IT Trends Report 2021

Building a Secure Future

July 2021

solarwinds

Contents

Overview 3

Rising to the Challenge 4

Key Findings: State of Risk 5

Key Findings: Risk Mitigation 9

Key Findings: Tech Investments 11

Key Findings: Looking Ahead 15

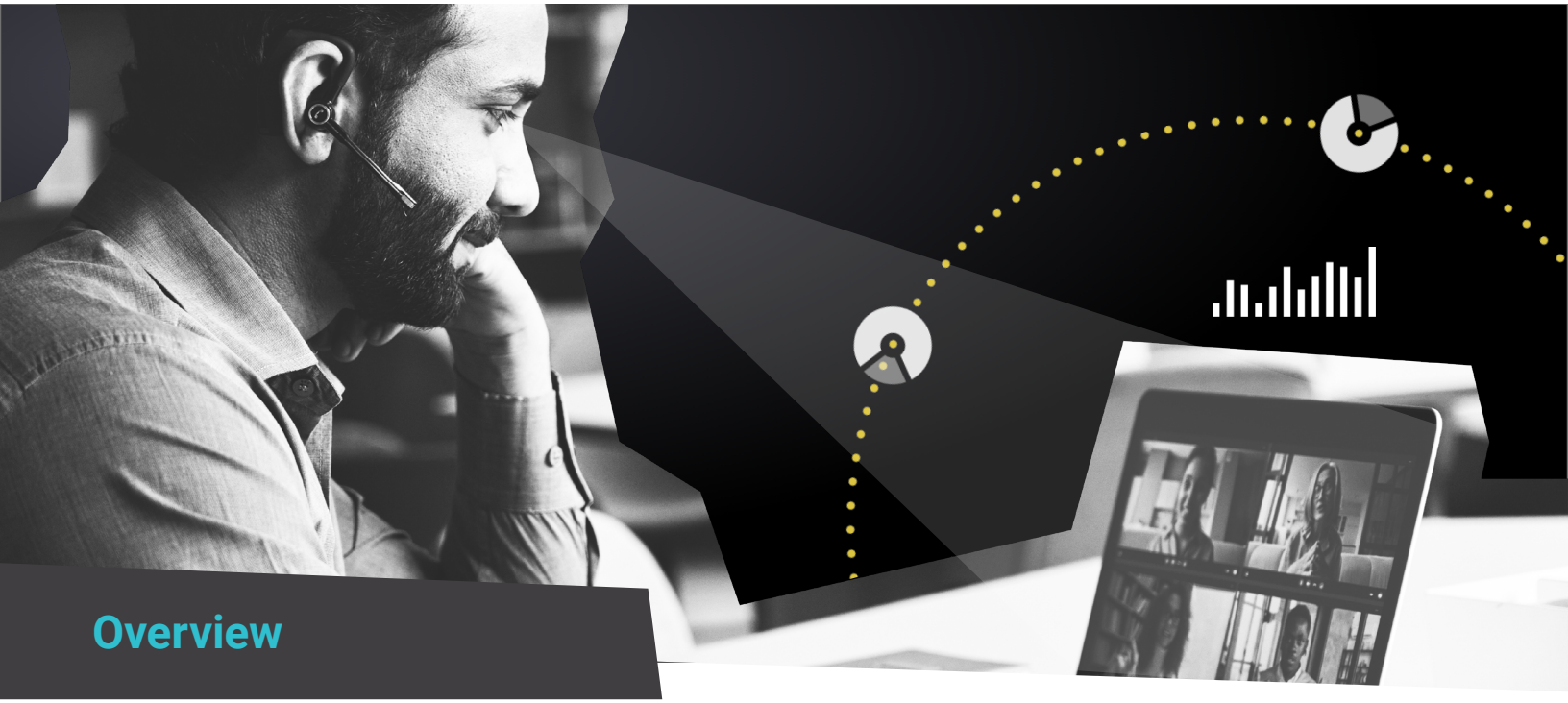
Recommendations 17

Study Overview: Respondent Demographics 21

Study Overview: In-House vs. Outsourced Technology Environments 22

Study Overview: Risk Exposure 23

Study Overview: Managing/Mitigating Risk 30



Overview

In 2020, the global pandemic transformed the way we work, rapidly matured a distributed global workforce, and accelerated digital transformation efforts.

Public cloud services consumption increased sharply. Organizations pivoted seemingly overnight to implement technologies to ensure the lights stayed on and employees were empowered to be successful working from home.

Against this backdrop, nearly every industry was confronted with the rise of high-level cybersecurity breaches, highlighting the potential risk of incomplete security policies and procedures. A year of unprecedented upheaval has ultimately served as a critical catalyst for a broader exploration of organizations' exposure to enterprise IT risk of all kinds—including risk introduced by the implications of remote, distributed work—and the degree to which organizations are prepared to manage, mitigate, and prevent risk in the future.

The findings are based on a survey fielded March/April 2021, yielding responses from 967 technology practitioners, managers and directors from public- and private-sector small, mid-size, and enterprise organizations worldwide.

Rising to the Challenge

The SolarWinds IT Trends Report 2021: Building a Secure Future seeks to facilitate a more transparent conversation by analyzing the state of enterprise IT risk within the industry today.

Specifically, it explores how tech pros perceive their organizations' risk management and mitigation readiness while providing guidance on workplace strategy, toolsets, preparedness, and leadership for companies as they work to construct an organization built to withstand risk.

The findings of the SolarWinds IT Trends Report 2021 uncover a reality in which exposure to enterprise IT risk is common across organizations—but perceptions of apathy and complacency surrounding risk preparedness are high as businesses exit a year of pandemic-driven "crisis mode." Tech pros have outlined key areas of technology investment and upskilling that prioritize cloud computing, network infrastructure solutions, and security/compliance—demonstrating an inherent awareness that falling behind is potentially the greatest risk of all. This year's study reveals the immense opportunity ahead for tech pros and IT leadership to align and collaborate on priorities and policies to best position not only individual organizations but the industry at large to succeed in a future built for risk.

*

Perceptions of apathy and complacency surrounding risk preparedness are high as businesses exit a year of pandemic-driven "crisis mode."

Key Findings

State of Risk

Security threats associated with external breaches and the internal impact of COVID-19 IT policies emerged as the leading macro trends influencing enterprise IT risk today.

The level of perceived risk exposure differs by size of organization. A sense of high-risk or extremely high-risk exposure is perceived more acutely by tech pros at mid-size organizations (27%) as compared to their enterprise (26%) and small business (18%) counterparts.

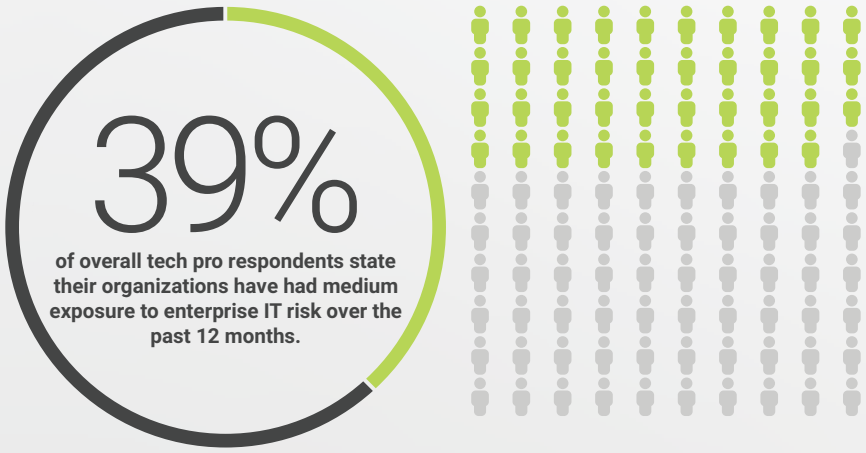


Figure 1: Exposure to enterprise IT risk over the past 12 months

Security breaches are perceived to be the biggest external factor influencing an organization's risk exposure, with 46% of respondents citing external security threats—like cyberattacks—as the top macro trend influencing their organizations' risk exposure.

Figure 2: Macro trends influencing risk exposure

However, COVID-19 also had a critical impact on organizations' risk exposure, with tech pros flagging these top associated risk-inducing factors:

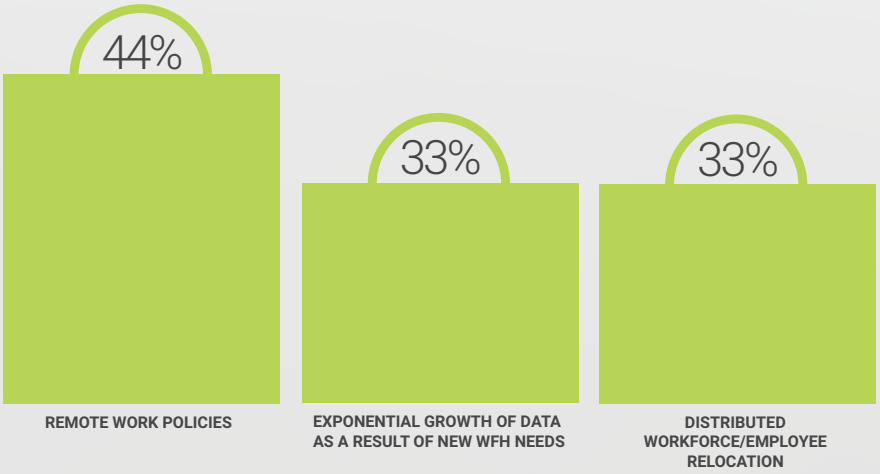


Figure 3: Top COVID-19 related risk-inducing factors

Likewise, 35% of respondents said the accelerated shift to remote working was the number-one aspect of current IT environments considered to increase an organization's risk exposure, followed closely by lack of skilled IT staff due to cost-cutting, consolidation, and/or outdated skill sets in employee base (34%).

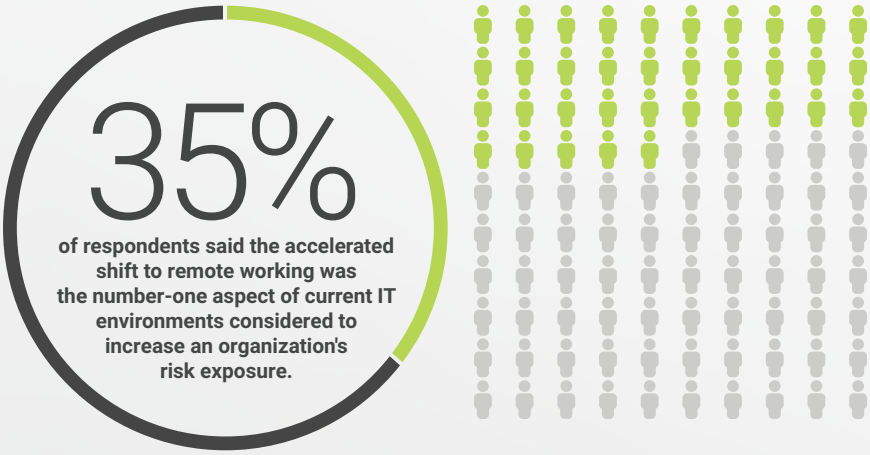


Figure 4: Respondents stating that accelerated shift to remote working was number-one aspect of current IT environments considered to increase an organization's risk exposure

50% of respondents say security and compliance ranked in the top three technologies most critical to managing/mitigating risk within their organizations, followed by network infrastructure (38%) and automation (25%).

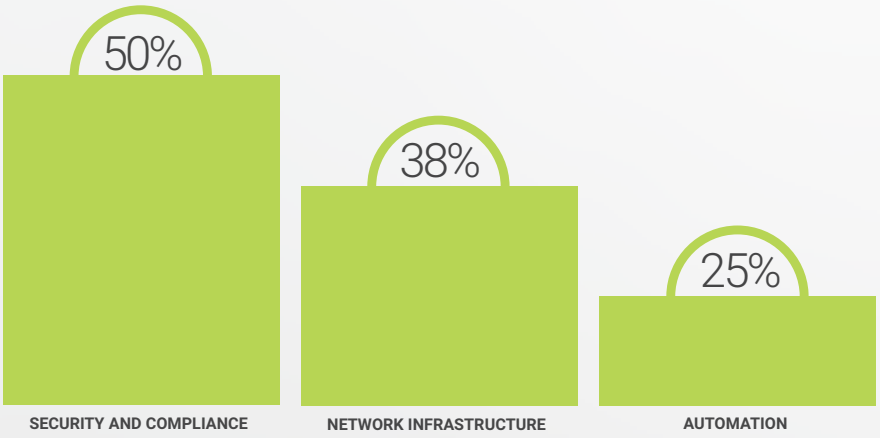


Figure 5: Technologies most critical to managing/mitigating risk within organizations

Although external security threats are the primary risk factor, internal vulnerabilities as a result of remote/distributed environments cannot be overlooked in today's work landscape.

Key Findings

Risk Mitigation

Respondents are confident in their risk management and mitigation preparedness strategies although enterprise IT risk exists within their organizations.

81% of respondents "agree" or "strongly agree" their IT organizations are prepared to manage, mitigate, and resolve risk factor-related issues due to the policies and/or procedures they already have in place.

Figure 6: Tech pros' confidence in their organizations' preparedness today

This finding is echoed by organizations' careful approach to technology adoption and implementations in response to shifting demands of COVID-19 distributed work environments: despite the accelerated timeline, over half (51%) of respondents said standard or heightened risk management protocols were followed.

Figure 7: Amount of the time protocols were followed in response to shifting demands caused by COVID-19

That said, as detailed in a recent McKinsey report, tech pros and their IT organizations must be careful to avoid complacency in today's ever-evolving risk landscape and be sure to refresh and strengthen their approach to risk management for the future.

Key Findings

Tech Investments

While tech pros prioritize investments in security and compliance, network infrastructure, and cloud computing as core technologies to help manage risk, implementation is hampered by dwindling resources and access to personnel training.

80% of respondents "agreed" or "strongly agreed" technology is the best way for organizations to manage, mitigate, and resolve issues related to risk.

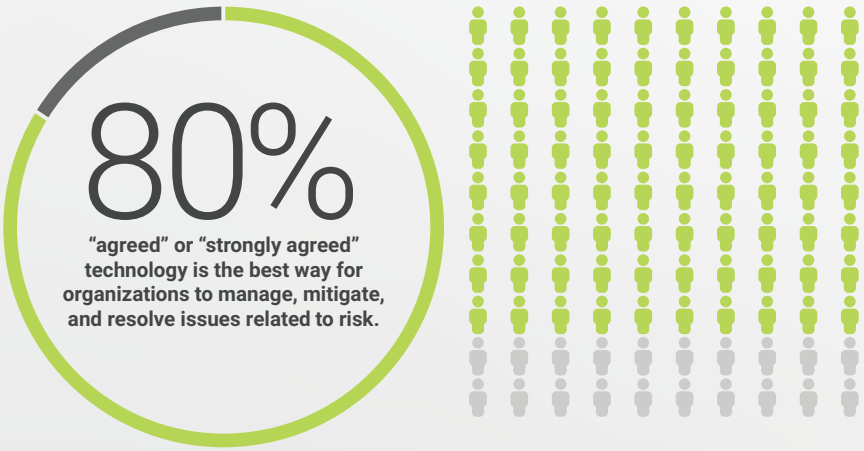


Figure 8: The best way to manage, mitigate, and resolve issues related to risk

IT teams prioritized investment in security and compliance (36%), network infrastructure (33%), and cloud computing (27%) to accommodate the unprecedented demands of COVID-19 and the shift to remote work.

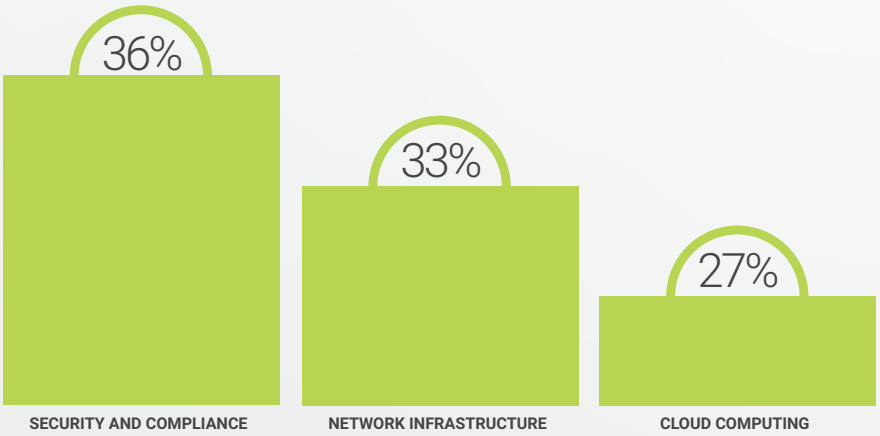


Figure 9: Priority tech investments to accommodate the unprecedented demands of COVID-19 and the shift to remote work

However, despite understanding technology can play a critical role in enterprise IT risk management, barriers to its adoption and implementation exist. The top three challenges to utilizing technology to mitigate and/or manage risk within organizations reported by respondents are:

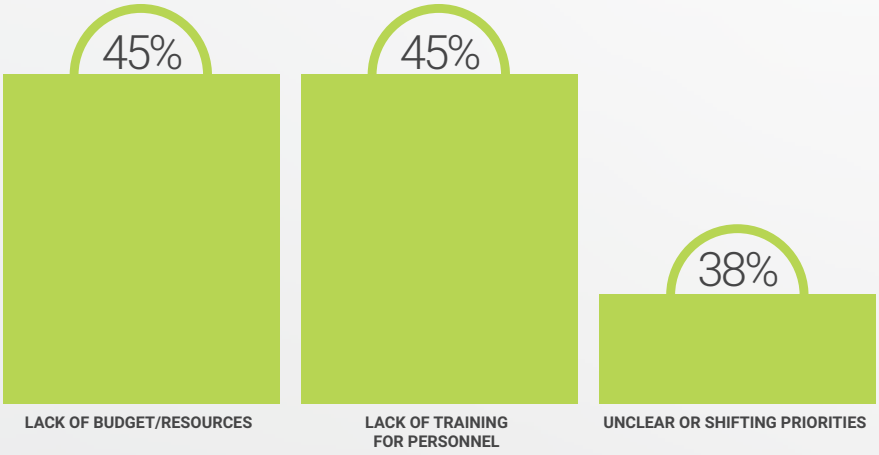


Figure 10: Top three challenges to utilizing technology to mitigate and/or manage risk within organizations

A larger percent of tech pros from mid-size companies (37%) identified poor management lack of direction within their top three challenges as compared to small businesses (28%) and enterprise-sized organizations (29%).

Implementation is further hampered by 37% of respondents admitting that while some of their monitoring/management tools are integrated to enhance visibility across their IT environment(s)—whether on-premises, cloud-based, or hybrid—other tools are still siloed.

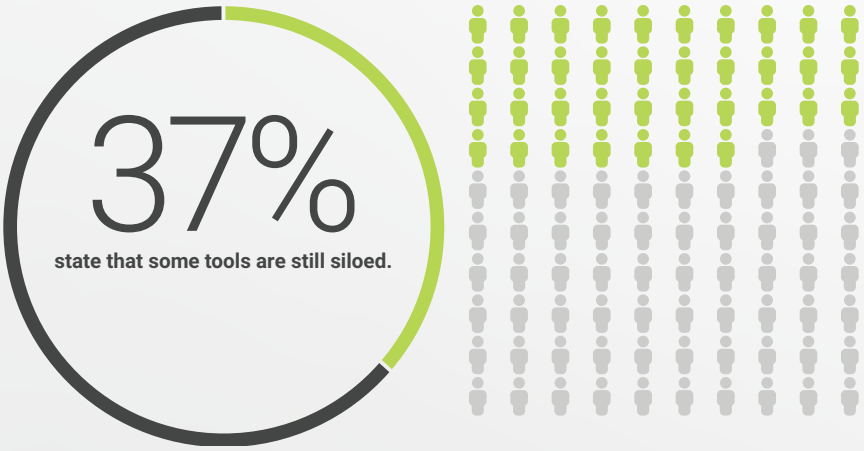


Figure 11: Siloed tools are a barrier to implementation

Tech pros are overcoming these barriers by:

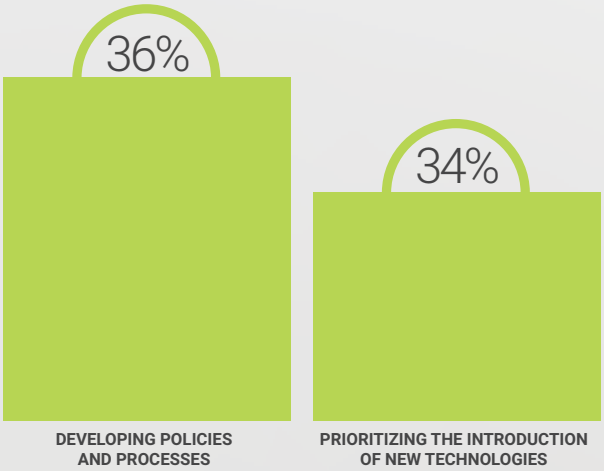


Figure 12: How tech pros are overcoming challenges

Key Findings

Looking Ahead

Tech pros are capitalizing on an opportunity to foster greater alignment and collaboration with senior leaders who will best position their organizations to manage and mitigate risks in the future.

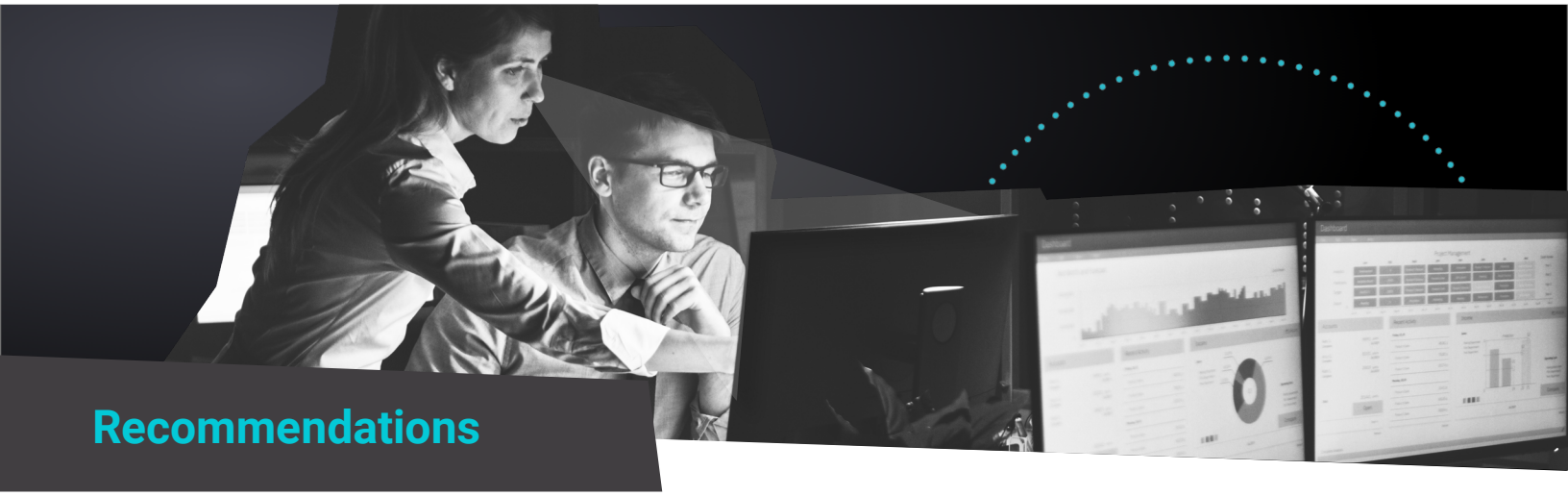
59% of respondents are confident or extremely confident their IT organizations will continue to invest in risk management/mitigation technologies over the next three years.

Figure 13: Tech pros' confidence in continued investment in risk management/ mitigation technologies

58% perceive their organizations' senior leaders or decision-makers to have a heightened awareness of risk exposure, believing it's not "if" but "when" they will be impacted by a risk factor. But while 31% believe their organization is prepared to mitigate and manage risk, 27% said their senior leaders have difficulty convincing other leaders of this reality, ultimately limiting resources to address risk.

Figure 14: Senior buy-in and alignment when it comes to risk exposure, mitigation, and resources

This reinforces how one-third of respondents state their IT organizations are improving alignment between IT business goals and corporate leadership in response to other tech adoption barriers, like a lack of available IT management tools and decreased staff size.



Recommendations

Beware Security Apathy:

After a year of IT on the frontlines of COVID-19-driven digital transformations, tech pros and organizations are on the cusp of exiting "crisis mode." Although the shift to remote work was cited as a leading factor in heightened risk exposure for businesses over the past year, many tech pros have reached the point where they're confident with WFH/remote work policies—but this moment in time represents a critical inflection point for organizations, as hubris can sink into widespread security apathy and complacency.

As a tech pro, it can be easy to think about security as an add-on or expect ownership to sit with a discrete security team. This is especially true of tech pros who have worked at a company for several years and resist change or have outsized complacency. Unfortunately, those perceptions no longer reflect the world we live in (certainly not the world we're returning to as we emerge from the pandemic). Apathy and complacency are surefire ways to reduce exposure to new technologies, better ways of working, or worse, a lack of awareness to other areas of risk within an organization that aren't always obvious.

Security 101 demands security be every tech pro's responsibility: most of the risk is produced by us humans and our behavior, and we need to think of ourselves as part of the extended security team. It's important for IT teams to examine current processes from the outside in and deploy solutions to provide complete visibility into all systems to identify areas of risk and opportunity. Even small changes like faster upgrades and patches, the use of password managers, and MFA solutions can strengthen an organization's overall security posture. That said, tech pros must apply a certain level of rigor in evaluating those solutions—it's common to be bombarded with marketing messages that can distract from a tool's true functionality or capabilities. Remember to trust but verify: are all statements made by in a solution's marketing true in all environments? IT teams should build sufficient evaluation frameworks that will help separate fact from fiction when it comes to a solution's ability to deliver on the capabilities as promised. Ultimately, tech pros should always be assessing their risk management, mitigation, and protocols to avoid falling into complacency and being "blind" to risk.

* Security 101 demands security be every tech pro's responsibility.

The Business of IT:

It's promising that respondents are confident their organizations will continue to invest in risk management/mitigation technologies over the next three years. However, investment takes time and needs guidance. Many respondents also indicated senior leaders believe it's "when" not "if" the business will experience the impact of risk exposure, but this doesn't mean the right actions and investments are being implemented. It's the IT team's job to know exactly where risk management investments should go beyond generic recommendations. Tech pros must present proof points and justifications to gather senior buy-in, so policies and technologies can be implemented effectively and at scale. Add facts and figures wherever possible to reinforce the recommendation. Pinpoint the impact on customer trust should the game of risk not go in the organization's favor. Likewise, bring consequences to life for decision-makers who aren't in the IT trenches: how long would business be down if there was an issue? How does the financial impact of an incident compare to how much it would cost to invest in a better risk strategy? Strategic conversations between the IT teams and senior business leaders are imperative and making a strong case for these investments is equally critical after a year of cuts and restrictions for many companies—everyone is fighting for a slice of the budget.

* **Tech pros must present proof points and justifications to gather senior buy-in, so policies and technologies can be implemented effectively and at scale.**

Normalize Risk Aversion:

This year's SolarWinds IT Trends Report found tech pros around the world said their organizations experienced medium exposure to enterprise IT risk over the past year. Although these respondents simultaneously felt their existing risk mitigation and management policies/procedures are sufficient, it's absolutely critical for organizations and tech pros to adopt a mentality in which even "medium" risk exposure is unacceptable. The consequences are hugely variable by business size—yet the perception of exposure and preparedness are closely aligned. As an industry, we need to shift our threshold for interpreting risk exposure. The impact of COVID-19 has amplified the hybrid IT reality, fragmented policy, configuration, and visibility, and threat surfaces reach from on-premises data centers to the public cloud, the IoT, and beyond. Tech pros and the IT community at large must normalize a sense of risk aversion—that is, to move from simply accepting the current exposure to a mindset in which any level of risk exposure is unacceptable. That means beginning to evaluate and implement the principles of a secure enterprise, starting first and foremost with the understanding that security compromises will happen as cyber hackers deploy more sophisticated attacks. Tech pros should also implement detection, monitoring, alerts, and response along the kill chain, and engage in redteam/tabletop exercises to measure effectiveness. These principles will help organizations more fully prepare to defend against any level of risk exposure as the threat landscape expands. Ultimately, tech pros and organizations must collaborate to ensure policies and risk procedures are continually updated and enhanced in lockstep with the evolving threat landscape to minimize risk exposure.

*

It's absolutely critical for organizations and tech pros to adopt a mentality in which even "medium" risk exposure is unacceptable.

Prioritize Development:

As in previous editions of the SolarWinds IT Trends Report, tech skills development has emerged as a key focus area for tech pros. Also similar to past findings are the barriers to prioritizing those needs, ranging from lack of training for personnel, lack of resources to facilitate upskilling, and finding time for skills development. These annual findings are often at odds with the reality that tech pros are required to complete numerous certifications by their organizations each year—but do these certifications support larger strategies and initiatives? Tech pros should feel empowered to push back on the business (when appropriate) and ask how certain certifications or training initiatives map back to the organization's priorities. In the same vein, this underscores the importance of IT teams learning the "language of business," so tech pros can communicate what training can bring value to the organization and allow IT teams and business leaders to prioritize accordingly.

Investment in upskilling and training is good, creating time for it is great, but truly prioritizing skills development is even better—and will have the most significant impact to an organization's bottom line.

* Investment in upskilling and training is good, creating time for it is great, but truly prioritizing skills development is even better.

Study Overview: Respondent Demographics

These findings are based on an online survey fielded in March/April 2021, yielding responses from 967 technology practitioners, managers, and directors from public- and private-sector small, mid-size, and enterprise organizations worldwide.

Fig 1 - Organization Size (number of employees)

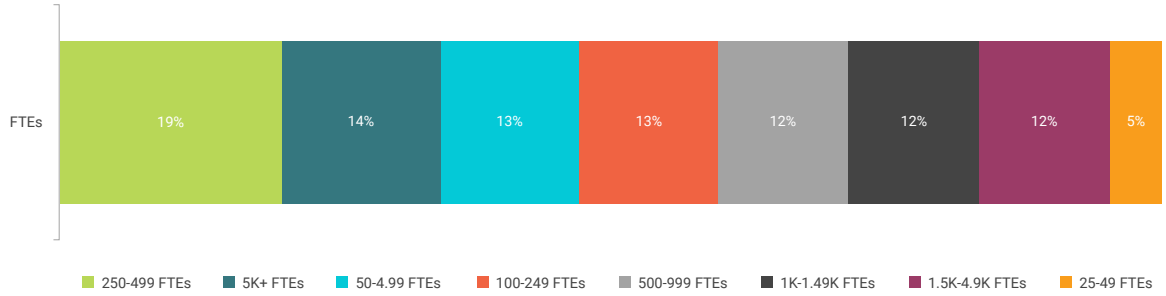


Fig 2 - Tech Pro's Role

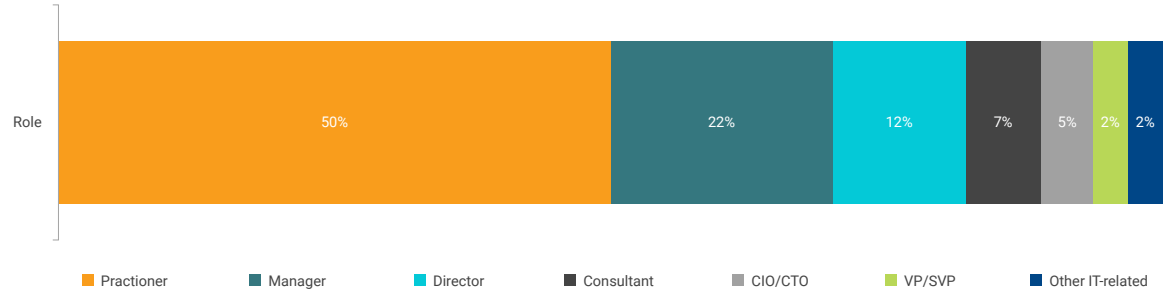
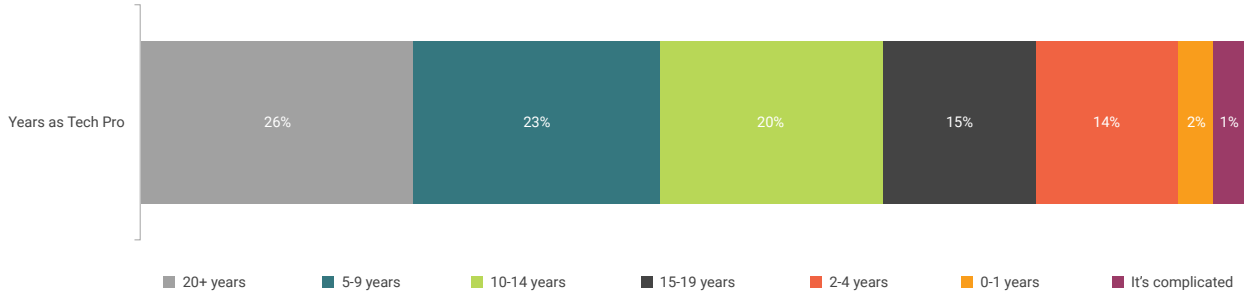


Fig 3 - Years as a Tech Pro



Study Overview: In-House vs. Outsourced Technology Environments

Fig 4 - Tech Environments Managed In-House (not mutually exclusive)

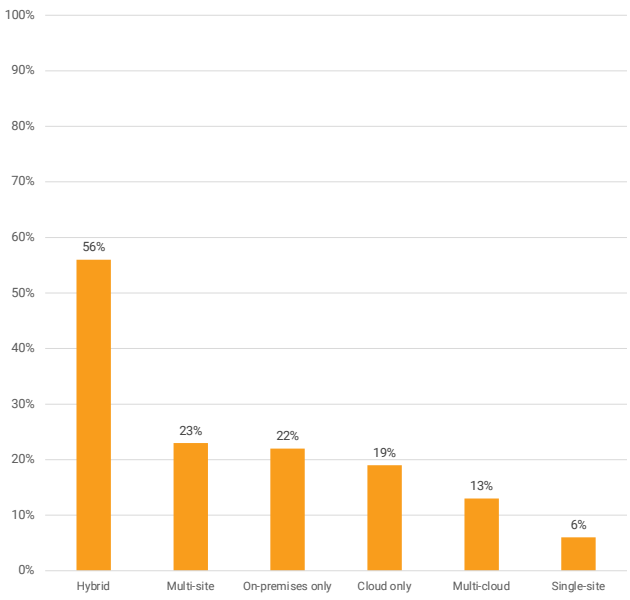
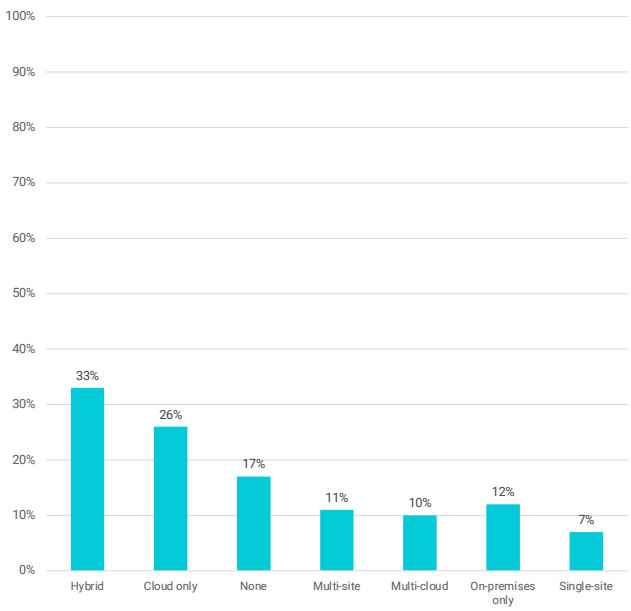


Fig 5 - Technology Environments Outsourced (not mutually exclusive)



Study Overview: Risk Exposure

We asked:

For the purposes of this study, "Enterprise IT Risk" is defined as various events or incidents compromising IT and causing adverse impacts on the organization's business processes or mission, ranging from inconsequential to catastrophic in scale. How would you describe your organization's exposure to "enterprise IT risk" over the past 12 months?

Tech Pro's Description of Their Organization's Exposure to "Enterprise IT Risk" Over Past 12 Months

Fig 6a - Overall

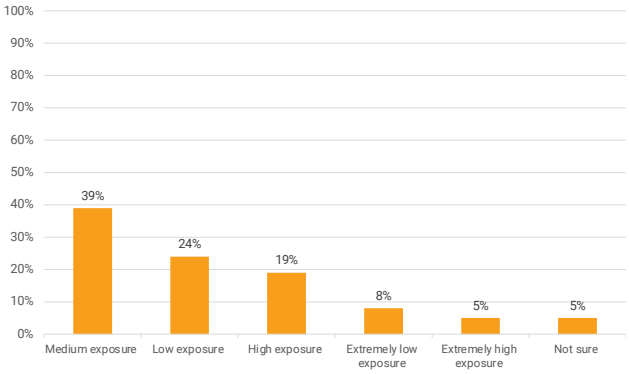


Fig 6b - Small Business

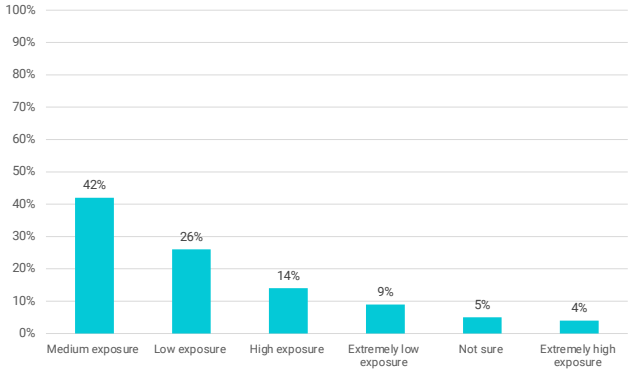


Fig 6c - Mid-Size Business

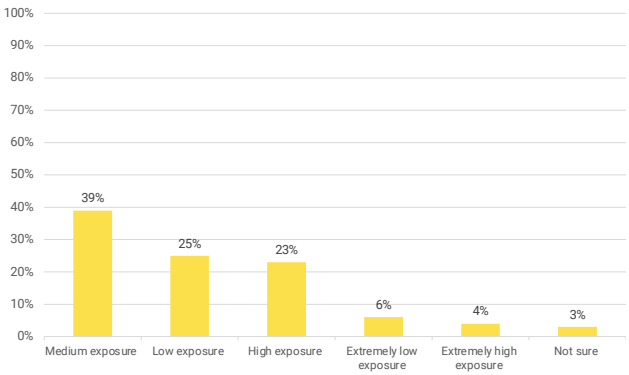
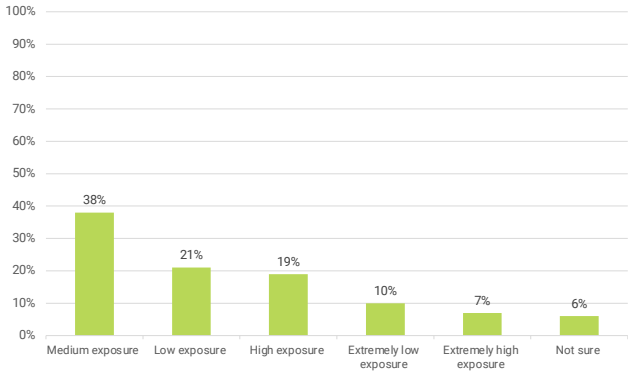


Fig 6d - Enterprise



Study Overview: Biggest Influence on Organization's Risk Exposure

We asked:

Which of the following macro trends will have the biggest influence on your organization's risk exposure moving forward?

Macro Trends with Biggest Influence on Organization's Risk Exposure Moving Forward (Ranked in Order of Importance by Tech Pros)

Fig 7a - Overall

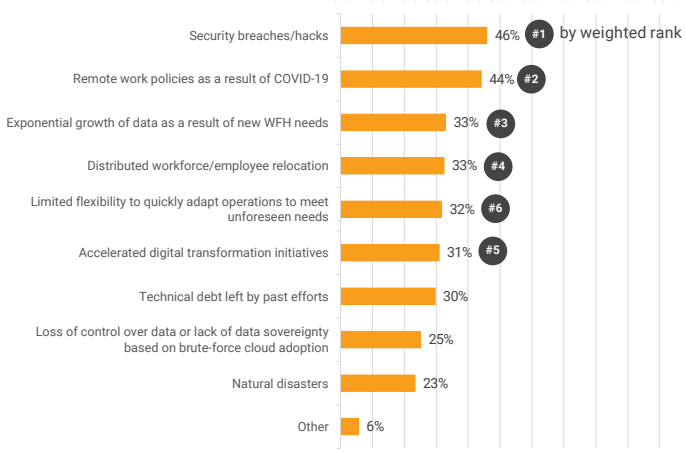


Fig 7b - Small Business

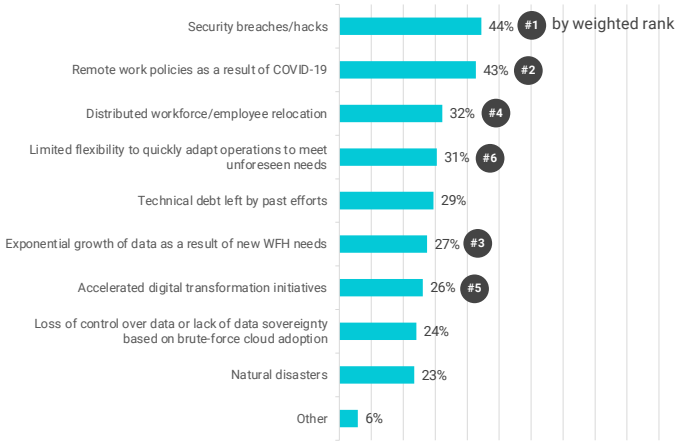


Fig 7c - Mid-Size Business

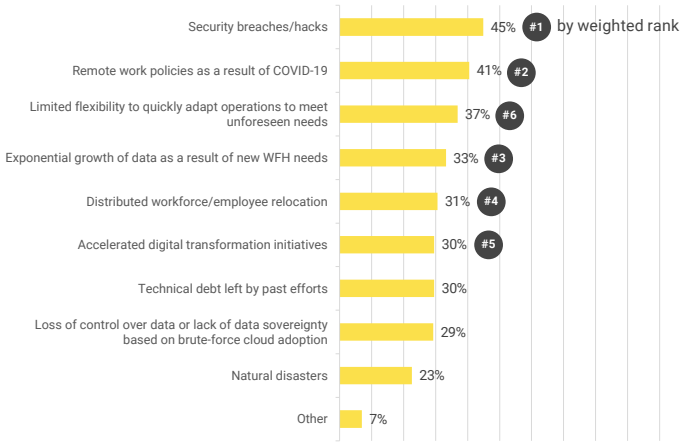
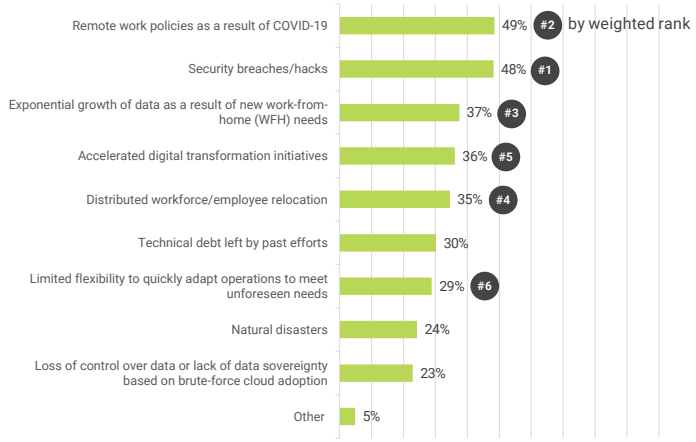


Fig 7d - Enterprise



Study Overview: Behaviors Increasing Organization's Risk Exposure

We asked:

Which of the following aspects (and/or associated behaviors of each) within your current IT environment are increasing your organization's risk exposure?

Aspects and Associated Behaviors Increasing Organization's Risk Exposure (Ranked in Order of Biggest Risk Exposure by Tech Pros)

Fig 8a - Overall

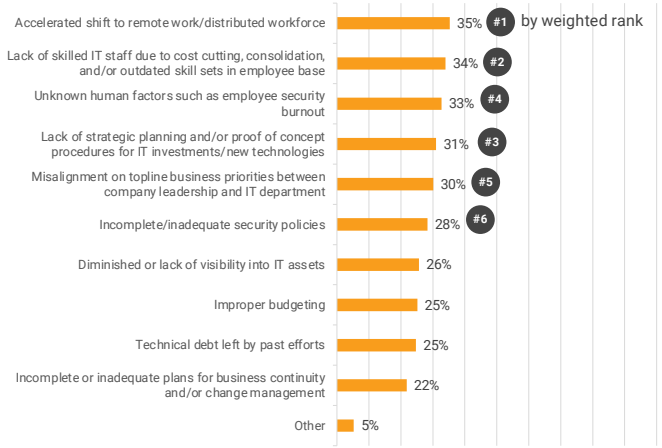


Fig 8b - Small Business

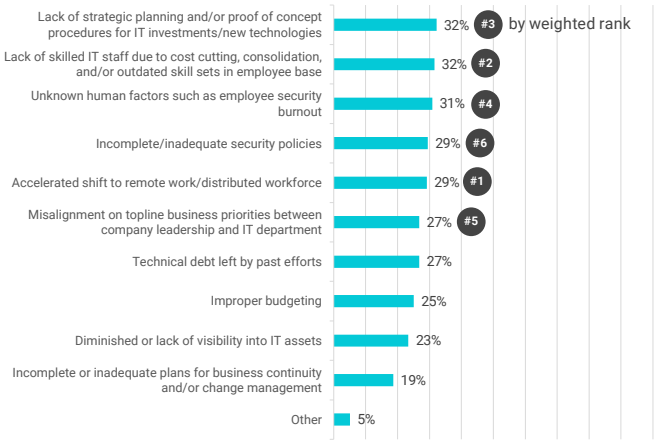


Fig 8c - Mid-Size Business

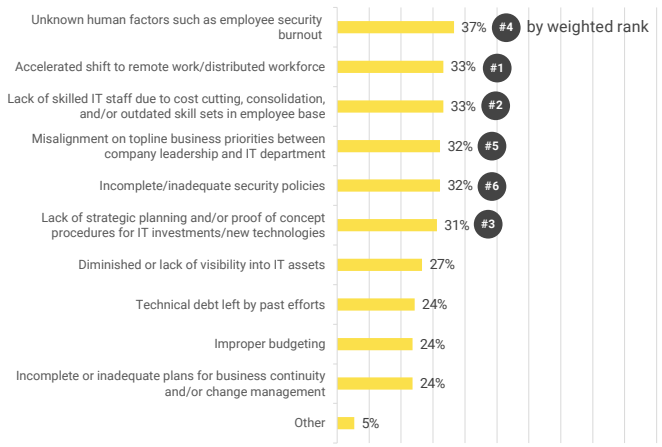
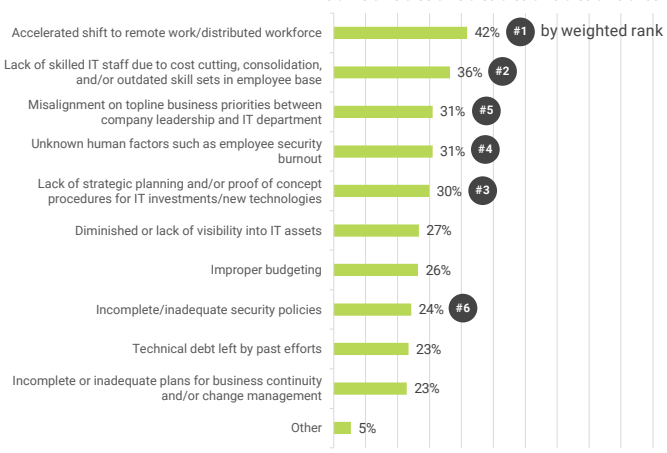


Fig 8d - Enterprise



Study Overview: Demands of Distributed Work Due to COVID-19

We asked:

COVID-19 required businesses of all sizes to shift to remote WFH policies almost overnight. In which of the following technologies did your IT team prioritize investment?

Technologies in Which IT Teams Prioritized Investment to Accommodate the Unprecedented Demands of Distributed Work Due to COVID-19

Fig 9a - Overall

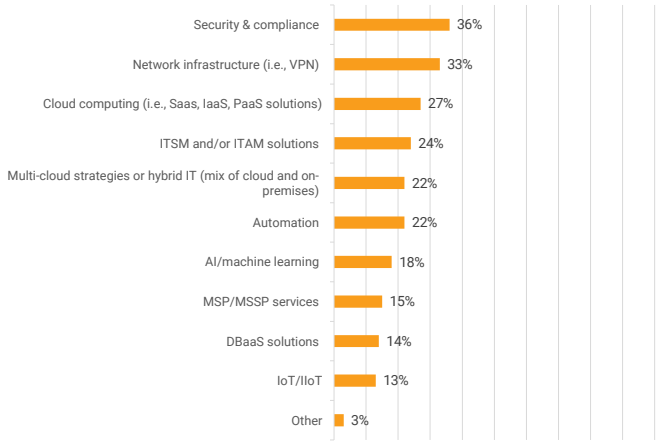


Fig 9b - Small Business

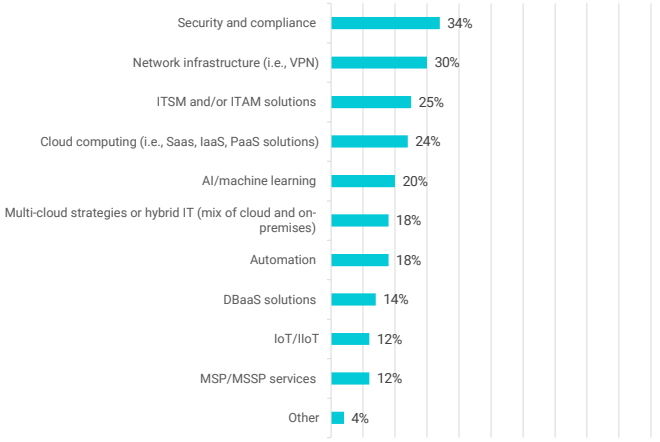


Fig 9c - Mid-Size Business

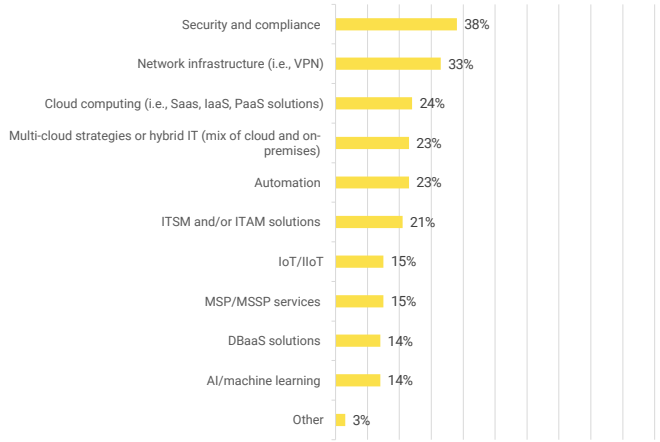
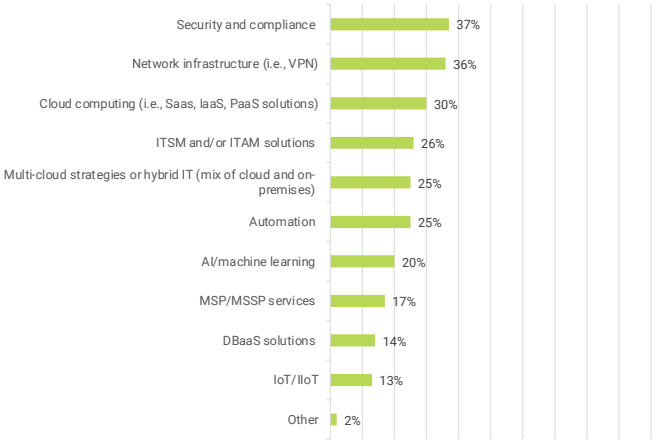


Fig 9d - Enterprise



Study Overview: Organization's Planning Process for IT Investment

We asked:

How would you rate the RIGOR of the planning process within your organization as IT investment was prioritized to accommodate the unprecedented IT demands of distributed work due to COVID-19?

Tech Pro's Rating of Rigor Within Organization's Planning Process for IT Investment Prioritized to Accommodate Unprecedented Demands

Fig 10a - Overall

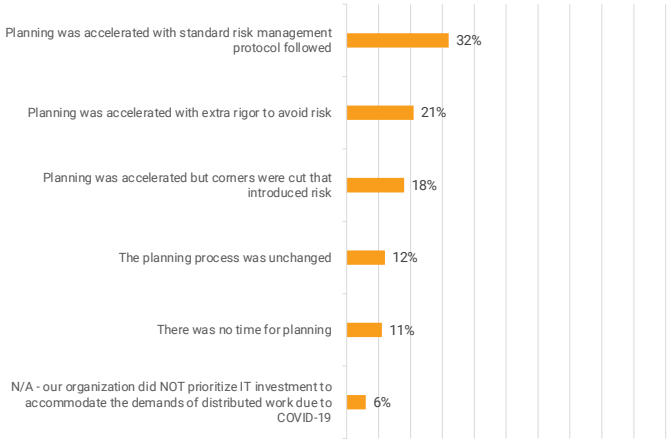


Fig 10b - Small Business

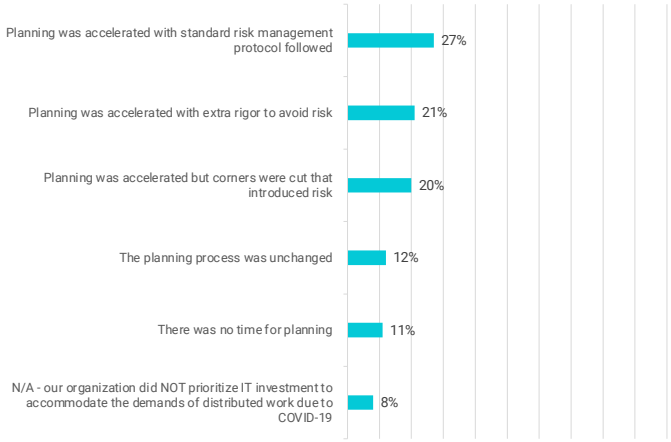


Fig 10c - Mid-Size Business

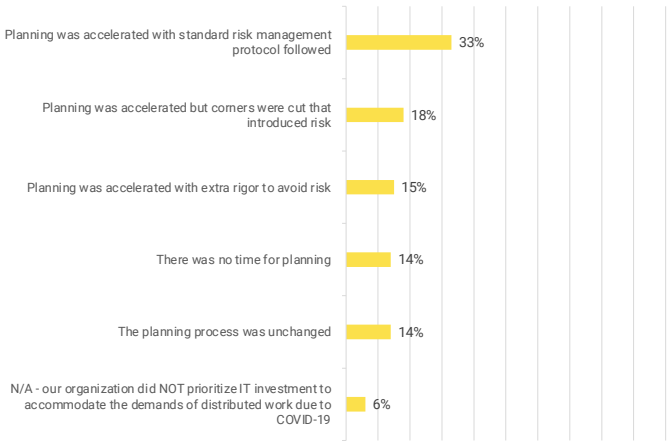
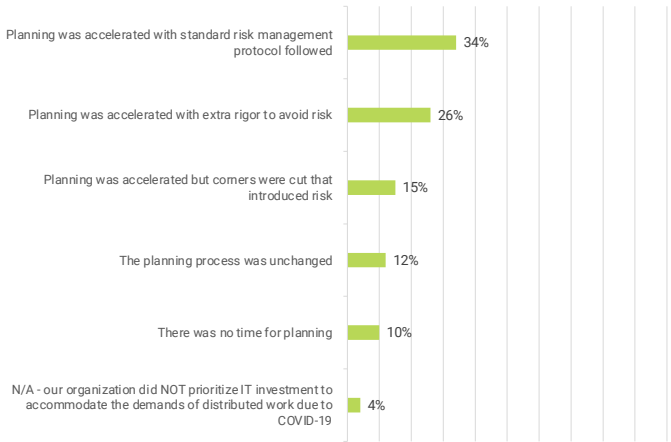


Fig 10d - Enterprise



Study Overview: Resolve Risk Factor-Related Issues

We asked:

How much do you agree or disagree with the following statement: My IT organization is prepared to manage, mitigate, and resolve risk factor-related issues due to the policies and/or procedures we already have in place.

Tech Pro's IT Organization Is Prepared to Manage, Mitigate, and Resolve Risk Factor-Related Issues Due to the Policies and/or Procedures They Already Have in Place

Fig 11a - Overall

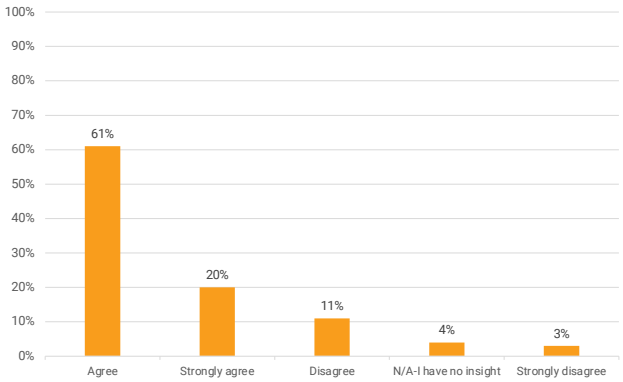


Fig 11b - Small Business

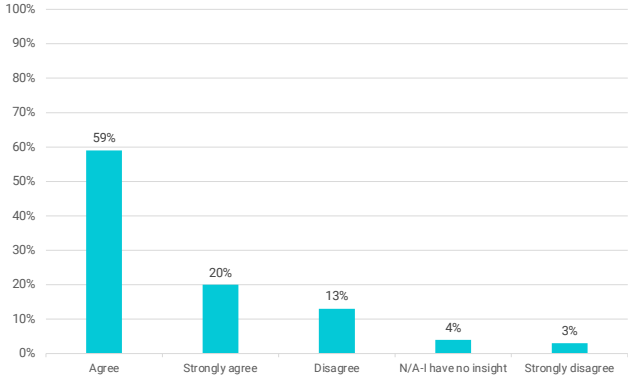


Fig 11c - Mid-Size Business

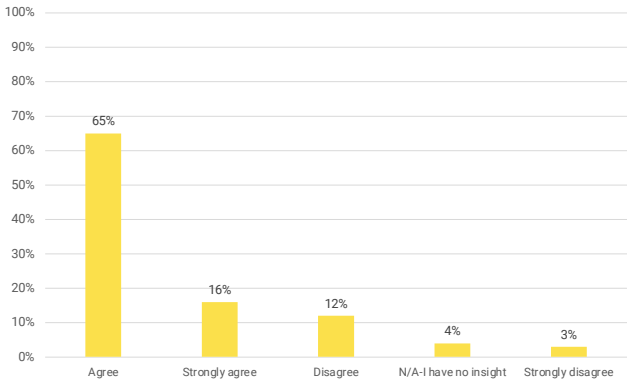
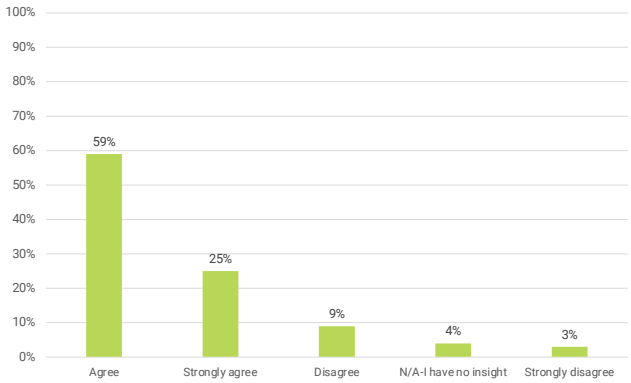


Fig 11d - Enterprise



Study Overview: Resolve Issues Related to Risk

We asked:

How much do you agree or disagree with the following statement: Technology is the best way for organizations to manage, mitigate, and resolve issues related to risk.

Technology Is the Best Way for Organizations to Manage, Mitigate, and Resolve Issues Related to Risk

Fig 12a - Overall

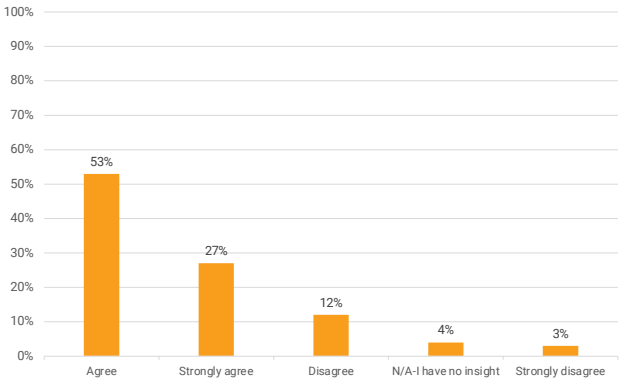


Fig 12b - Small Business

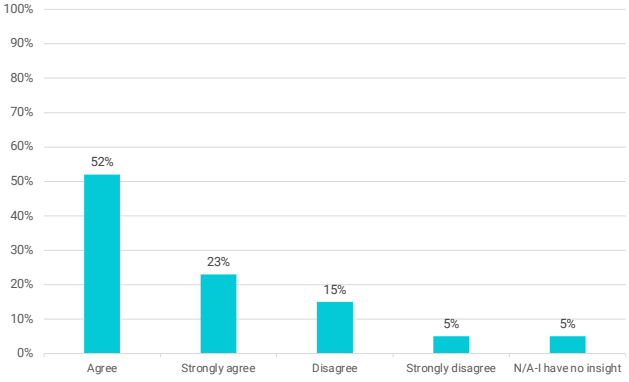


Fig 12c - Mid-Size Business

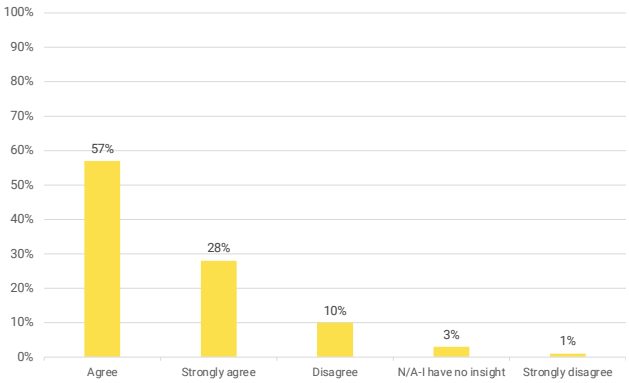
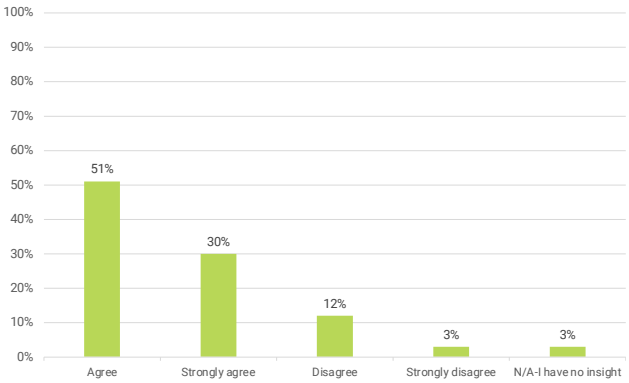


Fig 12d - Enterprise



Study Overview: Managing/ Mitigating Risk Within Organization

We asked:

Which of the following technologies are most critical to managing/mitigating risk within your organization?

Tech Pro's Top Three Technologies Most Critical to Managing/Mitigating Risk Within Organization

Fig 13a - Overall

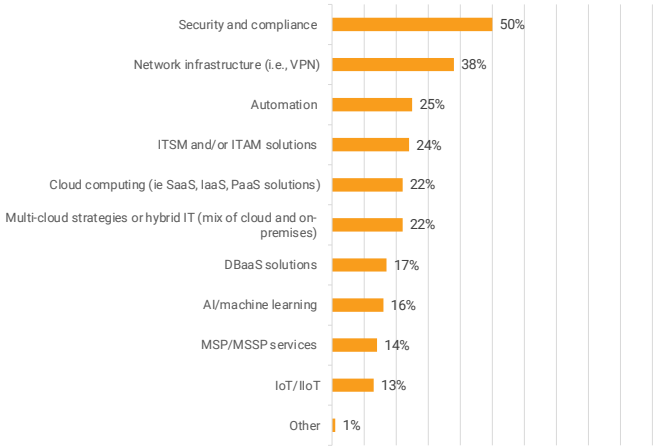


Fig 13b - Small Business

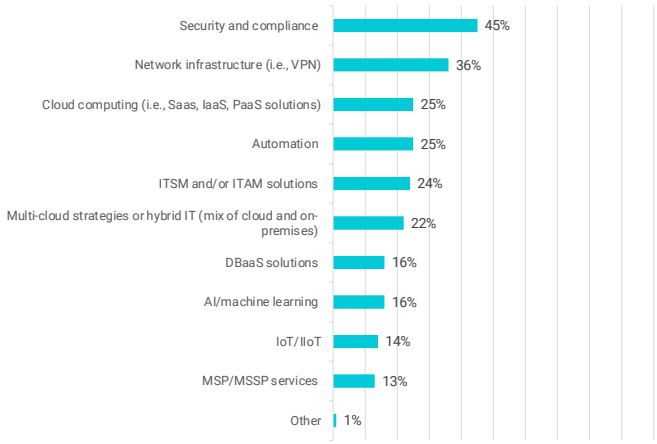


Fig 13c - Mid-Size Business

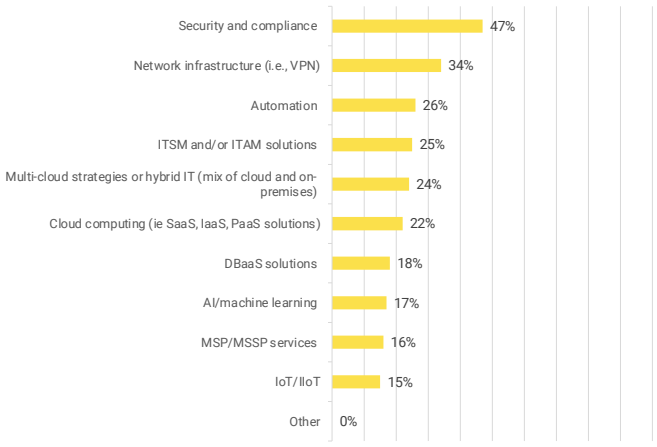
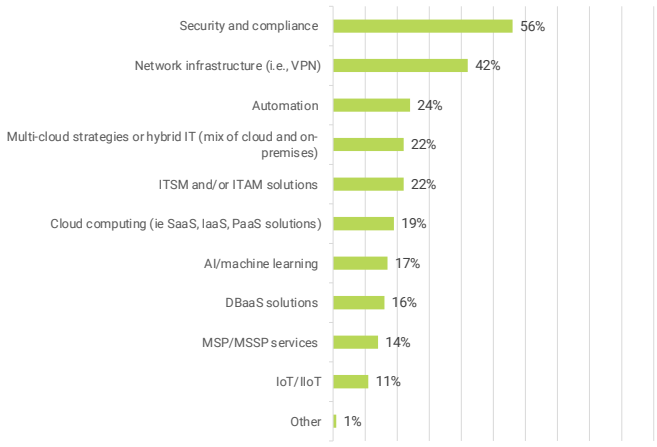


Fig 13d - Enterprise



Study Overview: Mitigate/Manage Risk Within Organization

We asked:

What are the top three barriers/challenges to utilizing technology to mitigate and/or manage risk within your organization?

Tech Pro's Top Three Barriers/Challenges to Utilizing Technology to Mitigate/Manage Risk Within Organization

Fig 14a - Overall

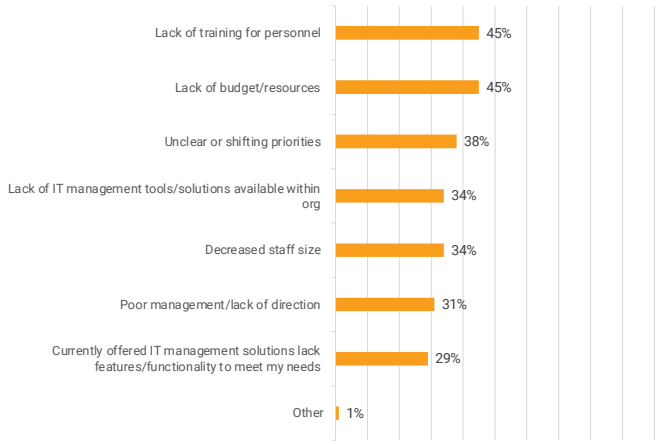


Fig 14b - Small Business

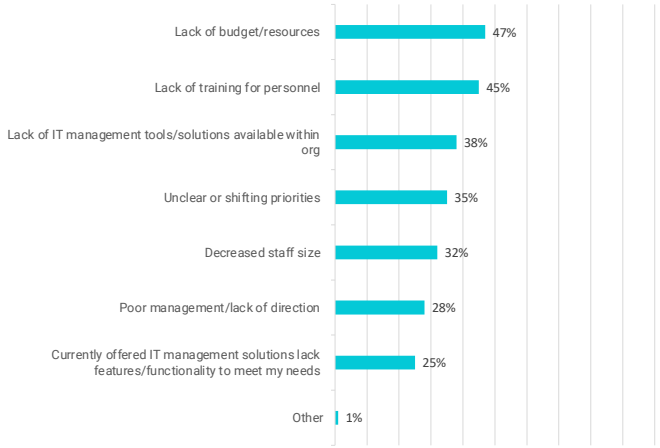


Fig 14c - Mid-Size Business

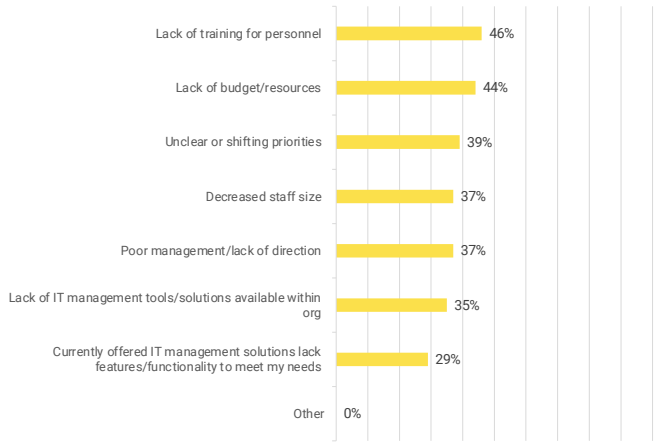
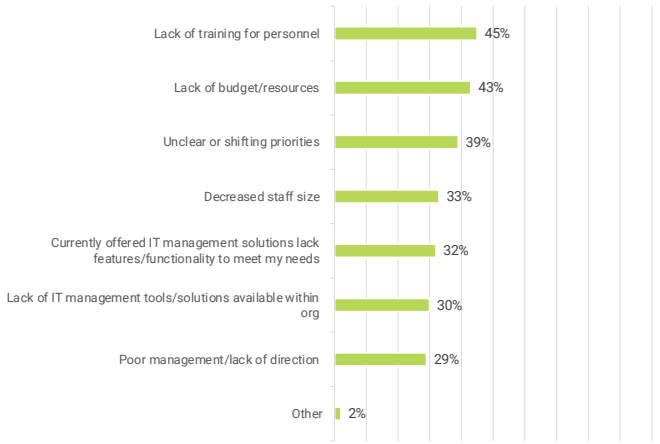


Fig 14d - Enterprise



Study Overview: Utilizing Technology for Risk Mitigation/ Management

We asked:

Which of the following areas is your IT organization prioritizing to address the challenges associated with utilizing technology for risk mitigation/management?

Areas IT Organization Is Prioritizing to Address Challenges Associated With Utilizing Technology for Risk Mitigation/Management

Fig 15a - Overall

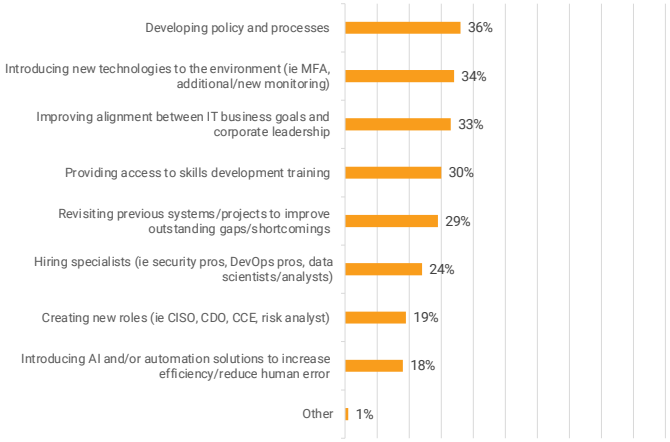


Fig 15b - Small Business

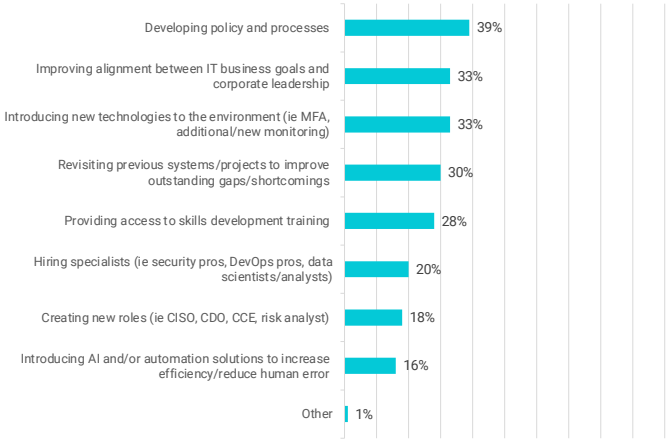


Fig 15c - Mid-Size Business

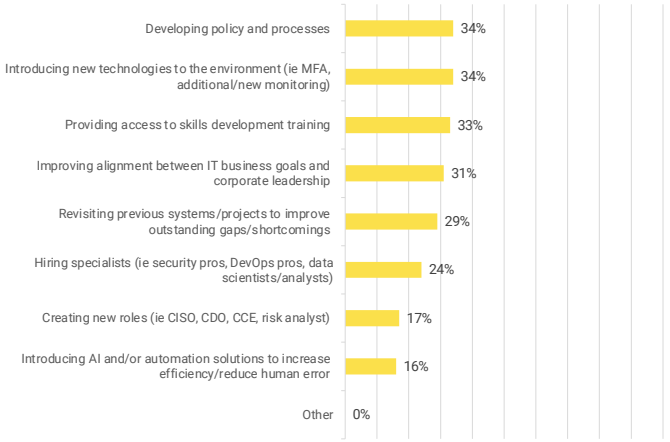
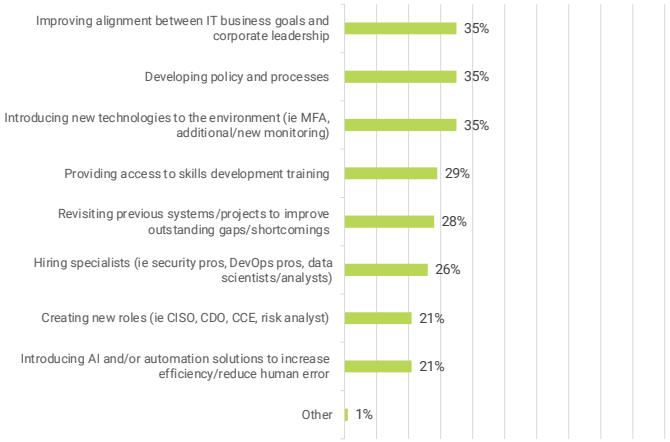


Fig 15d - Enterprise



Study Overview: Organization in Mitigating/ Managing Risk

We asked:

Which of the following do you consider when evaluating a technology/solution provider to aid your organization in mitigating/managing risk?

Tech Pro's Considerations When Evaluating a Technology/Solution Provider to Aid Organization in Mitigating/Managing Risk

Fig 16a - Overall

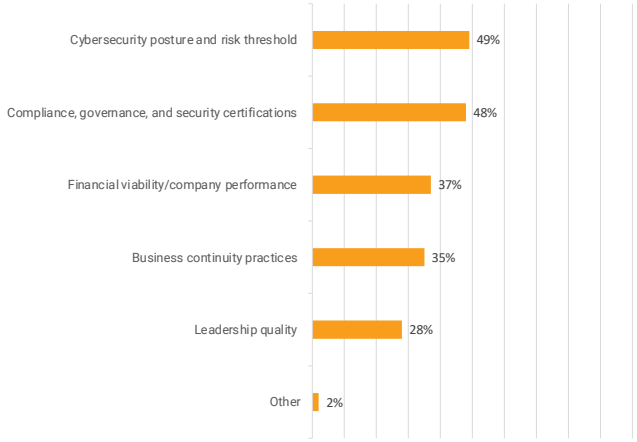


Fig 16b - Small Business

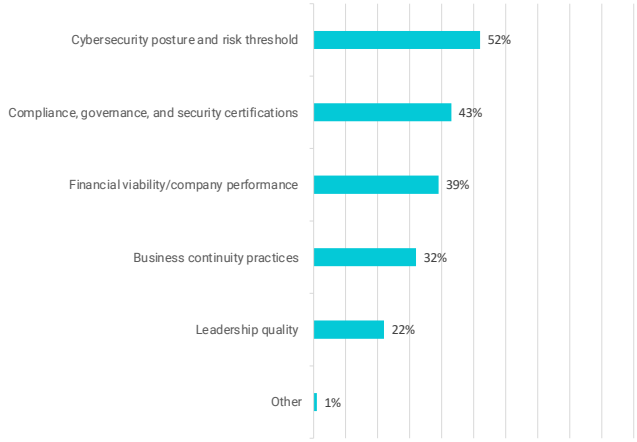


Fig 16c - Mid-Size Business

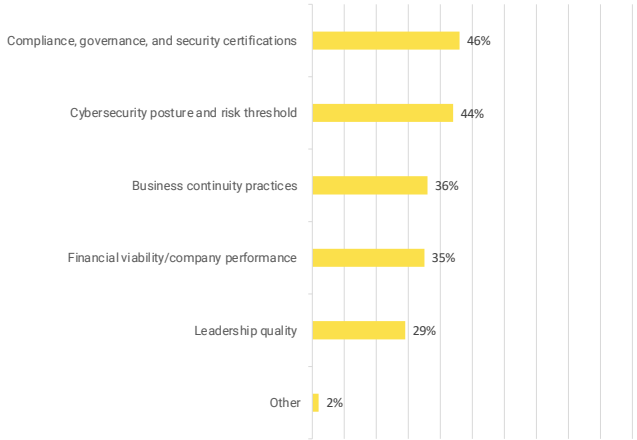


Fig 16d - Enterprise

Study Overview: Management Tools to Enhance Visibility Across IT Environment

We asked:

Are you using integrated monitoring/management tools to enhance visibility across your environments (whether on-premises, cloud, or hybrid)?

Tech Pro's Use of Integrated Monitoring/Management Tools to Enhance Visibility Across IT Environment(s)

Fig 17a - Overall

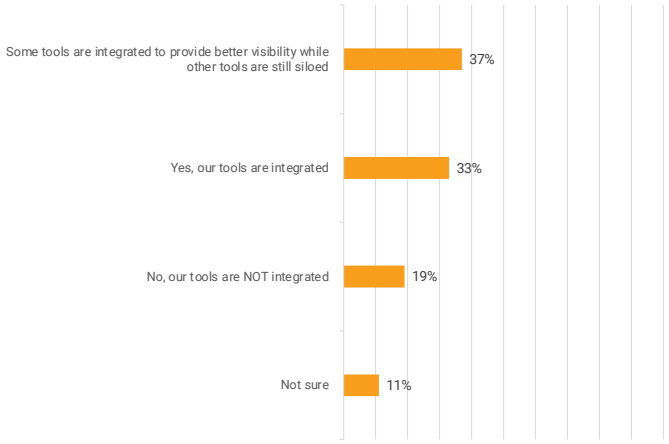


Fig 17b - Small Business

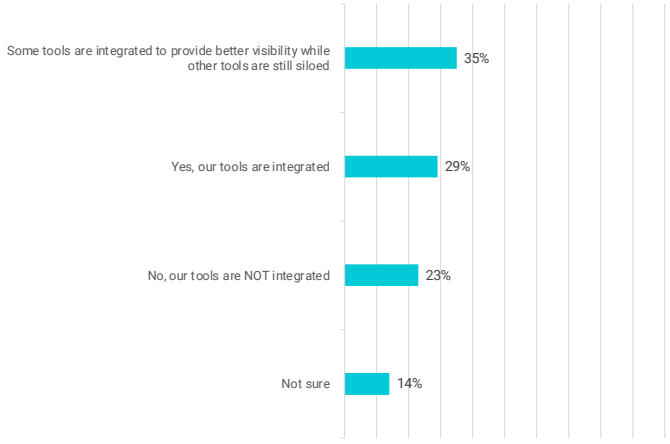


Fig 17c - Mid-Size Business

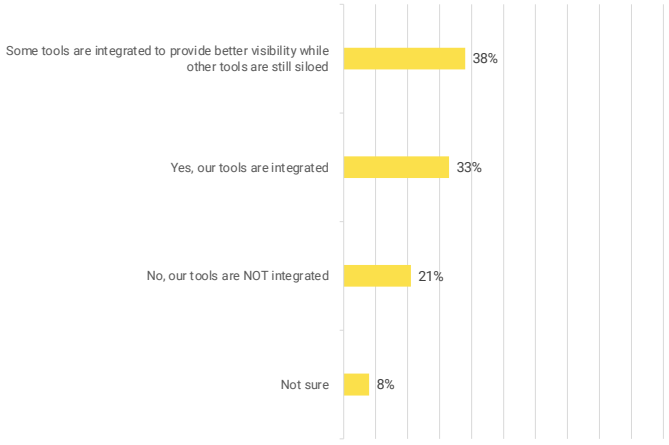
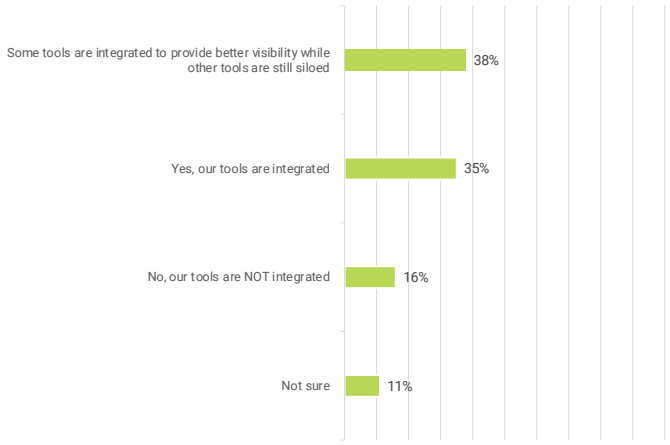


Fig 17d - Enterprise



Study Overview: Decision Makers' Mindset as It Relates to Risk

We asked:

Which of the following best describes the mindset of senior leaders/decision makers within your IT organization as it relates to risk?

Tech Pro's Perception of IT Organization's Senior Leaders/Decision Makers' Mindset as It Relates to Risk

Fig 18a - Overall

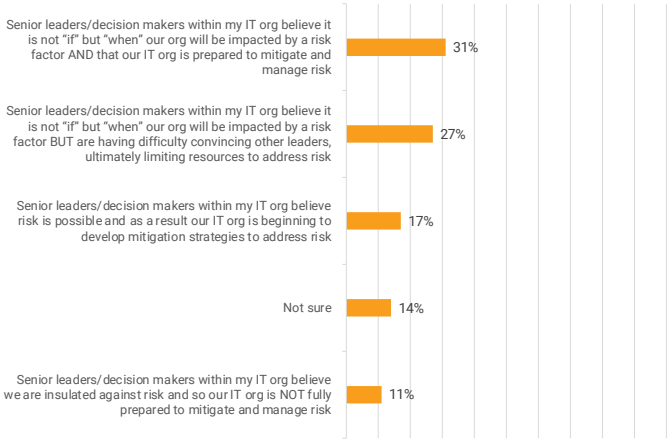


Fig 18b - Small Business

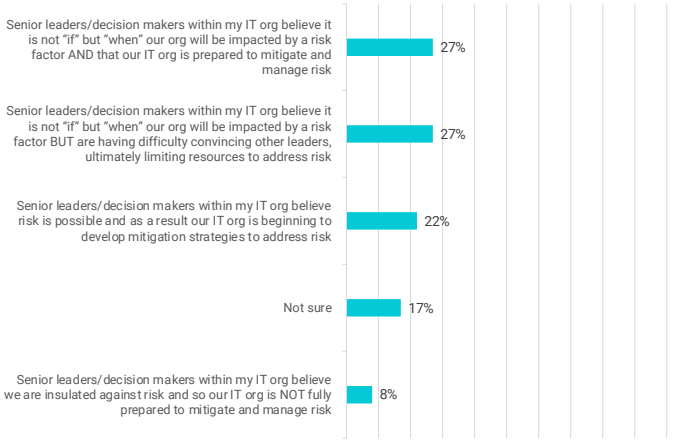


Fig 18c - Mid-Size Business

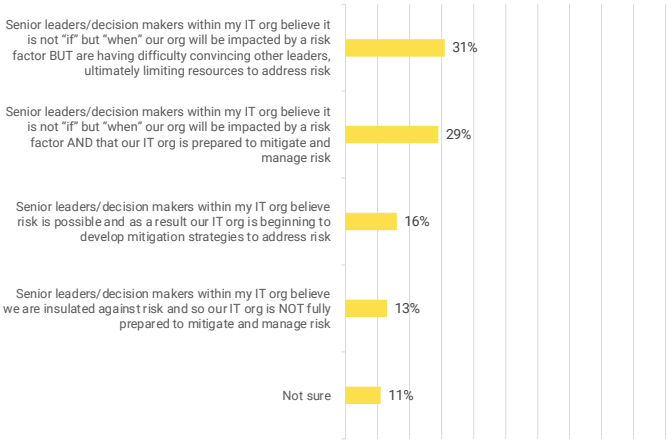
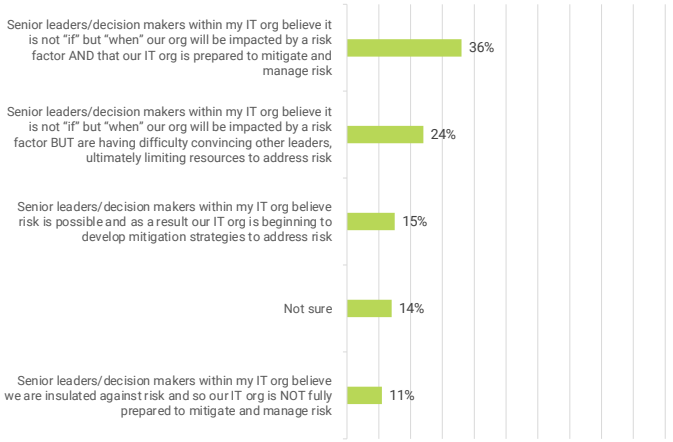


Fig 18d - Enterprise



Study Overview: Risk Management/ Mitigation Technologies Over the Next 3 Years

We asked:

Driven by the range of potentially risk-inducing events of 2020, risk awareness has recently increased. As the global IT community begins to adapt to the "next normal," sensitivity to risk will likely decrease. How confident are you that your IT organization will continue to invest in risk management/mitigation technologies over the next three years?

Tech Pro's Confidence That IT Organization Continues To Invest in Risk Management/Mitigation Technologies Over Next 3 Years

Fig 19a - Overall

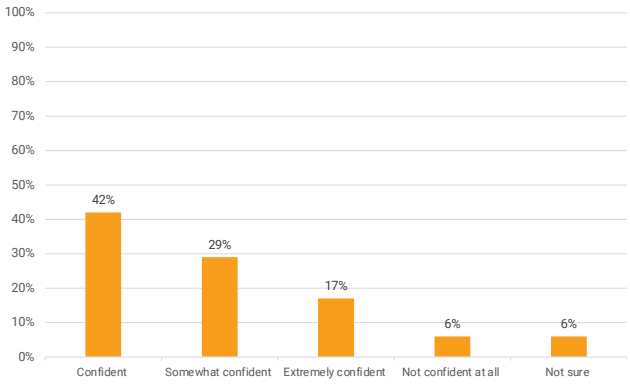


Fig 19b - Small Business

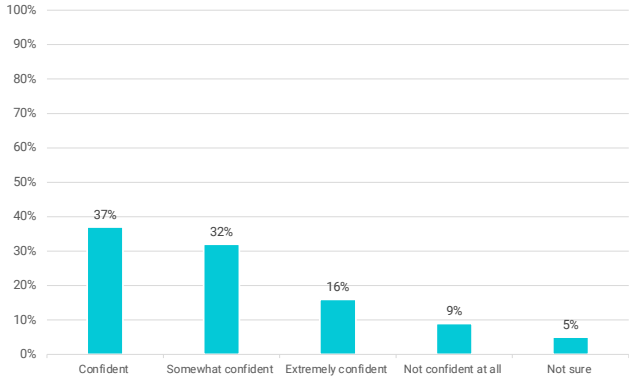


Fig 19c - Mid-Size Business

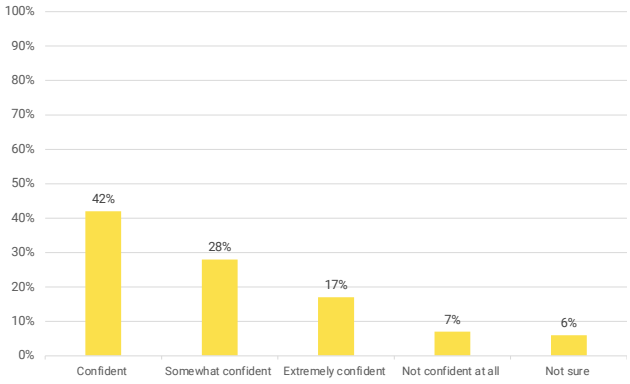
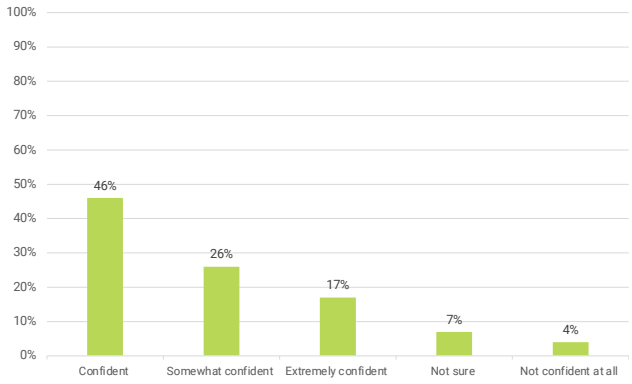



Fig 19d - Enterprise