

STATE OF AFFAIRS:

Is Tech Meeting the Changing Needs of Business?

The COVID-19 pandemic has not only upended our daily lives but also changed the environment in which organizations operate. Business leaders have been exposed to certain shortcomings in their modus operandi as well as introduced to new challenges.

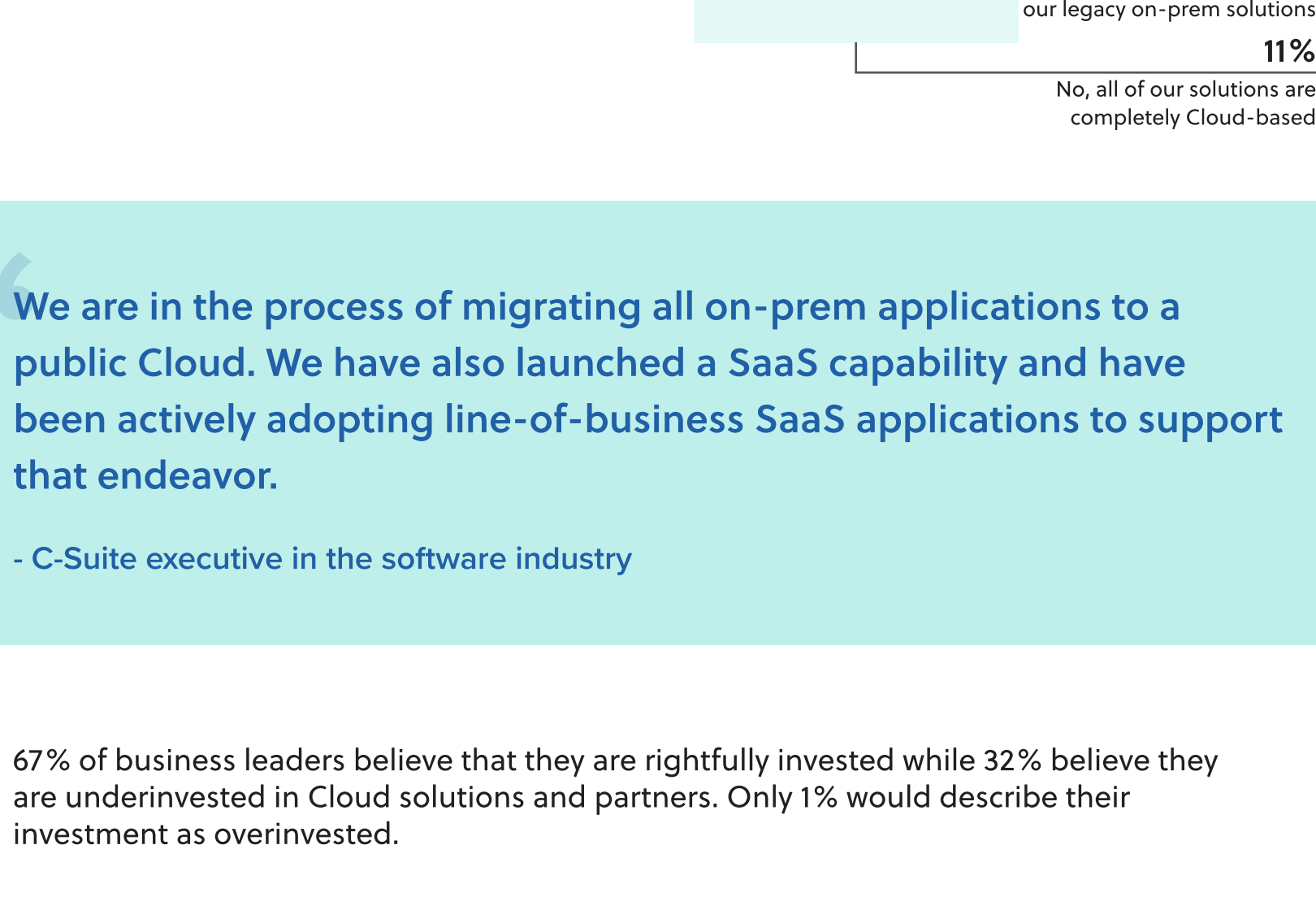
As many re-evaluate their priorities, business leaders are struggling to balance ongoing Cloud transformation projects, while waking up to the need for personalized remote workforce management and better cybersecurity solutions. **Pulse surveyed 100 business executives to understand how their priorities around technology solutions and the partners that deliver them are being shaped in light of the revolving door of problems served up by the global pandemic.**

Data collected from May 17 - June 16, 2021

Respondents: 100 business executives

The pandemic did not derail major Cloud implementation projects

23% of respondents revealed to have already purchased a Cloud solution in the past year with another 28% in the process of evaluating a Cloud solution. Meanwhile, 8% are sticking to their on-premises or legacy solutions.



“We are in the process of migrating all on-prem applications to a public Cloud. We have also launched a SaaS capability and have been actively adopting line-of-business SaaS applications to support that endeavor.”

- C-Suite executive in the software industry

67% of business leaders believe that they are rightfully invested while 32% believe they are underinvested in Cloud solutions and partners. Only 1% would describe their investment as overinvested.

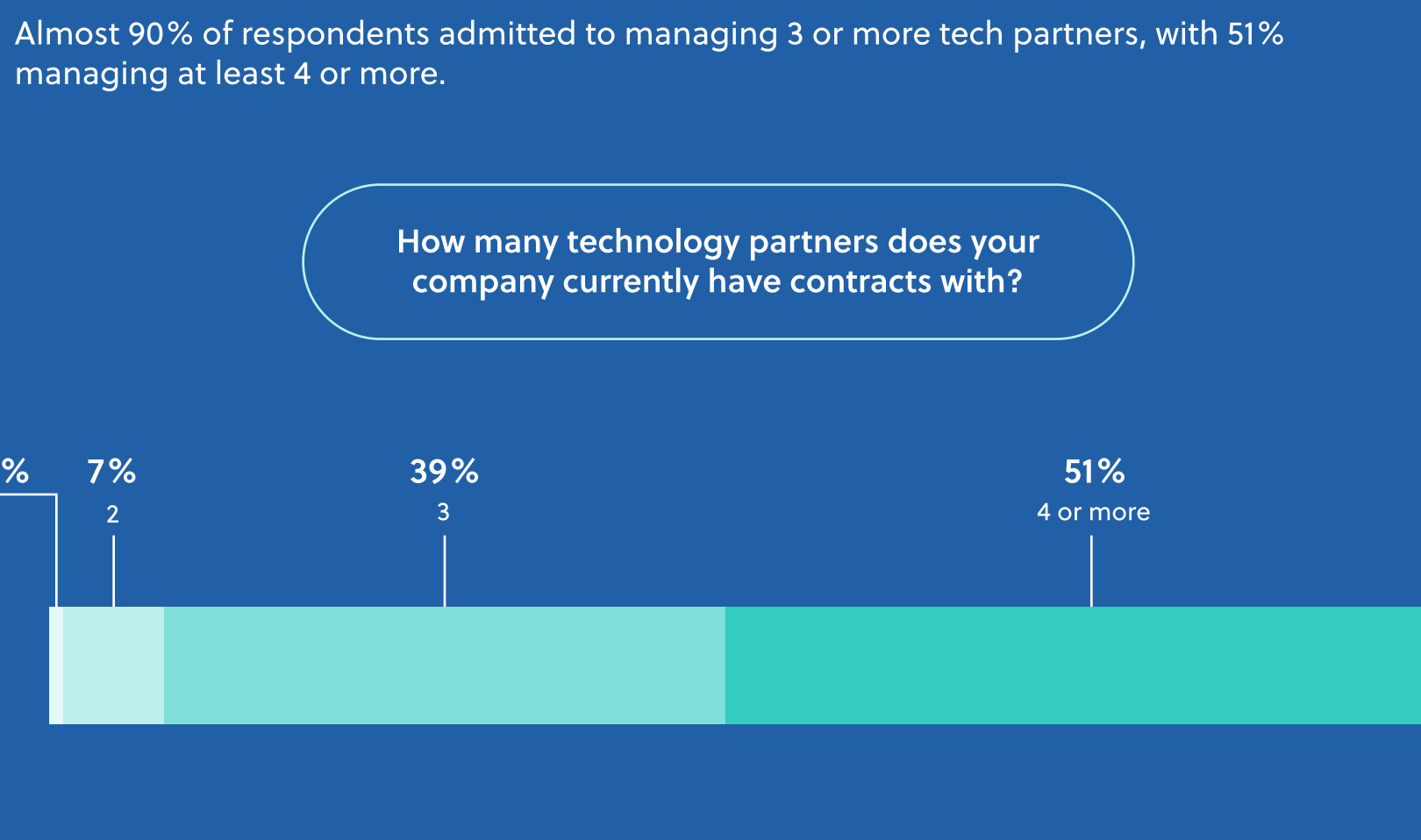


“We reduced costs on some items, and increased spending on solutions to weather the storm of the pandemic – such as Cloud solutions and tools to improve mobility and cybersecurity.”

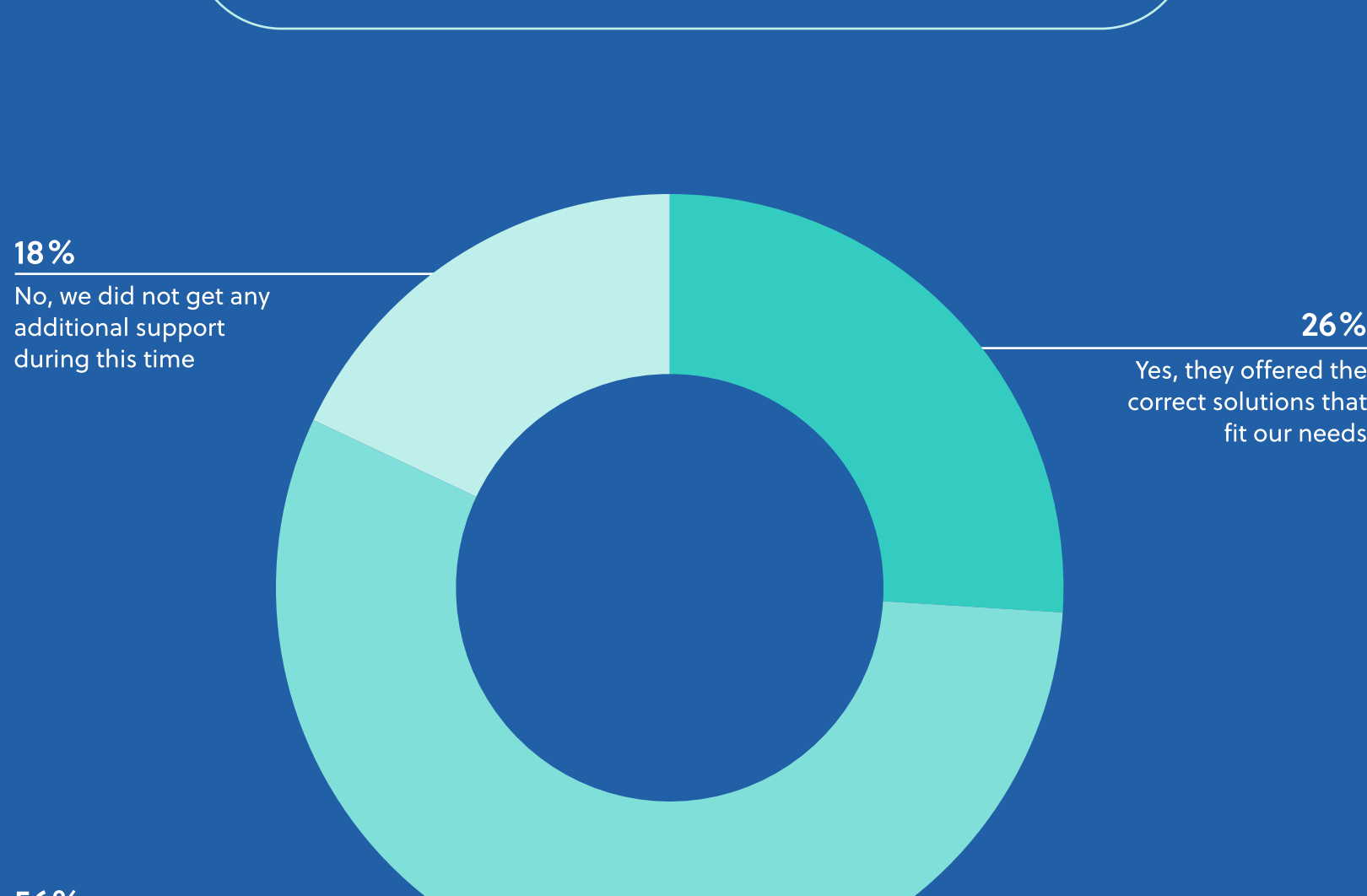
- VP in telecommunications industry

Executives are seeking greater personalization from their technology partners

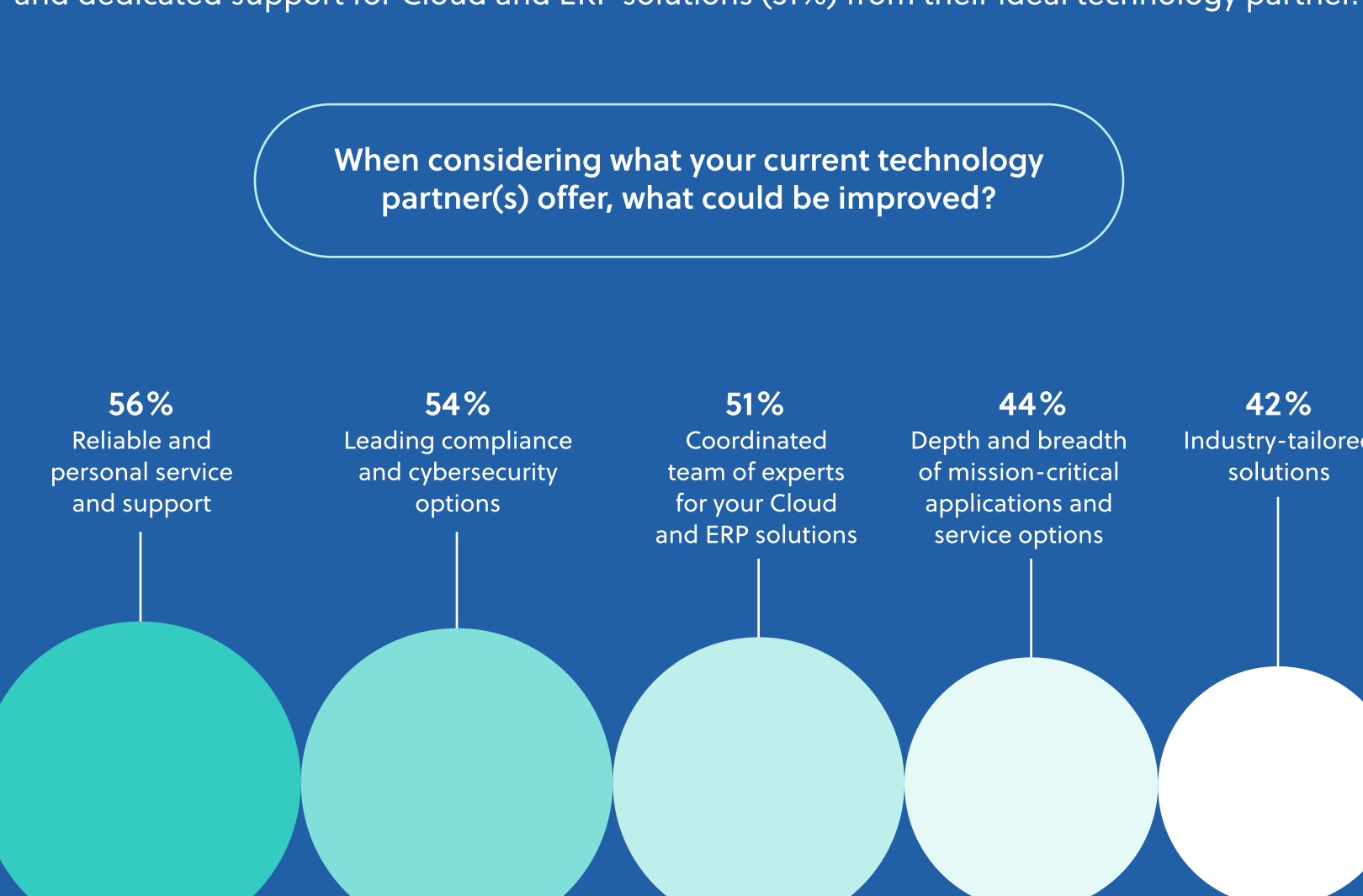
Although Cloud projects remained on course as the pandemic prevailed, business leaders faced continuity challenges supporting remote work. 87% of business executives have dealt with some form of stress trying to adapt and manage a dispersed workforce.



Almost 90% of respondents admitted to managing 3 or more tech partners, with 51% managing at least 4 or more.



Despite the relatively high number of tech partners at their disposal, 74% of business executives revealed their current technology partners were unable to support their remote work needs during the pandemic.

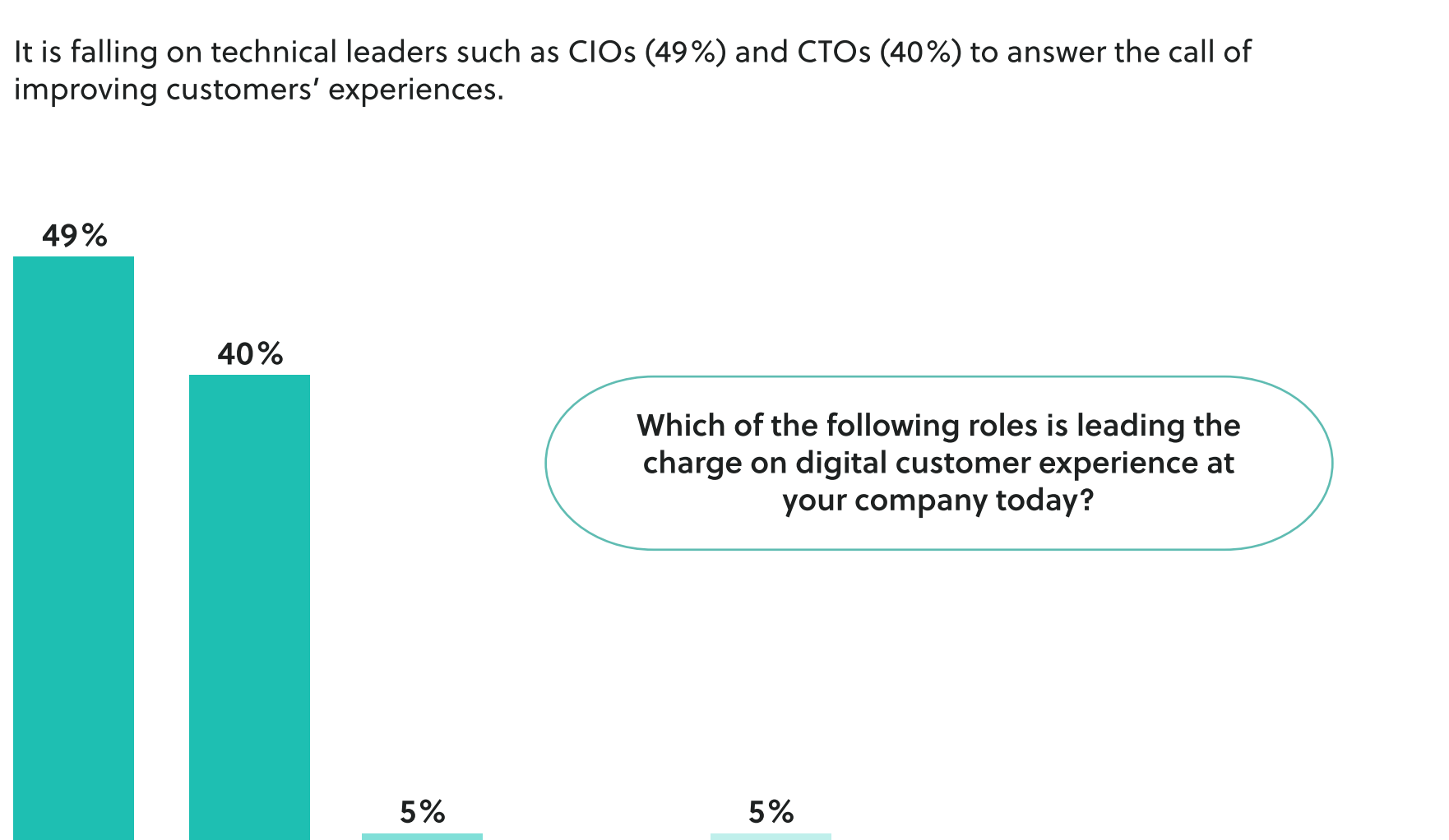


Business executives are seeking partners who can provide specialized attention to address unique business needs beyond remote workforce support. More than half desire greater reliability and personalized support (56%), options for compliance and cybersecurity (54%) and dedicated support for Cloud and ERP solutions (51%) from their ideal technology partner.

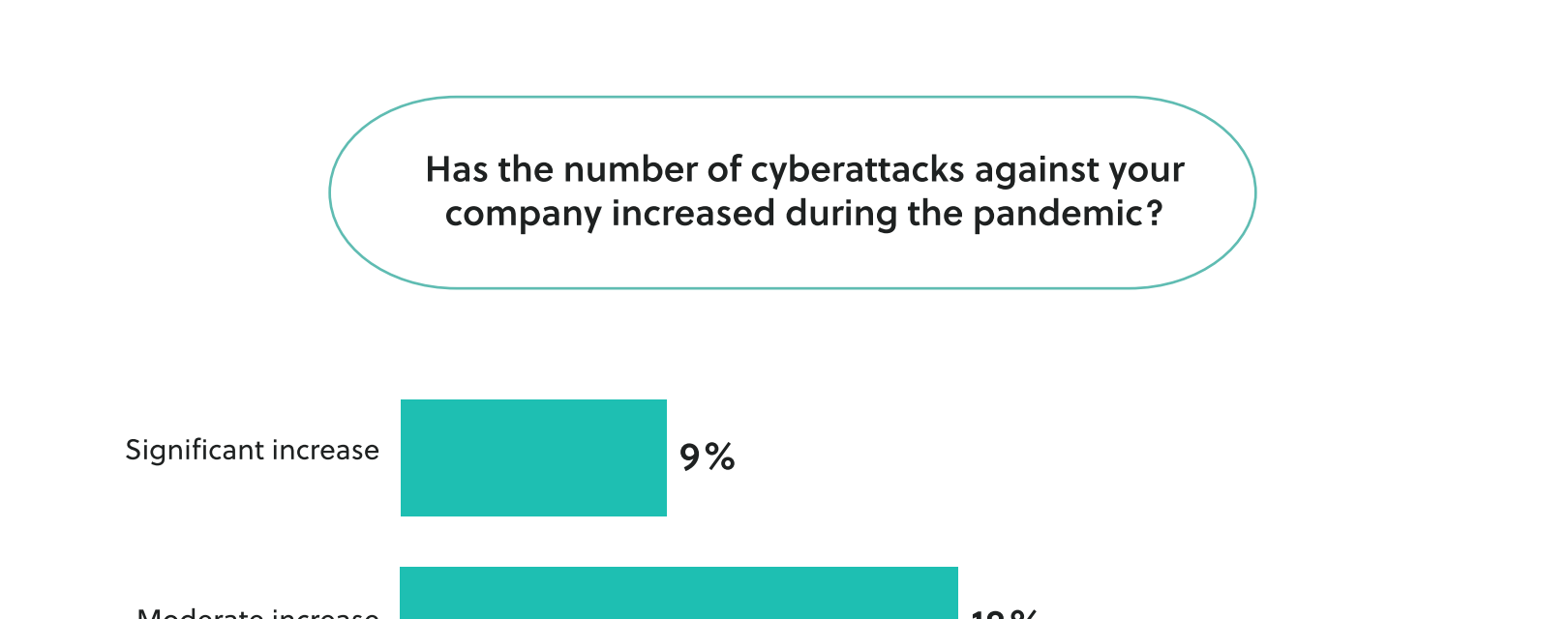


As their own businesses undergo digital transformation, executives are faced with new demands in customer experience and cybersecurity

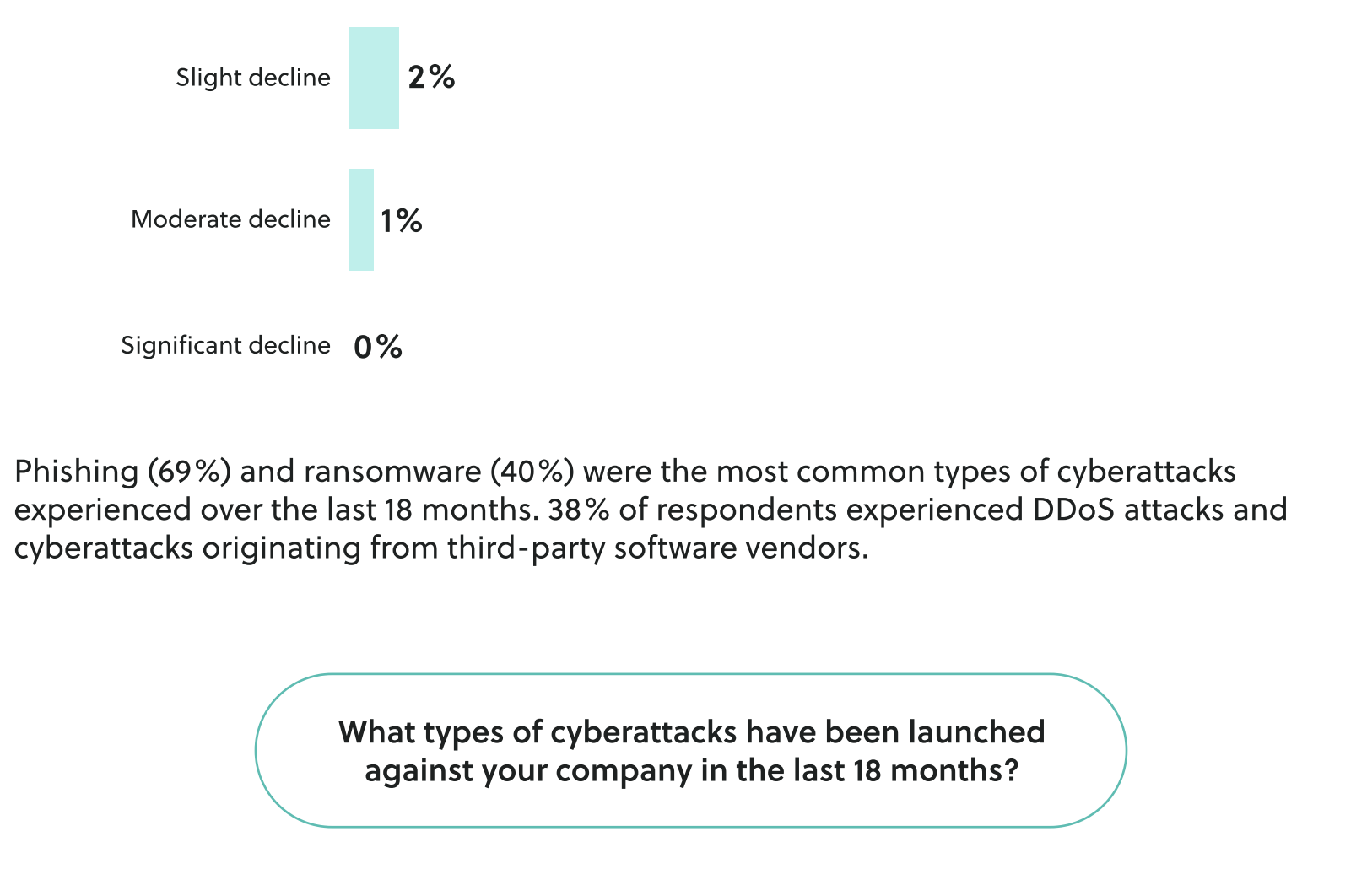
As businesses have become increasingly digital, customer experiences are being affected. For 35% of leaders, the most significant impact has been the importance of building an emotional connection between customer and brand, while 24% are seeing a major change in how online environments and communities have become part of the customer service ecosystem. In addition, 20% of leaders pointed out their customers' expectations for faster and more seamless multi-channel experiences.



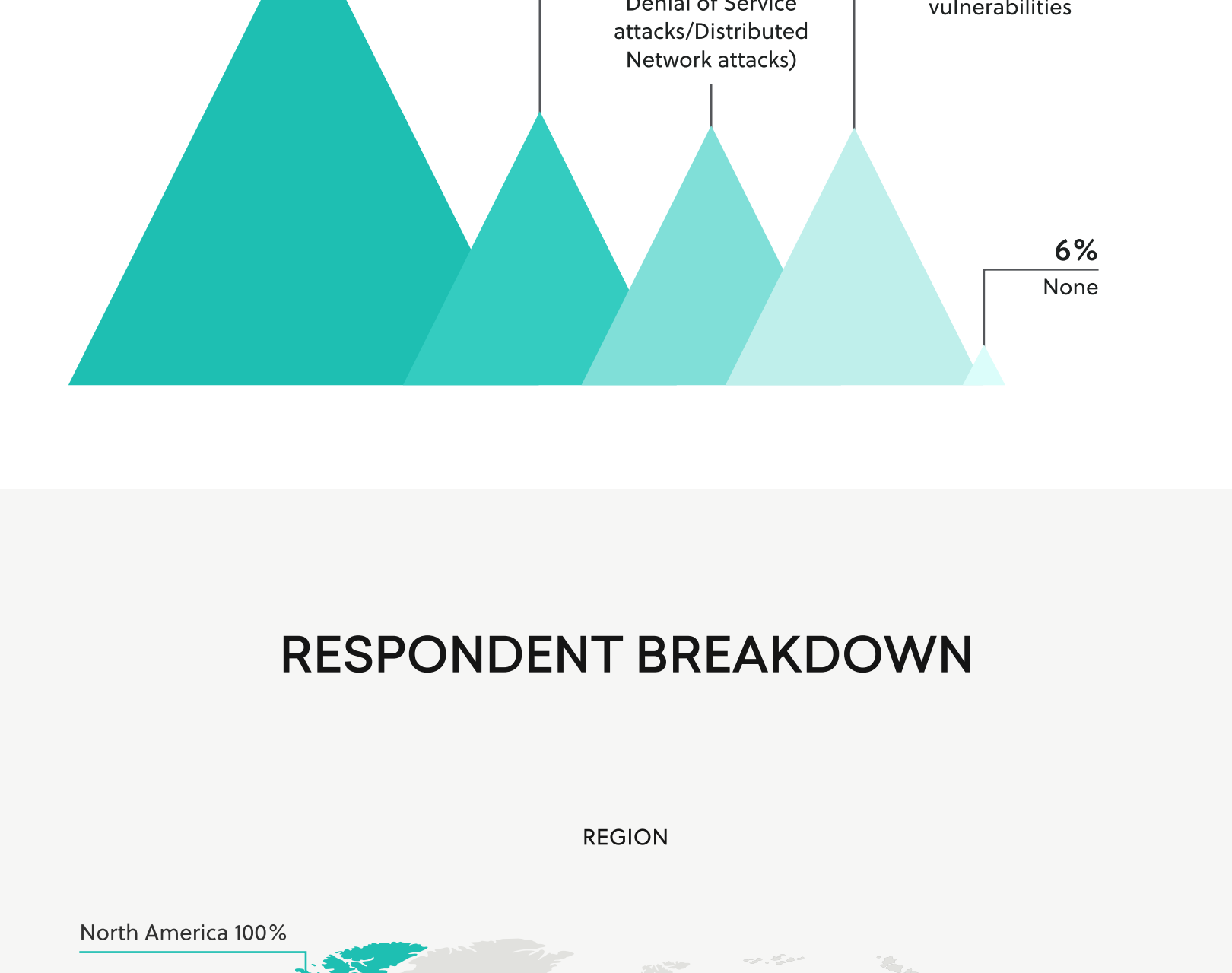
It is falling on technical leaders such as CIOs (49%) and CTOs (40%) to answer the call of improving customers' experiences.



The accelerated transition to digital experiences has also led to increased corporate cyberattacks for 62% of executives. Only 35% of leaders report no change in terms of cyber threats followed by a mere 3% reporting a decline.



Phishing (69%) and ransomware (40%) were the most common types of cyberattacks experienced over the last 18 months. 38% of respondents experienced DDoS attacks and cyberattacks originating from third-party software vendors.



RESPONDENT BREAKDOWN

