kyndryl

Survey findings

What IT decision makers say about the state of IT risk

IT risk has become a board-level discussion.

In a world where organizations rely on complex, geographically dispersed, hybrid IT systems, a network outage, malware attack, or other system disruption can devastate a brand's productivity, reputation, and bottom line.

So boards of directors are pressing their executive teams for details about readiness.

Given the high stakes, we sought to gauge perceptions of IT risk and what organizations do to enable cyber resilience. We surveyed a worldwide panel of IT decision makers and risk/compliance professionals to learn the adversity they've experienced, the IT risks that most concern them, and what their organizations do to anticipate, protect against, withstand, and recover from the risks.

The results compose this 2023 state of IT risk report.

Our findings confirm that organizations' IT systems are, indeed, being disrupted. We learned what most often gets in the way of efforts to mitigate disruptions. We also found—and were surprised by—high levels of confidence among IT leaders in their organizations' abilities to manage and recover from IT disruptions.

We invite you to consider the findings as a benchmark for your IT risk mitigation strategy. In addition to the survey findings, we offer nine steps for charting a path to cyber resilience. On The Progress Report, I also discussed the findings with Ricardo Morales, CISO of Banorte, one of Mexico's largest commercial banks.

How we got the data

We engaged a third-party research firm to conduct an online survey with 300 IT decision makers from large enterprises (i.e., 1,000+ employees). Responses were collected from March to April, 2023.

Respondent locations:

- → 65% North America
- → 19% United Kingdom
- → 16% India

Industry breakdown:

- → 18% Financial services
- → 17% Government
- → 17% Manufacturing
- → 14% Telecommunications
- → 14% Media
- → 20% Other

About the author

Kris Lovejoy, an internationally recognized leader in the field of cybersecurity and privacy, is Kyndryl's Global Practice Leader of Security and Resiliency.

Finding: Organizations rely on IT to operate critical business processes.

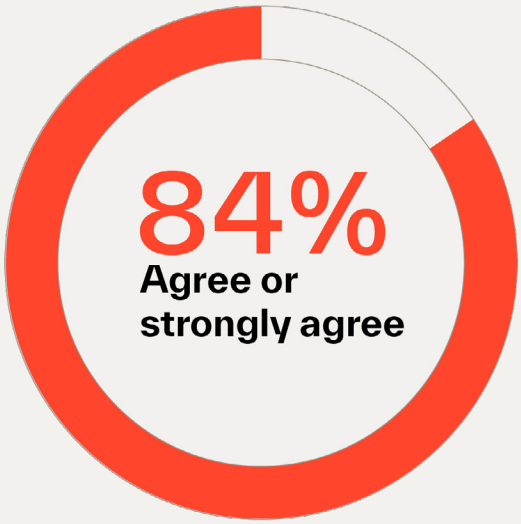
To anchor the discussion about IT risk, we asked respondents to suggest the extent to which their day-to-day business relies on IT.

84% agreed or strongly agreed that their organization relies heavily on IT assets to operate critical business processes.

The result is not surprising, given pervasive and daily commentary about digital transformation.

More surprising may be that the response was not even more emphatic.

Q: How much do you agree or disagree: "My organization relies heavily on IT assets to operate critical business processes."



Finding: Most organizations have experienced disruptions to their IT systems.

We not only validated the criticality of IT systems, but also that disruptions go with the territory. 92% of respondents said their organization has experienced an adverse event in the past two years that compromised or disrupted IT systems. Yes, to be in business is to assume IT risk.

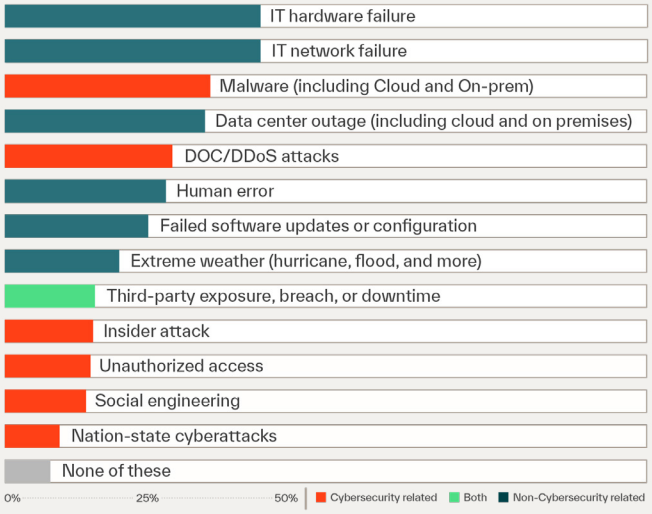
Most respondents said they've experienced three or four different types of disruption events. While cyberattacks tend to garner headlines, the findings reflect that a much broader aperture is warranted when discussing and addressing IT risk.

While 71% of respondents said they have experienced a cybersecurity-related event, 88% report they have experienced an adverse event that was non-cybersecurity related (these groupings are not either/or). In fact, three of the top five adverse events experienced were not related to cybersecurity:

- IT hardware failure
- IT network failure
- Datacenter outage

Notably, human error also remains a key source of disruption. (It's sixth among the 13 specific disruptions we asked about. It was consistently Top 3 for respondents from the financial service sector.)

Q: In the past 24 months, have any of the following adverse events compromised or disrupted your IT systems/data?



Finding: IT system disruptions have damaged brands, caused fines, and more.

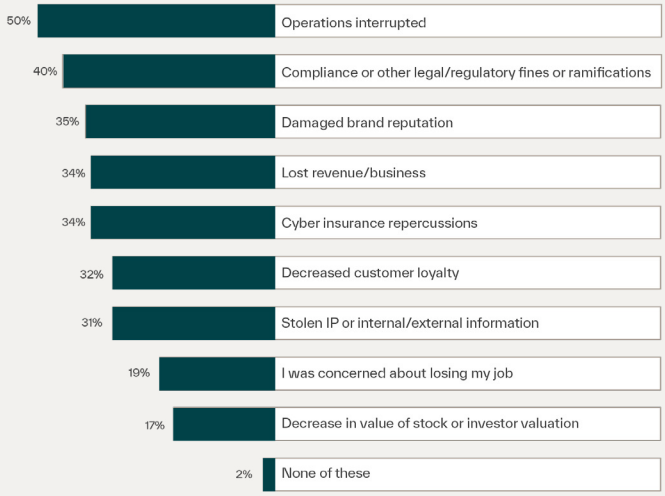
Building on the point of how critical IT is for day-to-day operations, respondents ranked operational disruptions as the most common impact experienced as a consequence of adverse IT events.

Compliance or other legal/regulatory fines or ramifications was the second most experienced impact. This was particularly true for respondents from financial services, government, and media industries.

Not only were operational disruptions and the compliance category most experienced, but respondents also ranked them the two most concerning categories of impact if IT assets were to become unavailable or compromised in the future. Denial-of-service disruptions and data leaks, for example, can carry steep fines.

35% of respondents said their organization's brand reputation was damaged as a consequence of IT disruptions. This rang particularly true among respondents from media organizations, 63% of whom noted such impact. The always-on news cycle and customers' activity on social media make any adverse event today more visible than ever before.

Q: Which, if any, of the following impacts did your organization experience from adverse events [in the past 24 months]?



Finding: There are consistent challenges to getting ahead of IT risks.

We anticipated the global IT skills shortage would rank high among mitigating factors, but it didn't quite top the list. A lack of ability to recover systems and data from an encrypted, clean backup featured most often as a top challenge respondents face in managing the impact of adverse events. We see this often among the organizations that ask about our services, as well. We encourage them to:

- → Invest in automating and orchestrating recovery processes
- → Assess and establish how best to mitigate human error in restoring from backups
- → Test incident response plans repeatedly and often

Rounding out respondents' top three challenges in mitigating risk were expanding IT footprints and abilities to stay up-to-date with emerging threats. Lack of skilled IT staff ranked fourth.

Q: What are the top three challenges you face in managing the impact of adverse events?

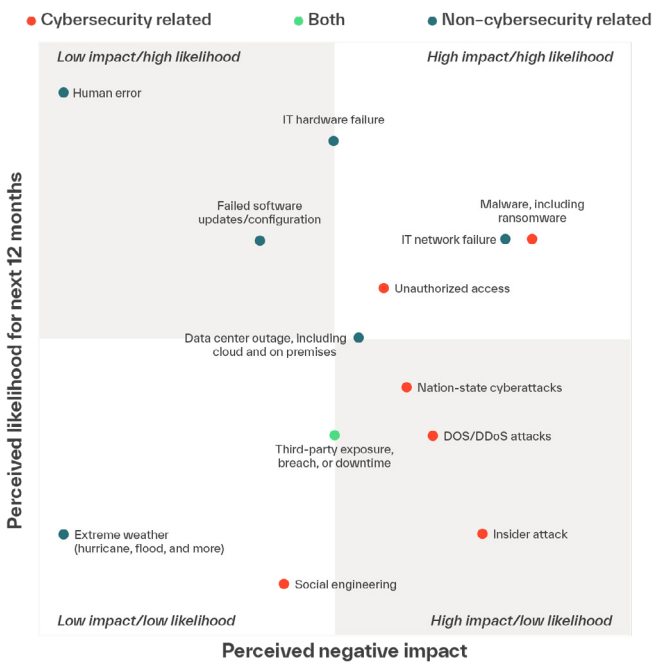
Finding: Looking ahead 12 months, malware events are perceived as the highest IT risk in terms of of likelihood and most negative impact.

We asked respondents to tell us the adverse events they most anticipate in the next 12 months, as well as the level of impact on their organizations, were the events to occur.

Human error was seen as most likely to occur, but the expected impact is lower than most other events. Malware, on the other hand, stood out as the IT risk most anticipated and most threatening.

Given the rise in malware, particularly ransomware, the result is not surprising. In view of the aforementioned challenges in recovering data from encrypted, clean backups, it also suggests reason for heightened attention. Whether or not your organization is challenged with backups, a complicating factor is that ransomware attackers increasingly target backups. In those scenarios—when backups have been compromised—organizations not only can't restore systems, but they also can't check for malware. Risk and potential impacts therefore skyrocket.

Another highly anticipated and potentially highly impactful risk—unauthorized access—also would be perceived to have significant negative consequences. Zero trust principles will play a continually important role to manage unauthorized access. The principles call for organizations to identify their high-value assets, determine privileged access, and leverage technologies, such as multi-factor authentication, to validate.

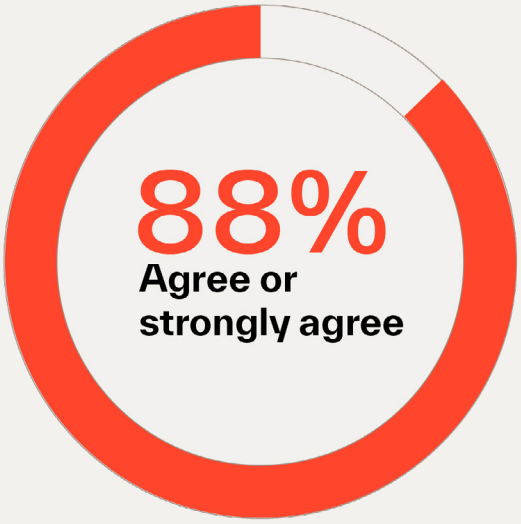


Finding: Despite perceived risks, IT decision makers remain confident.

Earlier in this report, we mention surprise at IT decision makers' confidence, given global events and noted challenges. In fact, 88% of respondents agreed that their organization is well prepared to manage and recover from any adverse conditions, attacks, or compromises that disrupts their organization's IT assets.

Asked to compare themselves to peers, 65% rate their organization's preparation for adverse events ahead of other organizations. Only 8% rate themselves at least somewhat behind others. The high level of confidence particularly catches our attention, given the aforementioned 92% who also confirmed their organizations have experienced adverse events. The duality is at least curious, if not reason to question if such confidence is justified.

Q: How much do you agree or disagree: My organization is well-prepared to manage and recover from any adverse conditions, attacks, or compromises that disrupt my organization's IT assets.



9 steps for IT leaders to chart a path toward cyber resilience

We undertook this study to benchmark how IT decision makers perceive the current state of IT risk, and what actions—across four pillars of cyber resilience—their organization takes to mitigate those risks.

- → **Anticipate:** Actions to assess and understand IT risk posture to better mitigate potential threats and navigate potential regulations.
- → **Protect:** Actions to harden defenses of IT assets to ensure they remain protected from adverse events.
- → **Withstand:** Actions to handle disruptions and reduce the impact.
- → **Recover:** Actions to help mitigate the impact after any disruption and quickly recover critical IT environments.

Respondents consistently rated their organizations as performing well—hence the high confidence scores. On average, across all activities, 75% of respondents considered their performance very good to excellent. A nuance we found was respondents who reported strong executive buy-in for security investments were more likely to give themselves top marks for cyber resilience-related activities.

To help you garner that buy-in, as well, we offer nine foundational steps to chart a path toward cyber resilience.

1 **Engage the business from the start.**

IT organizations too often operate in a silo, separate from other parts of the business. The surest path for a cyber resilience strategy to succeed is to break the silo. Invite voices from outside IT to the table and anchor conversations about cyber resilience in the organization mission. Make it part of the organizational culture.

2 **Align on risk tolerance.**

A level of risk tolerance often is dictated by industry. For example, the tolerance level for a highly regulated financial institution likely would be very low. Whatever the level, define the risk tolerance for your organization, and communicate it with your teams.

3 **Establish your minimum viable company.**

A minimum viable company represents the pieces of the organization that are critical to sustain operations and move business objectives. Your cyber resilience strategy not only should identify the critical pieces, but also the impact tolerances for how quickly the underlying data for these systems need to be back online.

4 **Take inventory.**

As demonstrated in the survey findings, many organizations are challenged by an ever-expanding IT footprint. Identify and map the IT assets that are critical to your minimum viable company. These assets will be top priority to protect, and worst-case, recover following an adverse event.

5 **Move to a zero trust framework.**

We recommend the deny-by-default standard to ensure that only those who need to access systems can get it, while those who don't need to, can't.

6 **Establish a crisis management plan.**

Sometimes adverse events are unavoidable. (Case in point: human error as the most anticipated cause of disruptions.) Defining roles and responsibilities across teams, establishing a communication process, documenting processes, and improving transparency often helps reduce the impact of an adverse event.

7 **Practice for a disruption.**

Plans are too often created but then shelved and rarely practiced. When an adverse event occurs, an untested plan leads to confusion, slow response time, and the impact becomes more severe.

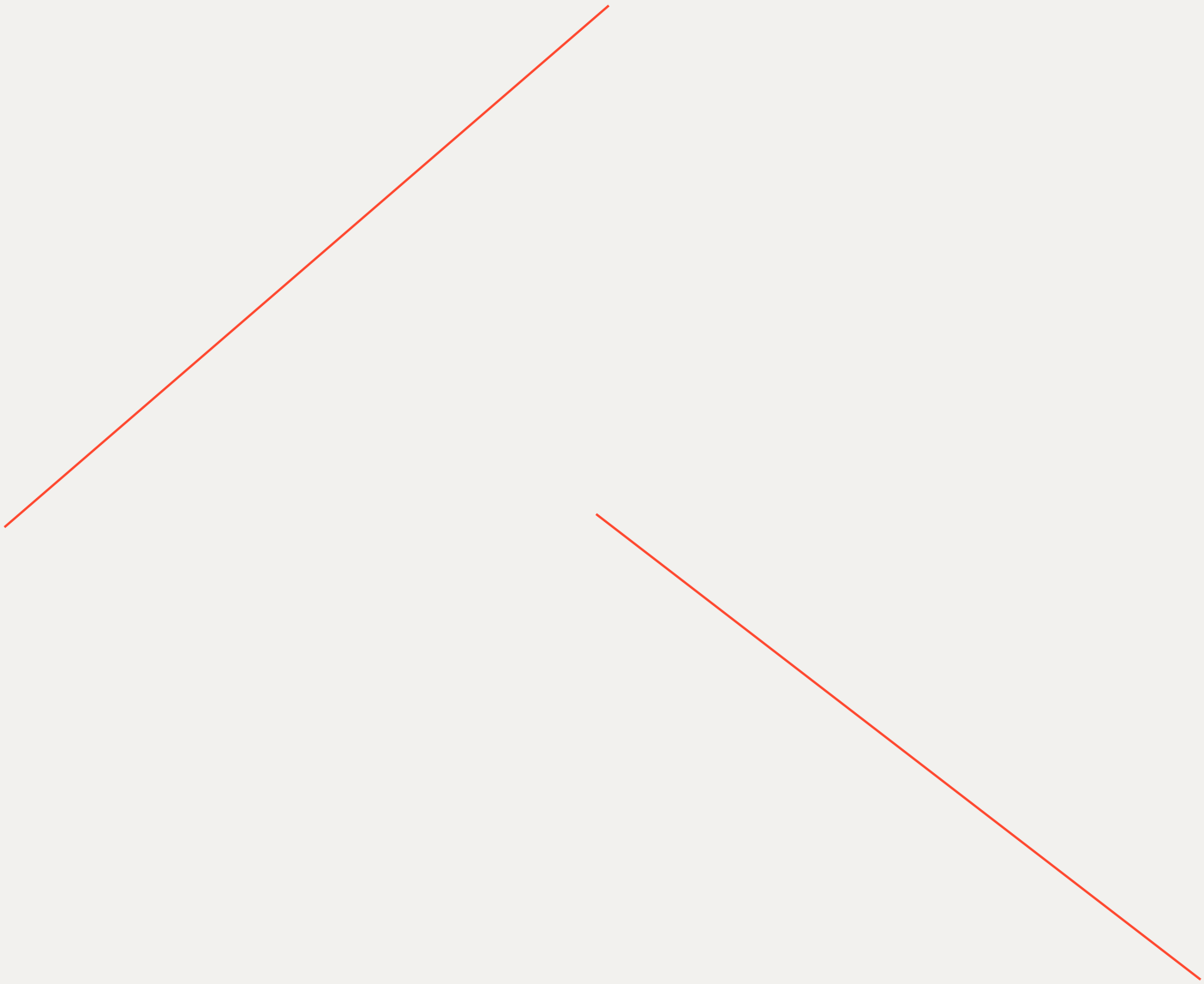
8 **Modernize your cyber resilience strategy—continuously.**

Organizations are living entities. Business pursuits shift, IT estates becomes more complex, and external forces (e.g., regulations) can require changes. To ensure your cyber resilience strategy is effective, the aforementioned steps must be part of a continual discussion.

9 **Build awareness at the board level.**

We end this survey report where we began—calling attention to the fact that cyber resilience has become a topic of board-level discussions, worldwide.

Keeping your board informed about IT risks and plans to mitigate those risks can help drive top-down organizational alignment and provide air cover for changes necessary to ensure cyber-enabled systems can remain operational during adverse events.



kyndryl