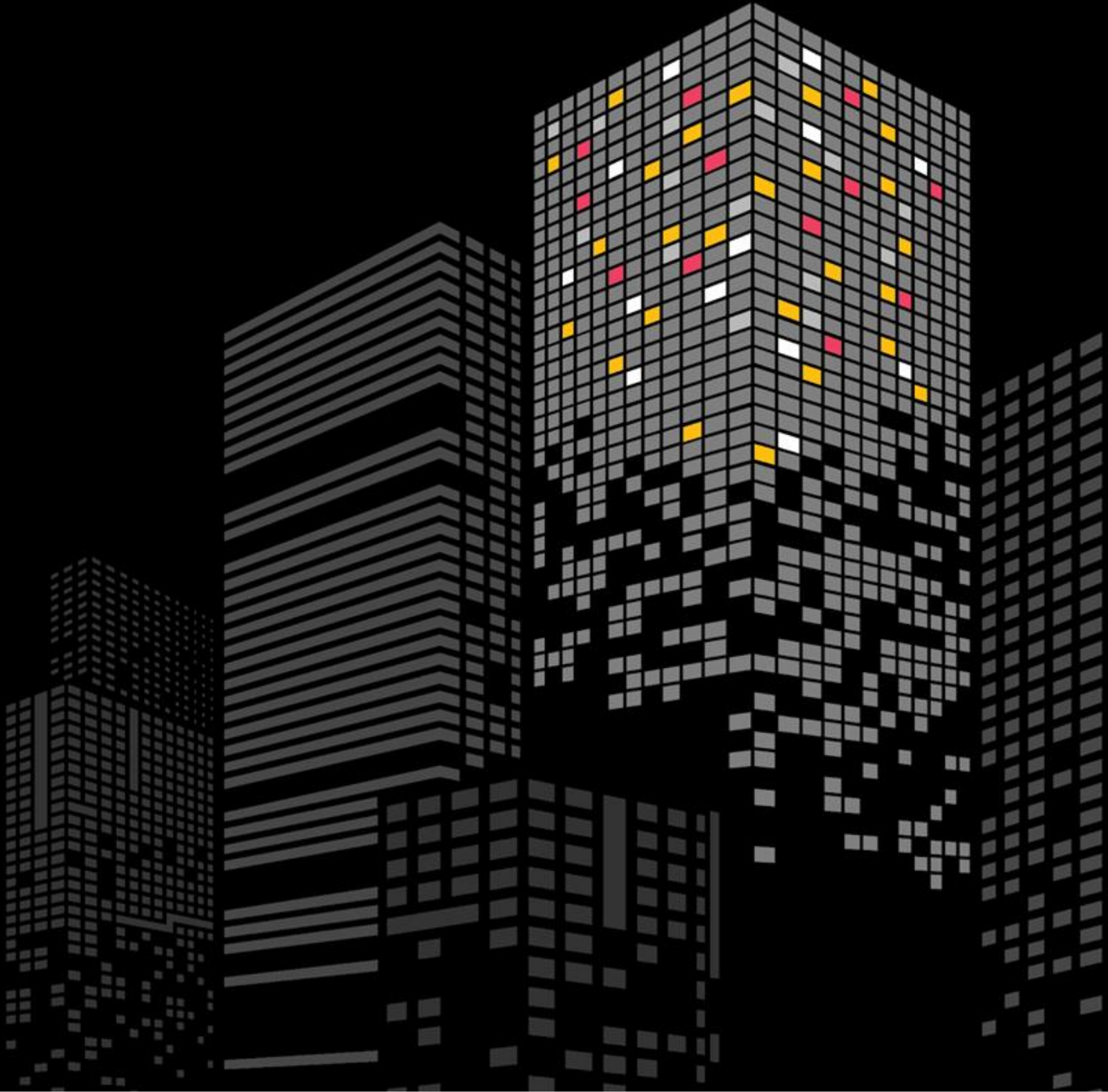
2023 Global Digital Trust Insights

The C-suite playbook on cybersecurity and privacy



Agenda

1. Introduction 03
2. The threat outlook 06
3. Reporting and disclosure 10
4. Cyber in the suite spot 14
5. The need for C-suite collaboration 29
6. About the survey 36

It’s a bold new world in business

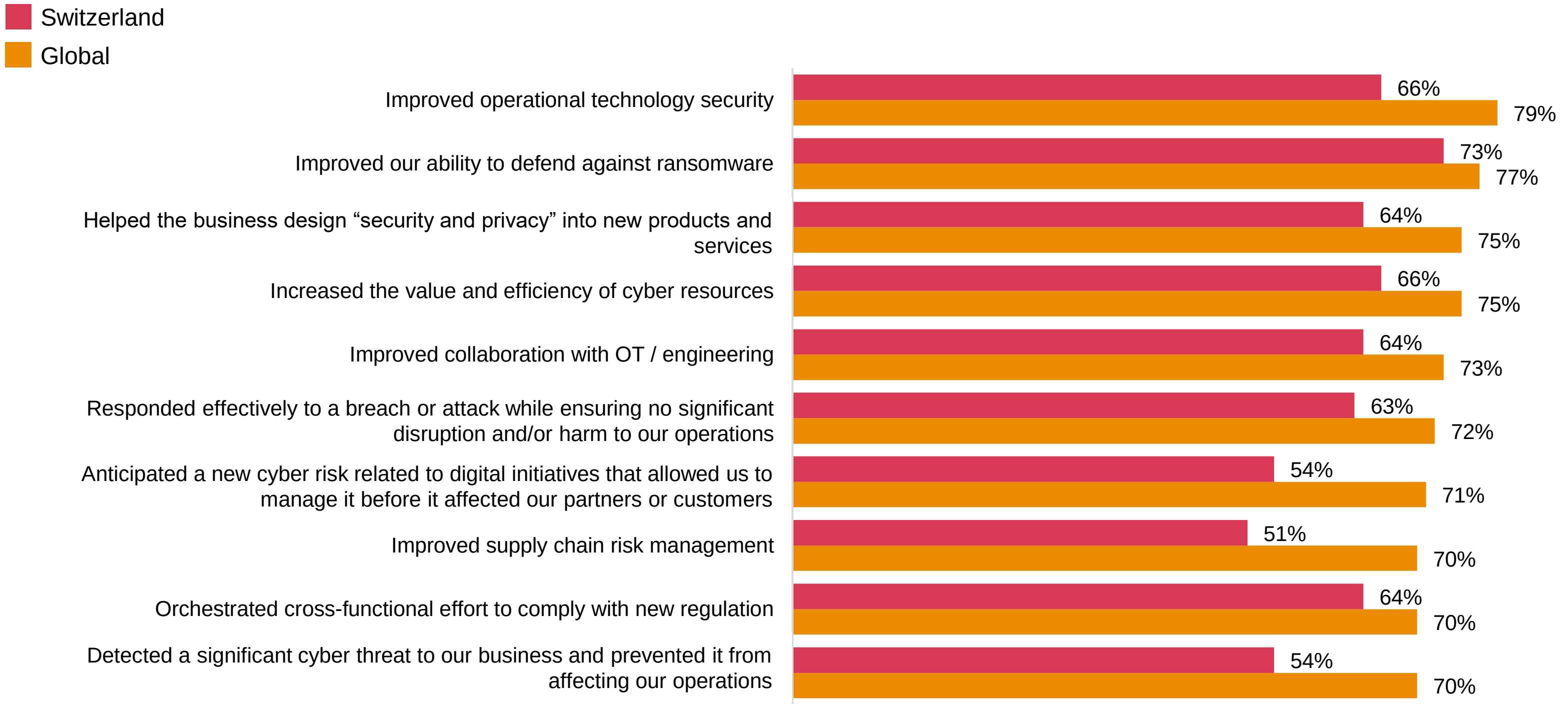
More than 70% of 3,522 respondents observed improvements in cybersecurity in the past year — thanks to cumulative investments and C-suite collaboration.

Cyber has progressed on many fronts, C-suite execs report

70%

of 3,522 business and tech executives saw improvements in their enterprise's cybersecurity this year, **26%** say they accomplished all 10

Cyber has progressed on many fronts, C-suite exec. reports
% who say their cybersecurity team accomplished this in the past 12 months



Question: Please indicate whether or not your organisation's cybersecurity team has accomplished the following in the past 12 months.
Base: 3,522 survey respondents | 70 Swiss respondents

Fewer than 40% have fully mitigated emerging cyber risks

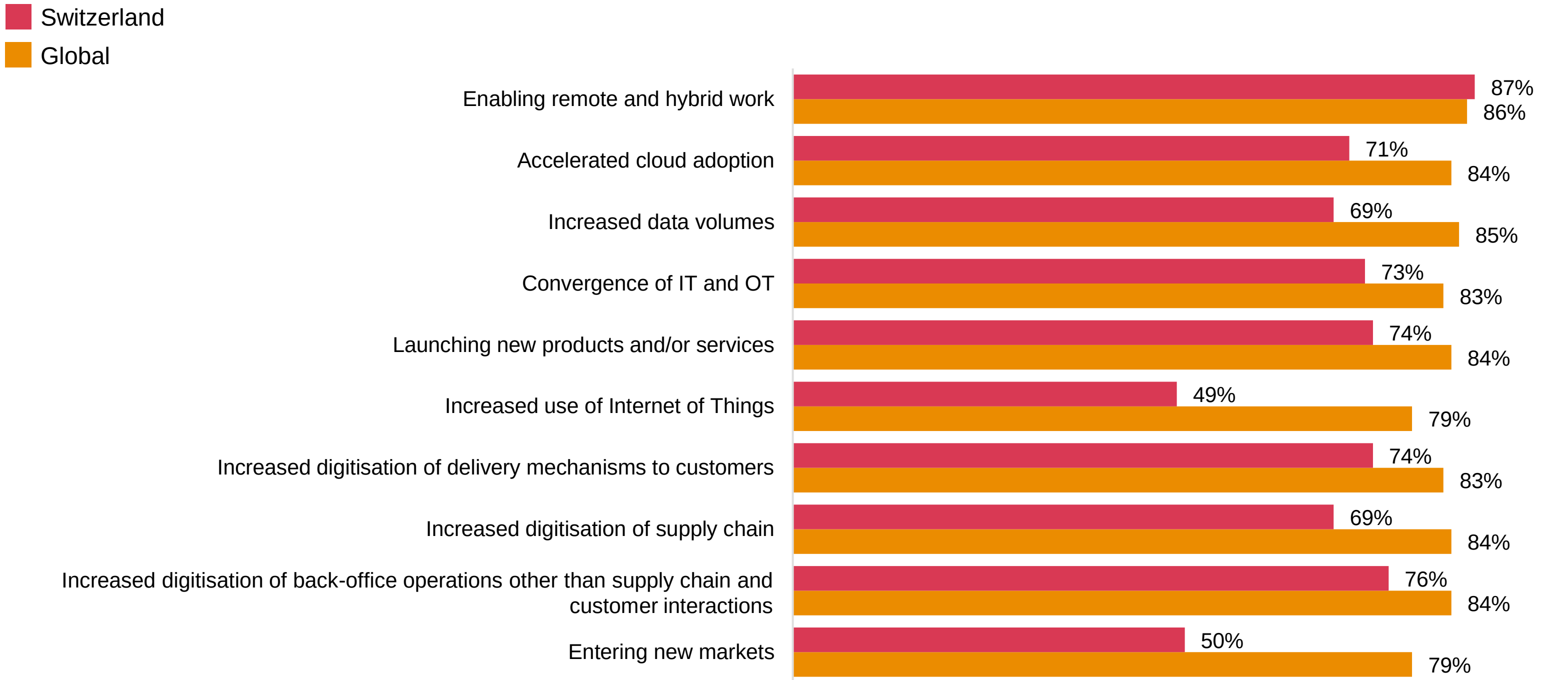
Technology, media & telecommunications organisations are more likely to be fully mitigated for accelerated cloud adoption (40%)

Large organisations (greater than $1B) are significantly more likely to state they have “fully mitigated” against all cyber risks shown

North American organisations are significantly more likely to select “fully mitigated”, whereas Western and Eastern European organisations are significantly less likely to do so

Fewer than 40% have fully mitigated emerging cyber risks

% who say they have fully or moderately mitigated cybersecurity risks with these



Question: 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 survey respondents | 70 Swiss respondents
Respondents who stated ‘Fully / moderately mitigated’

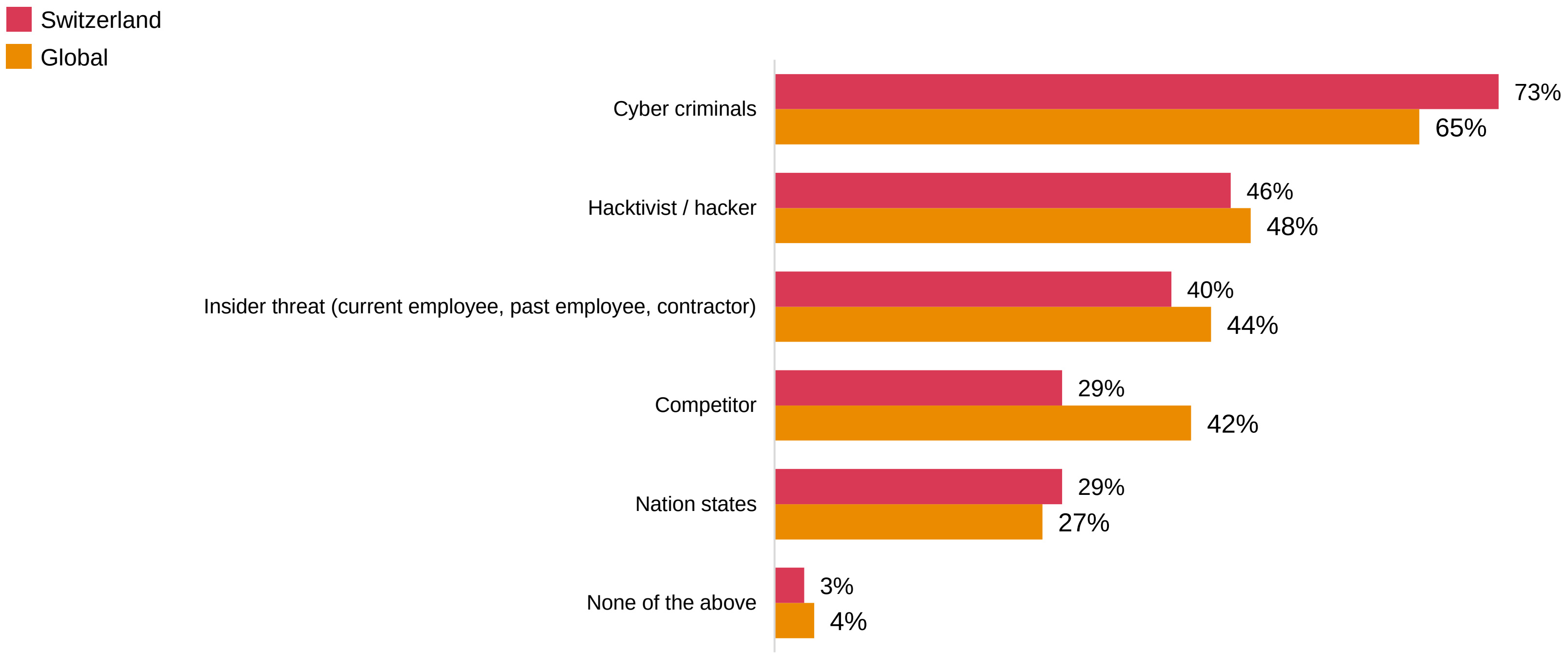
The threat outlook

There's more work to do — and in a tough economic environment.

Threat actors significantly affecting organisations in 2023 compared to 2022

65%

of executives consider cyber criminals to be the most significant threat actor to their organisation in the coming year



Organisations worry about more threats and cyber events in 2023
% who say these threat actors will significantly affect their organisation in 2023 compared to 2022

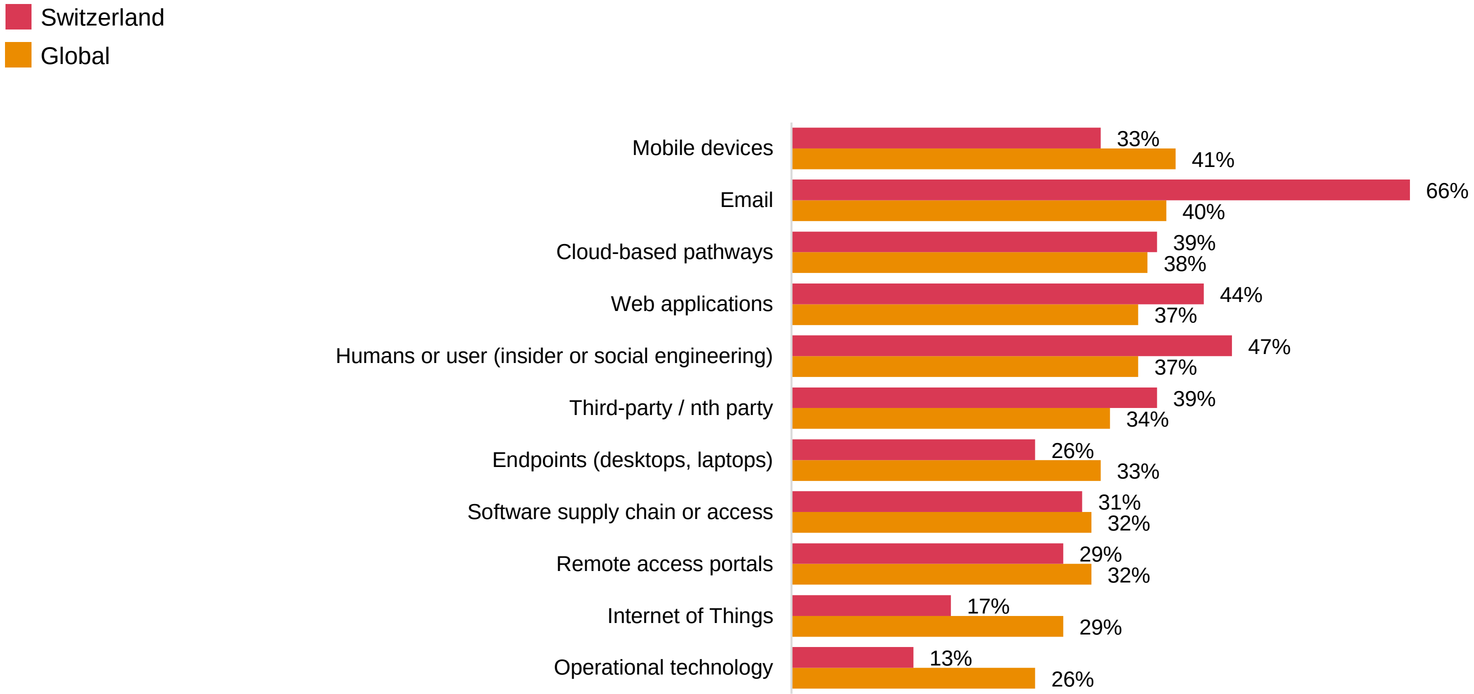
Question: For each of the threat actors below, which do you expect to significantly affect your organisation in 2023 compared to 2022?
Base: 3,522 survey respondents | 70 Swiss respondents

Pathways that adversaries will significantly affect organisations

Larger organisations are significantly more likely to be affected by software supply chain (35%), cloud-based pathways (43%) and operational technology (29%)

Pathways for attacks

% who say that threats via these pathways will affect them significantly in 2023 compared to 2022



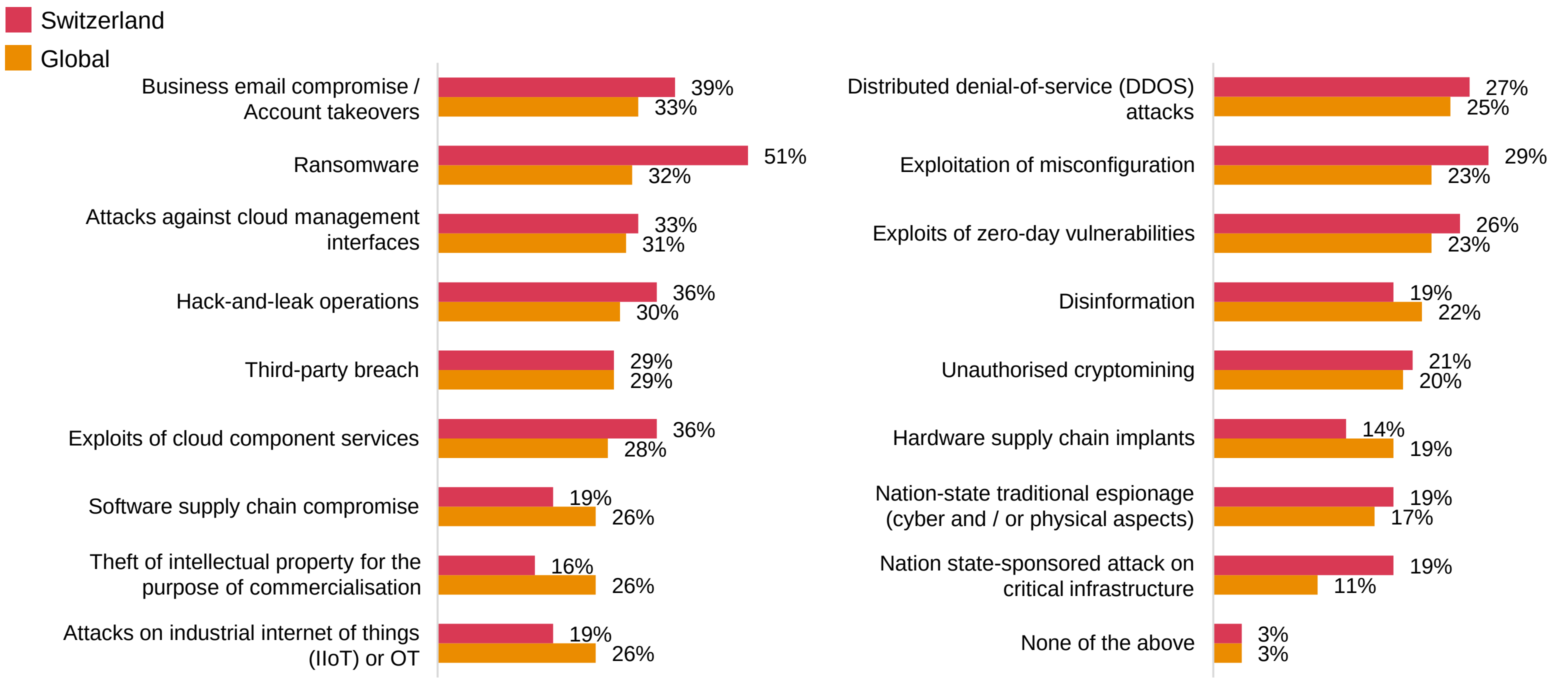
Question: For each of the pathways by which adversaries can gain access to your systems, please select those that you expect to significantly affect your organisation in 2023 compared to 2022.

Base: 3,522 survey respondents | 70 Swiss respondents

Organisational attacks significantly increasing from 2022 to 2023

CISO/CIO/Tech roles are significantly more likely to select:

- Ransomware (45%)
- Exploits of cloud component services (36%)
- Exploits of zero-day vulnerabilities (31%)
- Exploitation of misconfiguration (31%)
- Third party breach (42%)



Cyber events

% who say these attacks to their organisation will increase from 2022 to 2023

Question: Which of the following attacks to your organisation do you expect to significantly increase in 2023 compared to 2022?
Base: 3,522 survey respondents | 70 Swiss respondents

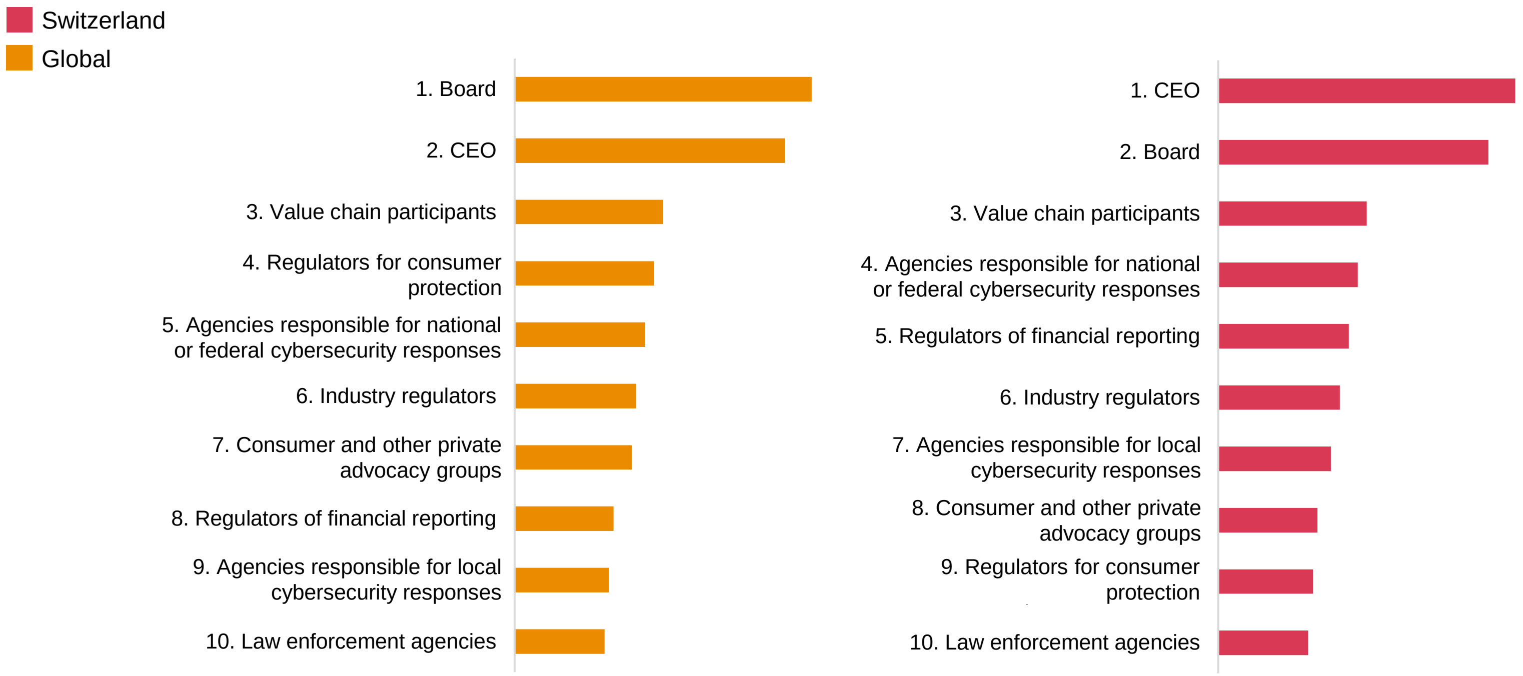
Reporting and disclosure

Disclosure benefits everyone, and companies can learn from the attacks on other companies. Four-fifths of organisations globally agree that mandatory disclosure of cyber incidents, with comparable and consistent formats, is necessary to gain stakeholder confidence and trust.

Good reporting on cyber is key to successful collaboration, which is of the essence in security.

Good reporting and visibility on cyber are key to successful collaboration, which is critical in security. And the CEO and the Board play a pivotal role in launching and improving security programmes.

Organisation priority in terms of addressing stakeholders
(Ranked index)



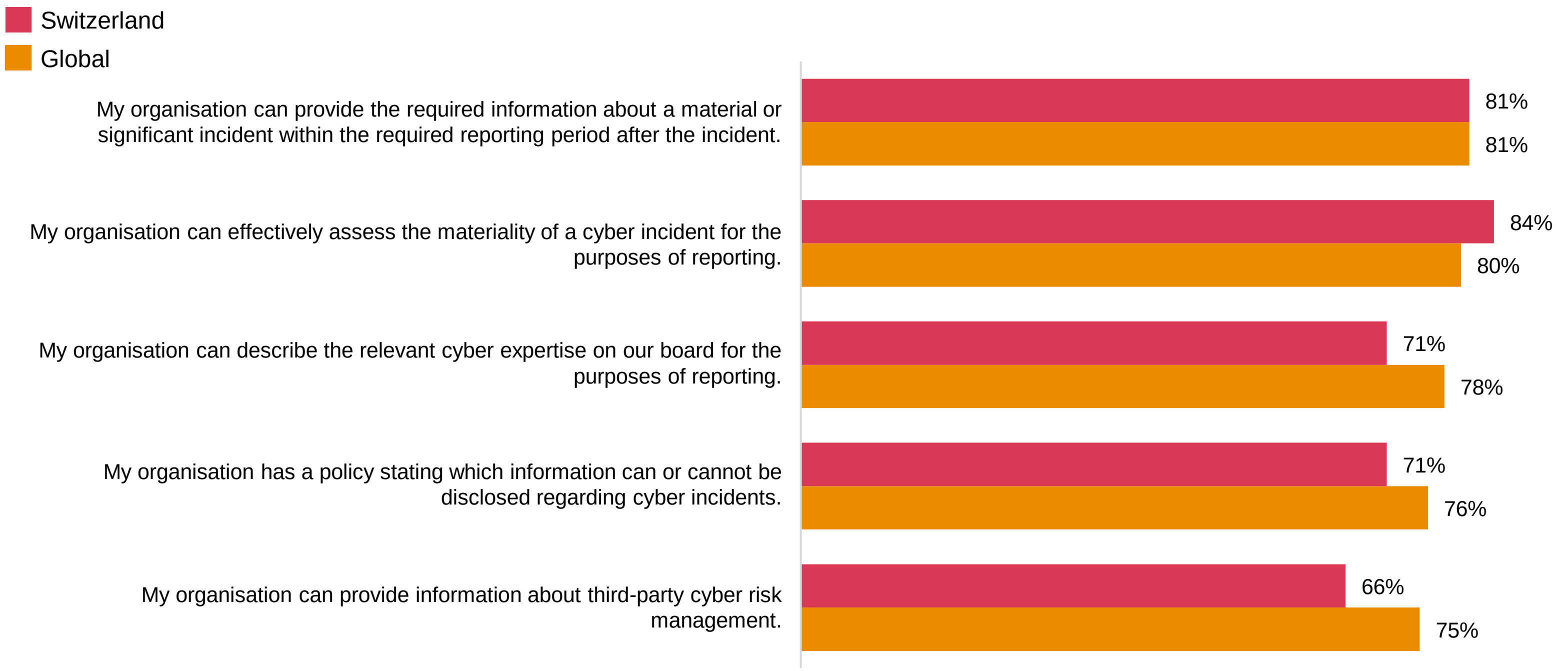
Question: Thinking about reporting to each of the following stakeholders, please rank these stakeholders in order of priority for your organisation to address over the next 12 months.
Base: 3,522 survey respondents | 70 Swiss respondents

Fewer than 50% feel confident that they can effectively disclose cyber practices, strategy and incidents to outside entities.

Less than 10% are confident in all five areas.

Organisations who have experienced an increase in cyber breaches are significantly more likely to strongly agree or agree to all answer options.

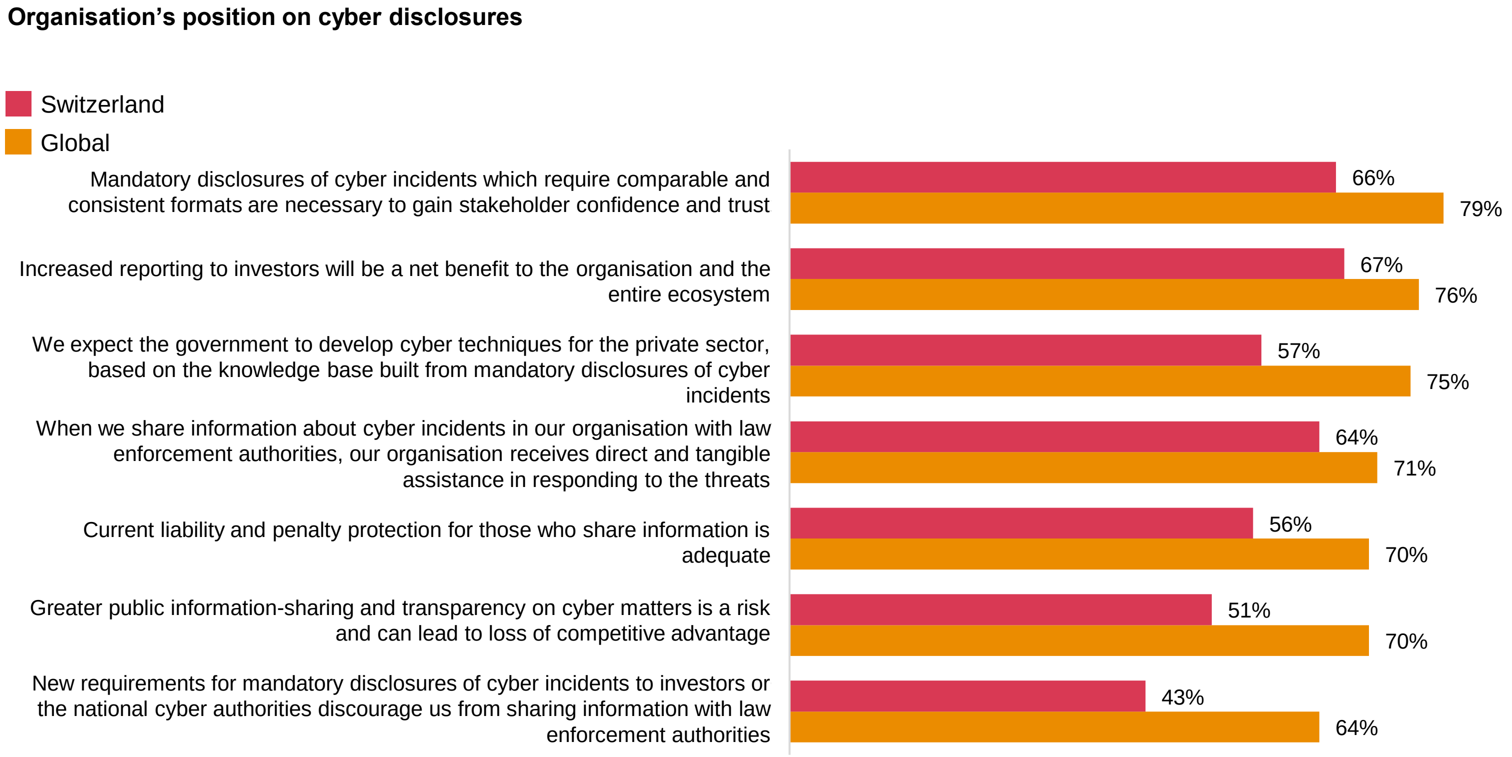
Organisation's ability to disclose cyber practices, strategy and incidents externally



Question: To what extent do you agree or disagree with the following statements regarding your organisation's ability to disclose cyber practices, strategy and incidents externally?
Base: 3,522 survey respondents | 70 Swiss respondents
Respondents who stated 'Strongly agree / Agree'

Organisation’s position on cyber disclosures

Mandatory disclosure of cyber incidents, with comparable and consistent formats, is necessary to gain stakeholder confidence and trust. Four-fifths of organisations agree.



Question: To what extent do you agree or disagree with the following statements regarding your organisation's position on cyber disclosures?
Base: 3,522 survey respondents | 70 Swiss respondents
Respondents who stated ‘Strongly agree / Agree’

Cyber in the suite spot

The C-suite playbook on cybersecurity and privacy, featuring findings from our latest Global Digital Trust Insights survey, shares how executives can work together for cyber-ready futures.

CISO

+

CEO

+

BOARD

Where can you, the CEO and Board, make the most difference in cybersecurity?

51%

of CEOs and Board members demand cyber risk management plans for major business or operational changes

Digitisation makes security everyone’s business and the change in culture starts with the CEO. Improving resilience amid a tight cyber labour market can only happen if the C-suite works as a team with the CISO — which CEOs are starting to encourage.

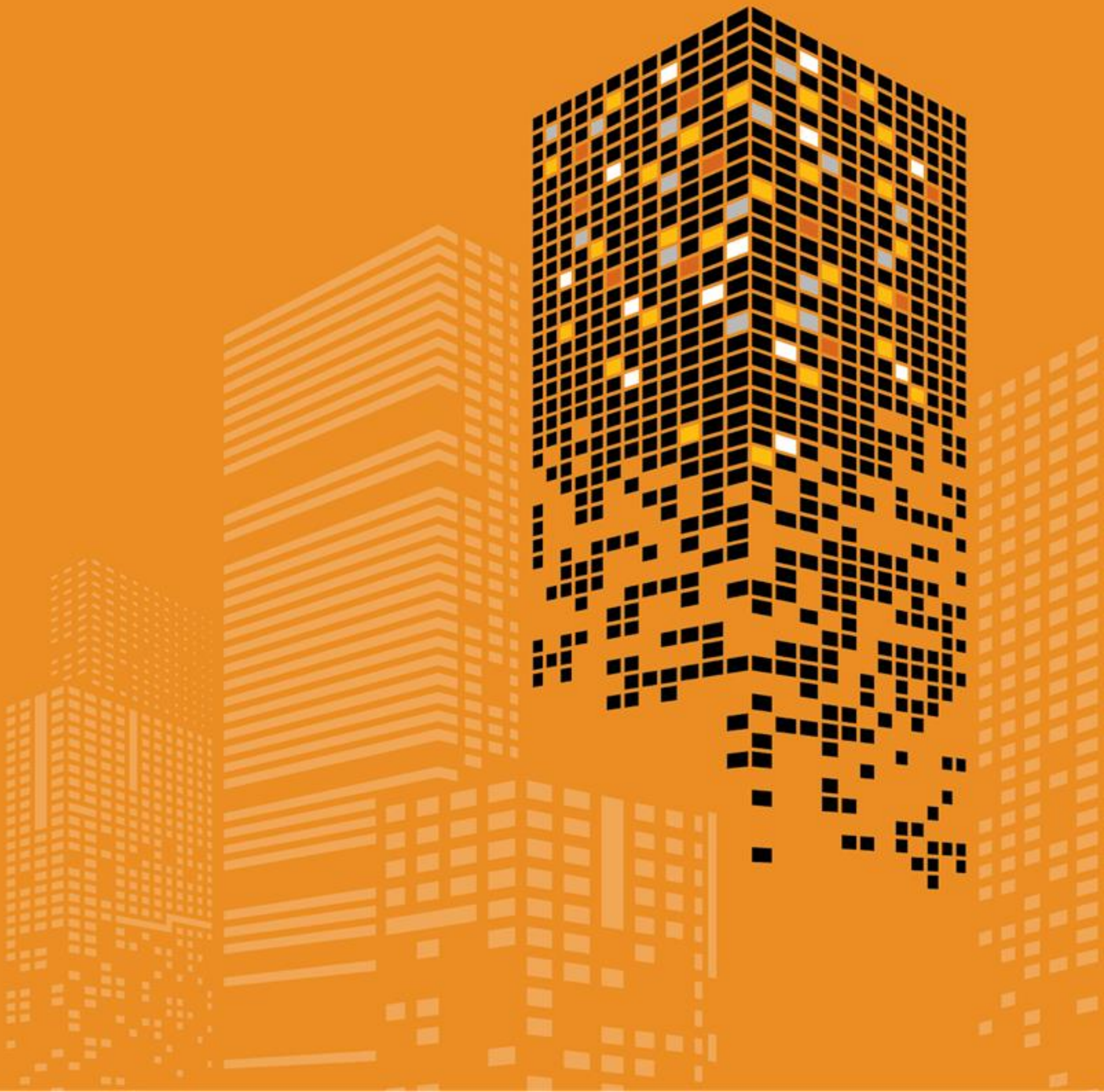
Call to action:

- Speak about your commitment to cybersecurity
- Use your influence to inspire changes
- Remove organisational barriers to C-suite coordination

CISO

+

CIO/CTO



Is our cloud security plan as agile as our business is, itself, on the cloud?

19%

of CIOs, CISOs, CTOs, are fully confident that the company has taken steps to secure against four common causes of cloud breaches

CIOs and their DevOps teams set the pace when it comes to cloud transformations, but you'll need to work more closely with your CISO and compliance teams to allay C-suite and board fears of cloud-based cyber breaches.

Almost **two-thirds** of executives say their risks via the cloud are not fully mitigated.

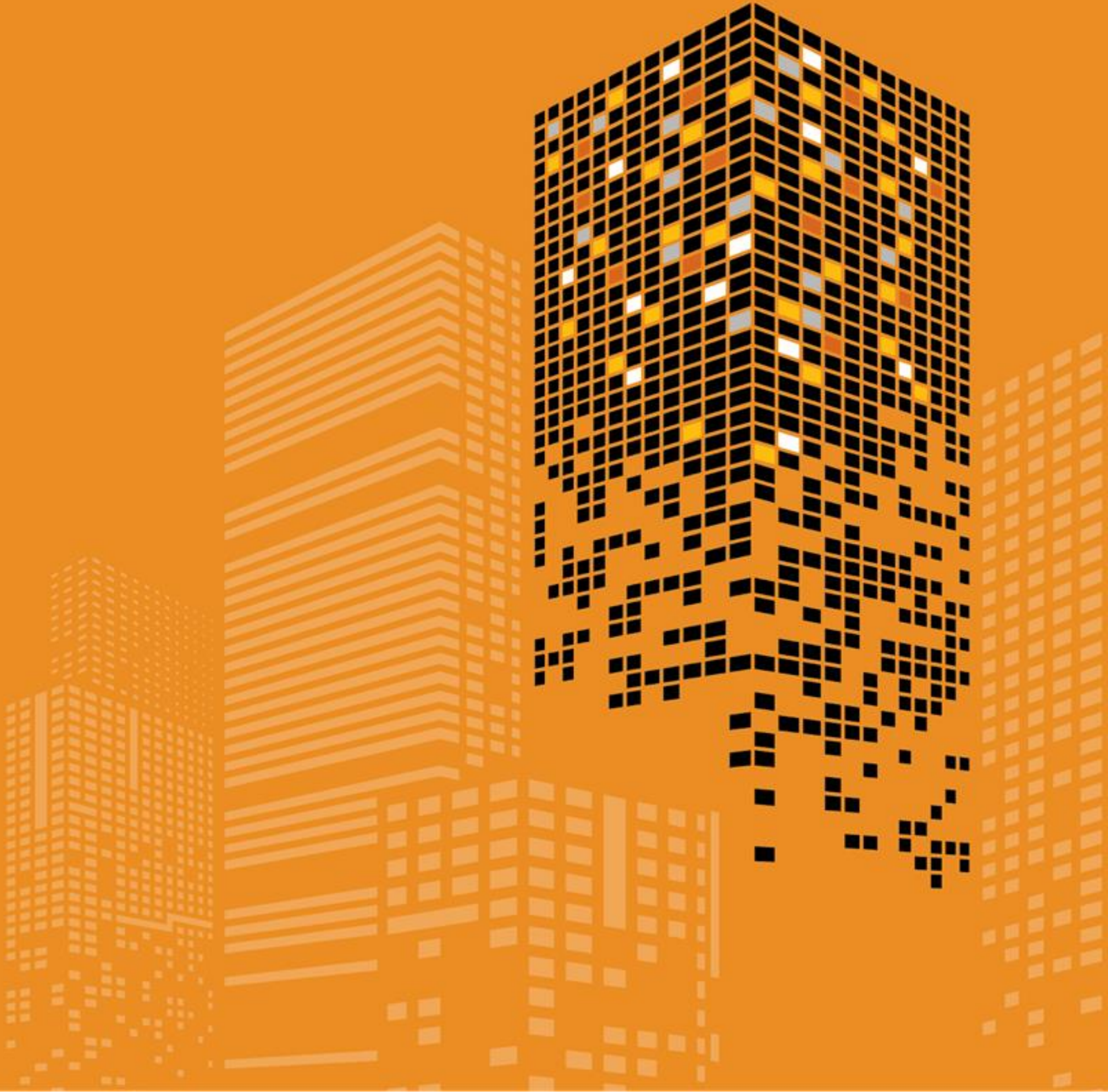
Call to action:

- To secure your back-end, front-end, internet of things, and operational technologies, work with the CISO to lock down your cloud environments — early and always.

CISO

+

CFO



Are we spending enough and in the right areas? Are we getting the right amount of cyber risk reduction from our investments?

39%

of CFOs say having more cyber tech solutions will help improve cyber posture

Many CISOs and CFOs have changed the way they invest in cyber: They're using data to make funding decisions with business goals and their top risks in mind.

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.

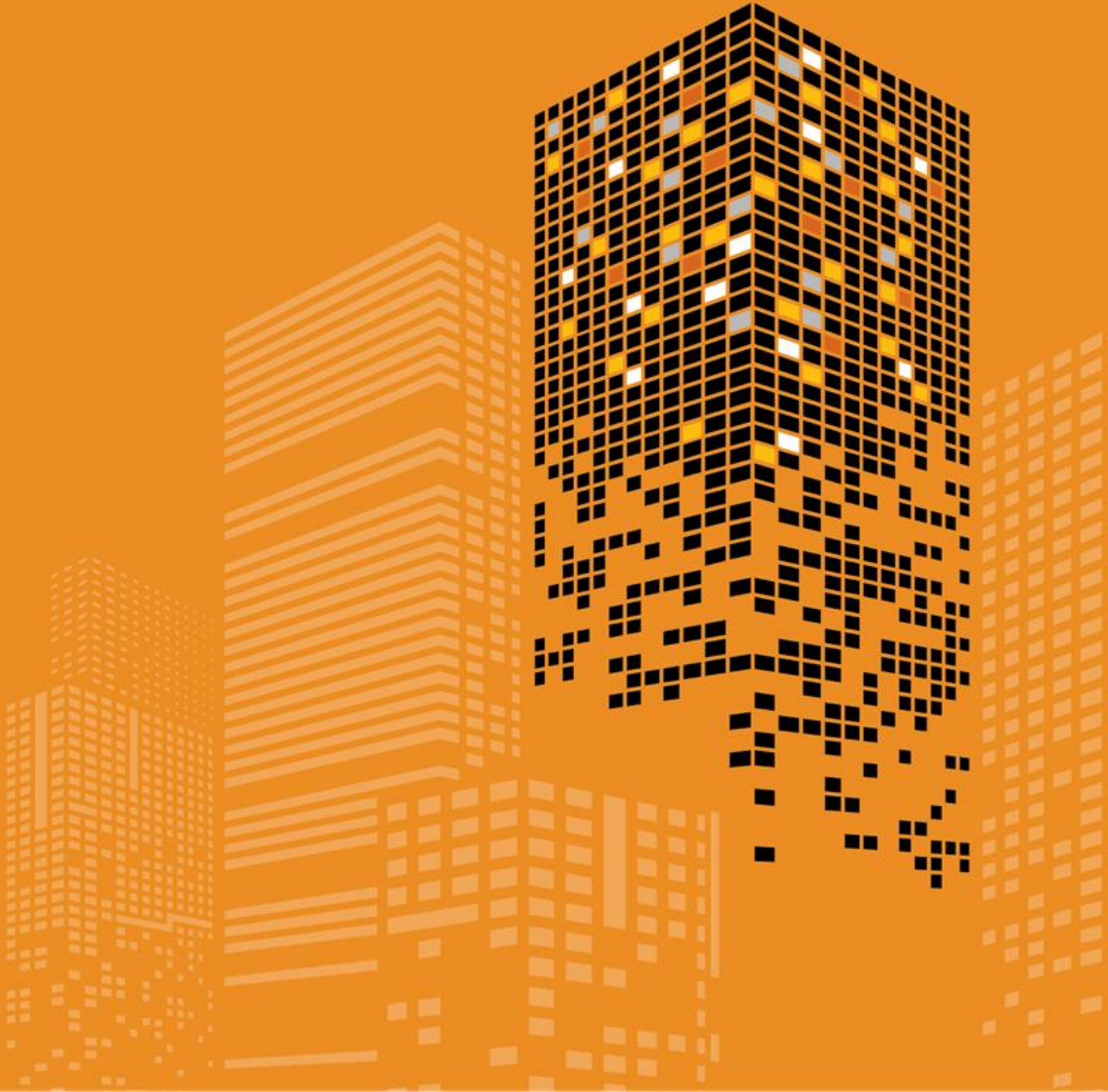
Call to action:

- As you modernise and simplify IT, ask how you can get the most cyber risk reduction per incremental dollar invested.

CISO

+

COO



What should we do to make our supply chain and operations less vulnerable and more resilient to cyber attacks?

56%

of CROs, COOs are extremely or very concerned about their company's ability to withstand supply chain attacks

The supply chain is a focal point for cyber and other threats, competitive and macroeconomic pressures, and ESG concerns. You're beginning to address security challenges by training your operations workers, investing in tech, and better managing third-party risks.

But the growing allure of operational tech (OT) to cyber threat actors means you must pay special attention to safeguarding it against attack.

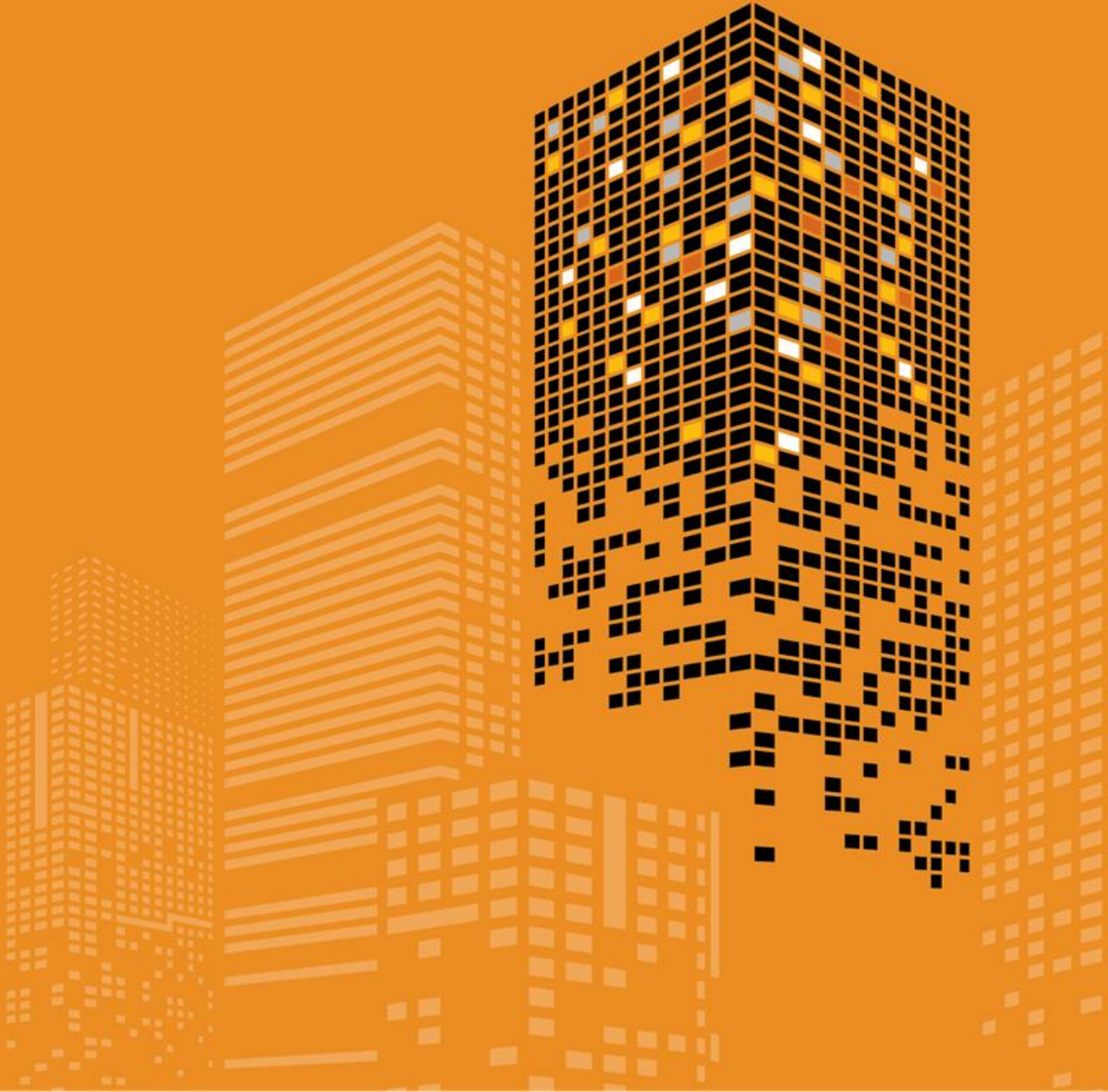
Call to action:

- Plan with the CISO and CIO how to advance in the way you secure your operational technology along with IT

CISO

+

CRO



How does the cyber risk profile affect our organisation’s risk tolerance? How engaged are the business unit leaders in managing cyber risks?

46%

of CROs and COOs say that they have controls in place throughout the organisation to prevent serious cyber disruptions

CISOs and CROs have been working together to include cyber risks in their organisation’s overall enterprise risk management programs. But many gaps remain.

Pursuing digitisation may mean more risks than your organisation’s appetite allows. And to fortify against ever more sophisticated cyber attacks, you’ll need to create, test, and put into place strong operational and technology resilience plans.

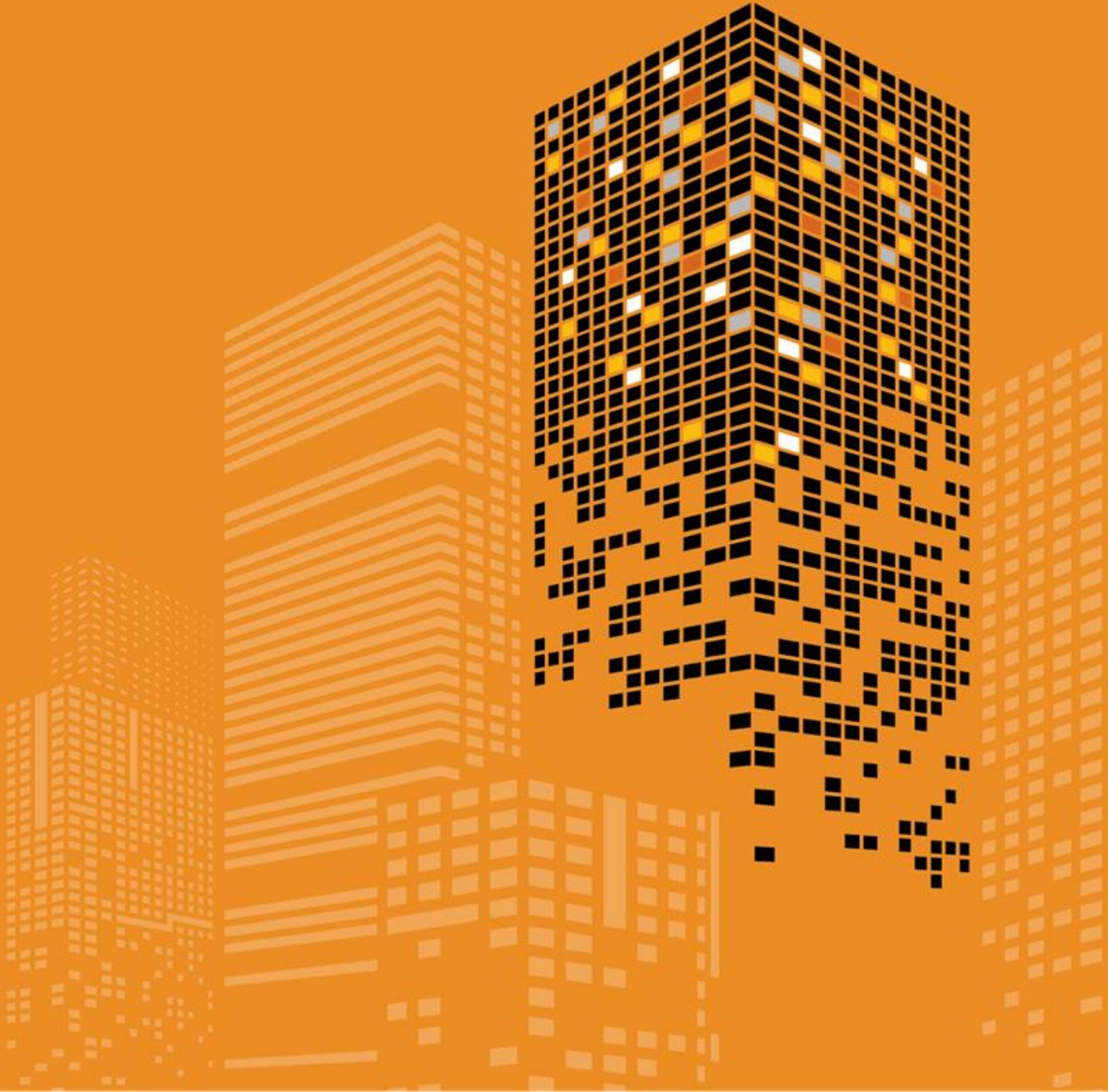
Call to action:

- Revisit your risk appetite.
- Rework crisis, business continuity, and disaster recovery plans into a cohesive enterprise resilience plan

CISO

+

CDO



How can we govern and secure our customer data so it’s private as well as safe for the business to use?

31%

of CDOs, CPOs, CMOs have “very effective” CISO relationships and consider privacy and security in marketing

Chief data officers (CDO) have taken on many challenges as data has become a focal point for good and for bad. **Half** of the leaders don’t feel confident enough in their organisation’s data governance and security to make decisions using data.

The good news: CDOs are seen by a growing number as chiefly responsible for data security and privacy. Partnering with your CISO can help you better protect data and privacy together.

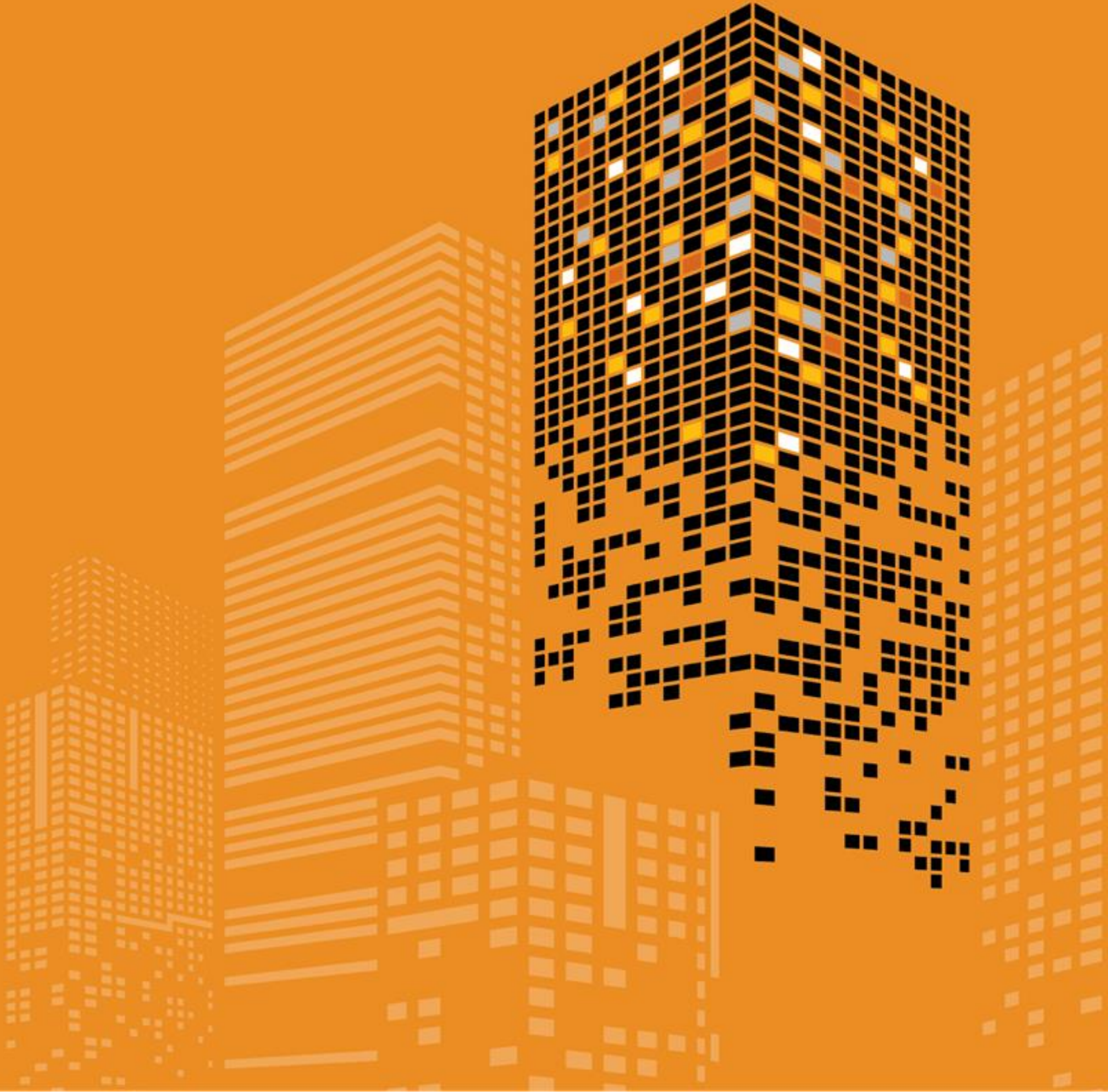
Call to action:

- Work with your CISO to address different stakeholders’ expectations, covering all the important angles of data security and privacy: governance, accessibility, accuracy and more.

CISO

+

CHRO



How can we fill our cyber positions faster and retain our talent?

54%

of CISOs and CIOs say that attrition is a problem. About **40%** are monitoring it closely. It's already hindering the progress of **15%** on cyber goals.

CISOs and CHROs are breaking old moulds, widening search parameters for hires beyond certifications and tech degrees. By recognising that some traits — such as problem-solving abilities — are at least as important, you're enlarging your pool of candidates.

Meanwhile, you're training existing employees and beginning to use managed services to help keep your company cyber secure.

Call to action:

- Ask which skills you really need in your cyber program, update how you recruit for those, and give your cyber talent incentives and growth paths that are reasons to stay.

The need for C-suite collaboration

A catastrophic cyber attack is the top scenario in 2023 resilience plans. Such an attack would surely put C-suite alliances to the test.

38% expect more serious attacks via the cloud in 2023

The breach:

Attackers exploit a misconfiguration in the company’s cloud-hosted app and pilfer user data to sell on the black market.

Consequences:

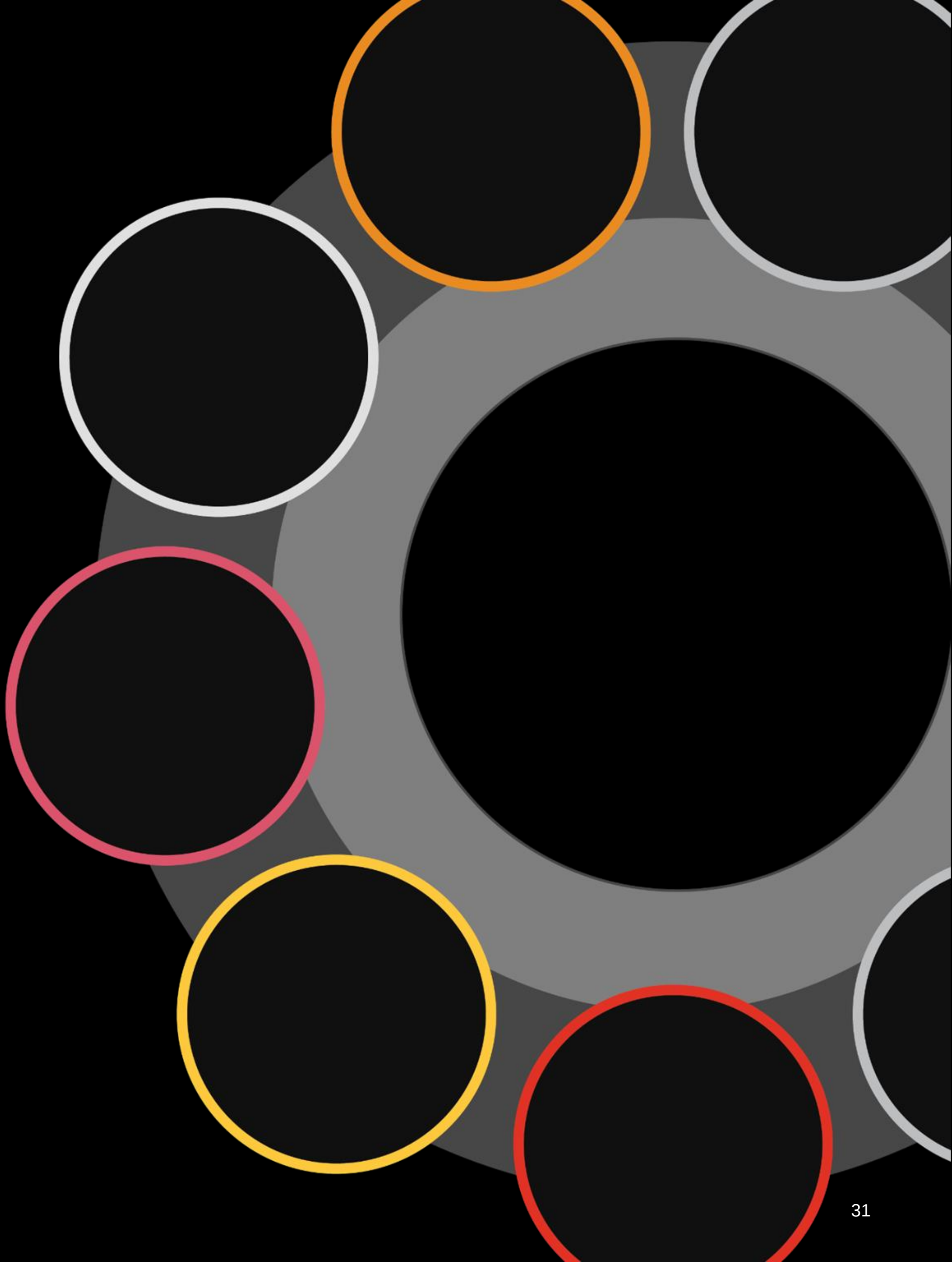
Costly notifications to data owners. Victims could file a class-action lawsuit against your company. The enterprise’s reputation suffers.

What went wrong:

Coding errors, inadequate testing of written and library code, improperly encrypted data.

How to work better for better cyber defence

- **CIO:** Insist on security-as-code in application development, as well as thorough testing pre-launch. Remediate misconfigurations from both users and automated deployments.
- **CISO:** Establish and enforce policies and procedures for securing applications, vulnerability testing, and regular patching.
- **CTO:** Require cloud service providers and third parties to provide dashboards and tools to detect misconfigurations across their environments.
- **CDO:** Ensure that your apps comply with privacy requirements and that customer data is partitioned for better protection. Put into place solutions that encrypt data at rest, in transit, and while in use.



29% of large organisations expect an increase in OT attacks

The breach:

Factory endpoints get breached via a web-facing Virtual Server Network.

Consequences:

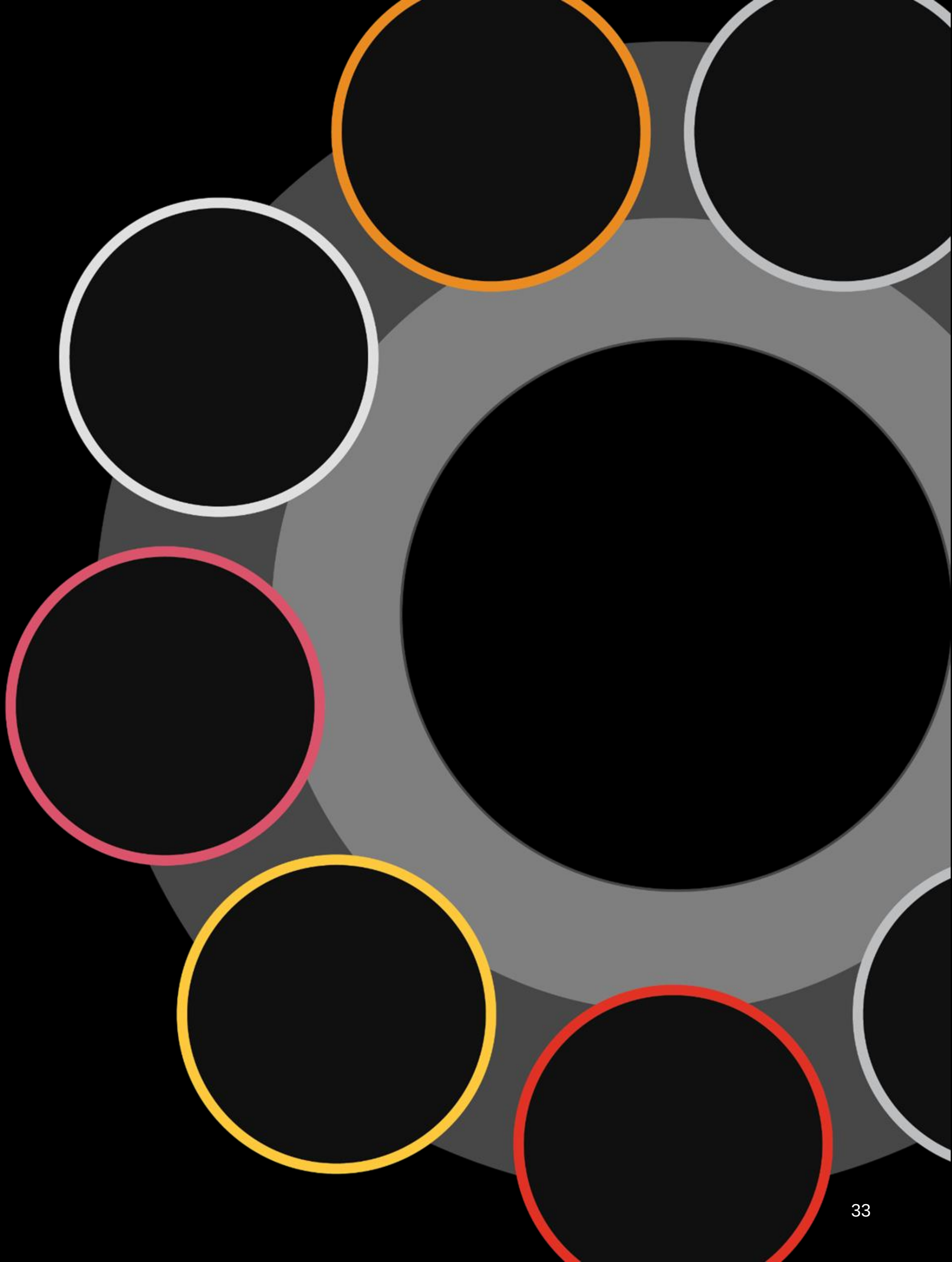
Production stops, as systems are shut down to prevent spreading damage; the effects of delayed production ripple through the supply chain.

What went wrong:

Hackers accessed exposed Virtual Network Computing servers without having to go through authentication, allowing them into the systems that control industrial processes.

How to work better for better cyber defence

- **CIO:** With CIO and CTO, map convergences and critical interdependencies between IT and OT systems.
- **CISO:** Require off-web VNC access or via a VPN. Train IT operators, OT operators, and security personnel to recognise the indicators of potential compromise.
- **CTO:** With CISO and CIO, create a plan for patching and monitoring endpoints.
- **CRO:** Assess VNC risks. Develop and practice incident response procedures that join IT and OT response processes.
- **COO:** Weigh cybersecurity in procurement process for industrial control systems, contracting with cloud providers, and defining service agreements with external service providers.



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:

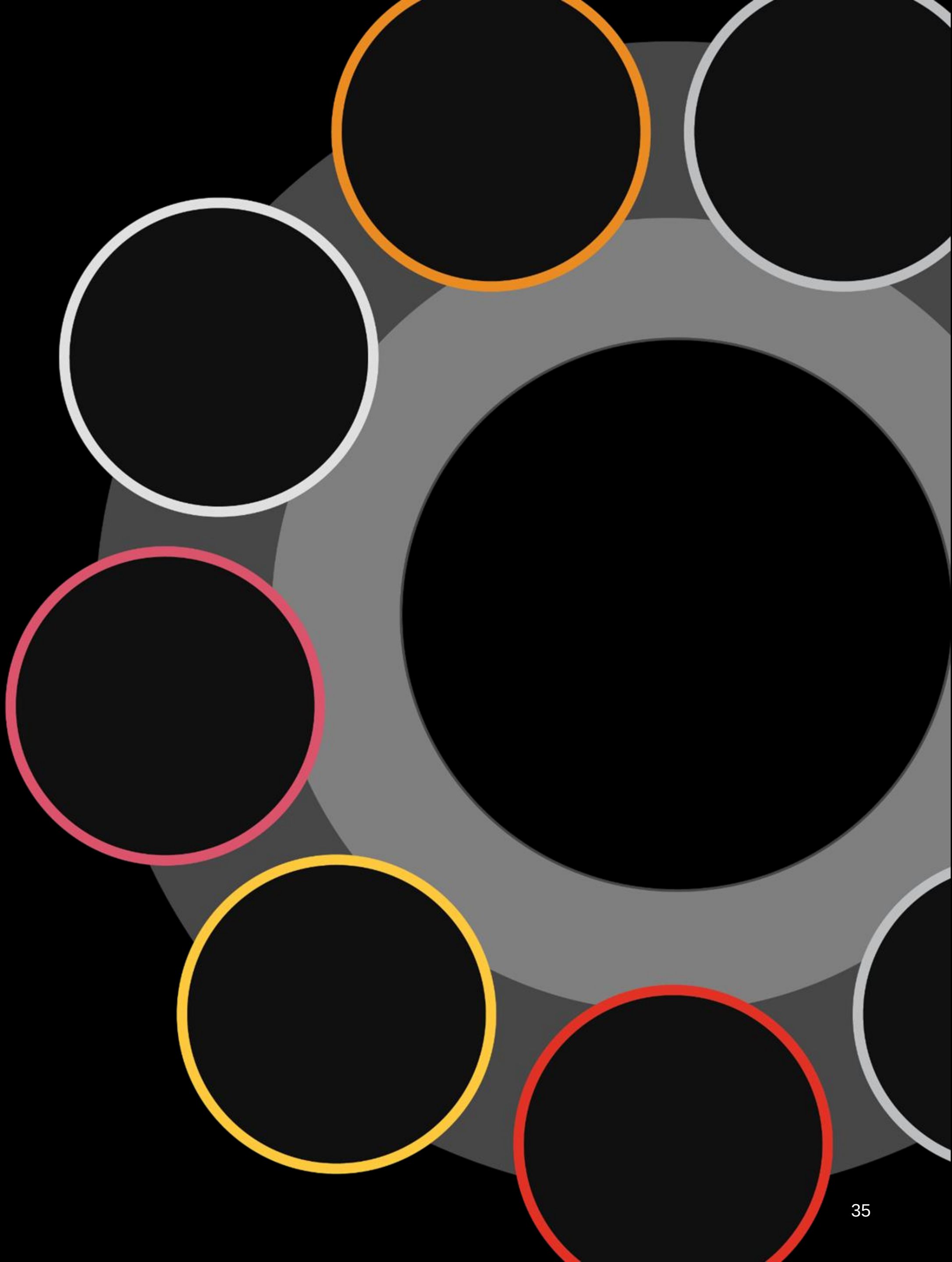
Service disruption and a near-complete shutdown of networks.

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 eight weeks, the cyber criminals 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 better for better cyber defence

- **CEO:** Support security awareness training throughout the organisation.
- **CIO:** Review the connections between IT systems and the healthcare environment.
- **CTO:** Assess the vulnerability of medical devices in a scenario that targets devices.
- **COO:** Help CIO, CISO size up effects on patient safety.
- **CISO:** Bridge security gaps between IT and healthcare 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 policy for ransomware payment.
- **Board:** Get insight on management’s table top exercise to prepare for a ransomware attack. Confirm when the board will be informed about a cyber incident or ransomware attack.



About the survey

The 2023 Global Digital Trust Insights is a survey of 3,522 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers) conducted in July and August 2022. Female executives make up 31% of the sample.

Fifty-two percent of respondents are executives in large companies ($1 billion and above in revenues); 16% are in companies with $10 billion or more in revenues.

Respondents operate in a range of industries: Industrial manufacturing (24%), Tech, media, telecom (21%), Financial services (20%), Retail and consumer markets (18%), Energy, utilities, and resources (9%), Health (5%), and Government and public services (3%).

Respondents are based in various regions: Western Europe (31%), North America (28%), Asia Pacific (18%), Latin America (12%), Eastern Europe (5%), Africa (4%), and Middle East (3%) .

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

Urs Küderli

Partner
Leader Cybersecurity and Privacy,
PwC Switzerland

Tel: +41 58 792 42 21
urs.kuederli@pwc.ch

Johannes Dohren

Partner
Head of Cyber Resilience and Defence,
PwC Switzerland

Tel: +41 58 792 22 20
johannes.dohren@pwc.ch

Yan Borboën

Partner
Digital Assurance &
Cybersecurity and Privacy,
PwC Switzerland

Tel: +41 58 792 84 59
yan.borboen@pwc.ch

Thank you www.pwc.ch/dti2023

pwc.com