Building a Secure Future

July 2021
## 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.
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

39% of overall tech pro respondents state their organizations have had medium 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.

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

- **REMOTE WORK POLICIES**
- **EXPONENTIAL GROWTH OF DATA AS A RESULT OF NEW WFH NEEDS**
- **DISTRIBUTED WORKFORCE/EMPLOYEE RELOCATION**
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%).

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.
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.
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.

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.
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:

- **Lack of Budget/Resources**: 45%
- **Lack of Training for Personnel**: 45%
- **Unclear or Shifting Priorities**: 38%

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%).

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

REPORT: IT TRENDS 2021: BUILDING A SECURE FUTURE
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:

- Developing policies and processes (36%)
- Prioritizing the introduction of new technologies (34%)

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.

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.
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.
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.
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.
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?
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

Security breaches/hacks: 46%
Remote work policies as a result of COVID-19: 44%
Exponential growth of data as a result of new WFH needs: 33%
Distributed workforce/employee relocation: 33%
Limited flexibility to quickly adapt operations to meet unforeseen needs: 32%
Accelerated digital transformation initiatives: 31%
Technical debt left by past efforts: 30%
Loss of control over data or lack of data sovereignty based on brute-force cloud adoption: 25%
Natural disasters: 23%
Other: 6%

Fig 7b - Small Business

Security breaches/hacks: 44%
Remote work policies as a result of COVID-19: 43%
Distributed workforce/employee relocation: 32%
Limited flexibility to quickly adapt operations to meet unforeseen needs: 31%
Technical debt left by past efforts: 29%
Exponential growth of data as a result of new WFH needs: 27%
Accelerated digital transformation initiatives: 26%
Loss of control over data or lack of data sovereignty based on brute-force cloud adoption: 24%
Natural disasters: 23%
Other: 6%

Fig 7c - Mid-Size Business

Security breaches/hacks: 45%
Remote work policies as a result of COVID-19: 41%
Exponential growth of data as a result of new WFH needs: 37%
Distributed workforce/employee relocation: 33%
Accelerated digital transformation initiatives: 31%
Technical debt left by past efforts: 30%
Loss of control over data or lack of data sovereignty based on brute-force cloud adoption: 29%
Natural disasters: 23%
Other: 7%

Fig 7d - Enterprise

Security breaches/hacks: 48%
Remote work policies as a result of COVID-19: 45%
Exponential growth of data as a result of new work-from-home (WFH) needs: 37%
Accelerated digital transformation initiatives: 36%
Distributed workforce/employee relocation: 35%
Technical debt left by past efforts: 30%
Limited flexibility to quickly adapt operations to meet unforeseen needs: 29%
Natural disasters: 24%
Loss of control over data or lack of data sovereignty based on brute-force cloud adoption: 23%
Other: 5%
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

- Accelerated shift to remote work/distributed workforce
- Lack of skilled IT staff due to cost cutting, consolidation, and/or outdated skill sets in employee base
- Unknown human factors such as employee security burnout
- Lack of strategic planning and/or proof of concept procedures for IT investments/new technologies
- Misalignment on top line business priorities between company leadership and IT department
- Incomplete/inadequate security policies
- Diminished or lack of visibility into IT assets
- Improper budgeting
- Technical debt left by past efforts
- Incomplete or inadequate plans for business continuity and/or change management
- Other

Fig 8b - Small Business

- Lack of strategic planning and/or proof of concept procedures for IT investments/new technologies
- Lack of skilled IT staff due to cost cutting, consolidation, and/or outdated skill sets in employee base
- Unknown human factors such as employee security burnout
- Incomplete/inadequate security policies
- Accelerated shift to remote work/distributed workforce
- Misalignment on top line business priorities between company leadership and IT department
- Technical debt left by past efforts
- Improper budgeting
- Diminished or lack of visibility into IT assets
- Incomplete or inadequate plans for business continuity and/or change management
- Other

Fig 8c - Mid-Size Business

- Unknown human factors such as employee security burnout
- Accelerated shift to remote work/distributed workforce
- Lack of skilled IT staff due to cost cutting, consolidation, and/or outdated skill sets in employee base
- Misalignment on top line business priorities between company leadership and IT department
- Incomplete/inadequate security policies
- Lack of strategic planning and/or proof of concept procedures for IT investments/new technologies
- Diminished or lack of visibility into IT assets
- Technical debt left by past efforts
- Improper budgeting
- Incomplete or inadequate plans for business continuity and/or change management
- Other

Fig 8d - Enterprise

- Accelerated shift to remote work/distributed workforce
- Lack of skilled IT staff due to cost cutting, consolidation, and/or outdated skill sets in employee base
- Misalignment on top line business priorities between company leadership and IT department
- Unknown human factors such as employee security burnout
- Lack of strategic planning and/or proof of concept procedures for IT investments/new technologies
- Diminished or lack of visibility into IT assets
- Improper budgeting
- Incomplete/inadequate security policies
- Technical debt left by past efforts
- Incomplete or inadequate plans for business continuity and/or change management
- Other
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?

<table>
<thead>
<tr>
<th>Technologies in Which IT Teams Prioritized Investment to Accommodate the Unprecedented Demands of Distributed Work Due to COVID-19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security &amp; compliance</td>
</tr>
<tr>
<td>Network infrastructure (i.e., VPN)</td>
</tr>
<tr>
<td>Cloud computing (i.e., SaaS, IaaS, PaaS solutions)</td>
</tr>
<tr>
<td>ITSM and/or ITAM solutions</td>
</tr>
<tr>
<td>Multi-cloud strategies or hybrid IT (mix of cloud and on-premises)</td>
</tr>
<tr>
<td>Automation</td>
</tr>
<tr>
<td>AI/machine learning</td>
</tr>
<tr>
<td>MSP/MSSP services</td>
</tr>
<tr>
<td>DBaaS solutions</td>
</tr>
<tr>
<td>IoT/IIoT</td>
</tr>
<tr>
<td>Other</td>
</tr>
</tbody>
</table>

**Fig 9a - Overall**

| Security and compliance | 34% |
| Network infrastructure (i.e., VPN) | 30% |
| ITSM and/or ITAM solutions | 25% |
| Cloud computing (i.e., SaaS, IaaS, PaaS solutions) | 24% |
| AI/machine learning | 20% |
| Multi-cloud strategies or hybrid IT (mix of cloud and on-premises) | 18% |
| Automation | 18% |
| DBaaS solutions | 14% |
| IoT/IIoT | 12% |
| MSP/MSSP services | 12% |
| Other | 4% |

**Fig 9b - Small Business**

| Security and compliance | 38% |
| Network infrastructure (i.e., VPN) | 13% |
| Cloud computing (i.e., SaaS, IaaS, PaaS solutions) | 24% |
| Multi-cloud strategies or hybrid IT (mix of cloud and on-premises) | 23% |
| Automation | 23% |
| ITSM and/or ITAM solutions | 21% |
| IoT/IIoT | 15% |
| MSP/MSSP services | 13% |
| DBaaS solutions | 14% |
| AI/machine learning | 14% |
| Other | 3% |

**Fig 9c - Mid-Size Business**

| Security and compliance | 37% |
| Network infrastructure (i.e., VPN) | 36% |
| Cloud computing (i.e., SaaS, IaaS, PaaS solutions) | 30% |
| ITSM and/or ITAM solutions | 26% |
| Multi-cloud strategies or hybrid IT (mix of cloud and on-premises) | 25% |
| Automation | 25% |
| AI/machine learning | 20% |
| MSP/MSSP services | 17% |
| DBaaS solutions | 14% |
| IoT/IIoT | 13% |
| Other | 2% |

**Fig 9d - Enterprise**

| Security and compliance | 37% |
| Network infrastructure (i.e., VPN) | 36% |
| Cloud computing (i.e., SaaS, IaaS, PaaS solutions) | 30% |
| ITSM and/or ITAM solutions | 26% |
| Multi-cloud strategies or hybrid IT (mix of cloud and on-premises) | 25% |
| Automation | 25% |
| AI/machine learning | 20% |
| MSP/MSSP services | 17% |
| DBaaS solutions | 14% |
| IoT/IIoT | 13% |
| Other | 2% |
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**

- Planning was accelerated with standard risk management protocol followed: 32%
- Planning was accelerated with extra rigor to avoid risk: 21%
- Planning was accelerated but corners were cut that introduced risk: 18%
- The planning process was unchanged: 12%
- There was no time for planning: 11%
- N/A - our organization did NOT prioritize IT investment to accommodate the demands of distributed work due to COVID-19: 6%

**Fig 10b - Small Business**

- Planning was accelerated with standard risk management protocol followed: 27%
- Planning was accelerated with extra rigor to avoid risk: 21%
- Planning was accelerated but corners were cut that introduced risk: 20%
- The planning process was unchanged: 12%
- There was no time for planning: 11%
- N/A - our organization did NOT prioritize IT investment to accommodate the demands of distributed work due to COVID-19: 8%

**Fig 10c - Mid-Size Business**

- Planning was accelerated with standard risk management protocol followed: 33%
- Planning was accelerated but corners were cut that introduced risk: 18%
- Planning was accelerated with extra rigor to avoid risk: 15%
- There was no time for planning: 14%
- The planning process was unchanged: 14%
- N/A - our organization did NOT prioritize IT investment to accommodate the demands of distributed work due to COVID-19: 6%

**Fig 10d - Enterprise**

- Planning was accelerated with standard risk management protocol followed: 34%
- Planning was accelerated with extra rigor to avoid risk: 36%
- Planning was accelerated but corners were cut that introduced risk: 15%
- The planning process was unchanged: 12%
- There was no time for planning: 10%
- N/A - our organization did NOT prioritize IT investment to accommodate the demands of distributed work due to COVID-19: 4%
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.
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

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and compliance</td>
<td>50%</td>
</tr>
<tr>
<td>Network infrastructure (i.e., VPN)</td>
<td>38%</td>
</tr>
<tr>
<td>Automation</td>
<td>25%</td>
</tr>
<tr>
<td>ITSM and/or ITAM solutions</td>
<td>24%</td>
</tr>
<tr>
<td>Cloud computing (i.e., SaaS, IaaS, PaaS solutions)</td>
<td>22%</td>
</tr>
<tr>
<td>Multi-cloud strategies or hybrid IT (mix of cloud and on-premises)</td>
<td>22%</td>
</tr>
<tr>
<td>DBaaS solutions</td>
<td>17%</td>
</tr>
<tr>
<td>AI/machine learning</td>
<td>16%</td>
</tr>
<tr>
<td>MSP/MSSP services</td>
<td>14%</td>
</tr>
<tr>
<td>IoT/IIoT</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

Fig 13b - Small Business

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and compliance</td>
<td>48%</td>
</tr>
<tr>
<td>Network infrastructure (i.e., VPN)</td>
<td>36%</td>
</tr>
<tr>
<td>Cloud computing (i.e., SaaS, IaaS, PaaS solutions)</td>
<td>25%</td>
</tr>
<tr>
<td>Automation</td>
<td>23%</td>
</tr>
<tr>
<td>ITSM and/or ITAM solutions</td>
<td>24%</td>
</tr>
<tr>
<td>Multi-cloud strategies or hybrid IT (mix of cloud and on-premises)</td>
<td>22%</td>
</tr>
<tr>
<td>DBaaS solutions</td>
<td>16%</td>
</tr>
<tr>
<td>AI/machine learning</td>
<td>16%</td>
</tr>
<tr>
<td>IoT/IIoT</td>
<td>14%</td>
</tr>
<tr>
<td>MSP/MSSP services</td>
<td>13%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>

Fig 13c - Mid-Size Business

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and compliance</td>
<td>47%</td>
</tr>
<tr>
<td>Network infrastructure (i.e., VPN)</td>
<td>34%</td>
</tr>
<tr>
<td>Automation</td>
<td>26%</td>
</tr>
<tr>
<td>ITSM and/or ITAM solutions</td>
<td>25%</td>
</tr>
<tr>
<td>Multi-cloud strategies or hybrid IT (mix of cloud and on-premises)</td>
<td>24%</td>
</tr>
<tr>
<td>Cloud computing (i.e., SaaS, IaaS, PaaS solutions)</td>
<td>22%</td>
</tr>
<tr>
<td>DBaaS solutions</td>
<td>18%</td>
</tr>
<tr>
<td>AI/machine learning</td>
<td>17%</td>
</tr>
<tr>
<td>MSP/MSSP services</td>
<td>16%</td>
</tr>
<tr>
<td>IoT/IIoT</td>
<td>15%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
</tr>
</tbody>
</table>

Fig 13d - Enterprise

<table>
<thead>
<tr>
<th>Technology</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and compliance</td>
<td>56%</td>
</tr>
<tr>
<td>Network infrastructure (i.e., VPN)</td>
<td>42%</td>
</tr>
<tr>
<td>Automation</td>
<td>24%</td>
</tr>
<tr>
<td>Multi-cloud strategies or hybrid IT (mix of cloud and on-premises)</td>
<td>22%</td>
</tr>
<tr>
<td>ITSM and/or ITAM solutions</td>
<td>22%</td>
</tr>
<tr>
<td>Cloud computing (i.e., SaaS, IaaS, PaaS solutions)</td>
<td>19%</td>
</tr>
<tr>
<td>AI/machine learning</td>
<td>17%</td>
</tr>
<tr>
<td>DBaaS solutions</td>
<td>16%</td>
</tr>
<tr>
<td>MSP/MSSP services</td>
<td>14%</td>
</tr>
<tr>
<td>IoT/IIoT</td>
<td>11%</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Fig 14a - Overall</th>
<th>Fig 14b - Small Business</th>
<th>Fig 14c - Mid-Size Business</th>
<th>Fig 14d - Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of training for personnel</td>
<td>Lack of budget/resources</td>
<td>Lack of training for personnel</td>
<td>Lack of training for personnel</td>
</tr>
<tr>
<td>Lack of budget/resources</td>
<td>Lack of IT management tools/solutions available within org</td>
<td>Lack of training for personnel</td>
<td>Lack of budget/resources</td>
</tr>
<tr>
<td>Unclear or shifting priorities</td>
<td>Unclear or shifting priorities</td>
<td>Unclear or shifting priorities</td>
<td>Unclear or shifting priorities</td>
</tr>
<tr>
<td>Lack of IT management tools/solutions available within org</td>
<td>Decreased staff size</td>
<td>Decreased staff size</td>
<td>Decreased staff size</td>
</tr>
<tr>
<td>Decreased staff size</td>
<td>Poor management/lack of direction</td>
<td>Poor management/lack of direction</td>
<td>Poor management/lack of direction</td>
</tr>
<tr>
<td>Poor management/lack of direction</td>
<td>Currently offered IT management solutions lack features/functionality to meet my needs</td>
<td>Currently offered IT management solutions lack features/functionality to meet my needs</td>
<td>Currently offered IT management solutions lack features/functionality to meet my needs</td>
</tr>
<tr>
<td>Currently offered IT management solutions lack features/functionality to meet my needs</td>
<td>Other</td>
<td>Other</td>
<td>Other</td>
</tr>
<tr>
<td>Other</td>
<td>1%</td>
<td>1%</td>
<td>2%</td>
</tr>
</tbody>
</table>
**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**

- Developing policy and processes: 36%
- Introducing new technologies to the environment (e.g., MFA, additional/new monitoring): 34%
- Improving alignment between IT business goals and corporate leadership: 33%
- Providing access to skills development training: 30%
- Revisiting previous systems/projects to improve outstanding gaps/shortcomings: 29%
- Hiring specialists (e.g., security pros, DevOps pros, data scientists/analysts): 24%
- Creating new roles (e.g., CISO, CDO, CCE, risk analyst): 19%
- Introducing AI and/or automation solutions to increase efficiency/reduce human error: 18%
- Other: 1%

**Fig 15b - Small Business**

- Developing policy and processes: 39%
- Improving alignment between IT business goals and corporate leadership: 33%
- Introducing new technologies to the environment (e.g., MFA, additional/new monitoring): 33%
- Revisiting previous systems/projects to improve outstanding gaps/shortcomings: 30%
- Providing access to skills development training: 28%
- Hiring specialists (e.g., security pros, DevOps pros, data scientists/analysts): 20%
- Creating new roles (e.g., CISO, CDO, CCE, risk analyst): 18%
- Introducing AI and/or automation solutions to increase efficiency/reduce human error: 16%
- Other: 1%

**Fig 15c - Mid-Size Business**

- Developing policy and processes: 34%
- Introducing new technologies to the environment (e.g., MFA, additional/new monitoring): 34%
- Providing access to skills development training: 33%
- Improving alignment between IT business goals and corporate leadership: 31%
- Revisiting previous systems/projects to improve outstanding gaps/shortcomings: 29%
- Hiring specialists (e.g., security pros, DevOps pros, data scientists/analysts): 24%
- Creating new roles (e.g., CISO, CDO, CCE, risk analyst): 17%
- Introducing AI and/or automation solutions to increase efficiency/reduce human error: 16%
- Other: 0%

**Fig 15d - Enterprise**

- Developing policy and processes: 35%
- Improving alignment between IT business goals and corporate leadership: 35%
- Introducing new technologies to the environment (e.g., MFA, additional/new monitoring): 35%
- Providing access to skills development training: 29%
- Revisiting previous systems/projects to improve outstanding gaps/shortcomings: 28%
- Hiring specialists (e.g., security pros, DevOps pros, data scientists/analysts): 26%
- Creating new roles (e.g., CISO, CDO, CCE, risk analyst): 21%
- Introducing AI and/or automation solutions to increase efficiency/reduce human error: 21%
- Other: 1%
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
- Cybersecurity posture and risk threshold: 49%
- Compliance, governance, and security certifications: 48%
- Financial viability/company performance: 37%
- Business continuity practices: 35%
- Leadership quality: 28%
- Other: 2%

Fig 16b - Small Business
- Cybersecurity posture and risk threshold: 52%
- Compliance, governance, and security certifications: 49%
- Financial viability/company performance: 39%
- Business continuity practices: 32%
- Leadership quality: 22%
- Other: 1%

Fig 16c - Mid-Size Business
- Compliance, governance, and security certifications: 46%
- Cybersecurity posture and risk threshold: 44%
- Business continuity practices: 36%
- Financial viability/company performance: 35%
- Leadership quality: 29%
- Other: 2%

Fig 16d - Enterprise
- Compliance, governance, and security certifications: 53%
- Cybersecurity posture and risk threshold: 49%
- Financial viability/company performance: 37%
- Business continuity practices: 37%
- Leadership quality: 32%
- Other: 2%
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

- Some tools are integrated to provide better visibility while other tools are still siloed: 37%
- Yes, our tools are integrated: 33%
- No, our tools are NOT integrated: 19%
- Not sure: 11%

Fig 17b - Small Business

- Some tools are integrated to provide better visibility while other tools are still siloed: 35%
- Yes, our tools are integrated: 29%
- No, our tools are NOT integrated: 23%
- Not sure: 14%

Fig 17c - Mid-Size Business

- Some tools are integrated to provide better visibility while other tools are still siloed: 38%
- Yes, our tools are integrated: 33%
- No, our tools are NOT integrated: 21%
- Not sure: 8%

Fig 17d - Enterprise

- Some tools are integrated to provide better visibility while other tools are still siloed: 38%
- Yes, our tools are integrated: 35%
- No, our tools are NOT integrated: 16%
- Not sure: 11%
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

<table>
<thead>
<tr>
<th>Fig 18a - Overall</th>
<th>Fig 18b - Small Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor AND that our IT org is prepared to mitigate and manage risk</td>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor AND that our IT org is prepared to mitigate and manage risk</td>
</tr>
<tr>
<td>31%</td>
<td>27%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor BUT are having difficulty convincing other leaders, ultimately limiting resources to address risk</td>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor BUT are having difficulty convincing other leaders, ultimately limiting resources to address risk</td>
</tr>
<tr>
<td>27%</td>
<td>27%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe risk is possible and as a result our IT org is beginning to develop mitigation strategies to address risk</td>
<td>Senior leaders/decision makers within my IT org believe risk is possible and as a result our IT org is beginning to develop mitigation strategies to address risk</td>
</tr>
<tr>
<td>17%</td>
<td>22%</td>
</tr>
<tr>
<td>Not sure</td>
<td>Not sure</td>
</tr>
<tr>
<td>14%</td>
<td>17%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe we are insulated against risk and so our IT org is NOT fully prepared to mitigate and manage risk</td>
<td>Senior leaders/decision makers within my IT org believe we are insulated against risk and so our IT org is NOT fully prepared to mitigate and manage risk</td>
</tr>
<tr>
<td>11%</td>
<td>8%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fig 18c - Mid-Size Business</th>
<th>Fig 18d - Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor AND that our IT org is prepared to mitigate and manage risk</td>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor AND that our IT org is prepared to mitigate and manage risk</td>
</tr>
<tr>
<td>31%</td>
<td>36%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor BUT are having difficulty convincing other leaders, ultimately limiting resources to address risk</td>
<td>Senior leaders/decision makers within my IT org believe it is not “if” but “when” our org will be impacted by a risk factor BUT are having difficulty convincing other leaders, ultimately limiting resources to address risk</td>
</tr>
<tr>
<td>29%</td>
<td>24%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe risk is possible and as a result our IT org is beginning to develop mitigation strategies to address risk</td>
<td>Senior leaders/decision makers within my IT org believe risk is possible and as a result our IT org is beginning to develop mitigation strategies to address risk</td>
</tr>
<tr>
<td>16%</td>
<td>15%</td>
</tr>
<tr>
<td>Not sure</td>
<td>Not sure</td>
</tr>
<tr>
<td>13%</td>
<td>14%</td>
</tr>
<tr>
<td>Senior leaders/decision makers within my IT org believe we are insulated against risk and so our IT org is NOT fully prepared to mitigate and manage risk</td>
<td>Senior leaders/decision makers within my IT org believe we are insulated against risk and so our IT org is NOT fully prepared to mitigate and manage risk</td>
</tr>
<tr>
<td>11%</td>
<td>11%</td>
</tr>
</tbody>
</table>
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?