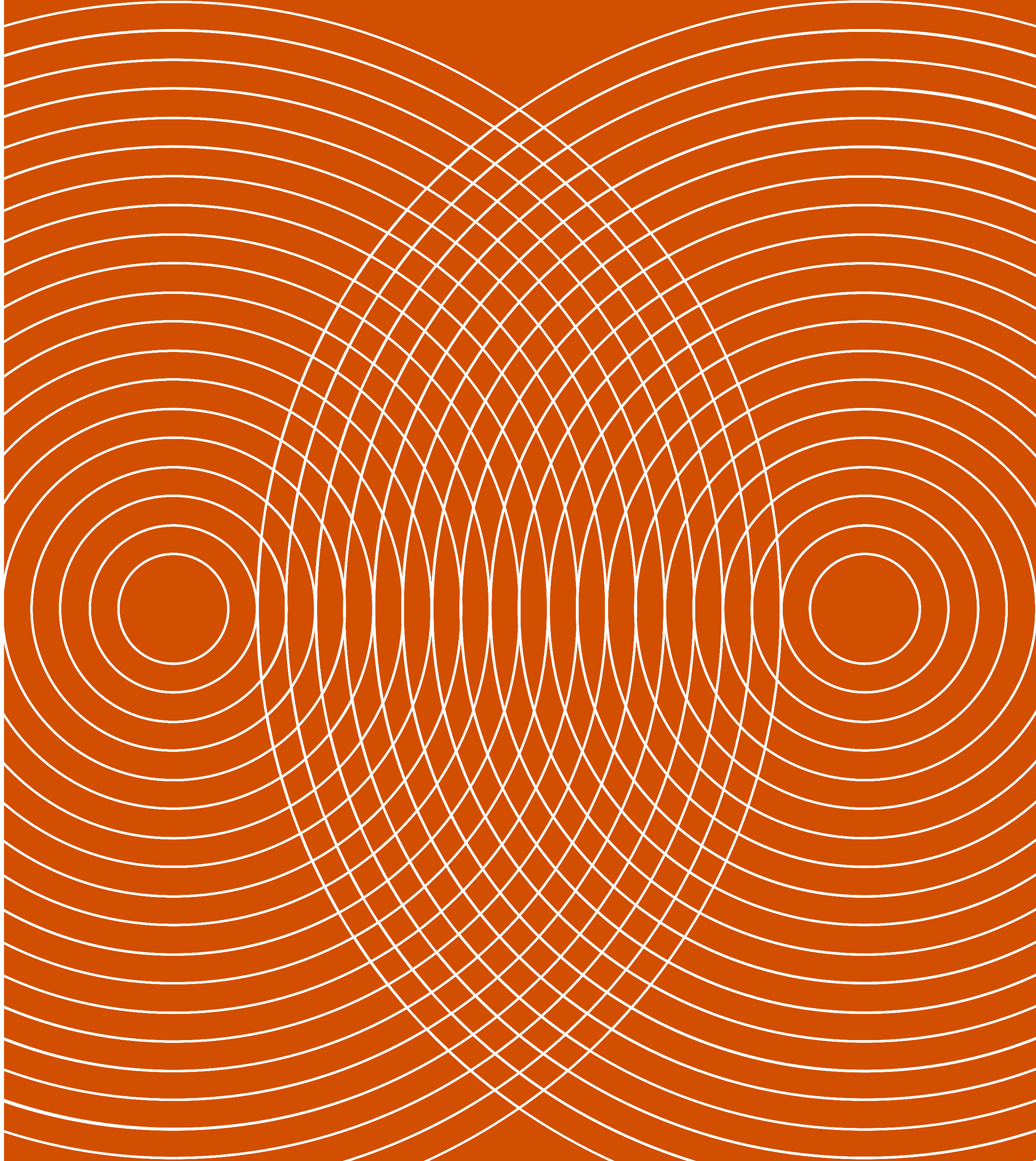
Sustaining collaboration across the C-suite with intelligent risk management solutions

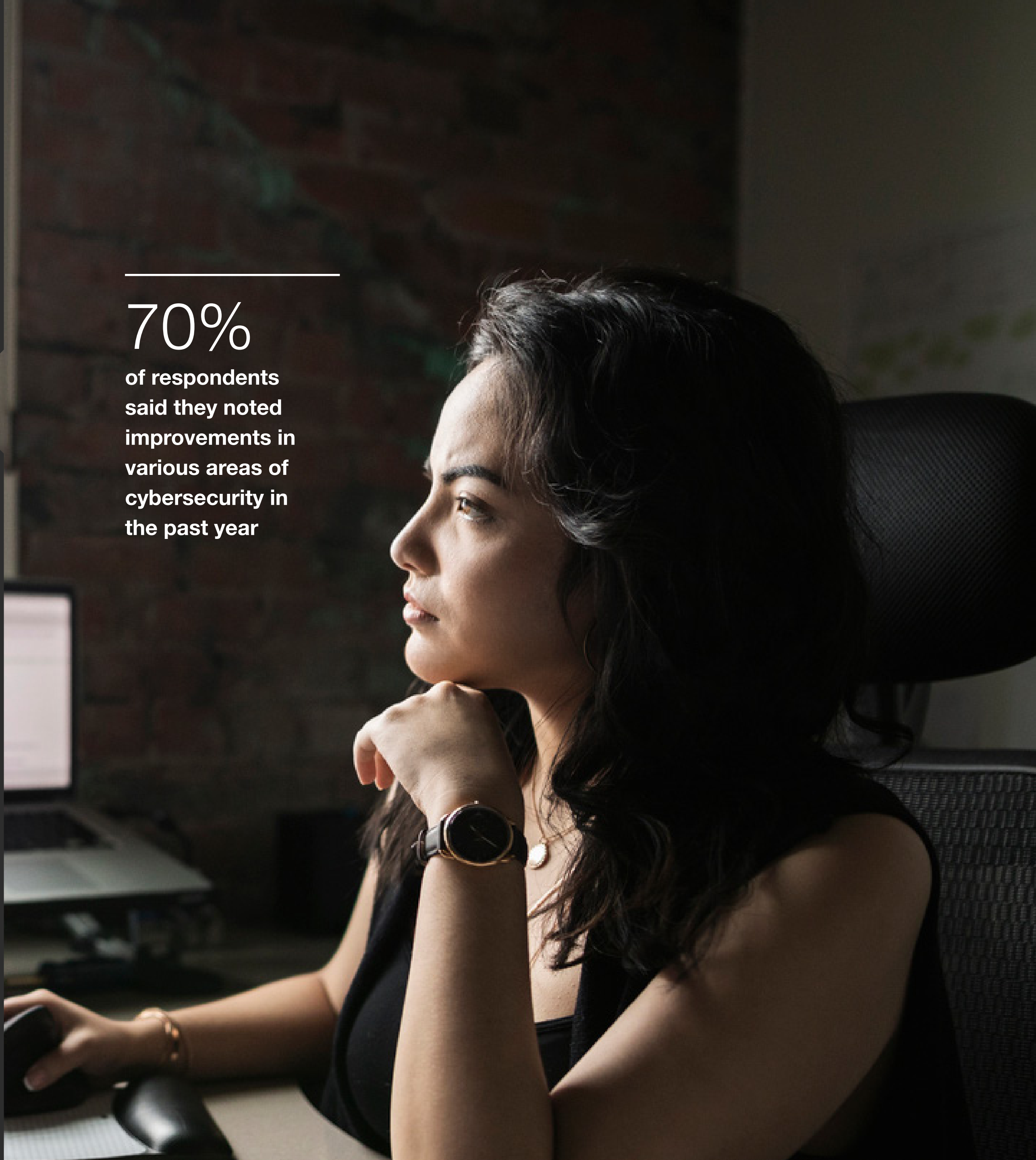
Your tech guide to the C-suite playbook on cybersecurity



Despite the onslaught of disruptions over the past few years, CISOs and cyber teams have risen to the challenge of mitigating cyber risk. Thanks to thoughtful investments and C-suite collaboration, more than 70% of respondents to our Global Digital Trust Insights survey said they noted improvements in various areas of cybersecurity in the past year.

These improvements are just the beginning of a long road ahead to cyber-ready futures. Ongoing human-led, tech-powered efforts are still needed. Cyber threats are still projected to proliferate. Two-thirds of executives consider cybercrime their most significant threat in the coming year.

Businesses need a proactive approach to cyber that starts at the top — and that works across the top. Just over half of CEOs and board members demand cyber risk management plans for major business or operational changes. This reach could be expanded. This guide helps C-level executives use their influence to broadcast the commitment to proactive strategy and back it up with investment in relevant technologies and resources.



70%

of respondents said they noted improvements in various areas of cybersecurity in the past year

Mission possible: Uniting C-suite with the right tech

For most organizations, 30-40% of cyber investments should be spent on protection, about 30% on detection, and 30% on response and recovery. Proactive investment in tech-enabled solutions can go a long way toward cyber-ready futures. The PwC Risk Management Portfolio can aid in engaging proactive risk management with risk detection and analysis built into the process to help you manage governance and security across your risk and compliance lifecycle as well as cybersecurity initiatives.

PwC conducted its 2023 Global Digital Trust Insights survey of 3,522 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and other C-suite officers) in July and August 2022 to generate a playbook for collaborating, investing and executing risk management strategy. This companion piece can serve as a guide to the right tech to help you work across top executive teams to bring your strategy to life.

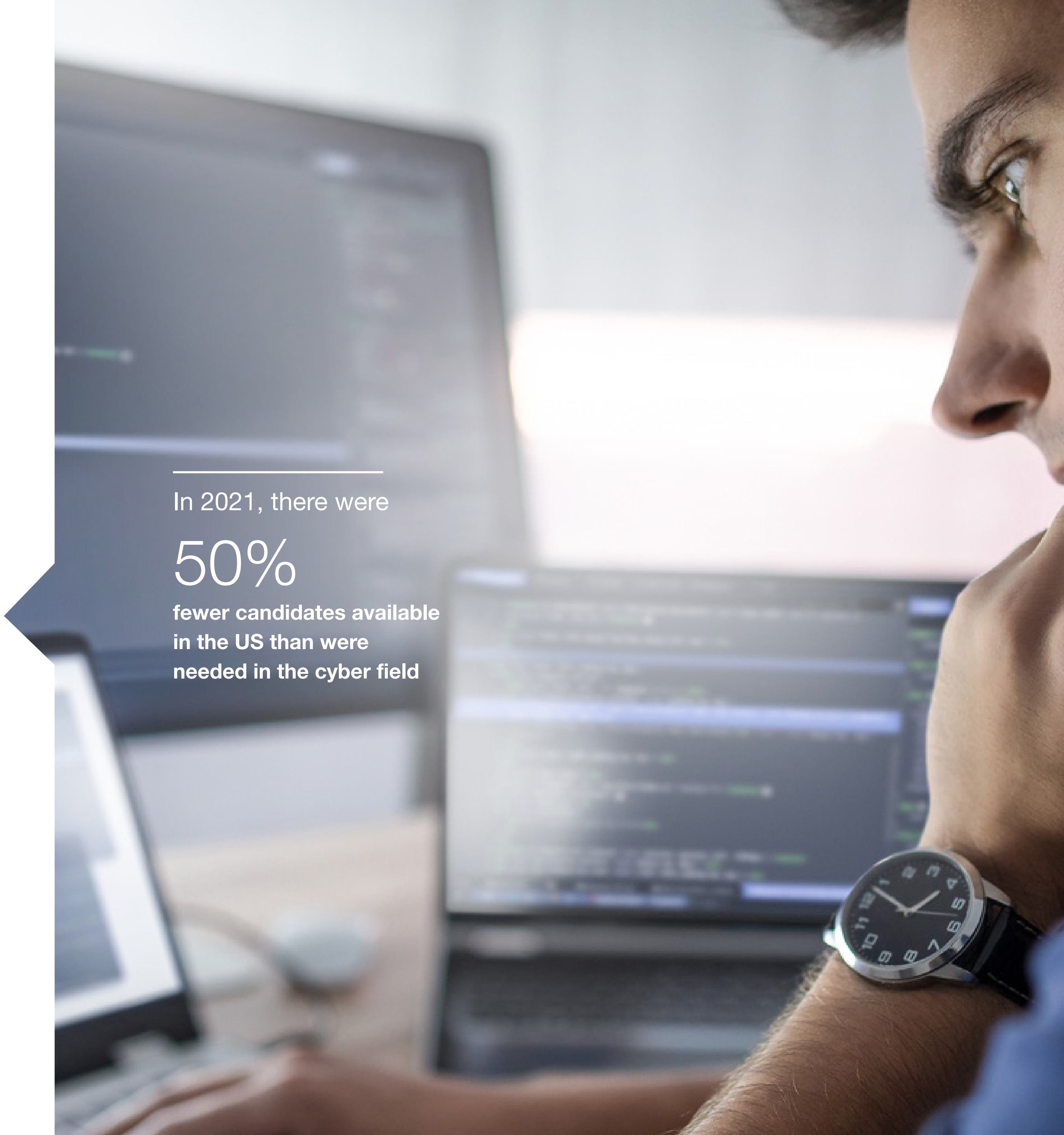
Here are seven key missions — should you choose to accept them — that you and your team of C-suite partners can embark on to help create a resilient and cyber-ready future.

1. Your mission: Address attrition that hinders cyber efforts by investing in upskilling

Your team: CISO + CHRO

The cybersecurity talent pool is in crisis mode. In 2021, there were 50% fewer candidates available in the US than were needed in the cyber field. Globally, it was estimated that 3.5 million cybersecurity jobs went unfulfilled.

More than half (51%) of executives say they planned to add full-time cybersecurity staff, but attracting talent is only the first hurdle in the race for top cyber talent. Keeping employees from leaving is a challenge in and of itself. Over half — 54% — of CISOs and CIOs say attrition on their cyber teams is a problem. And for 15%, attrition is actually hindering the process of meeting cyber goals.



In 2021, there were

50%

fewer candidates available in the US than were needed in the cyber field

Delivering function-specific upskilling in cyber to break through the talent impasse

For many cyber and tech executives, this feels like a stalemate. On one hand, organizations say having more cyber tech solutions will help improve cyber posture. On the other hand, they plan to upskill and hire talent. As organizations modernize and simplify IT, they're asking, "Are we balancing our dollars the right way?"

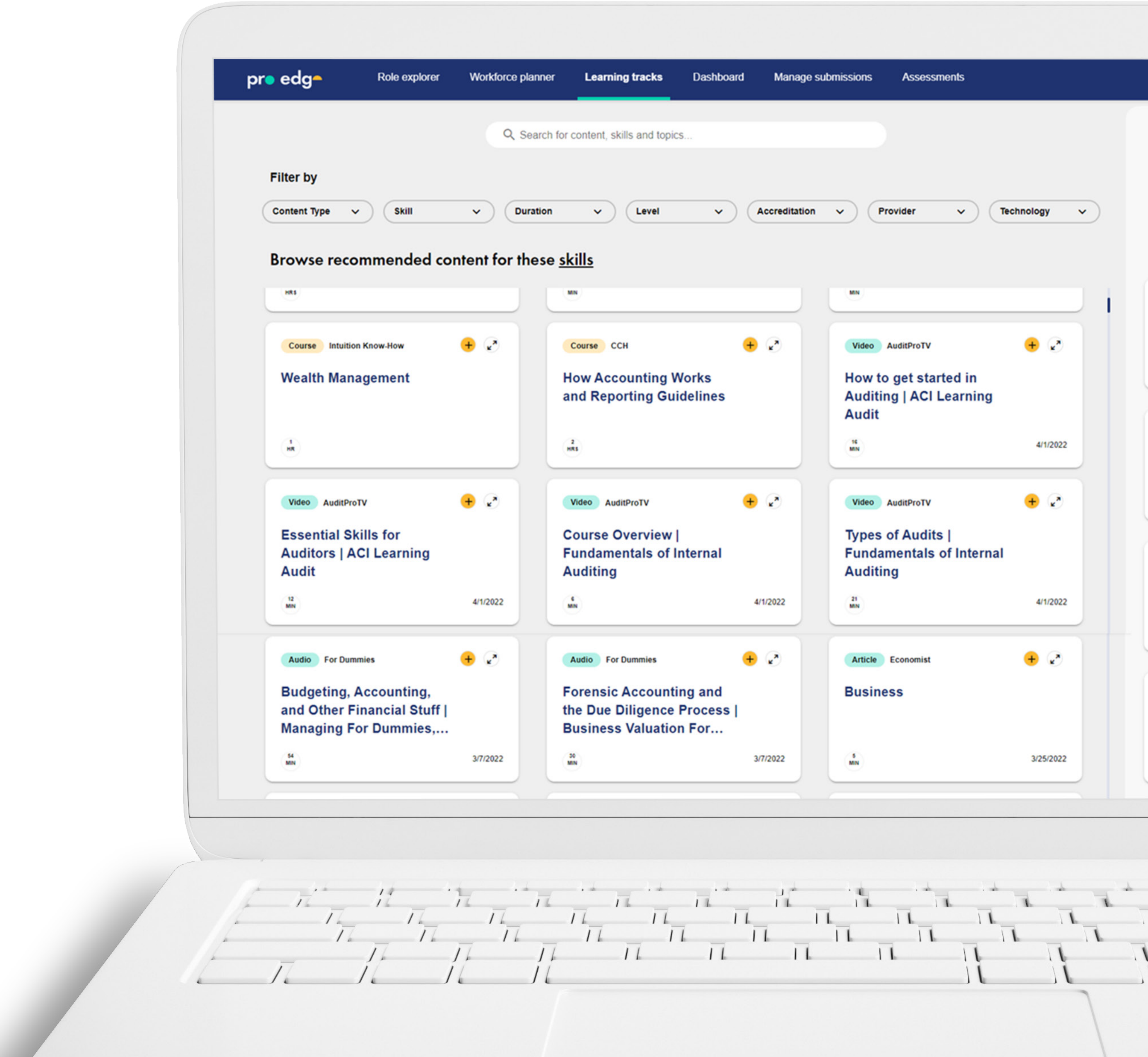
Upskilling answers the call for better tech solutions while creating a cyber-ready workforce. With the right upskilling platform, you can invest in your people to help get the most cyber risk reduction per dollar invested — and accelerate security-by-design decisions and solutions.

Your tech: ProEdge

- Understand skills gaps and opportunities to create learning pathways
- Access 1,000+ cybersecurity technical courses, including CPE courses for acquiring and maintaining cyber certifications
- Enable the development of 250+ in-demand cyber skills extracted from analysis of over 250M job listings
- Empower your staff with PwC-developed cyber learning paths and credentials

ProEdge, a PwC product, helps cyber professionals keep pace with the changing digital and cyber landscape. We've rigorously vetted thousands of pieces of content from industry-leading vendors to create personalized pathways so organizations can synchronize their workforce with the latest trends, skills and emerging cyber roles.

CISOs can benefit from security awareness, cross-training security operations and endpoint security training. Meanwhile, employees are empowered to apply what they learn right away, like building an incident response report or automated bot to validate account data. This powerful combination paves way for more engagement and retention that's needed for ongoing endurance against cyber threats.


pro edge
Role explorer
Workforce planner
Learning tracks
Dashboard
Manage submissions
Assessments
Search for content, skills and topics...
Filter by
Content Type
Skill
Duration
Level
Accreditation
Provider
Technology
Browse recommended content for these skills
Course
Intuition Know-How
Wealth Management
Course
CCH
How Accounting Works and Reporting Guidelines
Video
AuditProTV
How to get started in Auditing | ACI Learning Audit
4/1/2022
Video
AuditProTV
Essential Skills for Auditors | ACI Learning Audit
4/1/2022
Video
AuditProTV
Course Overview | Fundamentals of Internal Auditing
4/1/2022
Video
AuditProTV
Types of Audits | Fundamentals of Internal Auditing
4/1/2022
Audio
For Dummies
Budgeting, Accounting, and Other Financial Stuff | Managing For Dummies,...
3/7/2022
Audio
For Dummies
Forensic Accounting and the Due Diligence Process | Business Valuation For...
3/7/2022
Article
Economist
Business
3/25/2022

2. Your mission: Boost your cyber threat awareness with the right tech to monitor and prevent attacks

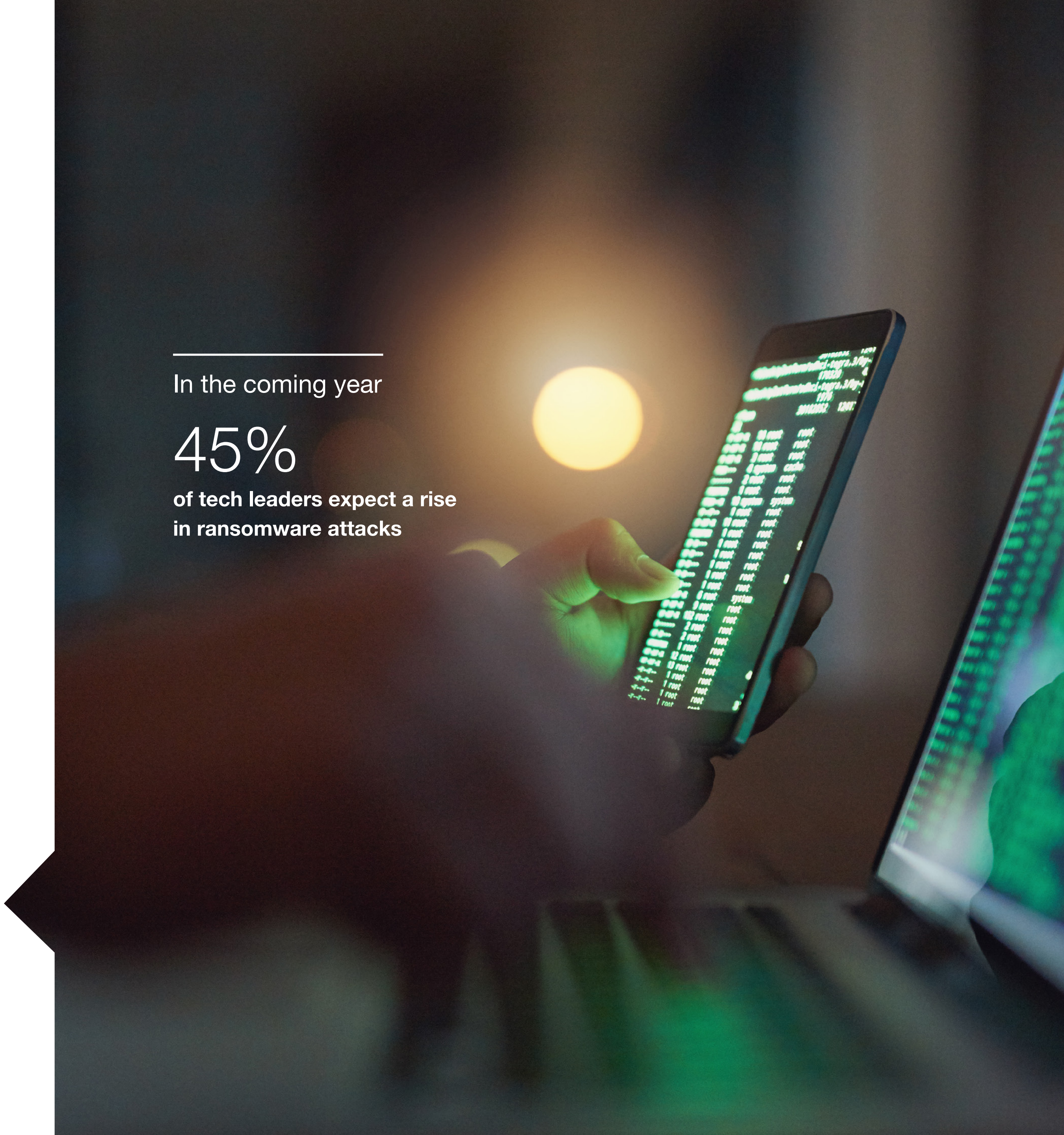
Your team: CFO + CISO + CIO + CTO

Organizations have made some bold moves in recent years — enabling remote and hybrid work, accelerating cloud adoption and taking on more volumes of data to enable personalization. Many CISOs are presenting their case to CEOs for cybersecurity investments — real-time threat intelligence, for example — that match this accelerated digital adoption.

But to really grab the ear — and earn the trust — of the CEO on these initiatives, this team should be able to gather and share details about their organization's inherent risks. The majority of CEOs demand it.

Fifty-one percent of CEOs require a cyber risk management plan for each of their major business or operational changes and 28% demand more frequent updates on cyber risks and mitigation measures.

More than one-third of CEOs want to do cyber risk assessments, business continuity, contingency and recovery plans and dashboards on key cyber risks — and with good reason. In the coming year, 45% of tech leaders expect a rise in ransomware attacks.



In the coming year

45%

of tech leaders expect a rise in ransomware attacks

Using cyber threat intelligence to earn trust and drive new capabilities

Digital acceleration has left many organizations with inconsistent risk methodologies, disparate systems, time-consuming manual processes and lacking auditability — creating dense fog in their search for a clear risk strategy.

A holistic cyber threat detection solution, like Threat Intelligence Portal, a PwC product, can help gain CEO buy-in for more cybersecurity capabilities by illustrating high-risk activity and risk exposure — and the methodologies used to mitigate and respond to threats across the enterprise.

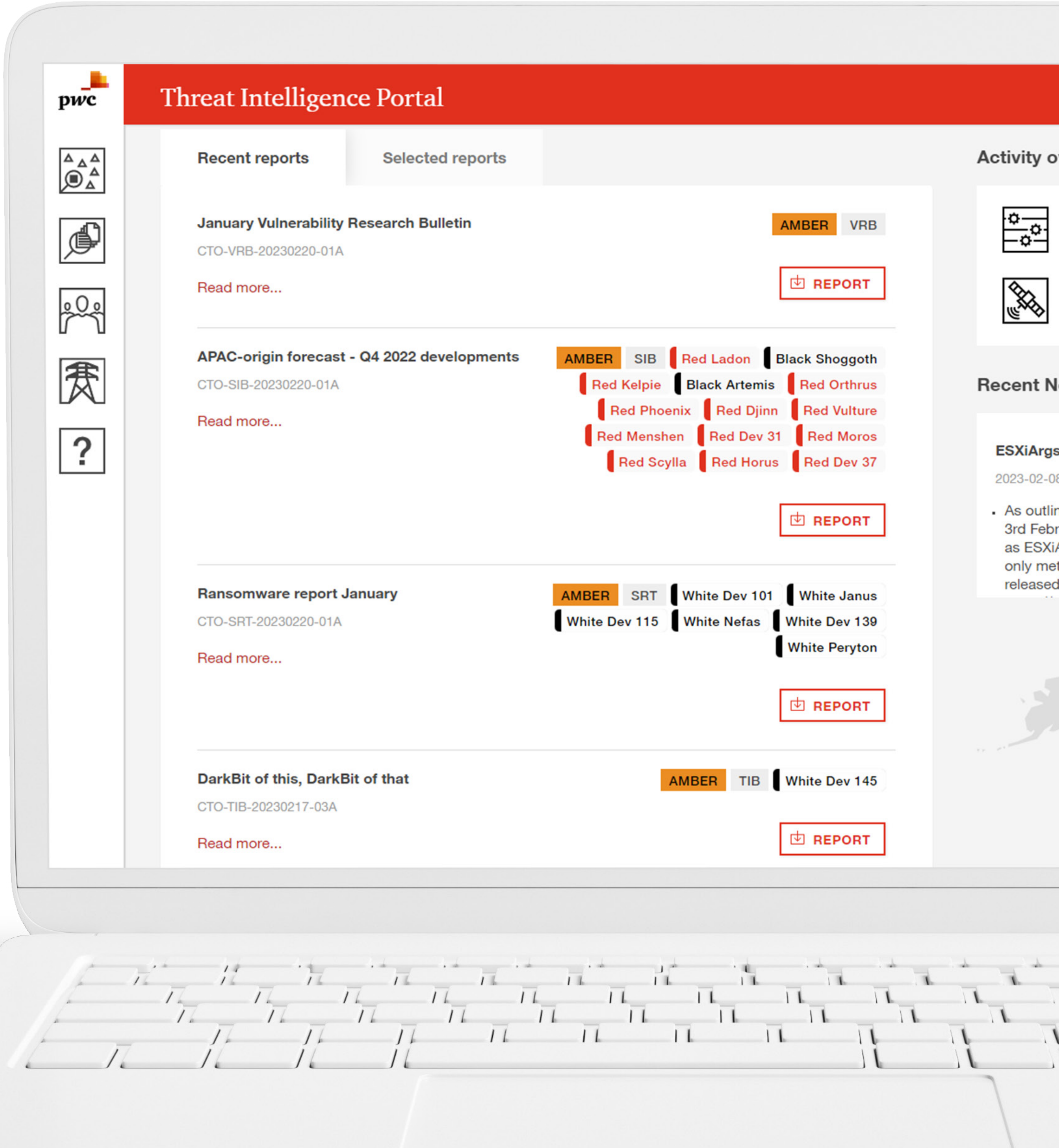
Your tech: Threat Intelligence Portal

- Access technical reports on new targeted attack campaigns specific to your region, sector or actor
- Monitor ongoing threats with access to network intrusion detection systems and file detection signatures
- Query threat data, research, indicators and actors from one place

Threat Intelligence Portal is a combination of technologies and community to help assess and respond to a global threat landscape. It offers strategic and technical reports such as new targeted attack campaigns and threat intelligence insights into relationships between indicators and threat actors — all accessible within a portal.

Risk practitioners and cyber teams can research and monitor threats that are closest to home. Threat Intelligence Portal monitors dark web forums, social media platforms, corporate digital estates, as well as keyword searches.

No one should fight off cyber threats alone. Threat Intelligence Portal's private collaboration space has direct access to PwC analysts, which gives you more context into the threats you're investigating. PwC cyber threat consultants can also help develop threat intelligence programs and threat modeling so your people and technology can operate at their fullest potential.



Threat Intelligence Portal

Recent reports | Selected reports

Activity o

January Vulnerability Research Bulletin — AMBER VRB
CTO-VRB-20230220-01A
Read more...
REPORT

APAC-origin forecast - Q4 2022 developments — AMBER SIB Red Ladon Black Shoggoth Red Kelpie Black Artemis Red Orthrus Red Phoenix Red Djinn Red Vulture Red Menshen Red Dev 31 Red Moros Red Scylla Red Horus Red Dev 37
CTO-SIB-20230220-01A
Read more...
REPORT

Ransomware report January — AMBER SRT White Dev 101 White Janus White Dev 115 White Nefas White Dev 139 White Peryton
CTO-SRT-20230220-01A
Read more...
REPORT

DarkBit of this, DarkBit of that — AMBER TIB White Dev 145
CTO-TIB-20230217-03A
Read more...
REPORT

Recent N

ESXiArgs
2023-02-08

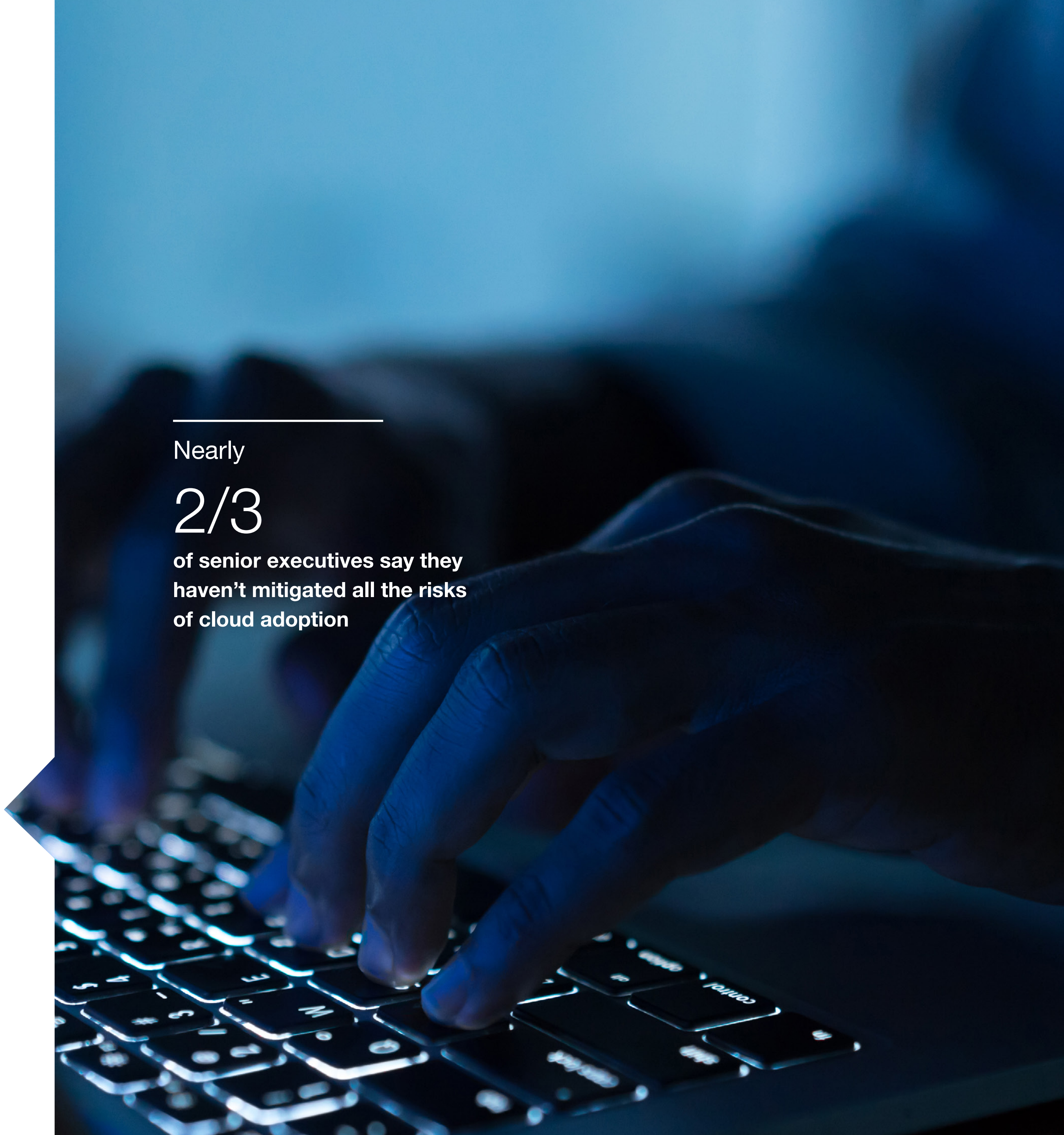
- As outlin
3rd Febr
as ESXiA
only met
released

3. Your mission: Reduce cloud risks by locking down cloud environments and bolstering defenses

Your team: CISO + CIO + CTO

While 78% of executives have adopted cloud in most or all parts of the business, many have not matured their cloud governance controls. Nearly two-thirds of senior executives say they haven't mitigated all the risks of cloud adoption and only a small number — barely 19% — of CIOs, CISOs and CTOs are confident their company has taken the steps needed to help prevent common cloud breaches. These gaps in security can leave companies vulnerable to cyber criminals.

The time for an offensive play is now. Organizations need a centralized risk assessment tool that gives leaders access to standard assessments, responses and remediation actions so cyber threats can be met with equal and consistent power.



Nearly

2/3

of senior executives say they haven't mitigated all the risks of cloud adoption

Supporting cyber defense risk management by making fast development and strong controls work

Cohesive risk assessment is a lynchpin to a cyber-ready, resilient and innovative future. Cloud-powered companies — those that have reinvented their business through the cloud — are two times more mature when it comes to cloud governance. They've been able to apply formal and distinct cloud controls, document shared responsibilities, improve workloads and enable cross-functional stakeholder agreement. Enabling strong and robust cloud controls is possible. The question is how to get there.

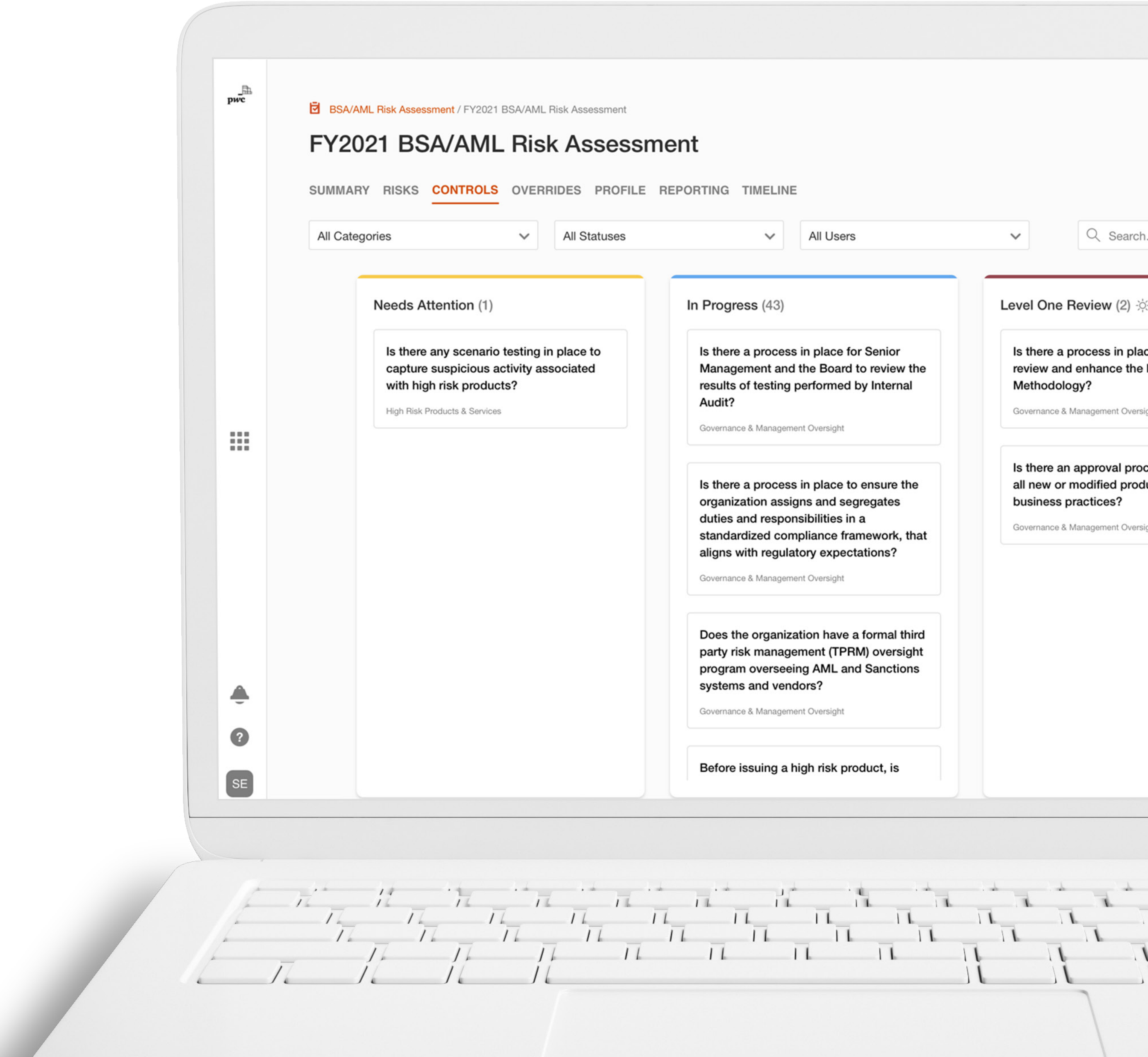
This team should bring together enterprise and cross-functional cloud security under one system — one that measures, tracks and automates the process of risk management for the cloud.

Your tech: Ready Assess

- Update your view of risk as new cloud risks arise
- Map controls to risks to identify weaknesses or gaps
- Engage directly with first line of defense stakeholders to assess qualitative emerging or operational cloud risk factors
- Share visual results with CEO in place of long-written reports

Ready Assess, a PwC product, streamlines cloud security protocols and assessments. It allows users to develop detailed action plans based on risk analyses that can be incorporated into workflows. Procedures like penetration testing and security event and incident monitoring (SIEM) can be established and enforced on demand.

The product can create standardized assessment frameworks to identify various cloud risks, access security controls and see how identified risks may create residual impact to business and strategic objectives.



Is there any scenario testing in place to capture suspicious activity associated with high risk products?

High Risk Products & Services

Is there a process in place for Senior Management and the Board to review the results of testing performed by Internal Audit?

Governance & Management Oversight

Is there a process in place to ensure the organization assigns and segregates duties and responsibilities in a standardized compliance framework, that aligns with regulatory expectations?

Governance & Management Oversight

Does the organization have a formal third party risk management (TPRM) oversight program overseeing AML and Sanctions systems and vendors?

Governance & Management Oversight

Before issuing a high risk product, is

Is there a process in plac review and enhance the Methodology?

Governance & Management Oversig

Is there an approval proc all new or modified produ business practices?

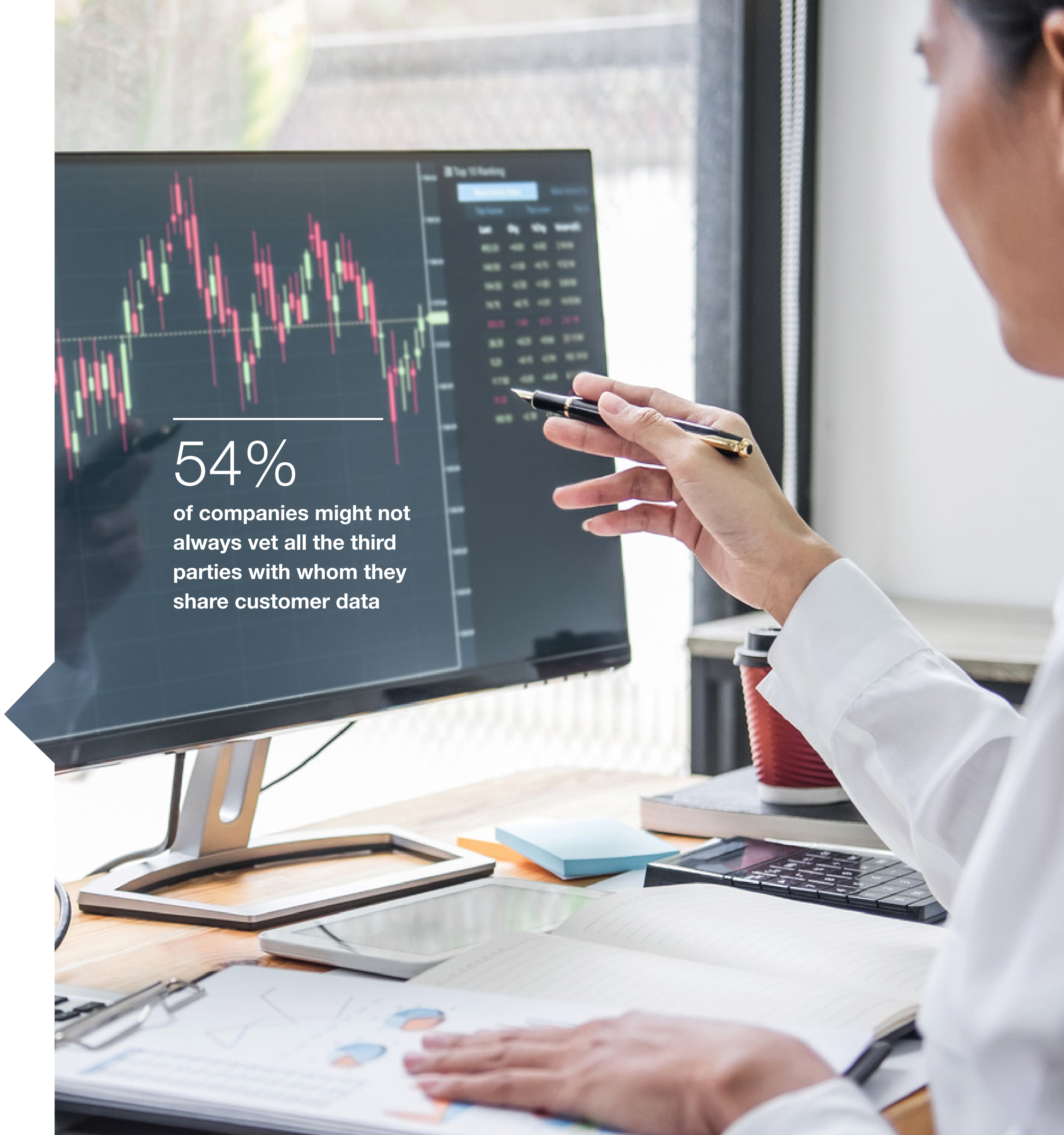
Governance & Management Oversig

4. Your mission: Mitigate supply chain challenges and third-party risk

Your team: CISO + COO + CRO

Cyber threat actors are always looking for the path of least resistance. As organizations shore up front-end and back-end security, many hackers may turn their sights to supply chain and third-party openings.

Organizations are dependent on third-party vendors, such as those that do payroll, benefits or data processing, to help keep their business operating efficiently. But 54% of companies might not always vet all the third parties with whom they share customer data and 56% worry that third parties are ill-equipped to protect them.



54%

of companies might not always vet all the third parties with whom they share customer data

Identifying risks from current and potential third-party partners

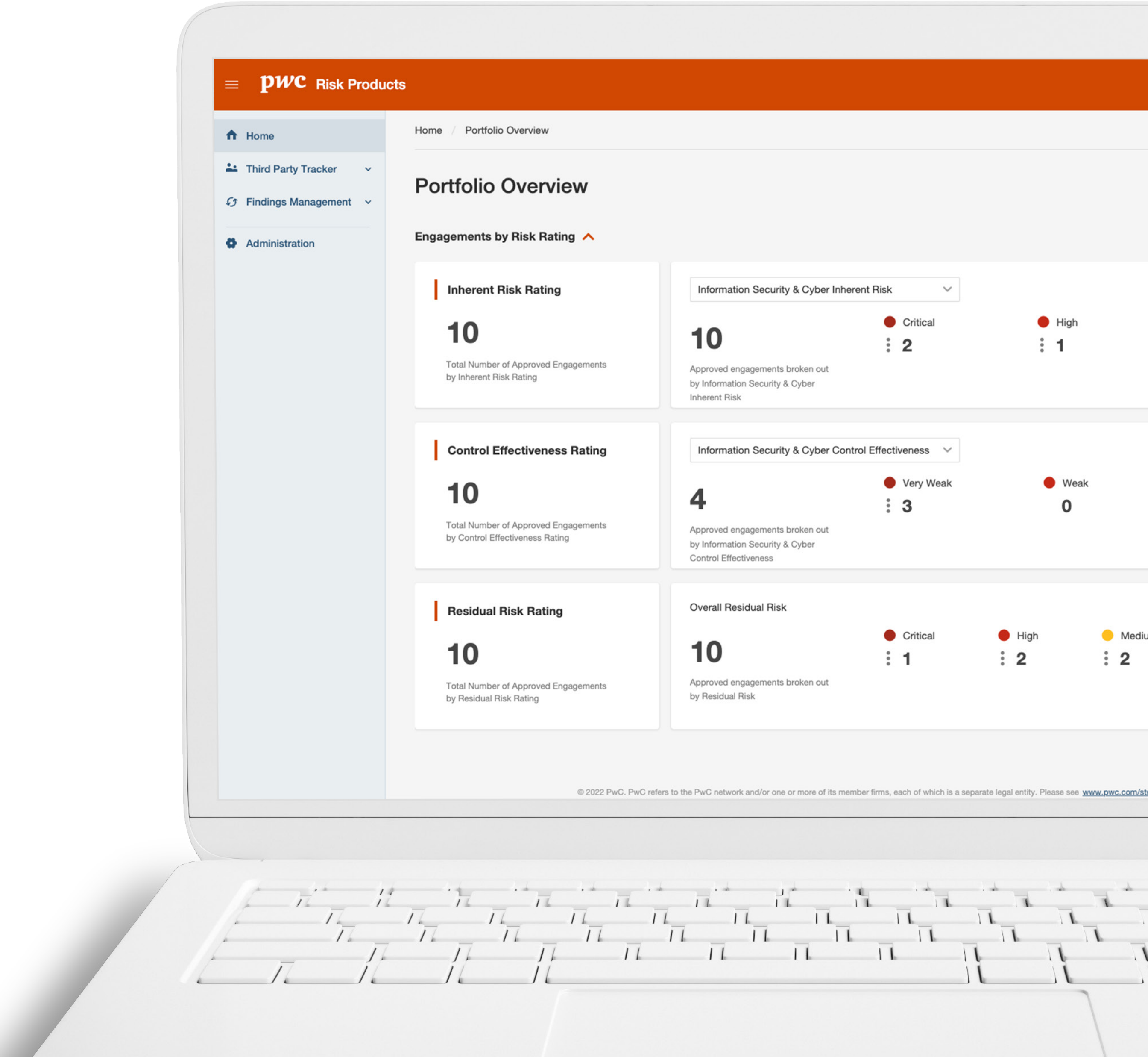
Without strong security controls, vendors may put companies at risk for catastrophic and highly-disruptive data breaches. A technology-enhanced third-party risk management (TPRM) program may provide companies with the advantage of quicker, data-driven decision-making by providing a thorough audit trail on various third-party relationships.

TPRMs can help you stay nimble, vigilant and proactive in protecting your business from double-dealing vendors and sidedoor attacks.

Your tech: Third Party Tracker

- Manage third-party risk from one centralized location
- Streamline operations and improve efficiency via a third-party intake process that includes customized surveys and risk assessments
- Continuously monitor emerging risks across many risk domains, including ESG, cyber, privacy and reputational risk
- Leverage data and analytics for insights into third-party relationships and get alerts on risk-related issues for review and remediation
- Increase transparency with executive dashboards and custom reporting

Third Party Tracker, a PwC product, helps screen and manage third parties, identify upfront cyber risks from potential partners, conduct due diligence and monitor risks throughout the lifecycle of third-party relationships. Gain more control over your relationships, business impact and reputation with capabilities that identify risks upfront before a new deal, help prioritize response tactics to reduce threats and push real-time alerts when third-party partners experience a cyber event.



Home / Portfolio Overview

Portfolio Overview

Engagements by Risk Rating

Inherent Risk Rating

10

Total Number of Approved Engagements by Inherent Risk Rating

Information Security & Cyber Inherent Risk

10

Approved engagements broken out by Information Security & Cyber Inherent Risk

● Critical 2

● High 1

Control Effectiveness Rating

10

Total Number of Approved Engagements by Control Effectiveness Rating

Information Security & Cyber Control Effectiveness

4

Approved engagements broken out by Information Security & Cyber Control Effectiveness

● Very Weak 3

● Weak 0

Residual Risk Rating

10

Total Number of Approved Engagements by Residual Risk Rating

Overall Residual Risk

10

Approved engagements broken out by Residual Risk

● Critical 1

● High 2

● Mediu 2

© 2022 PwC. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/st

5. Your mission: Prevent serious cyber disruptions with proactive monitoring

Your team: CISO + CRO

Day-to-day activities can be majorly disrupted by more than bad actors and cyber attacks. Global recessions, health crises, inflation — these are top organizational concerns over the next 12-24 months.

Applying capabilities that can respond to the full spectrum of emergencies — both man-made and natural — is necessary to build resilience, and possibly even thrive, during times of major disruption. Organizations are learning to monitor risks in a more holistic way, but responding and recovering — the core competencies that make up resilience — often fall short.

Managing risk assessments with broader control and transparency

Only 7% of organizations approach resilience in an integrated fashion. In the event that the risk turns into a breach, 53% of organizations are still using predefined processes.

When it comes to breaches, there is no one size fits all to remediating a unique, specific incident. Organizations will need to overcome fragmented remediation efforts with standardized — not blanket — approaches to business continuity, contingency and recovery.

Only

7%

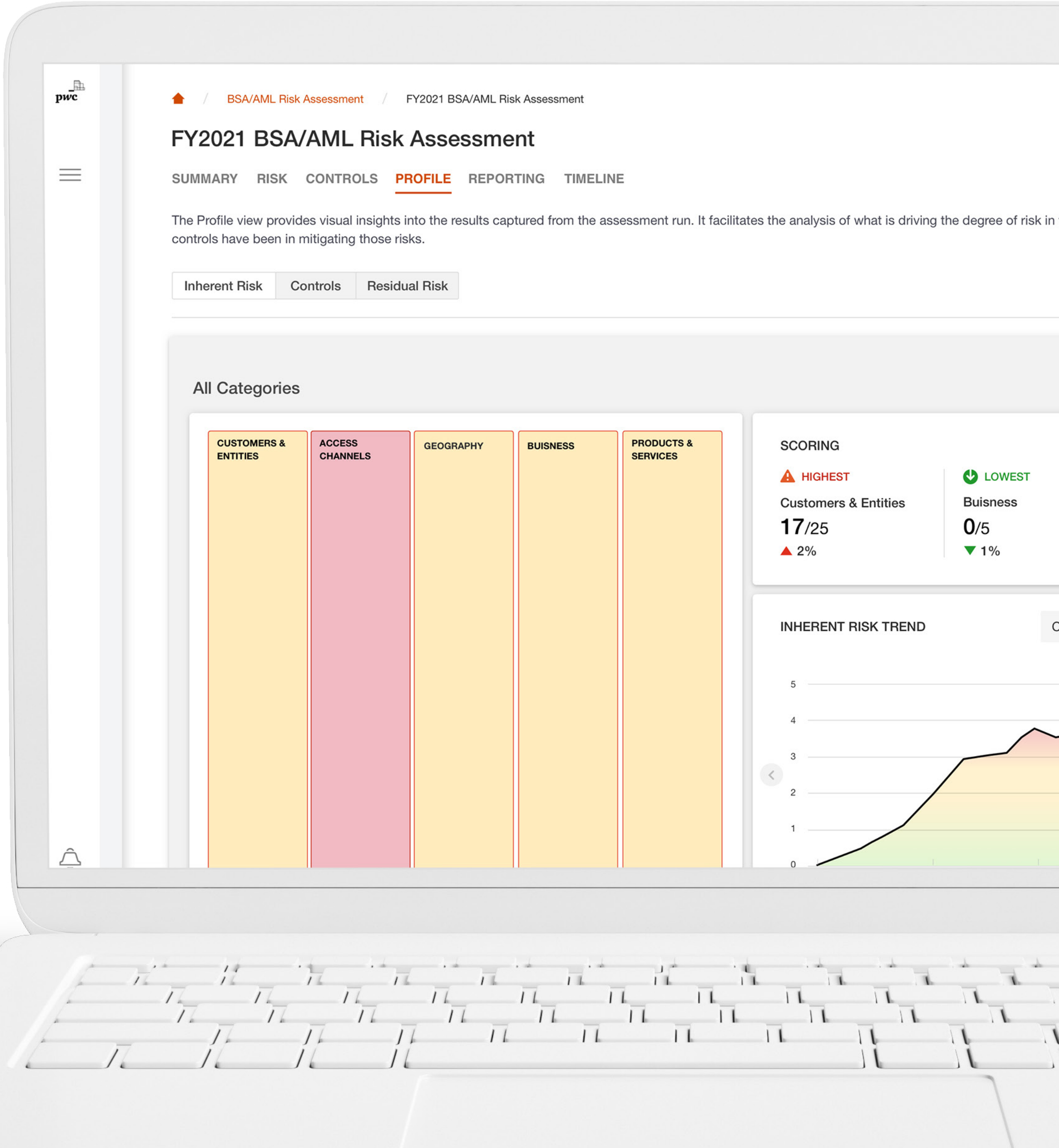
of organizations approach resilience in an integrated fashion

Your tech: Ready Assess

- Access assessments that help proactively identify prevent disruption
- Engage directly with first line of defense stakeholders to assess qualitative emerging or operational risk factors
- Map controls to risks to identify weaknesses or gaps
- Share visual results with automated templates and generated documents
- Develop detailed action plans based on your analysis and log them within workflows

Ready Assess is a dynamic, data-driven risk assessment platform. Access the risk assessment process from one place and build assessment templates to increase operational consistency and improve scoring across lines of business. Penetration testing and SIEM can also be established and enforced on demand to help monitor risks.

Ready Assess helps you analyze trends in risk exposure and effectiveness of controls, forecast the impact of changes to key risk indicators to test risk appetites and see how identified risks may create a residual impact to your business and strategic objectives. Dashboards allow your CEO and board members to understand historic decision-making and insight into results, investigations and what-if analyses.



BSA/AML Risk Assessment / FY2021 BSA/AML Risk Assessment

FY2021 BSA/AML Risk Assessment

The Profile view provides visual insights into the results captured from the assessment run. It facilitates the analysis of what is driving the degree of risk in
controls have been in mitigating those risks.

6. Your mission: Get your board more engaged in cyber

Your team: CISO + CEO + CRO + Board

As companies race to evolve, so do their cyber adversaries, and many have struggled to understand how and why. Less than half of board members, for example, believe they understand the causes and effects of cyber risks.

Board members don't want to sit idly by. Corporate directors want to receive more training, meet more often and see improved reporting on cyber incidents. C-suite members can help the board level up their cyber savviness by sharing scorecards and dashboards on key risk indicators, educating them on leading practice cybersecurity strategies and by using modeling data to help bring to life the impacts of cyber threats.

Companies are also facing increasing demand from the outside. Regulators want more visibility into cyber practices. Investors are looking for consistent and comparable disclosures. Citizens want to know how their data is being used and kept safe.

Less than

50%

of board members believe they understand the causes and effects of cyber risks.

Strengthening board oversight

Senior directors and boards may understand cyber risks in theory. But to gain more buy-in, support and investment, C-suite members should make cyber threat scenarios and their impacts more tangible.

The financial, operational and reputational dangers should be made clear. Only then can data-driven decisions and discussions take place in how executive leadership wishes to protect, mitigate and respond to cyber threats and attacks.

Your Tech: Board Central

- Cyber risk training for board members including templates for board reporting, key questions for management, information on regulations and a breakdown of current cyber risks

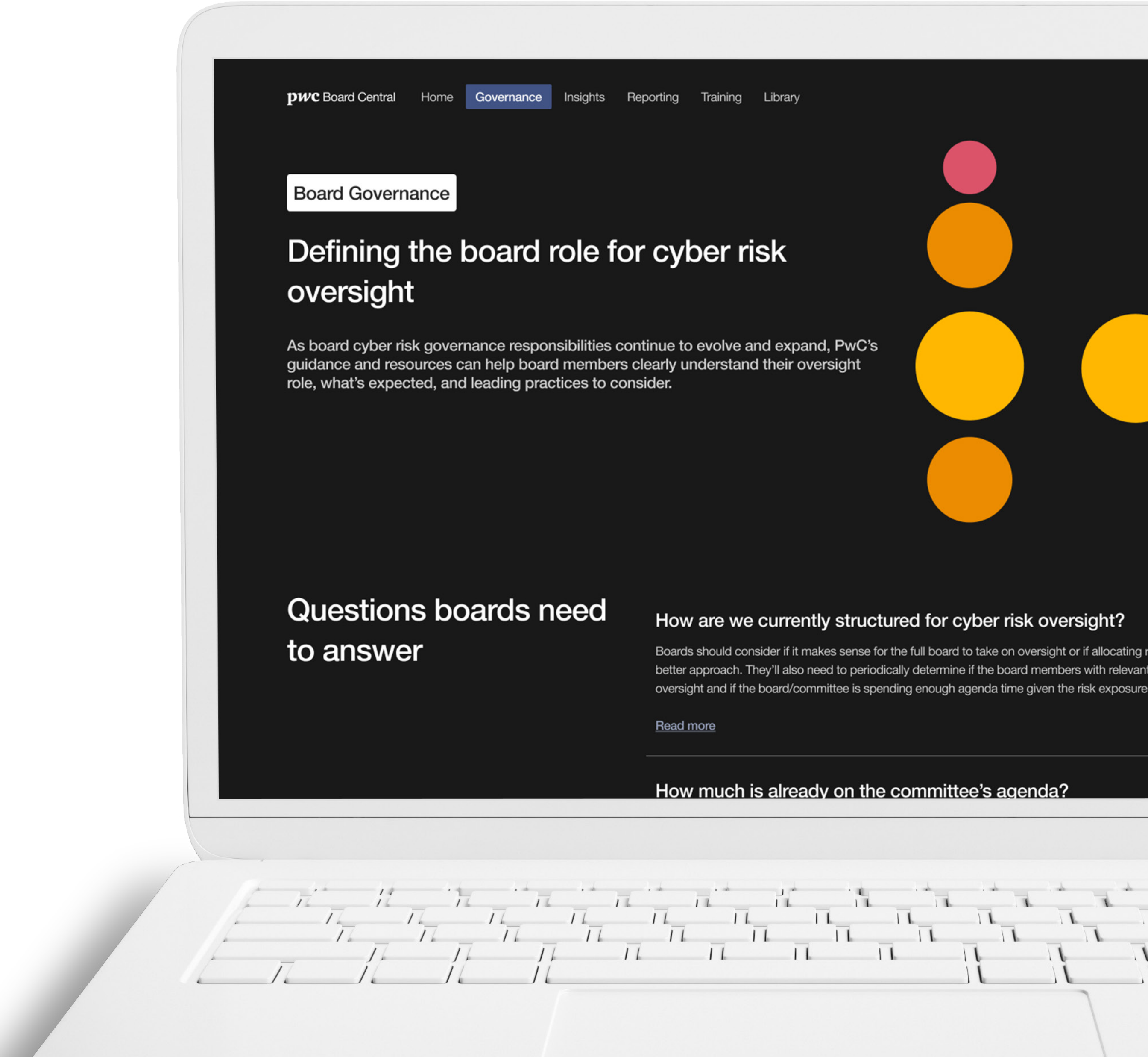
- Tailored cyber threat intelligence for board members on emerging cybersecurity threats, national cyber threats, cyber criminal threats, ransomware and notable incidents

- Benchmarking data so board members can compare their own cyber spend, staffing, maturity and vulnerability to industry peers

- Guidance for cyber risk reporting to help C-suite leaders collect and report on key data throughout the board reporting lifecycle

Board Central, a PwC product, is a digital platform that helps boards and senior directors better understand their cyber risk governance role and gain clarity on the organization's cybersecurity capabilities — and responsibilities.

Board Central helps you prepare for your next board briefing, strengthen board oversight and explain risk exposure. It combines PwC insights, personalized benchmarking data and training resources based on leading frameworks, so they know what the company needs to stay secure now and into the future.



Defining the board role for cyber risk oversight

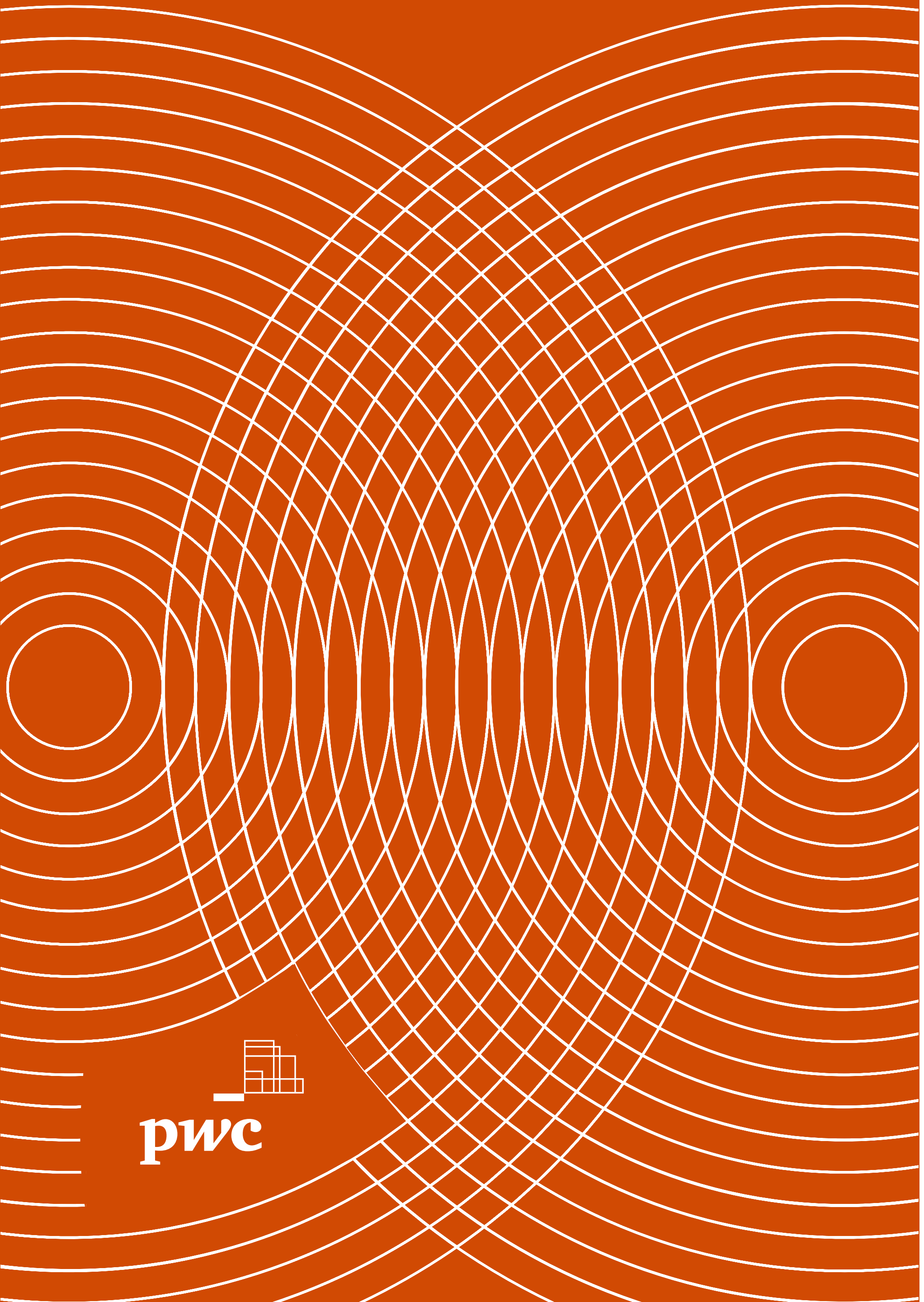
As board cyber risk governance responsibilities continue to evolve and expand, PwC's guidance and resources can help board members clearly understand their oversight role, what's expected, and leading practices to consider.

Questions boards need to answer

How are we currently structured for cyber risk oversight?

Boards should consider if it makes sense for the full board to take on oversight or if allocating
better approach. They'll also need to periodically determine if the board members with relevant
oversight and if the board/committee is spending enough agenda time given the risk exposure

How much is already on the committee's agenda?



PwC's Risk Management Products help you respond to the impact of tomorrow's threats today

Reimagine risk, unlock opportunity.

Connect with our team to learn more.

Contact us