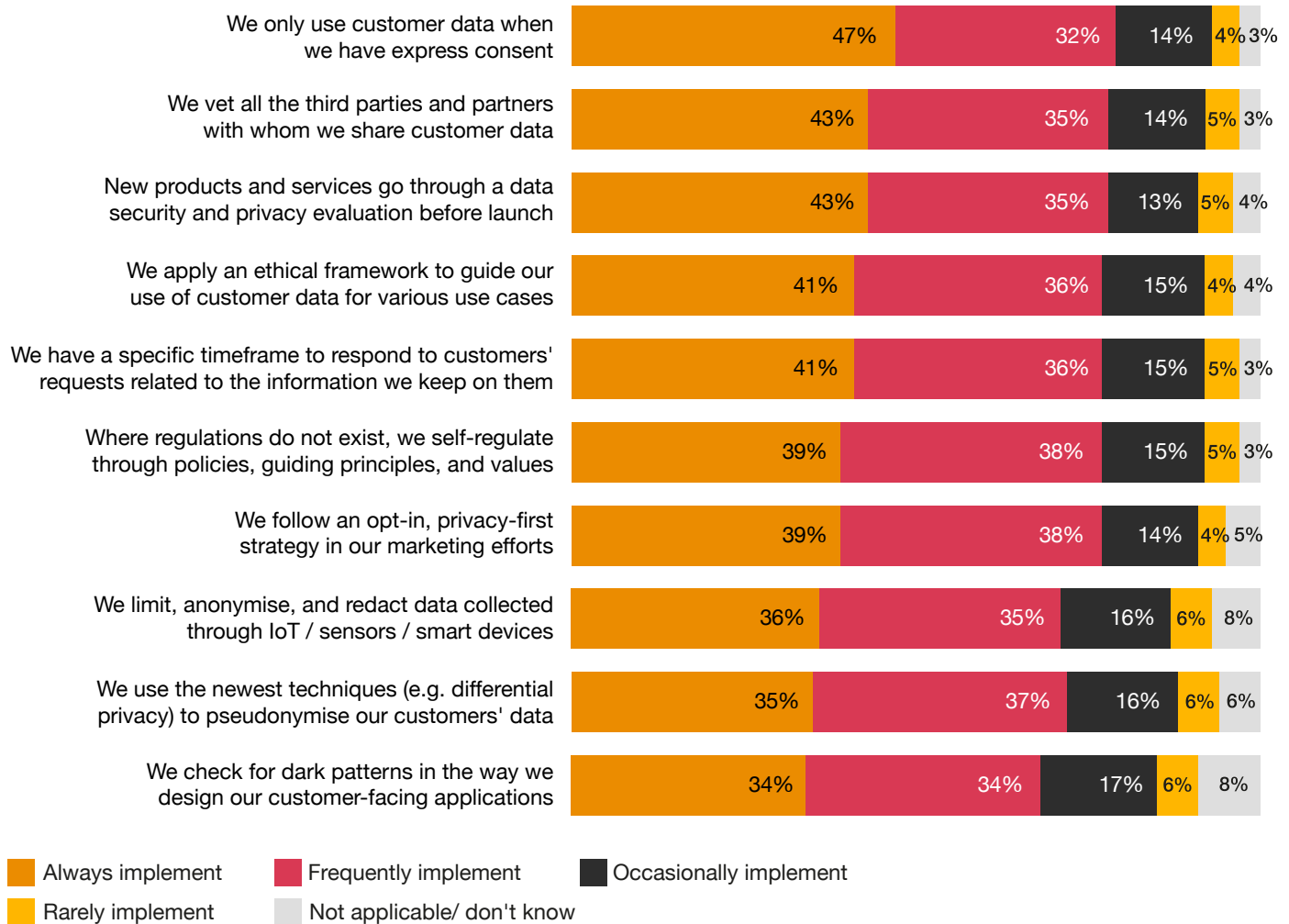
Q: To what extent does your organisation collect and process / use customer data for the following objectives?

Base: 412 CDOs, CPOs, CMOs and senior executives of customer-facing functions

Source: PwC 2023 Global Digital Trust Insights Survey

Data security and privacy are the Achilles' heel of many organisations

Only 5% always implement all these practices and policies



Q: On a scale of 1 to 10, to what extent has your organisation mitigated the cybersecurity risks associated with each of the following in the last 12 months?
 Base: 3,522
 Source: PwC 2023 Global Digital Trust Insights Survey

Half say they might sometimes use customer data without express consent.

Fifty-four percent might not always vet all the third parties and partners with whom they share customer data.

And the same percent might sometimes launch new products and services without a data security and privacy evaluation.

Almost 60% say they might not always check for dark patterns in the way they design the applications their customers use.

In fact, 50% of the executives say that a lack of security and governance is the top hindrance to their greater use of data for decision-making — edging out a want of data accessibility (47%), accuracy (42%), and usability (42%).



Only one-fifth to one-third of the CMOs, CDOs, CPOs, and CISOs strongly agree that their cyber and privacy programme or team:

- Gives them confidence in their ability to nurture trust (27%)
- Helps their marketing function comply efficiently and effectively with regulations (25%)
- Enables them to think through any trade-offs between security and privacy on the one hand and profitable growth on the other (24%)
- Gives them a competitive edge in the marketplace (24%)
- Gives them a competitive advantage with customers (21%)

Message to CDOs and CPOs

You know that you've got to do a better job of governing data and protecting privacy. Among winning companies identified in the PwC's [2022 Market Winners' Survey](#), handling of customer data to improve trust and sharing data-privacy terms in customer-friendly language ranked at the top of cybersecurity investment plans for the next two years.

The teams that would need to carry out these plans are already engaged. The CMOs, CDOs, and CPOs we surveyed say they have very effective working relationships with:

- Chief data officer (41%)
- Customer data analytics team (41%)
- Trust and safety team (41%)
- Chief data scientist (40%)
- Chief digital officer (40%)
- Privacy team (39%)
- Product development team (37%)
- Marketing risk officer (37%)
- DevOps teams (34%)
- CISO (31%)

The potential benefits of a [privacy-first business strategy](#) are massive in boosting customer loyalty, increasing increased consent to use data and improving customer satisfaction.

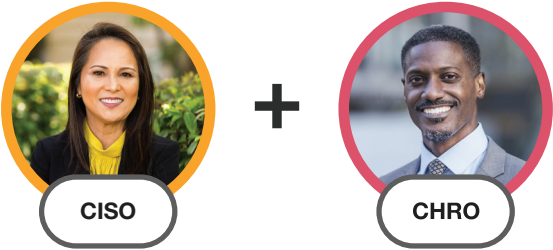
But the potential for disjointed efforts is also huge. Responsibilities overlap among the senior executives — CISO, CDO, and CPO — who can lead the charge on data governance and privacy protection.

Yet CDO positions don't exist in most organisations. Only 21% of the largest 2,500 companies worldwide have a CDO at senior executive level, and these are concentrated in a few sectors (insurance, banking and media and entertainment) and regions (the Americas), according to PwC's [2021 Chief Data Officer study](#). Forty-two percent of CDOs are not C-suite members.

How can you govern and secure your customer data so it stays private as well as safe for the business to use? Start with the governors. Articulate your goals, and understand the different responsibilities and the hand-offs.

CALL TO ACTION: The CDO, CPO, and CISO should create and work off one playbook to cover all the important angles of data security and privacy, including governance, accessibility and accuracy.

CISOs and CHROs are breaking old moulds



Attrition is a growing problem for 39% of CISOs, CIOs, and CTOs. It’s hindering progress on cyber goals for another 15%.

In response, perhaps, CISOs and CHROs are breaking old moulds to fill cyber positions faster and retain the talent they

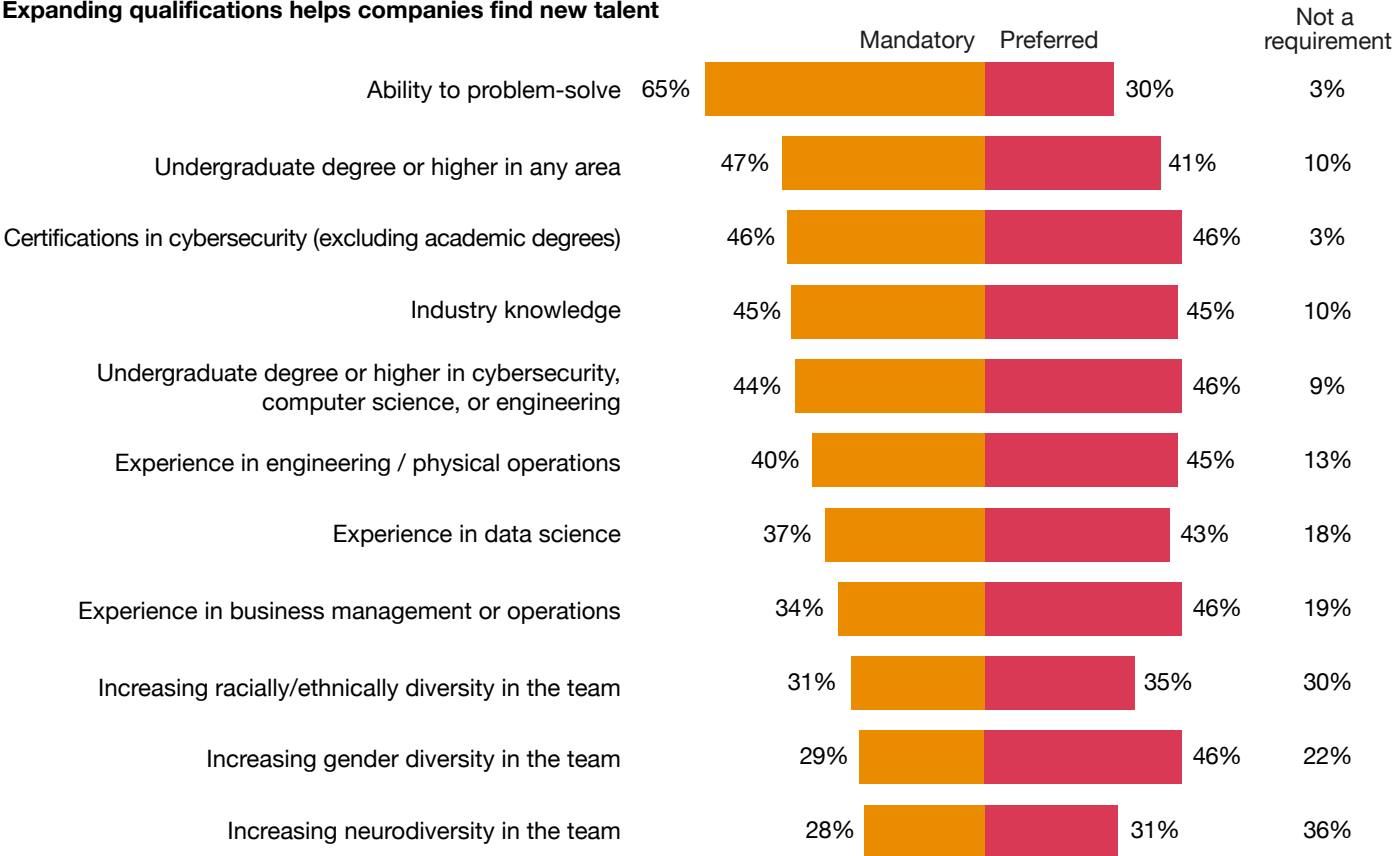
have.

They’re widening search parameters for hires beyond certifications and tech degrees, recognising that some traits — such as problem-solving abilities — are at least as important.

This new thinking can enlarge the pool of candidates. An undergraduate degree or higher in any area has edged out an undergraduate degree in cyber, computer science or engineering as a requirement. For about 10%, neither is even required.

Meanwhile, increasing gender diversity is preferred when candidates are evenly matched in all other qualifications.

Expanding qualifications helps companies find new talent



Q: In hiring for your cybersecurity team, to what extent do you consider the following characteristics in your final hiring decision?
Base: 465 CISOs
Source: PwC 2023 Global Digital Trust Insights Survey

To help close the talent gap, CISOs have found three approaches to be among the most effective:

- Upskilling (45%)
- Hiring incentives, e.g., sign-in bonuses (41%)
- Managed services for cyber (36%)

Securing your managed services

Managed security service is second only to network security as a top investment priority for cyber in 2023.

Just as spending and reliance on managed security providers (MSPs) is gaining steam, so has malicious cyber activity

targeting MSPs. In May 2022, the cybersecurity authorities of the United Kingdom, Australia, Canada, and the United States issued a joint [advisory](#) to companies for safeguarding themselves amid this trend.

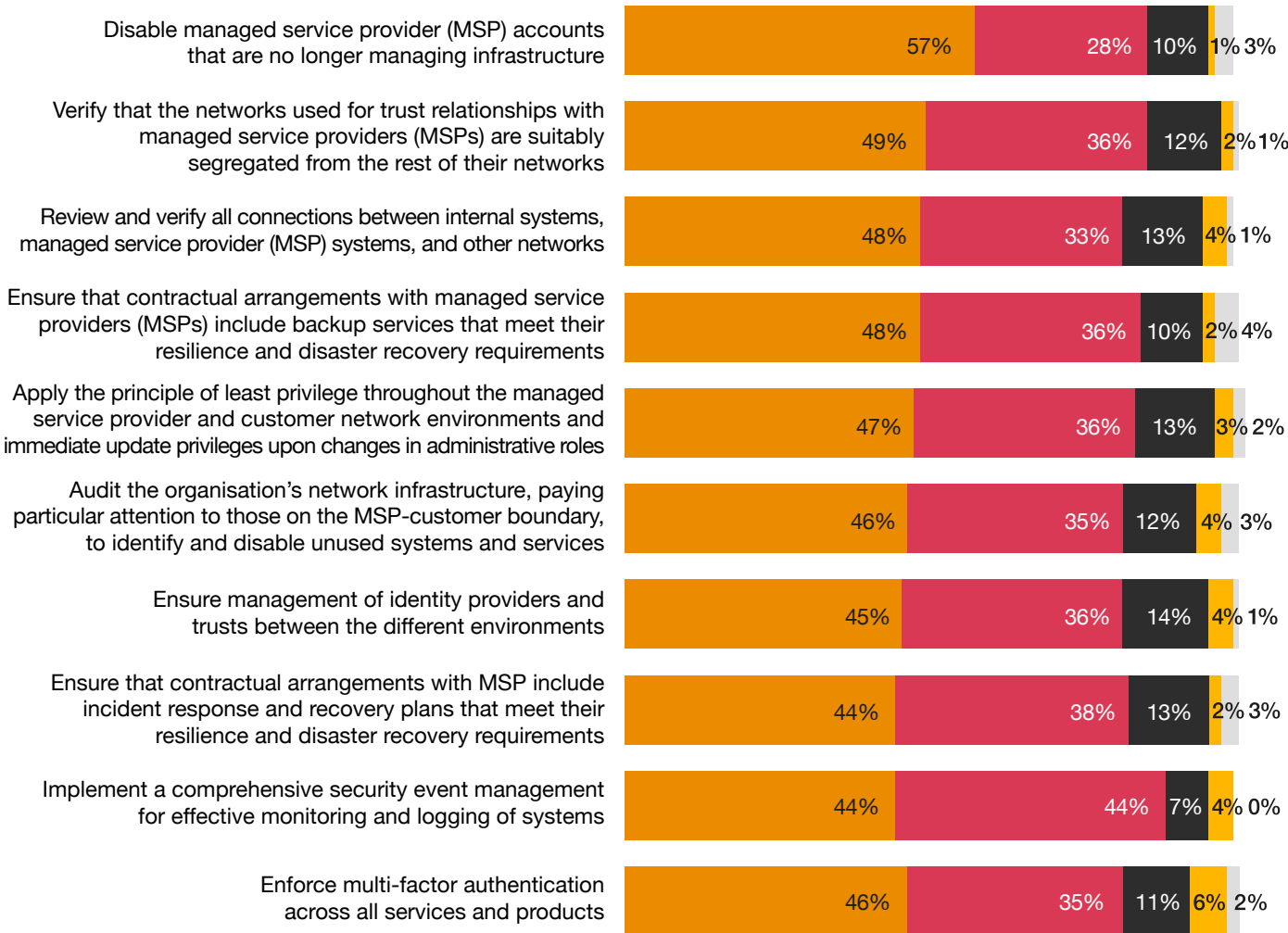
About half of the CISOs we surveyed have fully implemented a number of measures to manage their third-party risks.

Fifty-seven percent report disabling MSP accounts that are no longer managing infrastructure. Forty-five percent enforce multi-factor authentication across all services and products.

But more work remains. Only 2.2% have implemented all these security practices across the board.

Companies are finding ways to use managed services securely

Only 2.2% have fully implemented all 10 practices



Fully implemented Starting to implement Planning to implement Not implemented and not planning to Don't know

Q: Thinking about using managed cybersecurity services, to what extent has your organisation put the following measures in place to manage the risks associated with using external resources to address gaps in your cyber talent and capabilities?

Base: 278 respondents who selected managed services as one of the top effective approaches for addressing the gap in cyber talent

Source: PwC 2023 Global Digital Trust Insights Survey



Message to CHROs

Employee turnover is rising in a variety of markets, while fears of recession are causing companies anxiety about hiring plans. Amid the uncertainty, they might delay doing anything, especially when they know they need to try something new to avert the crisis amid the phenomena described variously as the “great rethink,” “great resignation” and “quiet quitting.”

CISOs and risk executives need to help CHROs ascertain the cumulative effects and cascading operational risks of employee attrition. No matter which creative responses businesses employ to retain and hire talent, senior executives also need to help manage reputational risks.

CALL TO ACTION: Ask which skills you really need in your cyber programme, update how you recruit for those, and give your cyber talent incentives and growth paths that are reasons to stay. Your reliance on managed services and other external talent resources will only grow. Add cybersecurity measures to contracts.

A background image of two men in a server room. One man, with a beard and glasses, is holding a laptop and looking at it. The other man is standing next to him, looking at the laptop. They are both wearing light blue shirts and dark trousers. The server racks in the background have many blue lights.

Scenarios to illustrate need for C-suite collaboration

We've selected three of the cyber event types most concerning to senior executives.

Although the tactics and techniques in these scenarios might require technical expertise to understand, this much should be clear: the consequences of each spill over to areas that executives in operations, finance, data, and enterprise risk management need to address.

The call to action for each C-suite executive isn't intended to be prescriptive. Instead it illustrates the various angles that might need to be addressed for a full and lasting response to cyber attack. In cyber, a disengaged executive is a point of failure.

Braced and ready for different scenarios

How will the scenarios organisations face in 2023 test senior executives' ability to work together amid crises and avoid business disruptions?

Catastrophic cyber attack is the nearly unanimous number-one concern. Only CFOs ranked it second, after global recession and alongside worries about another health crisis such as a COVID-19 resurgence.

These scenarios require the C-suite to work together, but cybersecurity may be the only problem that requires all hands on deck to resolve — and one over which an organisation arguably has some control.

Two-thirds of executives consider cybercriminals to be the most significant threat actor to their organisation in the coming year. Cyberattacks are a thriving business and make lucrative careers for cybercriminals.

Cybercrime-as-a-service and off-the-shelf tools allow criminals to perpetrate and orchestrate a variety of profitable attacks. Ransomware operations, for instance, now run as **businesses** with the main operator “leasing” the ransomware from affiliates. Cybercriminals can then deploy leased ransomware large-scale across multiple targets.

Starting in 2021, the PwC Threat Intelligence group also saw more **commercial quatermasters**, or companies selling cybercrime tools such as spyware, zero-day exploits, and other types of malware to more customers in many countries.

These global operations make it easier to get started in a life of cybercrime: no longer do threat actors need to develop their own malware. At the same time, distributed malware makes identifying the culprits more difficult.

These commercially available tools are effective against a wide array of targets including, perhaps, government officials and private sector executives. Organisations that have deemed these types of threats outside their realm need to think again.

Cyber tops a broad array of perceived threats

% who rank these in their top five scenarios



Q: 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.

Base: 3,522

Source: PwC 2023 Global Digital Trust Insights Survey

Scenario 1: Cloud-based attacks

38% expect more serious attacks via the cloud in 2023

The breach:

Attackers exploit a misconfiguration in the company's cloud-hosted internet-facing application and steal user data to sell on the black market.

Consequences:

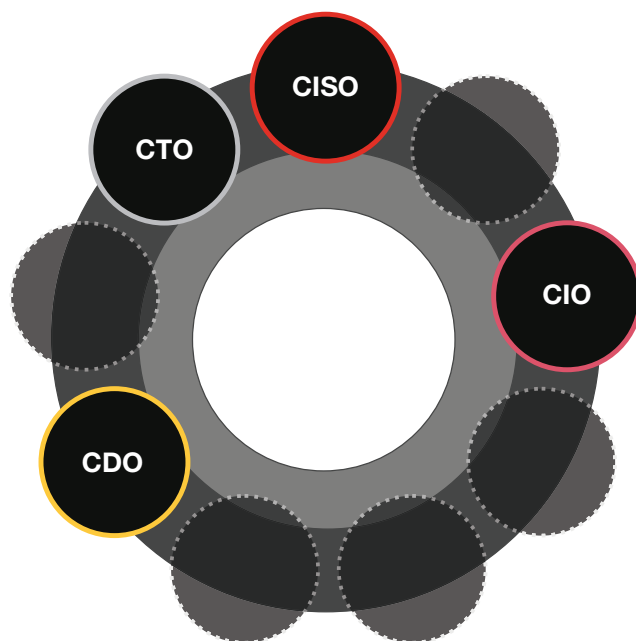
Costly notifications to data owners. A possible class-action lawsuit against the company. Damage to the enterprise's reputation.

What went wrong:

Inadequate security, no defence in depth, coding errors, inadequate testing of written and library code, improperly encrypted data.

How to work together for better defence:

- CIO: Enable DevSecOps in application development, as well as thorough prelaunch testing. Remediate misconfigurations from both users and automated deployments.
- CISO: Establish and enforce policies and procedures for securing applications and data, vulnerability and penetration testing, regular patching, continuous compliance monitoring, and security event and incident monitoring (SIEM).
- CTO: Require that cloud service providers and third parties provide dashboards and tools to detect misconfigurations across their environments.
- CDO: Confirm that apps comply with privacy requirements and that customer data is partitioned and encrypted for better protection. Put into place solutions that encrypt data at rest, in transit, and while in use.



Scenario 2: Attacks on operational technology

29% of large organisations expect an increase in OT attacks

The breach:

A manufacturing system is impacted by a ransomware event due to exploitable vulnerabilities existing in legacy operating systems.

Consequences:

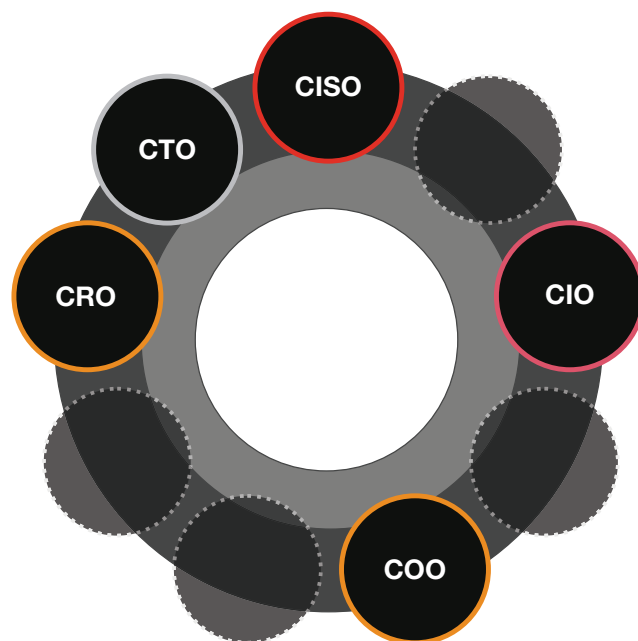
Production stops as affected systems are shut down to prevent damage from spreading. Impacts ripple through the supply chain.

What went wrong:

Hackers exploit unpatched vulnerabilities to inject ransomware. The exploited vulnerabilities were previously patched in enterprise systems, however due to a lack of patch management, monitoring and detection capabilities for the legacy systems, the vulnerabilities remained undetected.

How to work together for better defence:

- CIO: With CISO and CTO, map convergences and critical interdependencies between IT and OT systems.
- CISO: Work with CIO and CTO to require separation of IT and OT, develop a secure landing zone that obscures OT from direct access, and train employees on proper access and incident response roles.
- CTO: With CISO and CIO, create a plan for patching and monitoring endpoints.
- CRO: Develop methodology to assess the cyber risk present in the OT environment. Include scenarios and rehearse incident response procedures that join IT and OT response processes.
- COO: Weigh cybersecurity in the procurement process for your industrial control systems, in contracting with cloud providers, and in defining service agreements with external service providers.



Scenario 3: Ransomware

45% of security and IT execs expect further rise in ransomware attacks

The breach:

A medical employee opens a document in a phishing email, activating malware.

Consequences:

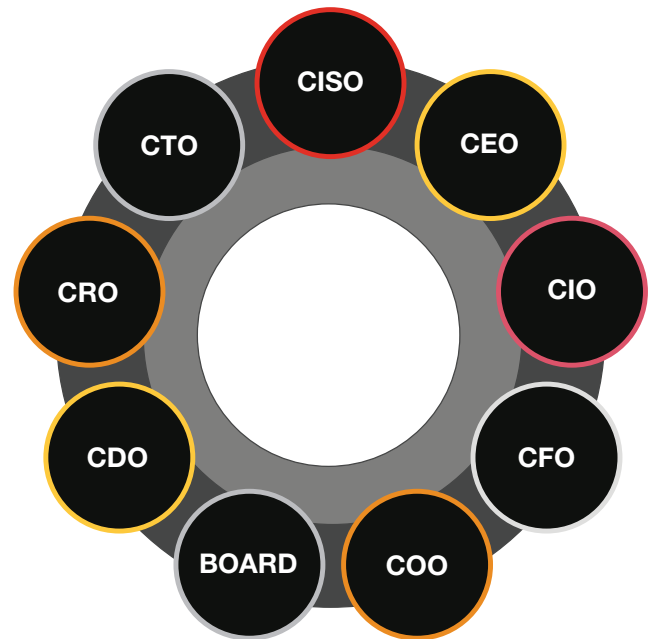
Service disruption and a near-complete shutdown of the hospital networks.

What went wrong:

Antivirus software was running out-of-date rules that failed to detect malware embedded in the malicious attachment. The lack of multi-factor authentication allowed the attackers to obtain initial access. Unnoticed on the corporate network for weeks, the cybercriminals conducted reconnaissance of the network and eventually compromised a domain admin account, giving them elevated privileges to launch malware that shut down much of the core IT infrastructure and compromised backups.

How to work together for better defence:

- CEO: Support security awareness training throughout the organisation.
- CIO: Review the connections between IT systems and the organisation's environment.
- CTO: Assess the vulnerability of medical devices in a scenario that targets devices.
- COO: Help CIO, CISO size up effects on patient safety in similar scenarios.
- CISO: Bridge security gaps between IT and operations.



- CDO: Work with COO, CISO, CPO to assess damage from theft/corruption of customer data.
- CRO: Conduct test of resilience with crisis and BC/DR teams.
- CFO: Work with CISO, CIO on any disclosures to regulators and the public. Review cyber spending, including cyber insurance, with CISO, CIO in light of discovered vulnerabilities. Decide on your policy for ransomware payment.
- Board: Get insight on management's tabletop exercise to prepare for a ransomware attack. Confirm when the board will be informed about a cyber incident or ransomware attack.

For an example of a post-incident review of a ransomware event, please see [Conti cyber attack on the HSE](#).



Contact us to learn more

Sivarama Krishnan

Partner & Leader - APAC Cyber & India Risk - Leader

sivarama.krishnan@pwc.com

PricewaterhouseCoopers Pvt Ltd

Building No. 8, 8th Floor, Tower - B, DLF Cyber City, Gurgaon - 122 022, India