Building digital trust: The partnership of leadership and operations

Security, tech, privacy and risk execs reveal current state of trust in third-party and data management

April 2021

pwc

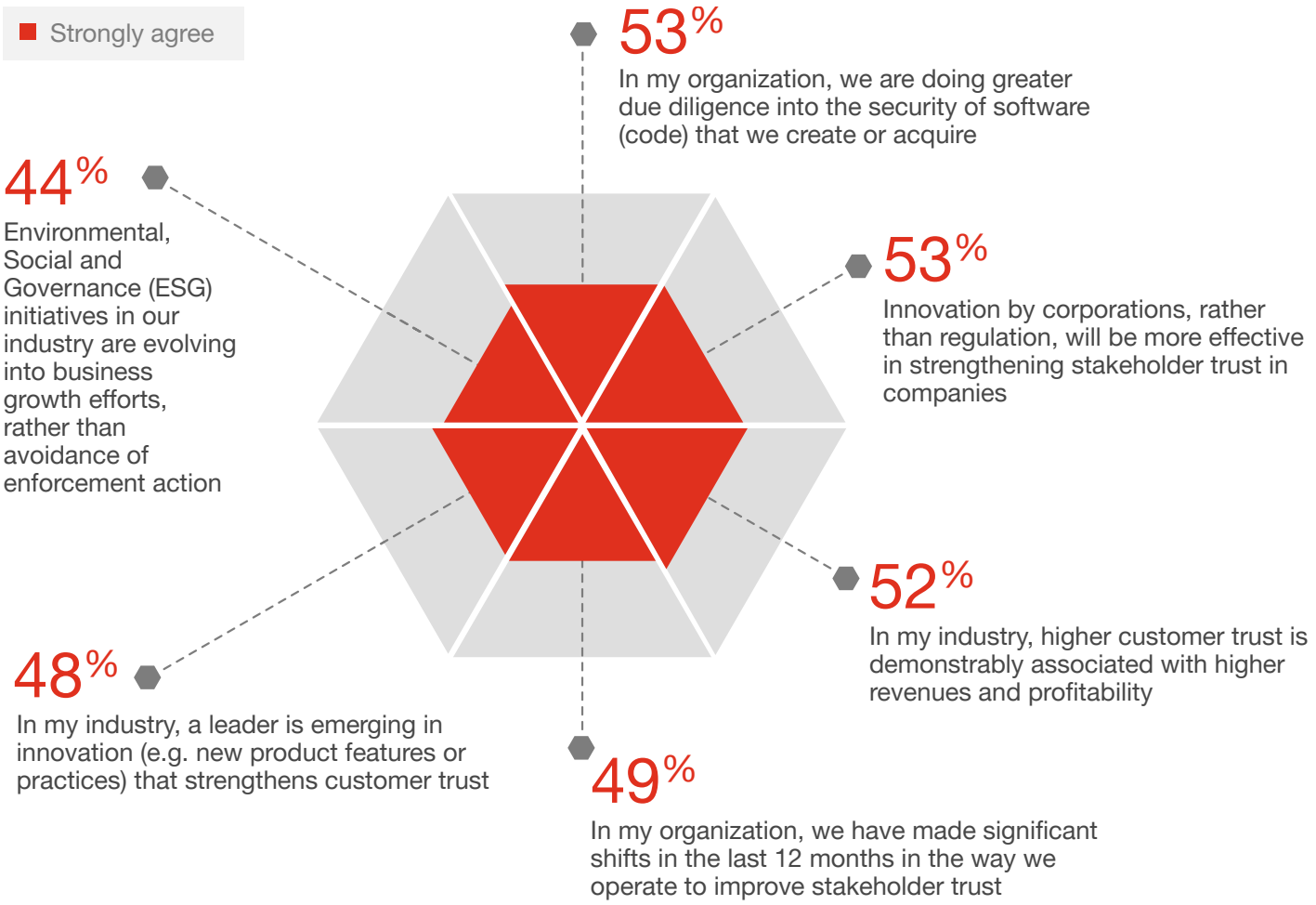
Contents

Building digital trust: the partnership of leadership and operations

How do tech, security, privacy and risk leaders approach stakeholder trust? We wanted to find out. So in the spring of 2021, PwC surveyed 311 executives of mid-size to very large companies across US sectors.

The results clearly indicate that change is afoot. More than half (53%) strongly agree that innovation by corporations, rather than regulation, will be more effective in strengthening stakeholder trust, and that higher customer trust is demonstrably associated with higher revenues and profitability (52%). Nearly half (48%) strongly agree that in their industry a leader is emerging in innovations that strengthen customer trust, and 49% told us they've made significant shifts in the last 12 months in the way they operate to improve stakeholder trust.

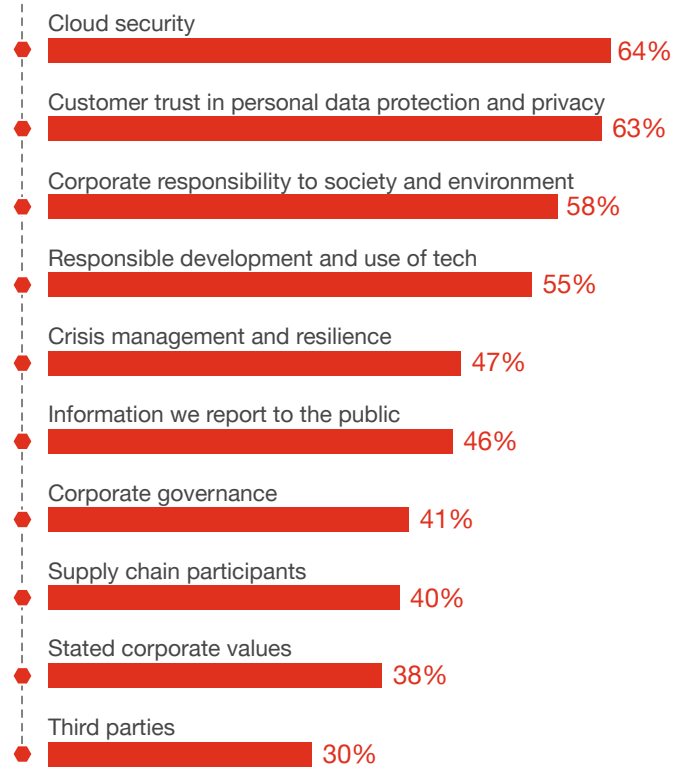
Customer focus and innovation kindle improvements in digital trust



A4. To what extent do you agree or disagree with the following statements? Base strongly agree (148 - 166), agree - strongly disagree (145 - 163)
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

With a significant majority of the executives actively focused on stakeholder trust, many are investing in multiple measures (at least four of them, on average). The top two focus areas for trust building are related to cybersecurity — cloud security (64%) and data protection and privacy (63%) — followed by corporate responsibility to society and environment (58%) and responsible development and use of technology (55%).

Cloud security, data protection and privacy: key to improving trustworthiness in 2021

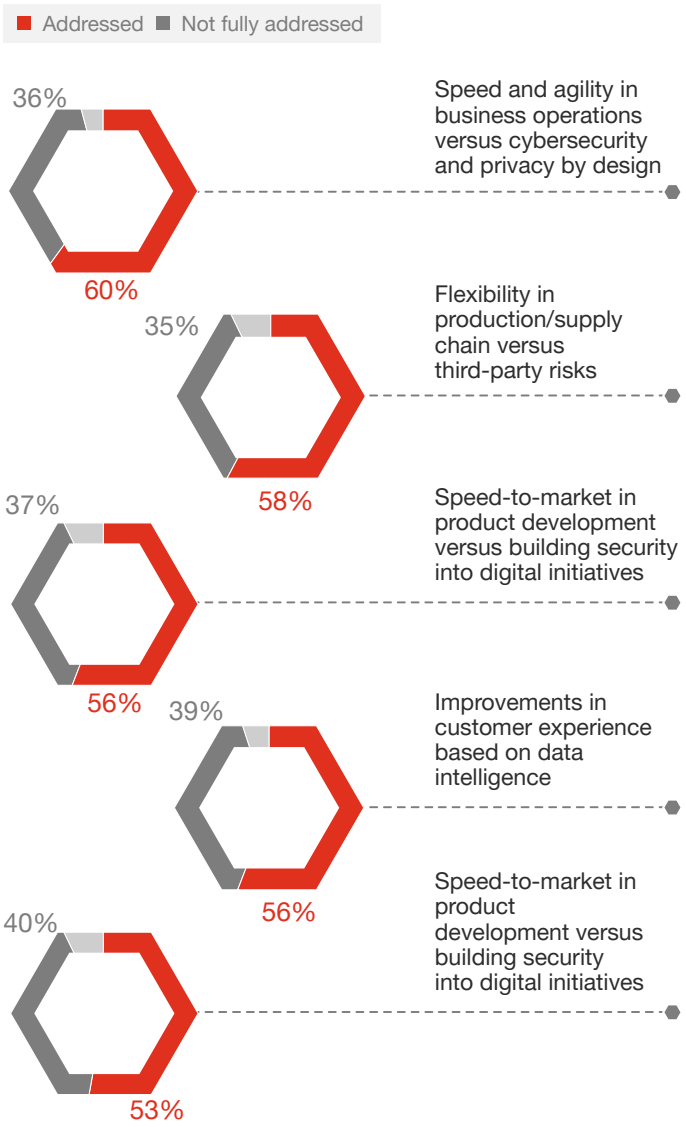


A1. In 2021, which of the following are most important for companies to tackle to become more trustworthy to their stakeholders? Rank up to 5 Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

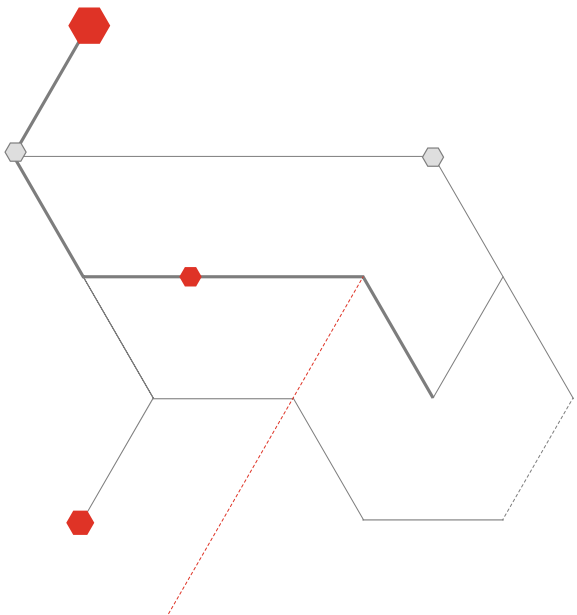
These executives face hard, even profound, strategic decisions touching on core issues such as balancing customer privacy with monetization of their data, moving with speed and agility while embedding security and privacy, flexibility in supply chains while managing third-party risks. Between 53% and 60% of executives say that their organizations have fully addressed these tensions — that is, they have crafted strategies and processes to address them. But with technology ever advancing and the business environment ever changing, leaders may have to revisit these time and again.

They may even create new solutions that achieve the balance between apparently conflicting choices. A company that chooses privacy as its primary value can build thriving business models around it. A company that honors consumers' right to opt into sharing their data might be more successful in reaching more consumers and earning their loyalty. An organization that takes the time to invest in supply chain security by design may encounter fewer operational disruptions down the road.

The most powerful role for leadership in trust-building: finding the balance between apparent trade-offs



A3. How has your organization addressed these trade-offs or tensions in your efforts to increase stakeholder trust? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.



The leadership and operational challenges of trust building

The business of building trust is all-encompassing: It is equally a leadership challenge and a design problem. It thus requires a two-pronged approach — both cultural and operational — and it requires buy-in from everyone.

The role of the CEO is to frame the choices among apparent trade-offs, to set a strategy that reflects the company's values and to imbue the culture with the spirit that animates their chosen direction — all with **board** confidence and oversight. They ask the question: which are genuine paradoxes that invite healthy tensions, and which are false tradeoffs? They lead imaginative thinking on new ways of doing business that can open deeper connections between trust and profitability — poised for a growth trajectory in a changing world. They speak up on their organization's efforts to win enduring trust.

The role of operational leaders like the CIO, CISO, chief privacy officer, chief data officer is to design and weave trust into the flesh and bones of the organization through detailed policies, controls and playbooks. Take the example of a new mobile app or a new IoT device: vetting users, verifying their identities, protecting the data they provide and generate on the app or device, using data for business intelligence or revenue generation, sharing data with business partners — all these should be set by policies, guarded through controls, and governed through playbooks.

Operational leaders should also serve as key advocates, offering counsel on the real-world consequences of the trade-off decisions leaders must make.

Just as companies are going beyond digitizing and reconceiving how they recreate value, so will they be innovating in the ways they can win stakeholder trust. Some are already re-shaping their organizations into security-first, privacy-first businesses, without waiting for regulations to set the new rules. Along the way, they're helping build the scaffolding for 21st century digital trust that can also facilitate more ambitious social, political, and economic goals.

Trust in third parties

At least one-third of our survey respondents said in the past year alone, they'd experienced significant disruptions due to third parties: software supply chain disruptions (47%), cloud breaches (45%), third-party platform exposures and outages and downtime (41%), data exfiltration (39%). And yet the trend of new third-party dependencies seen last year continues to gather steam.

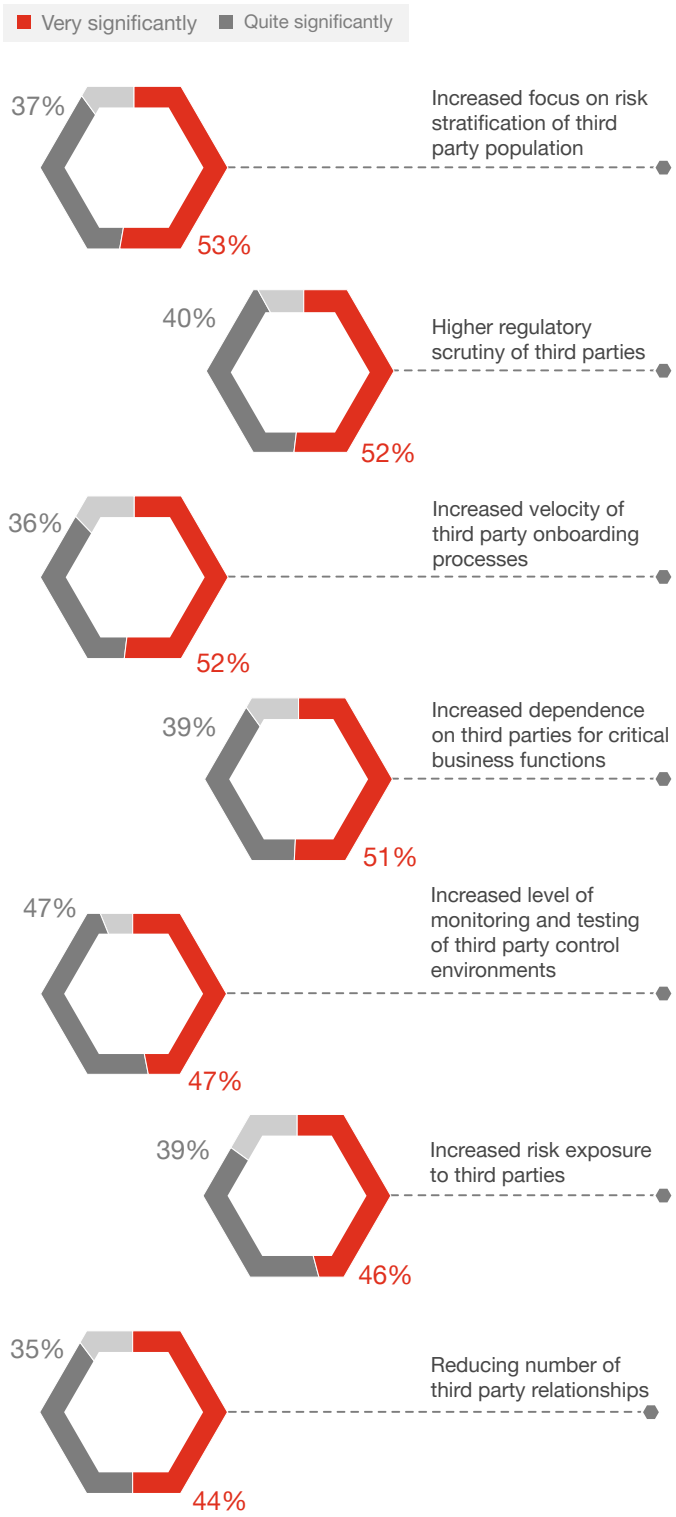
CEOs and corporate directors are increasingly asking CISOs, CIOs and CROs about their organizations' exposure to third parties. Our survey reveals why.

COVID-19 threw a monkey wrench into information security, sending risks ricocheting across the third-party ecosystem. Not only were organizations forced to intensify their reliance on outside service providers, they found the task of monitoring those providers via on-site assessments nearly impossible.

The survey illustrates changes in the business environment and the complex choices facing third-party risk managers at this inflection point.

The stakes are high. Even as 92% of businesses expect increased regulatory scrutiny of third parties — and 85% see their third-party risk exposure actually increasing — nine in ten still expect their dependence on third parties for critical business functions to grow. In response, 94% plan to strengthen their third-party controls, 90% say they'll focus more on risk stratification, and 88% expect to speed up their onboarding processes. A smaller share (79%) plan to reduce the actual number of relationships.

Executives expect significant operational changes regarding third parties in 2021

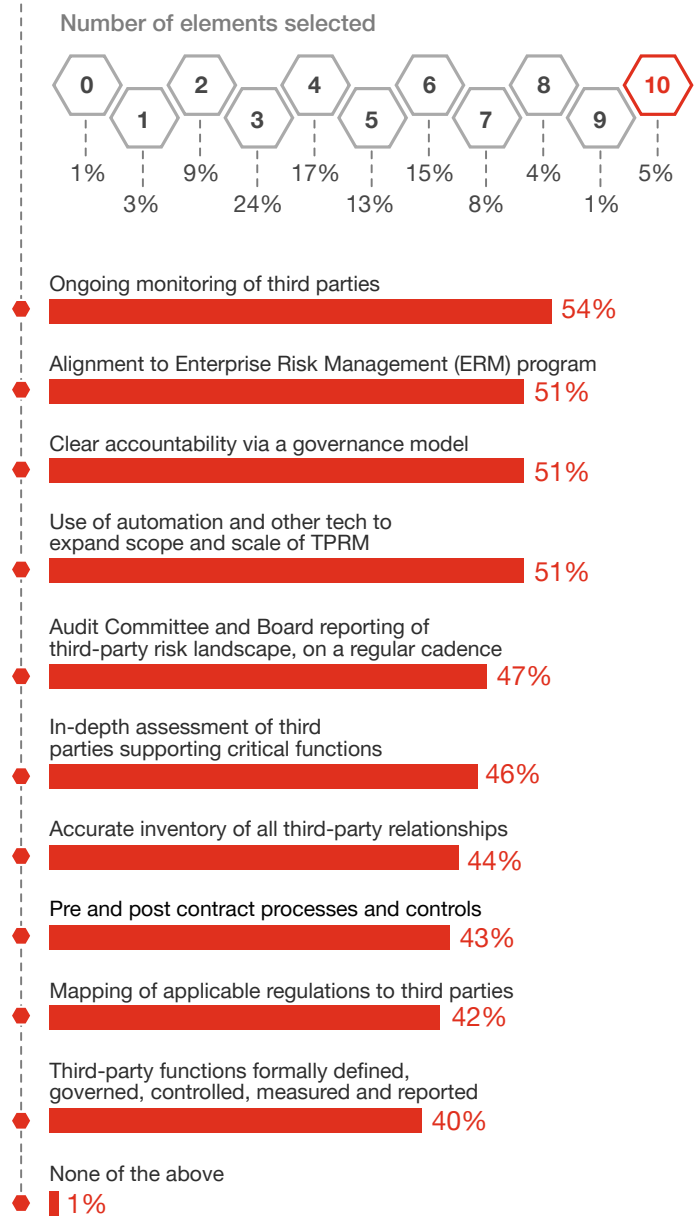


B1. Thinking about the businesses and economic environment you face in 2021, to what extent do you expect the following changes to affect your business? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

Trust is at a premium in times of turmoil — and companies rely all the more on their third-party risk management program (TPRM) to keep their operations secure. Yet in our survey, most businesses had implemented only three to six of the ten components of a robust program, and only 5% had a full complement. This is partly a reflection of the uneven state of third-party risk management across industries: lacking maturity in some industries, but advanced in sectors such as in financial services (with regulatory emphasis on resilience, for example) and aerospace and defense (with formal third-party certification of cyber practices).

The most frequently cited element of a TPRM program — ongoing monitoring of third parties — is conducted by 54%, yet only 40% have formally defined third-party functions that are subject to governance, controls, measures, and reporting.

Executives implement, on average, only 5 of 10 elements of a robust third-party risk management program

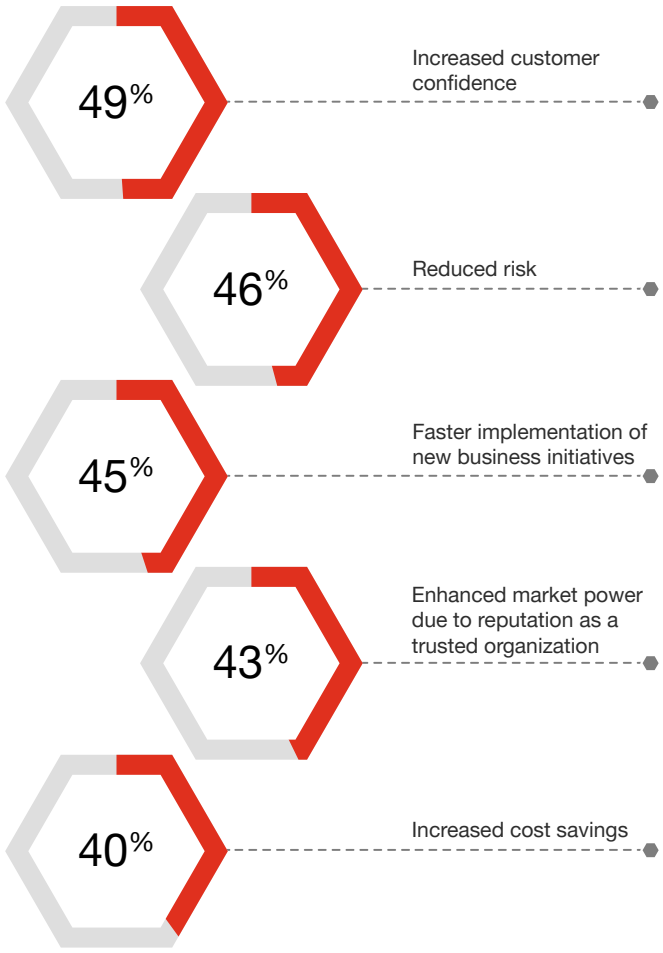


B3. Which of the following elements does your third-party risk manage program (TPRM) have today? Base: 311 (Multi-select)
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

While 70% of respondents were very confident that their TPRM program delivered demonstrable value to the organization in the past two years, less than half rated the value delivered on five measures at the highest levels (5 on a scale from 1 to 5).

Fewer than half say their third-party risk management program delivered significant value

% who say their organization derived significant value from their TPRM program (rated 5/5 in value)

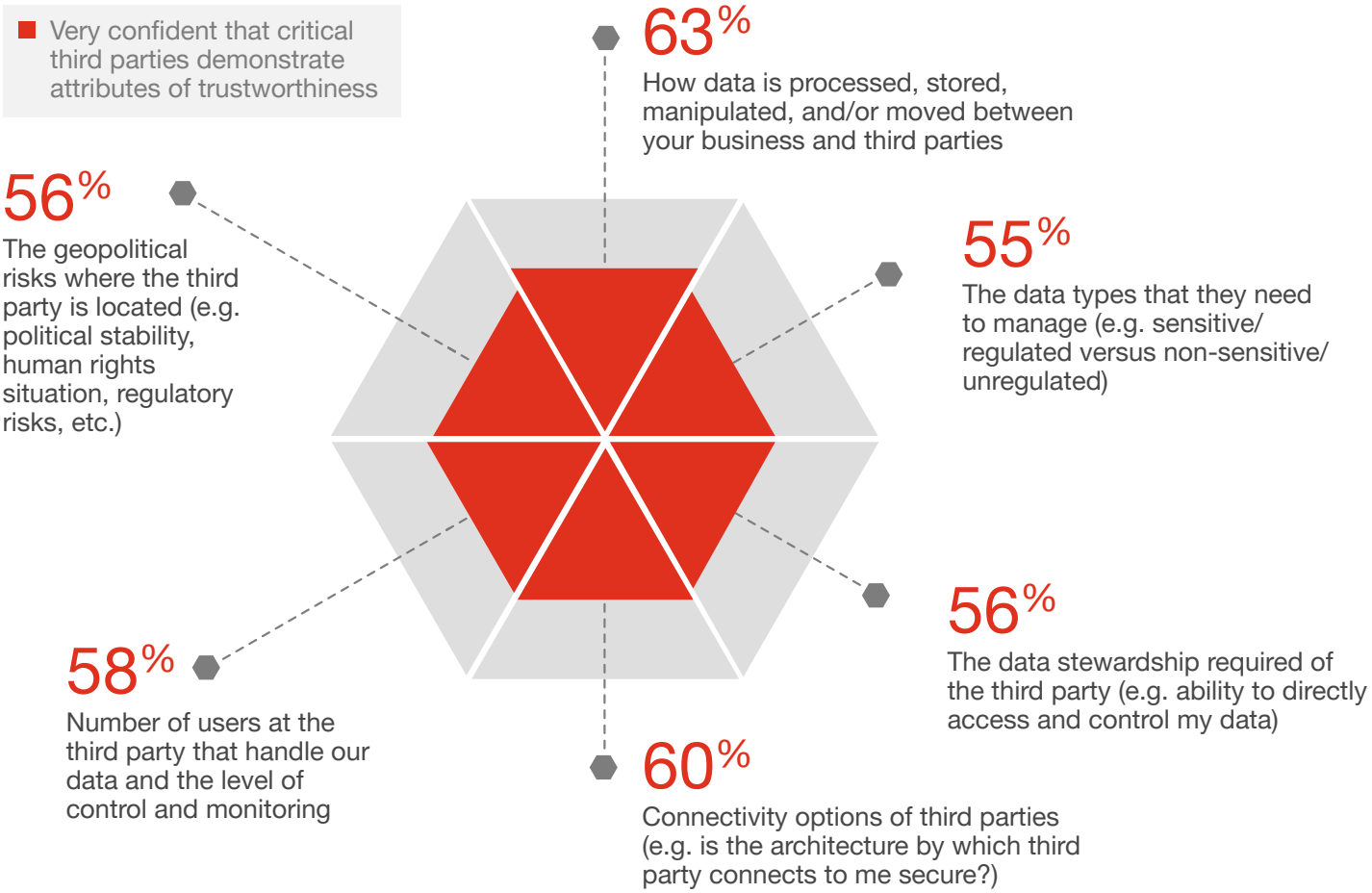


B4b. Which of the following does your organization derive value from your TPRM? (score from 1 to 5 where 1 = no significant derived value and 5 = significant value)
Base: 303
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

Unease about the current state of TPRM in their organization emerges also in the lack of confidence that their critical third parties meet their expectations of trustworthiness.

When it comes to the key attributes executives associate with trustworthiness — including how, and how securely, the company's sensitive data is transferred and handled, along with geopolitical or regulatory risk — no more than six in ten can say they're very confident that their critical third parties come up to expectations.

No more than 6 in 10 are very confident that their critical third parties can meet their trust expectations

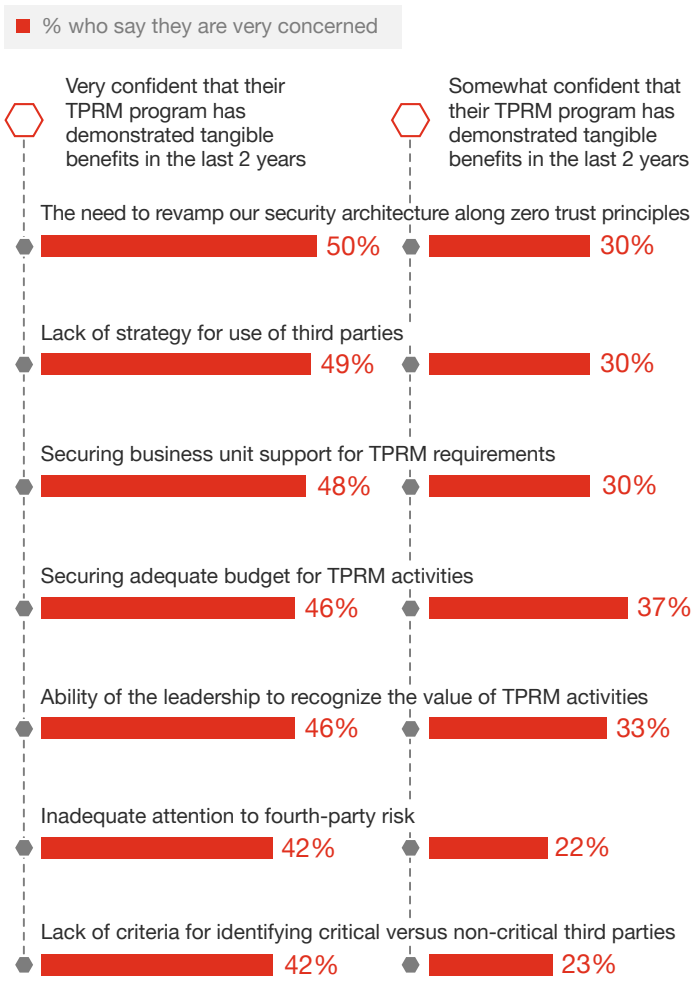


B2a. How important are the following when you determine how much you can trust your third parties (i.e. having more confidence in your third parties)? Base: 311
B2b. At this time, how would rate your most critical third parties on the attributes that are most important to your organization? All those who stated important at B2a Base: 291 - 301
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

A lack of complacency with the current state of affairs surfaces yet again in a third finding. The higher the confidence in the value delivered by their TPRM in the past two years, the higher the concern with getting the right strategic view, leadership support and resources to manage those risks better.

At least eight in ten worry about securing adequate support from within for their TPRM — be it in the form of budgets, leadership recognition or business-unit buy-in. A majority of the confident executives are very concerned about fundamentals: lack of strategy for use of third parties (49%), lack of criteria for distinguishing critical from noncritical third parties (42%) and inadequate attention to fourth/nth-party risks (42%). About half are very concerned about the adequacy of their security architecture.

The greater the confidence in past third-party risk management program performance, the higher the recognition of the need to do more



B4A. How confident are you that your TPRM program has demonstrated tangible benefits in the last two years? B5. To what extent are you concerned about the following, with respect to your TPRM? Base: Very confident 213, somewhat confident 90

Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

Two immediate actions to fortify your third-party risk management

Companies are growing more dependent on third parties for critical business functions. That's why how you manage third-party risks is more than a matter of curiosity to your stakeholders. Be ready to tell your business customers how your TPRM enables secure, reliable and resilient supply chains. If you're a direct-to-consumer business, be prepared to tell consumers how you handle privacy and data security and the value you place on this.

An appropriately designed TPRM can bring value to your organization and stakeholders in multiple, self-reinforcing ways. It enables customers to feel confident in sharing their data. It enables confidence in the reliability of your supply chain to deliver the quality you expect, on schedule. Your TPRM can also help you safely reduce the number of third parties in your ecosystem — improving your bargaining power, while lowering your risk profile. And that, in turn, can reinforce your consumers' confidence.

Here are two actions you should take to begin to future-proof your third-party risk management program and build trust in third parties you depend upon.

First, set up a third-party risk management office, or TPRMO, that acts as a kind of connective tissue to all of the third-party risk areas in scope. Several functions touch third-party risk management: the business units that engage with them directly, the legal and procurement departments that govern contracting, the internal auditors that create and monitor the controls, the IT and security teams, and the compliance group. Your TPRMO can uncover opportunities to eliminate duplications, identify gaps in coverage and simplify third-party risk management operations.

Consider an automotive company. Most new car electronics require periodic software upgrades, typically supplied by third parties. The OEMs are responsible for confirming that owners' personal information is protected when these upgrades take place — while also confirming that the cars themselves remain safe. How they handle these multiple stakeholders as they deliver the updates is critical. Without central coordination, the risks can fall through the cracks in the supply chain and scale up rapidly.

Consider also the growing ecosystem of third-party apps and tech providers across many industries. A central third-party risk office is better able to help guard against attacks like the hack via software-update revealed in December 2020 — and the software supply chain intrusions that significantly affected 53% of respondents in 2020.

As a set of capabilities focused on a category of risks, TPRM falls under the umbrella of enterprise risk management — and needs to evolve along with the ongoing transformation of risk management into an intelligence-driven one risk office.

Second, make the right investments in technology to automate third-party risk management processes — it's a huge opportunity for innovation. Third-party trackers expedite the monitoring of third parties at the initial assessments and throughout the life of the relationships. Automation helps speed up onboarding, without sacrificing deeper, more complete assessments of third parties. For example, an often-overlooked risk, given the increase in the use of third parties, is assessing providers at the vendor level, rather than at the level of the actual product or service being used. Many vendors have multiple points of access with organizations, and vetting them at the wrong level can inadvertently expose the company to risk.

Technologies such as Risk Command, ranging from single dashboards to real-time threat intelligence to real-time regulatory intelligence, can reduce the time to make intelligence-driven decisions and responses — mutually reinforcing your organization's data trust practices.

Respondents with more mature data trust practices stood out in multiple ways:

- significantly reduced their number of third-party relationships,
- increased their level of monitoring,
- deepened their assessment of third parties, and
- were confident that their TPRM had shown tangible benefits in the last two years — including increased cost savings, faster implementation of business initiatives, greater customer confidence and enhanced market power.

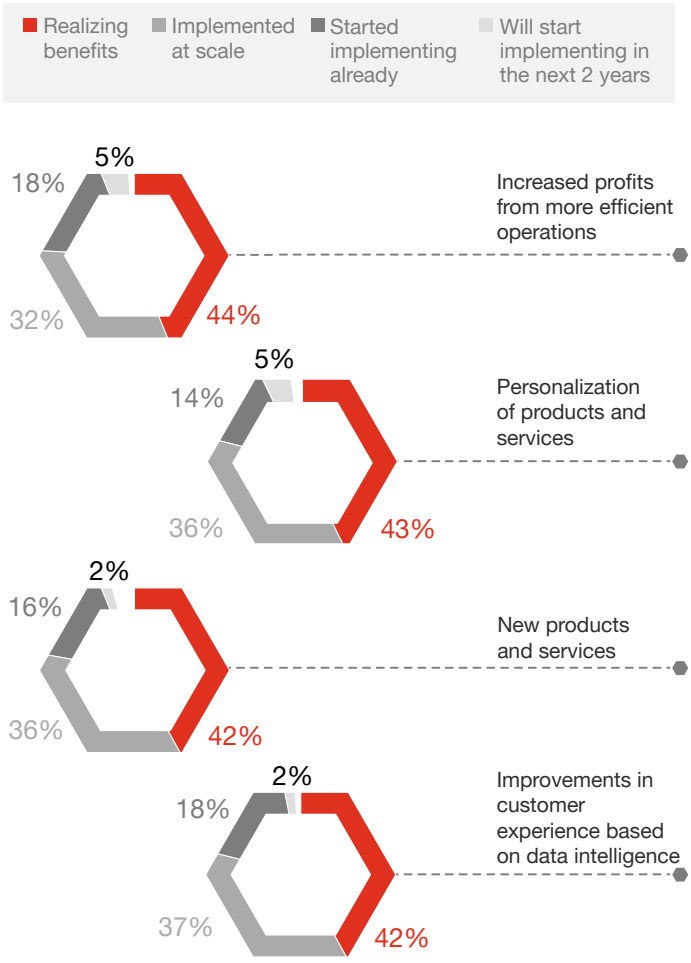
Trust in data

By virtually every metric, organizations with more mature information governance practices are better positioned to achieve growth in revenues or profits — and gain stakeholder trust. Four in ten respondents report realizing benefits from data monetization. And half report mature information governance practices. But considering the rush to monetize data and the explosion in concerns about data protection and privacy, there are plenty of risks, seen and unseen, that lie in wait for even the most mature company.

Nine in ten companies say they've already started implementing programs to monetize data. Just over four in ten are actually realizing benefits to date.

Turning data into something of value takes several forms: personalizing products and services (for example, a coffee chain or grocery that remembers your preferences and sends targeted ads to your smartphone); improving customer experience (a media streaming company or online learning app that makes recommendations based on your past interactions); offering new services; or improving processes and productivity.

More than 4 in 10 are already realizing benefits from data monetization



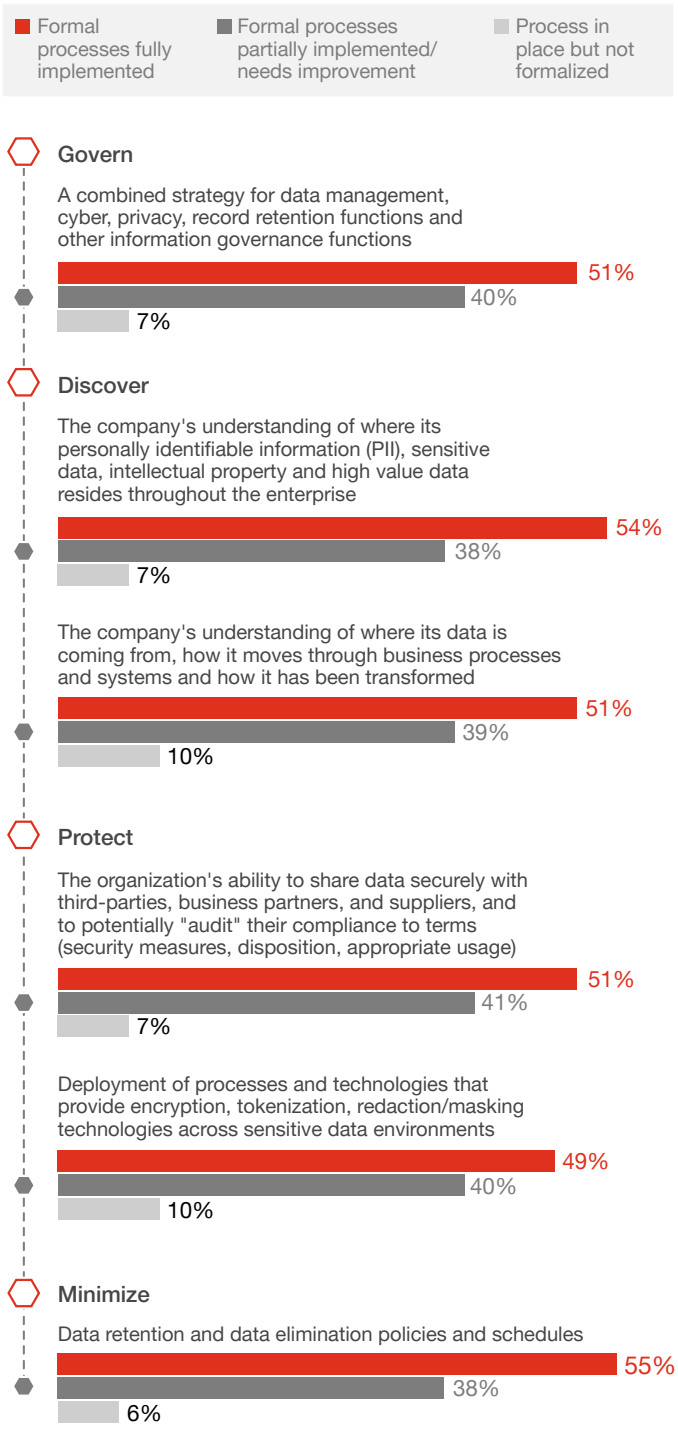
C1. To what extent are you monetizing data in your organization? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

Monetization should be predicated on trust. Consumers, business partners, regulators, employees, Wall Street, the media, the body politic — all have a stake. Not surprisingly, customer trust in personal data protection and privacy is second among the survey respondents' top five issues to tackle to improve stakeholder trust.

How much can companies be trusted with their use of data — both personally identifiable information and other data? It can seem daunting to gauge that, but we've distilled it into four capabilities within a data trust framework: how well a company governs, discovers, protects, and minimizes the data it holds. Data governance is the process, data trust is the outcome: data that decision makers can rely on, data use that is ethical, safe, and trustworthy.

According to our survey, about half are mature in their data trust practices, i.e., they have formalized processes and have fully implemented them. Fifty-one percent report having a combined strategy for different functions responsible for aspects of information governance (privacy, record retention, cyber, data management and others). More than half say they have formal processes to understand where the sensitive and high-value data reside in the organization (54%) and how the data is sourced and moves through the organization (51%). About half protect data sharing within their ecosystems with processes and technologies. Finally, 55% have formalized processes for data retention and elimination (a focus of new regulation such as the California Privacy Rights Act).

About 4 in 10 still need to fully implement formalized data trust processes. About 1 in 10 have yet to formalize them.



C2. How mature are the data trust practices in your organization? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

We found that companies with more mature data trust practices tend to be ahead in many respects. They realize financial benefits of data monetization via personalized services, greater operational efficiencies and better customer experiences. They strongly agree that higher customer trust leads to demonstrably higher revenue. They've done significant moves in the past year to improve stakeholder trust. And they're more confident in their third-party risk management program: they do more monitoring of third parties.

Overall, reporting on data security and privacy is heading towards greater transparency. Executives reported significant improvements in four areas: incorporating these risks to overall risk reporting (56%), reporting regularly rather than episodically (53%), providing sufficient detail on earnings and analyst calls (50%) and thorough, in-depth reporting to boards (49%).

Reporting on data security and privacy to boards and investors has greatly improved over the last year

C4. To what extent has your reporting on data security and privacy to the board and investors improved in the past 12 months? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.

Still, there's plenty of room for growth. While half of the respondents told us they have formal processes in place in relation to information governance, four in ten feel these are only partially implemented and need improvement. And about one in ten have not formalized processes at all.

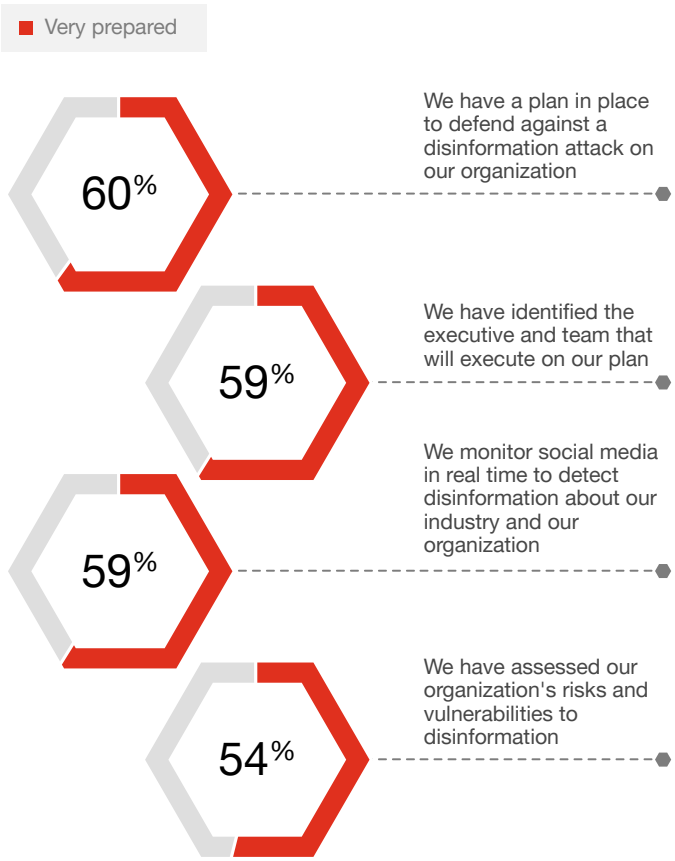
More importantly, the greater risks with data trust constellate as much around what you don't know, as around what you do know.

For example, how prepared are companies for a disinformation attack? Disinformation strikes at the heart of stakeholder trust — and in an era of fraying faith in institutions, falsehoods often spread farther, faster and deeper than accurate information. Nine in ten executives in our survey are confident that they're prepared to defend against a disinformation attack, with 60% saying they're very confident.

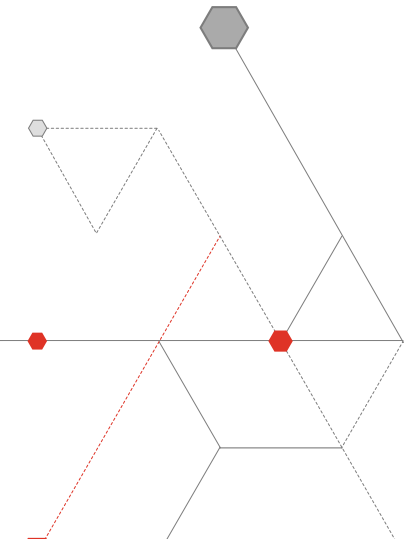
This near-unanimity invites some circumspection, if not outright skepticism. First, not many companies have experienced such an attack yet. Second, a disinformation attack is not like a typical financial fraud or crisis, and cannot be handled in the same way.

There are some frontier angles to consider as well. Does a corporation bear responsibility for what its employees publish — true or false — on social media? To what extent might employees be liable due to actions by (or aimed at) the organization or its senior leadership? Where, if at all, do the lines of responsibility meet? Defending against a disinformation attack, many will find, requires far more cross-functional leaders to work faster together; it requires a playbook that's rehearsed to the point of muscle memory.

More than half feel very prepared to defend against a disinformation attack



C3. In your view, to what extent is your organization prepared to defend against a disinformation attack? Base: 311
Source: PwC, Building digital trust, US Digital Trust Insights Snapshot, April 2021.



Armed for the frontiers

Executives across security, technology, privacy and legal functions begin to formalize information governance processes by answering three key questions: What are the key data that generate advantage for your organization? Where are the key data located? Who has access to the data? This knowledge, continuously updated as the organization evolves, gives your organization's data trust framework a firm footing.

That framework and its practices are sure to be continually tested. The sheer scope, volume and intimacy of data being surrendered by individuals to connected devices every day is staggering. Data is fueling smarter AI algorithms, which is helping businesses create still better products and experiences that attract more customers who share more data, producing even smarter AI. Responsible AI practices are evolving to govern this tech and to confirm that it's making accurate, bias-aware decisions and that it's not violating anyone's privacy. Newer regulations about data protection and privacy are changing norms, increasingly bending toward stronger exercise of consumer rights and government enforcement. Trust builders are challenging the backbones of systems such as search, advertising and financing, and they're introducing better ways to protect data and privacy. How are you engaged in thinking creatively about how to improve stakeholder trust in your stewardship of data?

About this survey:

PwC Research, PwC's Global Centre of Excellence for market research and insight, conducted the survey.

This special edition of the US Digital Trust Insights Snapshot Survey is a poll of 311 security and technology executives of US-based companies who are familiar with or involved in increasing trust among B2B customers and business partners. The survey was conducted from February 22 to March 5, 2021. Thirty-five percent of respondents are executives in very large companies ($5 billion or more in revenues); 38% are in large companies ($1 billion but less than $5 billion). Respondents come from a range of industries: consumer markets (21%), industrial manufacturing and automotive (20%), tech, media, telecom (19%), financial services (18%), health (15%), and energy, utilities and mining (7%).

Another US Digital Trust Insights Snapshot of 300 executives will be conducted in April-May focused on threat outlook and cyber investments in the next 12 months. The Global Digital Trust Insights, a survey of more than 3,000 business, security, risk, and tech executives around the world, will be conducted in July 2021.

Contact us

T.R. Kane
Principal, Cybersecurity, Privacy & Forensics, PwC US
t.kane@pwc.com
440-390-8502

Joseph Nocera
Cyber & Privacy Innovation Institute Leader, PwC US
joseph.nocera@pwc.com
312-925-6569

Dean Spitzer
Principal, Cybersecurity, Privacy & Forensics, PwC US
dean.v.spitzer@pwc.com
917-841-2976

Sean Joyce
Global and US Cybersecurity, Privacy & Forensics Leader, PwC US
sean.joyce@pwc.com
202-684-5782

Mir Kashifuddin
Partner, Cybersecurity, Privacy & Forensics, PwC US
mir.kashifuddin@pwc.com
817-683-8296

pwc.com/cybersecurity