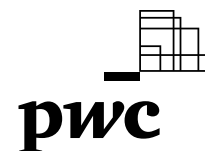




# Cyber-ready — today and for tomorrow

Why cyber-ready now is not enough

June 2021



# Contents

Introduction	2
The cyber-threat landscape: The digital rush left many exposed	4
Big bets: Cloud security, cloud security, cloud security	7
People in cyber: Going all-in on cyber starts from the top	11
Despite heightened risks, hope flourishes	13
About this survey	16

A sense of cyber-urgency has seized the public and private sectors. Cyber threats jumped to CEOs' number-one concern in the US, and number-two globally, according to our [24th Annual CEO Survey](#). These CEOs are putting their money where their worries are.

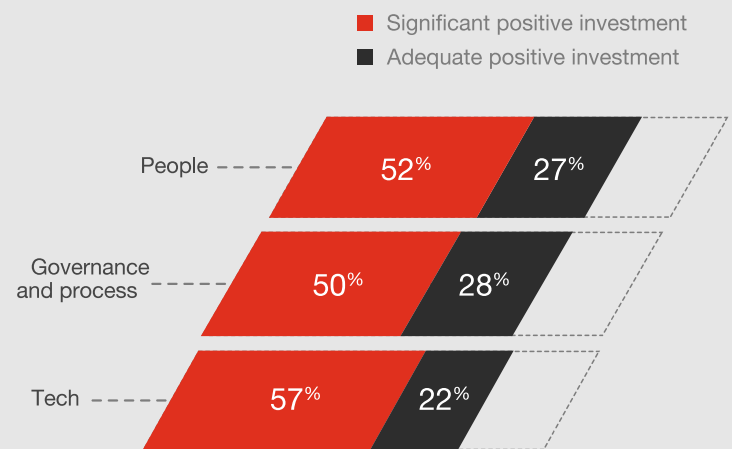
Companies are spending more on cybersecurity and privacy than ever before, as our US Digital Trust Insights (DTI) snapshot survey confirms. Our respondents — 322 CISOs and CIOs — told us in April that their organizations' cyber investments have gone up this year by significant amounts. And they expect cyber and privacy spending to rise even higher in 2022.

(Right after the survey closed, cybercriminals hacked into the IT systems of the biggest US gasoline pipeline company and the world's largest beef and poultry producer. The six-day precautionary pipeline shutdown triggered panic buying, gas price spikes and shortages in several states. The three-day halt in production at meatpacking plants is expected to lead to hikes in wholesale beef prices. Ransomware became a household term.)

Businesses and other organizations are allocating resources in people, processes (governance) and technology — the three legs of the cyber-transformation stool. But are they putting their money in the right place?

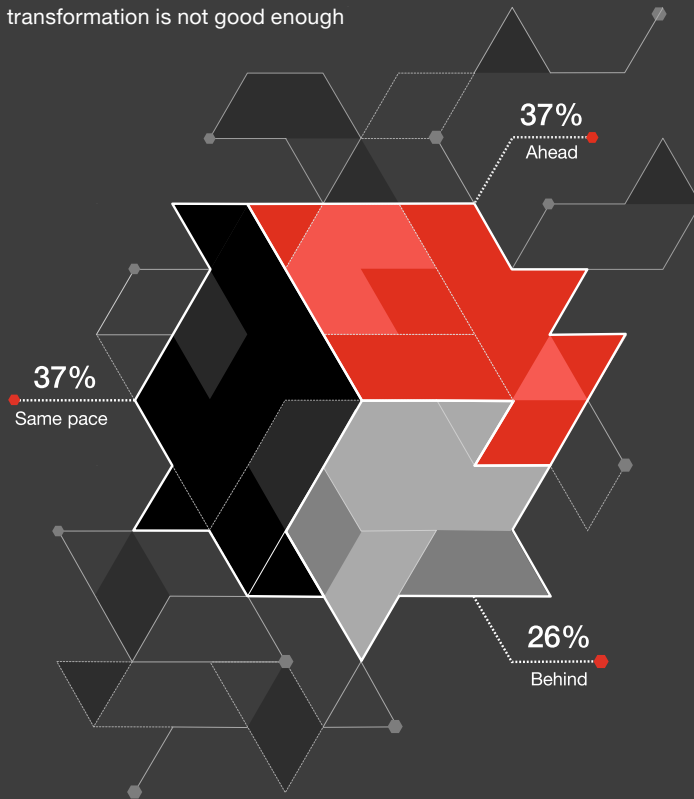
Cybersecurity transformations are either lagging behind digitization or merely keeping pace at most (63%) of companies. Neither is good enough, not at a time when the hits are coming fast and hard and show no sign of stopping.

## Cybersecurity is getting its due: Significant investments in tech, people, and governance and process



Q; How would you describe the level of cybersecurity support in your organization based on planned investments in the next 12 months?  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

**Invest in progress, not maintenance**  
 Being at pace with your organization's digital transformation is not good enough



Q: In enabling your organization's digital transformation, to what extent is your security function supporting it?  
 Source: PwC, US Digital Trust Insights SNApshot Survey 2021, June 2021. Base: 322

Given the unpredictable events of the last six months, your organization should stop fighting past battles. Instead, it needs to get the basics right to establish a foundation and position itself for agility to react to new and unexpected threats.

**This is what it means to be cyber-ready.**

You can't promise that your organization will not be breached, not when intrusions are happening by the thousands or millions every hour. But you should be able to say that, one, you've secured the infrastructure your organization's sustainable growth depends on and that, two, when the inevitable breach happens, your stakeholders can trust your organization to respond quickly and protect their interests.

To be able to realize that commitment, "on pace" with the business' transformations isn't good enough. Where is the industry headed? Where would your business need to compete in the future? Where might new technologies lead? You should have a point of view on these and make sure your security organization is prepared for those future scenarios.

The good news is that we're seeing more enterprises taking critical steps than ever before. How will yours use its resources to be cyber-ready for what comes next?

## Key findings and takeaways

**1**  
**64% expect a jump in reportable ransomware and software supply chain incidents in the second half of 2021**

The cyber-threat landscape:  
 The digital rush left many exposed

**2**  
**81% of those who quantify cyber risk say it helped increase productivity and focus on strategic matters**

Big bets: Cloud security, cloud security

**3**  
**Around 50% have restructured their security teams and embedded them in product development and business teams**

People in cyber: Going all-in on cyber starts from the top

**4**  
**Investments, CEO and board attention, and forward-looking CISOs make for a cyber-ready organization**

Despite heightened risks, hope flourishes

# The cyber-threat landscape: The digital rush left many exposed



## Key finding: 64% of the CISOs and CIOs we surveyed expect a jump in reportable ransomware and software supply chain incidents in the second half of 2021

As companies rushed to adapt to pandemic-inspired changes in work and business models, many seem to have left security behind. Half or more of the CISOs and CIOs in our survey say they haven't fully mitigated the risks associated with remote work (50%), digitization (53%) or cloud adoption (54%).

Securing **remote work** is still in progress. Seventy percent of organizations relied on a **password-centric** authentication approach as of March 2020 — even with advances in biometrics, multi-factor authentication (MFA) and tokenization. Meanwhile, employees — especially those of the millennial generation (51%) and generation Z (45%) admit to using applications and programs on their work devices that their employer has **expressly prohibited**. Remote work has pushed the edge of the organization to common home devices that are not hardened to the same degree as corporate networks.

Employees behind the keyboard can be unwitting participants to data breaches: 85% of breaches in 2020 involved a human element, according to Verizon's **2021 Data Breach Investigations Report**. **Phishing** accounts for the large majority of breaches via social engineering, with cloud-based email servers being a target of choice.

Securing **digitization** has become a catch-up game, as the pace of development accelerates. Fifty-seven percent of 4,300 developers and managers told the open DevOps platform **GitLab** that they're releasing code twice as fast as ever before. A year ago, only 35% said this. Nineteen percent said their code goes out ten times faster.

DevOps has clearly become more agile to support business needs. But where are the DevSecOps? Are companies

striking the **right balance** between speed to market, agility in operations, and security and privacy?

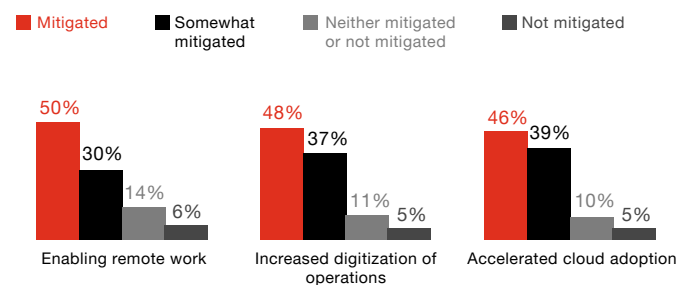
**Cloud security** is another major concern — and by failing to address it, businesses are hurting themselves. In PwC's inaugural US **Cloud Business Survey** of 524 C-suite executives, 53% told us they aren't getting the full value from the cloud.

An important reason why: Companies don't always take into account the unique security risks cloud adoption poses — or they don't consider these risks early enough to reap the full benefits of cloud and avoid extra costs.

**57% of developers are releasing code 2x faster. 19% are releasing code 10x faster.**

Gitlab survey of 4,300 developers and managers

## An incomplete grade: More than half haven't fully mitigated the risks from the big digital moves of 2020



Q: On a scale of 1 to 10, to what extent have you mitigated the risks associated with the following in the last 12 months? Mitigated (score 9-10); Somewhat mitigated (score 7-8); Neither mitigated or not mitigated (score 5-6); Not mitigated (score 1-4)  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

## Most believe rising incidents are inevitable

Hackers lost no time exploiting the veritable explosion in attack vectors that came with increased connections, devices, applications and data. At least half of organizations reported getting hit by malware via software update (54%), attacks on software supply chain (51%) and business email compromise (50%).

How prepared were they for the incidents they experienced in the last 15 months? Only 55% or fewer of victims said they were “well prepared” to address the breaches — meaning 45% weren’t.

**Software supply chain security** is now getting CEO and board attention. Companies run on code developed in-house, taken from open source and/or bought from tech vendors — in an ecosystem that runs on trust.

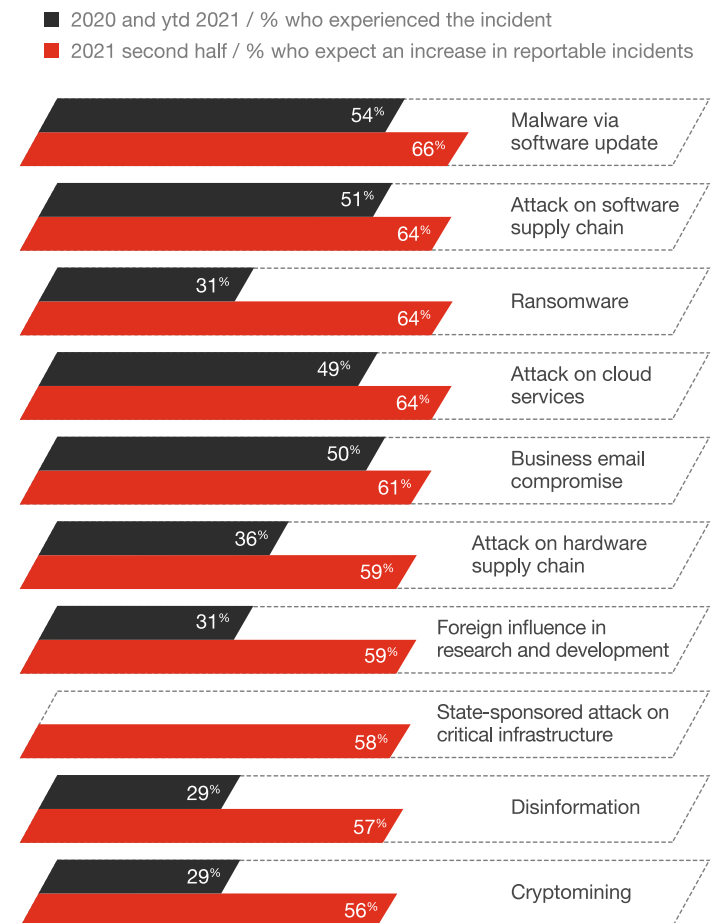
In late 2020, businesses became aware of an **espionage campaign** that successfully planted malware inside a software update months before activating the malware. In the second half of 2021, 64% of our survey respondents expect reportable **software supply chain attacks** to increase while 66% predict a rise in reportable malware-via-software-update incidents.

**Ransomware** is where CISOs and CIOs expect the biggest jump in reportable incidents — a prediction that has already been borne out within a month of our survey’s close.

**Ransomware** criminals are multiplying, attracting new cyber talent, innovating malware, and acting with impunity.

Ransomware demands — and payments — are on the rise. Attackers now commonly charge one sum to provide a digital key to unlock files and servers they’ve encrypted, and a separate ransom to not release any data they’ve stolen. In the US, Canada and Europe, the highest ransom payment doubled to **\$10 million** in 2020, a record quickly toppled in March 2021 with news of a \$40 million payment.

## More reportable cyber incidents expected in the second half of 2021



Q: Which of the following cyber and fraud incidents in 2020 and 2021-to-date has directly affected your organization?  
 Q: Please say how you expect a change in reportable incidents for these events in your organization in the second half of 2021 compared to the first half.  
 Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

## Threat watch: A spike is coming

Mobile and internet-of-things technologies along with the cloud are expected to be the fastest-growing threat vectors. Many CISOs and CIOs (29%) expect coordinated, organized nation-state attacks to surge this year. Cybercriminals edge out nation states as top threat actors among 31% of respondents.

Nation-state sponsored cyber attacks have long been with us, and they've made for gripping stories in books like *Countdown to Zero Day*, *The Cuckoo's Egg*, *Sandworm* and book-turned-to film *The Perfect Weapon*. But the scale and scope of these campaigns in 2020-2021 are commanding US business leaders' attention as never before.

Foreign adversaries attack not just our country's military and federal government agencies but our banks, hospitals, gas pipelines, power plants, food supply and major businesses. The number of organizations successfully hit speaks volumes about how much work remains to be done to respond to these threats.

## Takeaways

**Sharpen your threat modeling capabilities.** Effective threat modeling doesn't happen just once, and it shouldn't focus only on known methods of attack. Part art, part science, your threat modeling needs creativity and imagination. You and your teams should expect the unexpected and plan — and act — accordingly.

**Assess your cyber risks often.** Your business faces a unique and dynamic combination of threats and risks. To stay ahead, assess and prioritize early and often.

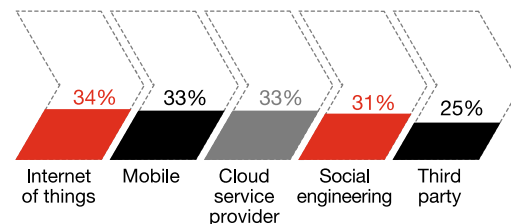
**Work on your resilience playbook with the business units, developers and risk managers.** In [survey](#) after [survey](#) we hear the same challenge: Teams that need to respond to incidents remain disconnected. Fragmented teams are no match for increasingly frequent and sophisticated attacks.

Methods favored by nation-state adversaries vary depending on their geopolitical and financial objectives. Traditional espionage campaigns are after information and communications. One nation-state adversary aims to enhance its power by degrading that of the US. A few nation-state adversaries steal intellectual property for commercialization or to advance their national industry champions. Others seek to access operations and wreak havoc in critical systems.

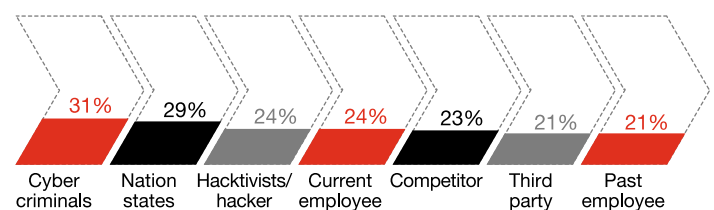
Sometimes the interests of cybercriminals intersect with nation states. Many ransomware criminal groups operate with at least tacit protection of their home government. It's all too common for US law enforcement authorities to identify, **sanction** and **indict** ransomware criminals in other countries to little effect. Home countries rarely cooperate. They may even work against holding the criminals responsible, instead co-opting them into the state. And they would sometimes issue competing extradition rules to get their citizens back home.

## Heightened threat activity expected in the second half of 2021

Significant increase in threats via these **vectors**



Significant increase in threats via these **actors**



Q: Among the following threat actors and threat vectors, please say how you expect each threat to change in the second half of 2021 compared to the first half?

Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

# Big bets: Cloud security, cloud security, cloud security



## Key finding: 81% of those who quantify cyber risk say it helped increase productivity and sharpen focus on strategic matters

We see it all the time: Companies convinced of the cloud's potential but overwhelmed by the complexities of properly securing it. Just 46% of CISOs and CIOs in our survey said they had mitigated the risks associated with accelerated cloud adoption.

Meanwhile, in PwC's inaugural US [Cloud Business Survey](#) of more than 500 C-Suite executives, 53% said they aren't getting substantial value from their cloud investments — a major concern given that they're spending millions or even billions of dollars.

The good news is that CISOs and CIOs — across all industries — are prioritizing cloud security for cyber investments over the next two years.

At the root of the problem of cloud security is a failure to recognize that cloud adoption is a major change. Identity and access management (IAM) that worked well to guard your contained, centralized on-premises system, for example, most likely won't protect the information and operations you place on the cloud because the two environments are so different.

What's more, businesses often use more than one cloud, and a combination of cloud types. Establishing processes, controls and technologies for these mixed environments becomes even more challenging. And how to keep a tight rein on access to companies within an ecosystem, each with its own cloud accounts?

"Fixing cloud security" is an encompassing endeavor. In addition to IAM, important components include third-party risk management (TPRM), real-time intelligence and zero trust. A well-thought-out, step-by-step approach to security can help [jump-start](#) stalled migration and/or modernization. It can even hasten the move so you finish faster than originally planned.

## Future of industry + security = successful transitions








Along with cloud security, each industry should customize its defenses, based on the risks it faces. The second and third cyber investment priorities of the survey respondents reflect that.

- The [future of manufacturing](#) relies on IoT, cloud and robotic process automation. Real-time threat intelligence and endpoint security investments can help address the growing attack surface and take advantage of data obtained in real-time connections.
- The future of healthcare will include [interoperability](#), which allows patients access to their data and healthcare professionals to share it for better results. Understandably, the sector's investments are centered on securing identities and access as well as security training of personnel.

- The **future of utilities** will mean greater connectedness to the customer, an expanding distributed network of renewable power and more power generation outside the utilities' traditional control. The **future of oil and gas** will likely see more digitization of wells, rigs and pipelines for greater efficiency and better predictive maintenance. Investments in better third-party risk management and business continuity/disaster recovery can help protect connections essential to reliable and continuous power supply.
- The **future of consumer markets** will certainly reflect current trends such as touchless checkout, omnichannel shopping and digital supply chains. Investments in identity and access management can secure massive data flows and real-time threat intelligence can help spot the potentially harmful intrusions among millions of transactions per second.
- The **future of financial services** is being shaped by AI and blockchain, so cyber investments are focused on software-defined perimeter approaches. Cybercrime and fraud via humans continues to evolve, and the industry is rightfully focused on ramping up security awareness and training.

Every new digital process and asset becomes a new potential vulnerability for cyber attack. Weaving security and privacy into your vision for the future increases the odds of success and helps guard against new risks.

## Big bets secure the future of industries

	1	2	3
 <b>Overall Total</b>	Cloud security	Security awareness training and cross training security operations	Endpoint security
 <b>Industrial manufacturing</b>	Cloud security	Real-time threat intelligence capabilities	Endpoint security
 <b>Financial services</b>	Cloud security	Security awareness training and cross training security operations	Software-defined perimeter
 <b>Tech, media, telecom</b>	Cloud security	Security awareness training and cross training security operations	Joint 3rd - Third-party risk management processes - Software-defined perimeter
 <b>Consumer markets</b>	Cloud security	Real-time threat intelligence capabilities	Enterprise identity and access management (e.g. Federation, SSO)
 <b>Health</b>	Cloud security	Security awareness training and cross training security operations	Enterprise identity and access management (e.g. Federation, SSO)
 <b>Energy, utilities, and mining</b>	Cloud security	Third-party risk management processes	Business continuity/ disaster recovery planning

Q: Given the nature and frequency of cyberattacks in 2020, which of the following are you prioritizing for future cyber investments to better prepare your organization in the next two years? Rank 3 options in order of priority. Base: Industrial manufacturing (74), Tech, media, telecom (61), Financial services (49), Consumer markets (49), Health (46), Energy, utilities, and mining (43). Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021.





## Evolving threats demand new security approaches

Judging from newer security measures they're implementing, organizations understand the need to plan ahead and get ahead.

**Cyber risk quantification** tops the list of measures they've taken over the past two years. And quantification has yielded results: **81% say it helps them increase productivity and focus on strategic matters.** Quantification, useful for prioritizing risks and for making the case for cyber-spending to the board, got especially high marks from companies in the energy, utilities and resources (EUR) and retail/consumer sectors.

A system for **cyber risk quantification** helps companies evaluate novel threats. For instance, a highly acquisitive company that quantifies cyber risks can evaluate deal opportunities faster and more systematically. A financial institution can assess threats and vulnerabilities daily or weekly to protect millions of transactions a day and stay alert to how well their controls are working.

**Autonomous threat response** ranked second on the list of most-implemented cyber strategies. This tool is particularly popular in the technology, media and telecom (TMT) and manufacturing sectors. Respondents reported almost immediate payoffs from 66% of those using autonomous threat response, but it has a downside: 49% said it takes significant time away from operations, likely due to false positives.

Autonomous response is a must for cyber today, however. Manual threat responses are no match for new threats, including AI-powered attacks. Rather than relying on traditional rule-based security controls, AI-driven autonomous threat response learns what's typical in the user's environment, then spots anomalies in email services, cloud applications, IoT devices and industrial systems. Stripped of noise in the data, AI-powered solutions can help security teams decide and act more quickly.

## Industries try their hand at new approaches

	1	2	3
Overall Total	Cyber risk quantification	Autonomous threat response	Differential privacy
Industrial manufacturing	Autonomous threat response	Cyber risk quantification	Confidential computing
Financial services	Differential privacy	Autonomous threat response	Confidential computing
Tech, media, telecom	Autonomous threat response	Differential privacy	Cyber risk quantification
Consumer markets	Cyber risk quantification	Differential privacy	Confidential computing
Health	Cyber risk quantification	Differential privacy	Autonomous threat response
Energy, utilities, and mining	Cyber risk quantification	Differential privacy	Evidence-based cyber controls

Q: Which of the following has your organization started to implement in the last two years? Rank all that apply in order of priority to your organization. Other approaches presented to respondents were confidential computing, Secure Access Service Edge, evidence-based cyber controls, zero trust, and security managed services.

Base: Industrial manufacturing (74), Tech, media, telecom (61), Financial services (49), Consumer markets (49), Health (46), Energy, utilities, and mining (43).

Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

**Differential privacy**, which lets companies collect and share personal information while protecting individuals' privacy, ranked third on the list. Most who use this approach report increased productivity and strategic focus (75%) as well as immediate payoffs (73%).

First developed in 2006, differential privacy is making a **significant transition** from theoretical approaches to practical applications in the government and private sector. Among the most active explorers are major **tech companies** as well as government agencies, including the **US Census Bureau** and the **National Science Foundation**.

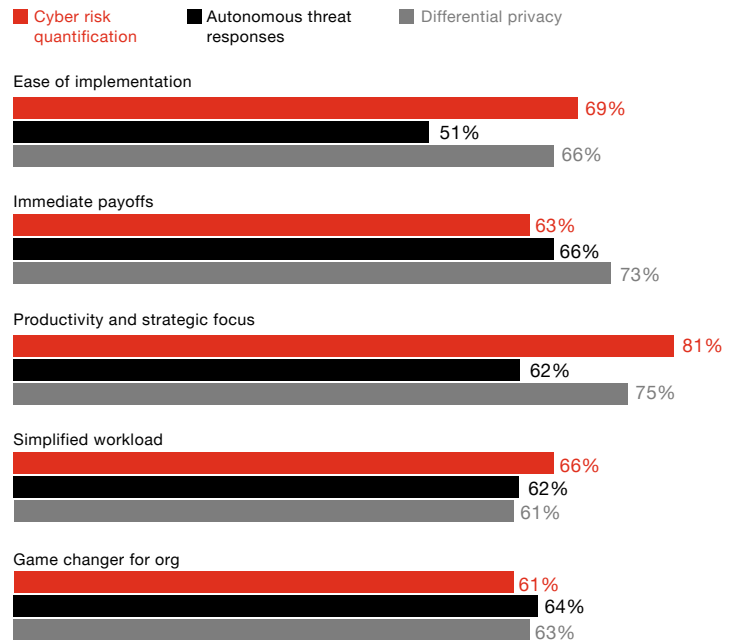
Coming in a close fourth — and ranking third in many sectors — is **confidential computing**, defined as encryption of data while it's in use (not just in transit or at rest). It complements differential privacy techniques in maximizing data use while protecting individual privacy.

## Takeaways

**Review how you budget.** Cyber is finally getting its due. Companies are investing more, and the C-suite is paying attention. But the expectations — and potential for disappointment — are high. Earn executives' confidence by modernizing your **budgeting process**, allocating budgets to help mitigate the most significant risks of the business.

**Work with other C-Suite executives to make your organization cyber-ready.** Step in as a partner to every executive who is driving a major transformation. Familiarize them with the benefits of security and privacy by design for smoother transitions and sustainable outcomes.

## Experience with implementation of new approaches



Q: For the new approach, how would you describe the process of implementation and impact on your organization's cybersecurity?  
 Base: Those who ranked 'cyber risk quantification' as top priority for implementation n=62; 'autonomous threat responses' n=74; 'differential privacy' n=56.  
 Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

# People in cyber: Going all-in on cyber starts from the top



## Key finding: Around half of the CISOs and CIOs in our survey have restructured their security teams and embedded them in product development and business teams

Successful CISOs now act as business enablers. They're no longer saying, "We can't do it," but rather are asking, "How can we do it?"

As a result, they may find themselves invited to join the conversation a lot sooner — ideally, on Day One as the enterprise begins planning its digitization and cloud migration/modernization moves.

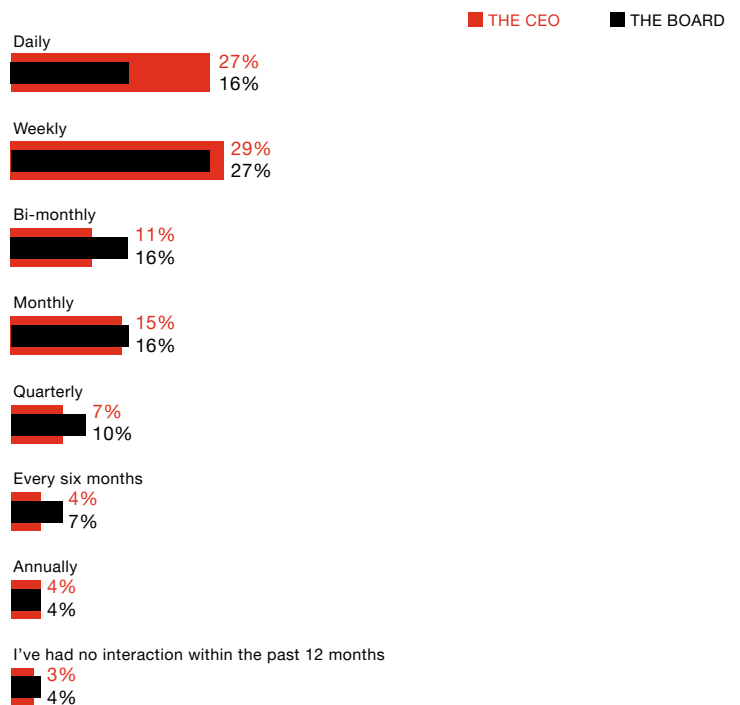
CISOs increasingly have the ear of the CEO and boards. Just two years ago, this was not the **norm**. More than half of the CISOs and CIOs we surveyed told us they interacted with the CEO at least weekly; 43% interacted with the board at least once a week, in the past 12 months.

At periodic meetings with the CEO and boards, CISOs should shift from focusing solely on immediate or technical challenges to discuss where the business is headed and the implications for the cyber program. Cyber-savvy senior execs know that when cybersecurity teams are playing catch-up to their organizations' ambitions, they're at a severe disadvantage. CISOs should help assure them that whatever the business' next venture, it can go forth boldly and securely — because the organization is cyber-ready.

These meetings and interactions are also a good opportunity to increase the cyber fluency — along with the digital savvy — of CEOs and boards.

Recent **MIT research** found that large enterprises whose executives understand emerging digital technologies' potential effects on business success outperformed comparable companies without digital savvy by more than 48%. And yet only 7% of the 1,984 large companies MIT studied have digitally savvy executive teams. This needs to change.

## CEOs and boards are getting cyber-savvy with their CISOs and CIOs



Q: In the last 12 months, how often did you interact with the CEO? With the board?  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

## The right place for security pros: Embedded in product development and in the business

Modern CISOs aren't satisfied with merely educating their C-suite and board. Half said they've restructured the security team, and another 44% plan to do so this year and next. TMT organizations lead the pack, with 62% having already restructured their teams.

One change they're making is in placing security team members on product development (49%) and business (48%) teams. We believe these moves put cybersecurity in its rightful place at the right tables at the right time, which is at the start of any strategy discussion and throughout implementation.

Putting security staff on product development and business teams can also help align cyber strategies to business strategies — **a major pivot** that has been going on for years. Another 45% said they are considering taking this step in 2021 and 2022.

TMT organizations are ahead in embedding security team members in business teams (56%), but lag in placing them on product development teams (41%). TMT (57%) and healthcare organizations (54%) are more likely to say they're considering doing so this year or next.

## Takeaways

**Look to the future.** In all your interactions — with the business, the board, the CEO, the product development teams — talk about what's coming. Put current fires and fixes in the context of longer-term goals and plans to help improve your cyber posture.

**Make it your business to demystify cyber.** Help those around you to become cyber-savvy. Speak the language of business. Find creative ways to explain complex cyber issues. These acts alone can help you make a greater difference and earn trust.

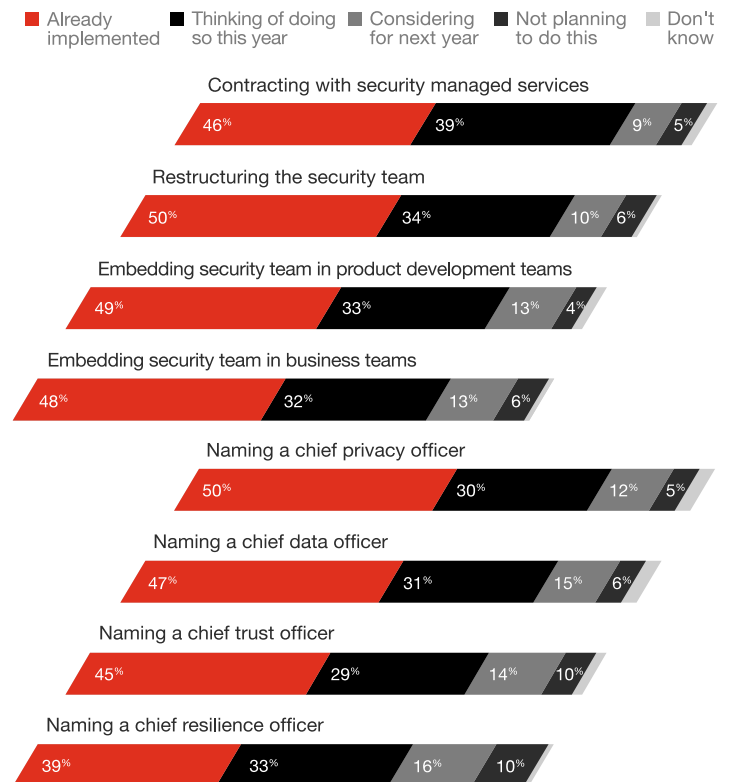
**Work with the CEO to understand competing values in building stakeholder trust.** CEOs face hard strategic decisions. How do we balance customer privacy with monetizing data? How do we manage third-party risks while enabling fast, agile work? Be a partner in creating solutions that balance conflicting choices.

Another thing organizations are doing to enhance security and privacy involves creating roles with specific responsibilities in domains adjacent to cybersecurity. Healthcare organizations are most likely to have appointed a chief privacy officer (61%) and over a quarter (28%) are considering naming a chief data officer next year — in a nod to the importance of data sharing and data-driven health outcomes in the industry.

Given increasing intrusions into supply chains and operations, industrial manufacturing organizations lag in appointing chief resilience officers (19%). That might soon change. Two-thirds (65%) are either “considering for next year” or “thinking of doing so this year.”

Forty-six percent of CISOs and CIOs have contracted with security managed services. We've seen how a **security managed services model** can help reduce personnel costs, scale up responses to sudden threats, and make the most of cybersecurity technologies without sending expenses spiralling. Financial services organizations tend to have large security teams, so they're least likely to have already contracted with security managed services (37%) but are most likely to be “thinking of doing so this year” (51%).

## A bigger focus on the human side of cybersecurity



Q: To what extent are you doing the following people initiatives?  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

# Despite heightened risks, hope flourishes



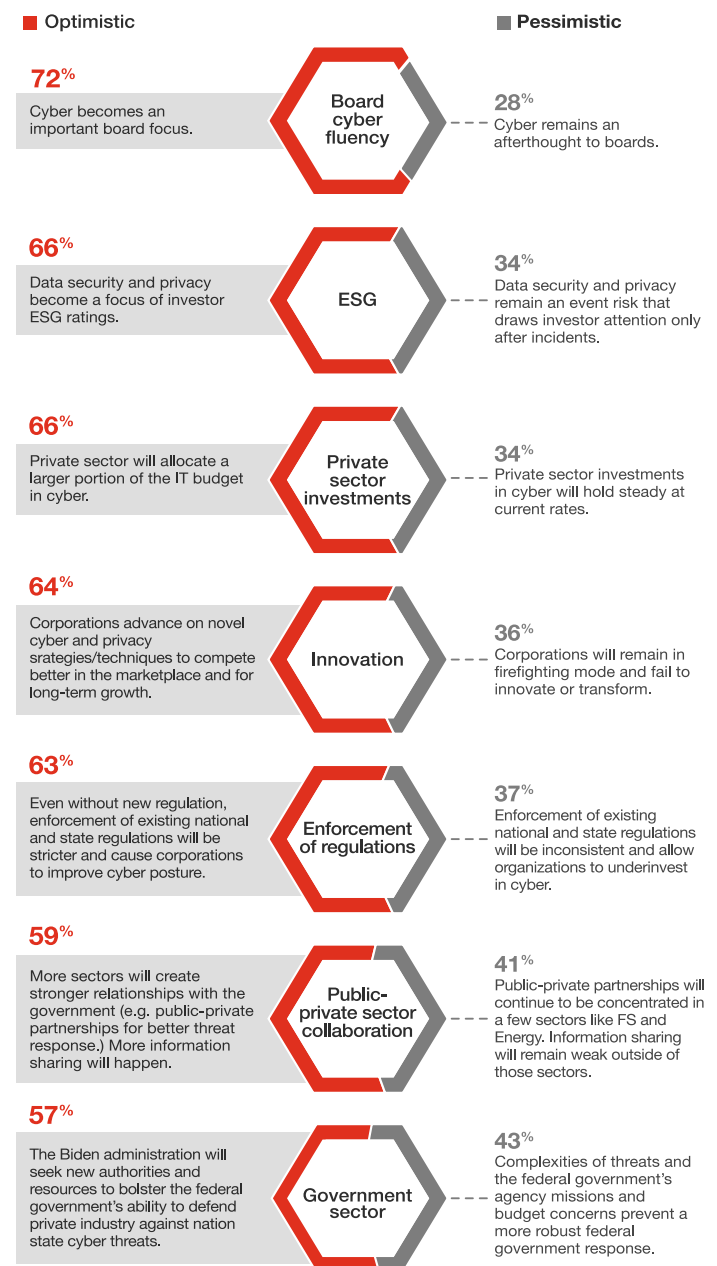
## Key finding: Investments, CEO and board attention, and forward-looking CISOs make for a cyber-ready organization

We identified the most prepared respondents — the top quartile that are likely to be (1) receiving significant investment in cybersecurity and privacy, (2) interacting more with CEOs and boards and (3) leading their security function ahead of the pace and scope of their organization’s digital transformation. These three conditions set them apart with a vastly different stance towards cybersecurity.

This “most prepared group” is more likely to:

- Have mitigated risks with remote work and accelerated cloud adoption.
- Prioritize cloud security investments over the next two years.
- Have named a chief privacy officer and chief data officer.
- Have restructured the security team.
- Have embedded its security team in product development teams.
- Participate in public-private collaboration opportunities.
- Participate in robust information sharing within a public-private collaboration group.

## Optimistic scenarios for 2021 resonate more with CISOs and CIOs



Q: Of the following outcomes, which do you think is more likely to happen in 2021?  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

There's general optimism among all respondents about their ability to get, and remain, cyber-ready. Given a choice between an optimistic outlook and a pessimistic view of the future, large majorities said optimism more closely represents their view. Thirteen percent were positive in all areas, and only 2% chose all the negative statements.

Most respondents view more attention from the board and investors as a positive. Nearly three-quarters (72%) expect cyber will become an important board focus as the year progresses. Two-thirds anticipate that data security and privacy will become a focus of investor ESG ratings.

Rising cyber budgets relative to IT budgets bolsters their positive outlook. Companies are innovating in cyber and privacy, not only solving immediate problems, 64% said. Worldwide spending on information security and risk management technology and services is forecast to grow **12.4% to reach \$150.4 billion** in 2021, according to the latest forecast from Gartner, Inc. Security and risk management spending grew 6.4% in 2020.\*

What do the respondents think of regulation? National and state regulatory enforcement will tighten and help improve cybersecurity, 63% agree. Only 37% think inconsistency in enforcement will allow poor cyber practices to continue.

\* Gartner Press Release, [Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed \\$150 Billion in 2021](#), May 17 2021.

Private-public collaboration didn't fare as well in our study. CISOs and CIOs were least optimistic about its improvement. They also indicated doubt in the federal government's ability to robustly defend private industry against nation-state cyber threats.

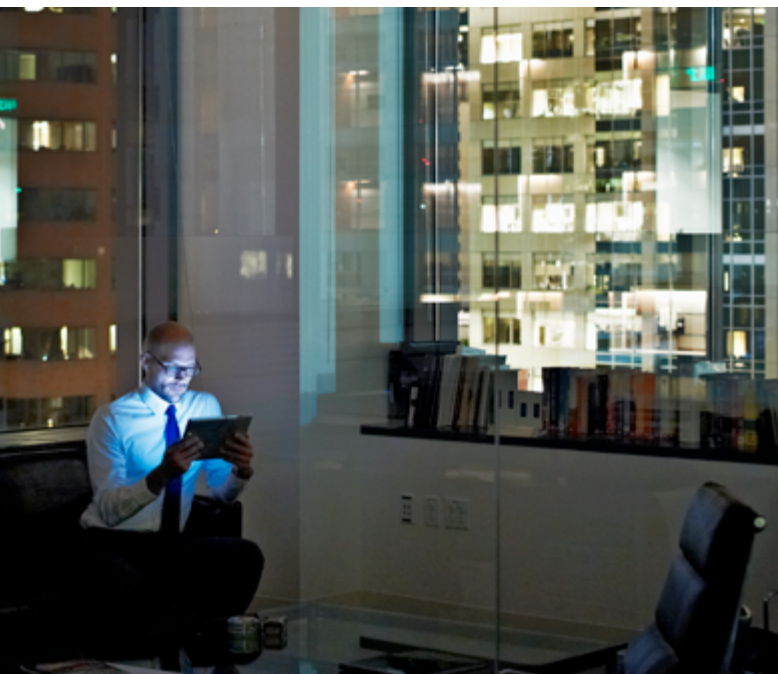
### Quality beats quantity for public-private cyber collaborations

Truly understanding and planning the response to a **major cyberespionage attack** is like putting together puzzle pieces — 90% of which are in the hands of private companies.

Most (84%) say they participate in public-private information-sharing — but how effective are their efforts when their collaborators are competitors or don't trust one another?

Companies don't generally do breach reporting well. Instead of volunteering details, they hide them away — hamstringing government efforts and creating a self-fulfilling prophecy. Absent a voluntary commitment to cooperate and collaborate, a federal data breach reporting law can force the issue. Companies, for their part, might want to know their disclosures are confidential, and to seek assurance that they won't face liability or be subject to enforcement action from the Federal Trade Commission or other regulators.

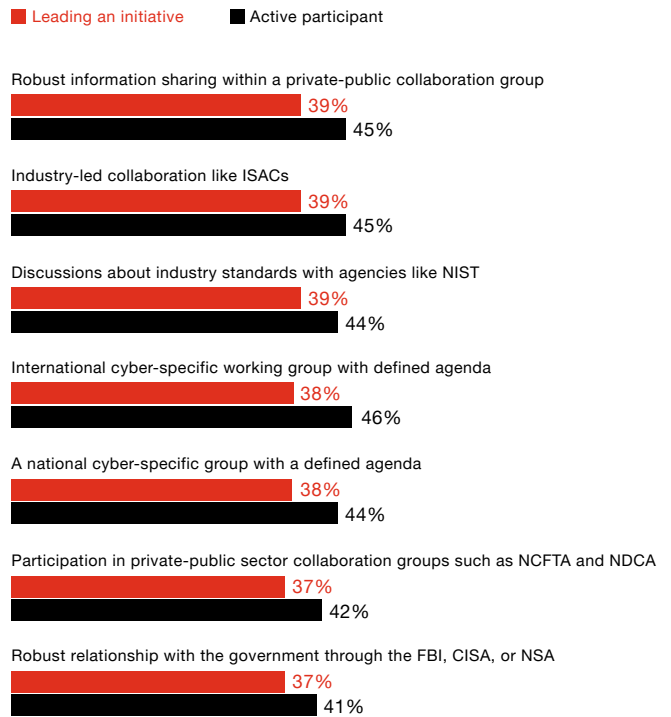
Without business participation, governments really can't defend against nation-state attacks. Private enterprise's reluctance to divulge breach information needs to change, especially given attackers' methods such as advanced persistent threats, which can cause widespread harm without detection. Effective defense demands a risk-based, strategic, carefully-crafted plan that changes as tactics do. To get it right, companies should put *all* their puzzle pieces on the table.



According to our survey, public-private collaboration is fairly commonplace. Nearly 40% say they lead a collaborative initiative, and another 45% are active participants. But companies should focus on the quality of those collaboration mechanisms.

The financial sector — guardian of our individual and collective wealth — provides a model for effective public-private collaboration under the **National Cyber-Forensics and Training Alliance (NCFTA)**. In these private-only meetings, no regulators are in the room. Companies share their information and aggregate the data. They use deconfliction, coordination and collaboration techniques to help solve common problems. And the NCFTA's reported outcomes are tangible, such as financial losses prevented.

### For collaboration that pays off, focus on quality and outcomes



Q: How engaged are you in private-public sector collaboration on cyber and privacy matters?  
Source: PwC, US Digital Trust Insights Snapshot Survey 2021, June 2021. Base: 322

## Takeaways

**Set priorities for better private-public collaboration using a risk-based approach.** Encourage industry associations and other private-sector groups to do the same. Persuade federal agencies to be outcome-oriented, setting security and resilience goals and using them to measure their partnerships' progress.

**Know what your company needs from the government.** Define how the government can better help your organization to defend itself, including the key cyber issues you face — and include your government relations people.

## About this survey

This US Digital Trust Insights Snapshot is a poll of 322 security and technology executives (CISOs, CIOs and similar titles) of US-based companies in April 2021. Sixty-nine percent of respondents are executives in large companies (\$1 billion and above in revenues); 9% are in companies with \$10 billion or more in revenues. Respondents come from a range of industries: Industrial manufacturing and automotive (23%), tech, media, telecom (19%), financial services (15%), consumer markets (15%), health (14%), and energy, utilities and mining (13%). [PwC Research](#), PwC's global Centre of Excellence for market research and insight, conducted this survey.

## Contact us

### Sean Joyce

Global and US  
Cybersecurity, Privacy &  
Forensics Leader, PwC US  
[sean.joyce@pwc.com](mailto:sean.joyce@pwc.com)  
202-684-5782

### Joseph Nocera

Cyber & Privacy Innovation  
Institute Leader, PwC US  
[joseph.nocera@pwc.com](mailto:joseph.nocera@pwc.com)  
312-925-6569

## [pwc.com/usdti](https://pwc.com/usdti)

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2021 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](https://www.pwc.com/structure) for further details. 920575-2021

