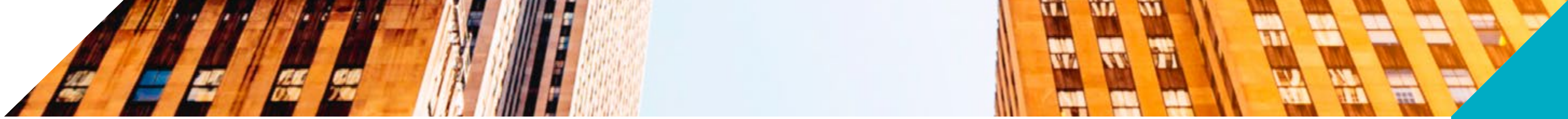
NC STATE Poole College of Management
Enterprise Risk Management Initiative

protiviti®
Face the Future with Confidence

EXECUTIVE PERSPECTIVES ON TOP RISKS 2019

Research Conducted by North Carolina State University's ERM Initiative and Protiviti

Key issues being discussed in the boardroom and C-suite



Introduction

Leaders of organizations in virtually every industry, size of organization and geographic location are reminded all too frequently that they operate in what appears to many to be an increasingly risky global landscape. Escalating concerns about the rapidly changing business environment and the potential for unwelcome surprises vividly illustrate the reality that organizations of all types face risks that can disrupt their business model over time and damage reputation almost overnight. The constantly evolving geopolitical landscape that is trending toward nationalism, ever-present concern of cyber disruptions, increasing market disruptions caused by born-digital organizations, effects of tightening labor markets, devastating impact of hurricanes and other natural disasters, volatility in energy prices, recurring shocks of terrorism around the globe, polarization of political viewpoints, the upward trajectory of interest rates, ease with which information can go viral via social media and other digital platforms, and ongoing negotiations to settle Brexit are a few of the drivers of uncertainty affecting the 2019 global business outlook. Insufficient focus on and attention to the web of complex enterprisewide risk events of varying velocity are likely to threaten an entity's brand, reputation, business model and, in some instances, its very survival. Boards of directors and executive management teams cannot afford to manage risks casually on a reactive basis, especially considering the rapid pace of disruptive innovation and technological developments in an ever-advancing digital world.

Protiviti and North Carolina State University's ERM Initiative are pleased to provide this report focusing on the top risks currently on the minds of global boards of directors and executives. This report contains results from our seventh annual risk survey of directors and executives to obtain their views on the extent to which a broad collection of risks is likely to affect their organizations over the next year.

Our respondent group, comprised primarily of board members and C-suite executives from all major regions of the world, provided their perspectives about the potential impact in 2019 of 30 specific risks across three dimensions:[1]

- **Macroeconomic risks** likely to affect their organization's growth opportunities
- **Strategic risks** the organization faces that may affect the validity of its strategy for pursuing growth opportunities
- **Operational risks** that might affect key operations of the organization in executing its strategy

[1] Two new risks were included in the 2019 survey. They replaced two risks we asked about in prior years. See Table 1 for a list of the 30 risks addressed in this study.

In presenting the results of our research, we begin with a brief description of our methodology and an executive summary of the results. Following this introduction, we discuss the overall risk concerns for 2019, including how they have changed from 2018 and 2017, followed by a review of results by size of organization and type of executive position, as well as a breakdown by industry, type of ownership structure (i.e., public company, privately held, not-for-profit and government), geographic location, and whether they have rated debt outstanding. We conclude with a discussion of organizations' plans to improve their capabilities for managing risk.

> "Looking forward, the message is that digital transformation is a main driver of risk impacting uncertainty over business model viability, customer preferences, the competitive landscape, workplace dynamics and the war for talent, and even regulatory demands. Clearly, organizations must align their culture, people, processes and intelligence gathering to embrace this rapidly changing business environment.
>
> — Pat Scott, Executive Vice President, Global Industry Program, Protiviti

Methodology

We are pleased that participation from executives was strong again this year. Globally, 825 board members and executives across a variety of industries participated in this survey. We are especially pleased that we received responses from individuals all over the world, with 371 respondents (45%) based in North America and 454 respondents (55%) based outside this region. In 2018, our responses by region were also 45% from North America and 55% of the organizations from other regions. We are pleased that this year's report reflects a more diverse geographic coverage from around the globe. As a result, this report again provides a perspective about risk issues on the minds of executives at a global level.

Our survey was conducted online in the fall of 2018. Each respondent was asked to rate 30 individual risk issues using a 10-point scale, where a score of 1 reflects "No Impact at All" and a score of 10 reflects "Extensive Impact" to their organization over the next year.

For each of the 30 risk issues, we computed the average score reported by all respondents. Using mean scores across respondents, we rank-ordered risks from highest to lowest impact. This approach enabled us to compare mean scores across the past three years to highlight changes in the perceived level of risk.

Consistent with our prior studies, we grouped all the risks based on their average scores into one of three classifications:

- Risks with an average score of **6.0 or higher** are classified as having a **"Significant Impact"** over the next 12 months.
- Risks with an average score of **4.5 through 5.99** are classified as having a **"Potential Impact"** over the next 12 months.
- Risks with an average score of 4.49 or lower are classified as having a **"Less Significant Impact"** over the next 12 months.

We refer to these risk classifications throughout our report, and we also review results for various subgroups (i.e., company size, position held by respondent, industry representation, organization type, geographic location and presence of rated debt). With respect to the various industries, we grouped related industries into combined industry groupings to facilitate analysis, consistent with our prior years' reports.

Table 1 on the next page lists the 30 risk issues rated by our respondents, arrayed across three categories — Macroeconomic, Strategic and Operational.

List of 30 Risk Issues Analyzed

TABLE 1

MACROECONOMIC RISK ISSUES

- Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address
- Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities
- Evolving changes in global trade policies may limit our ability to operate effectively and efficiently in international markets
- Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organization
- Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization
- Demands made by activist investors and other key stakeholders may significantly affect how we do business in the marketplace*
- Geopolitical shifts and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives
- Anticipated increases in labor costs may affect our opportunity to meet profitability targets
- Unexpected change in the current interest rate environment may have a significant effect on the organization's operations

* Represents a new risk issue added to the 2019 survey.

TABLE 1 (CONTINUED)

STRATEGIC RISK ISSUES

- Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model
- Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business
- Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered
- Shifts in environmental, social and governance (ESG) preferences as well as expectations of key stakeholders may be difficult for us to identify and address on a timely basis
- Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share
- Our organization may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation
- Growth through acquisitions, joint ventures and other partnership activities may be difficult to identify and implement
- Opportunities for organic growth through customer acquisition and/or enhancement may be significantly limited for our organization
- Substitute products and services may arise that affect the viability of our current business model and planned strategic initiatives
- Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base
- Performance vulnerabilities may trigger shareholder activism against our organization that may significantly impact our organization's strategic plan and vision

TABLE OF CONTENTS

TABLE 1 (CONTINUED)

OPERATIONAL RISK ISSUES

- The cultural behaviors and personal interactions with others exhibited by the organization's management team and other key representatives — as manifested through day-to-day decision-making, attitudes and conduct — may not be aligned with the long-term interests of shareholders, the board's risk appetite, compliance with laws and regulations, and/or the core values most accepted and rewarded by the marketplace*
- Uncertainty surrounding the viability of key suppliers, scarcity of supply, or stable supply prices may make it difficult to deliver our products or services at acceptable margins
- Risks arising from our reliance on outsourcing and strategic sourcing arrangements, IT vendor contracts, and other partnerships/joint ventures to achieve operational goals may prevent us from meeting organizational targets or impact our brand image
- Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets
- Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand
- Ensuring privacy/identity management and information security/system protection may require significant resources for us
- Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low-cost base for their operations, or established competitors with superior operations
- Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans
- Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations
- Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives

Executive Summary

Shifting cultural norms and expectations of accountability. Disruptive business models. Innovations triggered by emerging technologies. Changes in the geopolitical landscape. Negotiations surrounding Brexit. Shifting customer preferences and demographics. Natural disasters. Record lows in unemployment, tightening labor markets and escalating competition for specialized talent. Immigration challenges. Cyber breaches on a massive scale. Terrorism. Big data analytics. A strong U.S. dollar. These and a host of other significant risk drivers are all contributing to the risk dialogue happening today in boardrooms and executive suites.

Expectations of key stakeholders regarding the need for greater transparency about the nature and magnitude of risks undertaken in executing an organization's corporate strategy continue to be high. Pressures from boards, volatile markets, intensifying competition, demanding regulatory requirements, changing workplace dynamics, shifting customer preferences, uncertainty regarding catastrophic events and other dynamic forces are leading to increasing calls for management to design and implement effective risk management capabilities and response mechanisms to identify, assess and manage the organization's key risk exposures, with the intent of reducing them to an acceptable level.

TOP RISKS FOR 2019	
1.	Existing operations meeting performance expectations, competing against "born digital" firms
2.	Succession challenges and ability to attract and retain top talent
3.	Regulatory changes and regulatory scrutiny
4.	Cyber threats
5.	Resistance to change operations
6.	Rapid speed of disruptive innovations and new technologies
7.	Privacy/identity management and information security
8.	Inability to utilize analytics and big data
9.	Organization's culture may not sufficiently encourage timely identification and escalation of risk issues
10.	Sustaining customer loyalty and retention

One of the first questions an organization seeks to answer in risk management is, "What are our most critical risks?" The organization's answer to this question lays the foundation for management to respond with appropriate capabilities for managing these risks. This survey provides insights for 2019 from 825 respondents in C-suite and board positions in organizations around the globe. Here is a summary of the key findings:

KEY FINDINGS

01

Global business environment riskier in 2019 — Survey respondents indicate that the overall global business context is somewhat riskier in 2019 relative to the two prior years. Our prior year survey respondents only rated seven of the top 10 risks higher for 2018 relative to 2017; however, for 2019, respondents rated all of the top 10 risks higher for 2019 relative to 2018. A majority of respondents rated each of the top 10 risks as a "Significant Impact" risk, and eight of our top 10 risks had an overall average score exceeding 6.0 (on a 10-point scale), placing the profile of top risks as "Significant Impact" on an overall basis. Likewise, risk levels for nine of the top 10 risks in 2019 were higher than 2017. This suggests a potential shift in views about the riskiness of 2019 relative to the last two years.

02

Nature of uncertainty concerns varies across the world — These overarching views about uncertainty in the business environment seem to be global in reach, with respondents from six of the eight geographic regions of the world we examined agreeing that the overall magnitude and severity of risks are of a "Significant Impact" level for 2019. Except for North America-based organizations, respondents representing organizations in all other regions rate their top five risks at the "Significant Impact" level; in contrast, organizations in North America only rate two of their top five risks at that level. Organizations in Latin America/South America and in India indicate the highest level of concern about the magnitude and severity of risks for 2019.

03

Firms more likely to invest in risk management — Interestingly, respondents indicate that they are more likely to devote additional time or resources to risk identification and management over the next 12 months relative to their plans in the prior year, suggesting a greater desire to invest in strengthening risk management efforts. This is especially true for financial services organizations as well as the largest organizations (revenues greater than $10 billion) in our sample. Individuals serving on boards indicate the greatest desire to devote additional time or resources to risk management, perhaps to better inform their risk oversight processes. The overall reality of the riskiness of the global business environment continues to motivate boards and executives to renew their focus on effective risk oversight.

KEY FINDINGS (CONTINUED)

04

Notable shifts in the 2019 top 10 risks — There are noticeable shifts in what constitutes the top 10 risks for 2019 relative to last year. One risk jumped from the tenth position in the top 10 risks in 2018 to the number one spot for 2019: Concerns that existing operations and legacy IT infrastructure may not be able to meet performance expectations as well as competitors that are "born digital." Respondents in five of the six industry groups we examined selected that risk as a top five risk concern, and they rated it as a "Significant Impact" risk concern for 2019. One risk returned to the top 10 in 2019 after dropping off in the prior year. Respondents indicated their concerns about the increasing difficulty their organizations face in sustaining customer loyalty and retention in light of evolving customer preferences and demographic shifts in their customer base. This risk had appeared in the top 10 in our 2015, 2016 and 2017 reports. As in the prior year, seven of the top 10 risks represent operational risk concerns, while the remaining three top 10 risks represent strategic risk concerns. None of the macroeconomic risk concerns made the top 10 list of risks for 2019 for the overall sample.

05

Regulatory concerns persist, economic concerns vary across the globe — Interestingly, respondents (particularly in Europe) remain troubled over the threat of regulatory change and increased scrutiny, which has been a top 10 risk all seven years we have conducted this survey. But, for the first time, concerns about economic conditions fell out of the top 10 list of risks for 2019 for the overall survey. Despite that finding for the overall sample, respondents in Europe, Latin America/South America, the Middle East and Africa did include economic concerns as a top five risk concern for 2019. Perceptions of economic risks are like a swinging pendulum as perceptions can change quickly over a short period of time as new developments transpire (including after our survey period).

> These are challenging times as digital disruption, regulatory and economic uncertainties, and other issues are manifesting themselves across the global marketplace.
>
> — Andrew Clinton, Executive Vice President, International Operations, Protiviti

The list of top 10 global risks for 2019, along with their corresponding 2018 and 2017 scores, appears in Figure 1. With respect to the top five risks overall:

- **Existing operations and infrastructure unable to adjust to competitors "born digital" —** Overall, the top concern among respondents for 2019 relates to the ability of their organization — relative to their competitors — to adjust existing operations to meet performance expectations. That risk concern raced from the number 10 position in the top 10 list of risks for 2018 to the number one position for 2019. This concern may be a composite of several significant uncertainties — the company's digital readiness, its lack of resiliency and agility in staying ahead of or keeping pace with changing market realities, the restrictive burden of significant technical debt, the lack of out-of-the-box thinking about the business model and fundamental assumptions underlying the strategy, and the existence or threat of more nimble competitors. Hyperscalability of digital business models and lack of entry barriers enable new competitors to emerge and scale very quickly in redefining the customer experience, making it difficult for incumbents to see it coming at all, much less react in a timely manner to preserve customer loyalty. In this environment, established incumbents are leery of "born digital" players that can alter the game by operating more efficiently, digitizing new products and services, enhancing the customer experience, and/or transforming the business model. This risk was a

> "Digital transformation is a mindset. It is often said that organizations need to disrupt or be disrupted. Digital technologies make possible continuous evolution at pace and present opportunities for more fundamental and sudden change. The latest technology presents opportunities to rethink business models and to drive efficiencies and improve performance in core operations. To take advantage of these disruptive forces, as well as increase the likelihood that organizations spot them timely, they must learn to act and think digitally and be capable of executing digitally.
>
> — Jonathan Wyatt, Managing Director, Global Leader, Protiviti Digital

concern for all four size categories of organizations in our sample, except for the smallest organizations. For most large companies today, it's not a question of *if* digital will upend their business but *when*. Even when executives are aware of emerging technologies that obviously have disruptive potential, it is often difficult to clarify the vision or foresight that anticipates the nature and extent of change — particularly if the organization does not think or act digitally at its core.

- **Succession challenges and talent acquisition and retention —** The risk of succession challenges and the ability to attract and retain talent moved into the top five list of risks for 2019, likely triggered by a continued tightening labor market as unemployment in the United States hit the lowest jobless rate since 1969, as well as the growing gig economy.

To thrive in the digital age, organizations need to think and act digitally and have the capabilities to execute digital plans. This vital specialized knowledge and subject-matter expertise are becoming harder to acquire and retain on a cost-effective basis. What's at stake is sustaining the workforce with the requisite talent and skills needed to think out of the box in a rapidly changing digital marketplace, execute high-performance business models, and implement increasingly demanding growth strategies. The flip side is that talented people aspire to be a contributor in a contemporary, dynamic, digitally focused business with its best days ahead of it, rather than to be bound to a more mature company that is not capably structured to be innovative and dynamic even though it may have a strategy that asserts it will be. Respondents continue to perceive that significant operational challenges may arise if organizations are unable to sustain a workforce with the skills needed to implement their growth strategies.

- **Regulatory change and heightened regulatory scrutiny —** This risk continues to represent a major source of uncertainty among the majority of organizations. Sixty-nine percent of our respondents rated this risk as a "Significant Impact" risk. This risk dropped to the fourth risk in 2018 after having been in our top two risk concerns all prior years we have conducted this survey. However, concerns about regulatory change and increased regulatory scrutiny moved up one position for 2019, suggesting that respondents remain concerned about potential regulatory influences disrupting how they do business. While declining in significance in North America, regulatory concerns were rated a top five risk in both Europe and Asia Pacific (Asia and Australia/New Zealand). Perhaps the uncertainties over Brexit were top of mind for respondents from Europe. Political gridlock and checks and balances remaining present in governing institutions continue to be on the minds of respondents.

- **Managing cyber threats —** Threats related to cybersecurity are of major concern as respondents focus on how such events might interrupt core operations. It is no surprise that this risk continues to be one of the most significant operational risks overall and it is a top five risk for each of the four size categories of organizations, except for the very largest organizations, as well as for four of the six industry groups we examine. There are two categories of companies — those that have been breached and know it and those that have been breached but don't know it yet. Cybersecurity is a moving target as innovative digital transformation initiatives, cloud computing adoption, mobile device usage, machine learning and other applications of exponential increases in computing power continue to outpace the security protections companies have in place. Increasingly sophisticated attacks on the human perimeter by perpetrators of cybercrime add to the uncertainty.
- **Resistance to change —** Enabling change continues to be a significant priority for just about every organization on the planet, for change has become a way of life for most companies. Whether covert or overt, resistance to necessary change spawned by disruptive innovations that alter business fundamentals can be lethal. Strategic error in the digital economy can result in the ultimate price if a company continues to play a losing hand in the marketplace. Coupled with concerns about the inability to adjust existing operations and IT infrastructure to compete with more nimble competitors, respondents also highlighted a cultural concern related to overall resistance to change within their organizations. As major business model disruptors emerge, respondents are growing even more focused on the organization's potential unwillingness or inability to make necessary timely adjustments to the business model and core operations that might be needed to respond to changes in the overall business environment and industry.

TABLE OF CONTENTS

Top 10 Risks for 2019

FIGURE 1

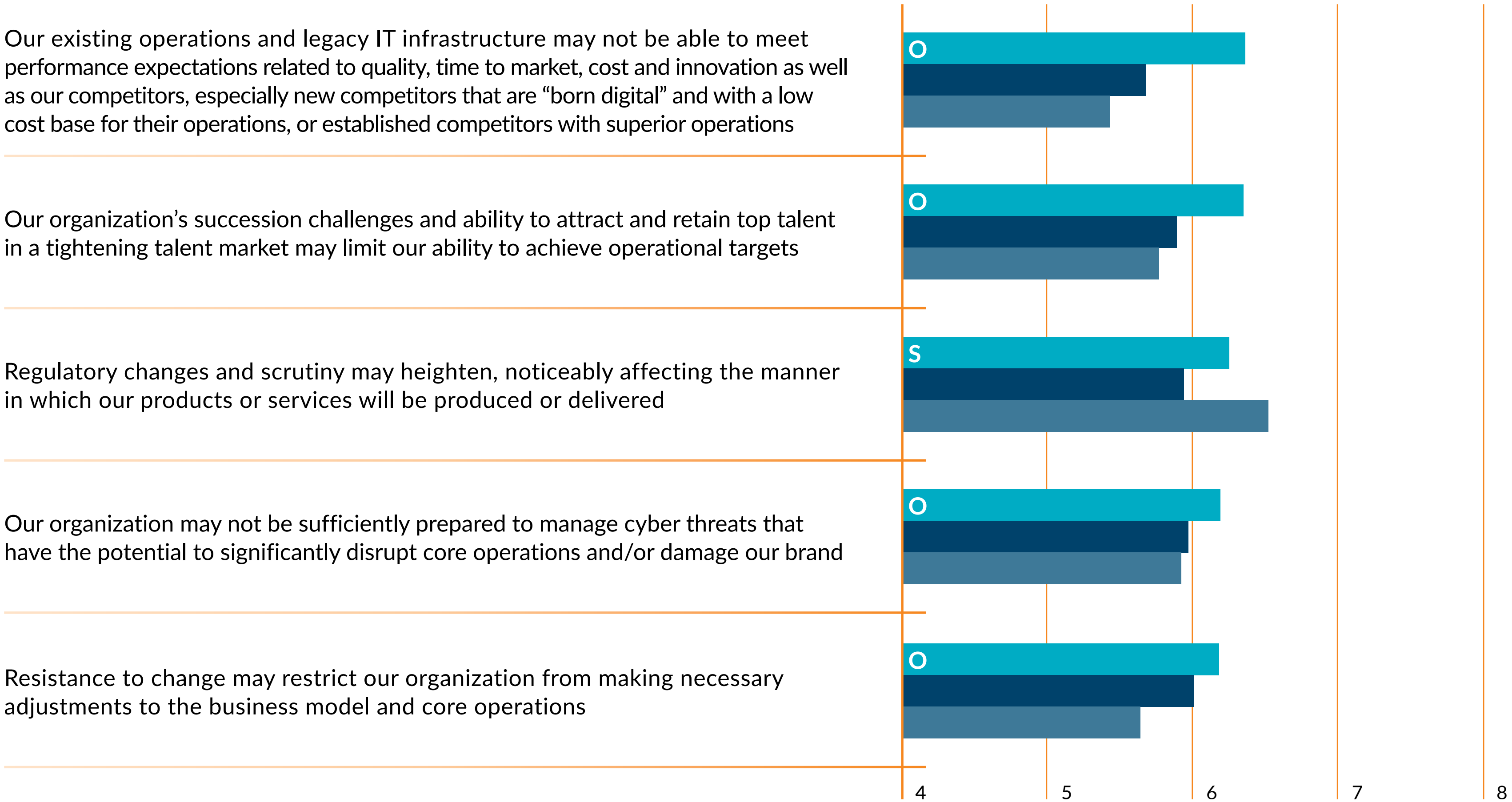
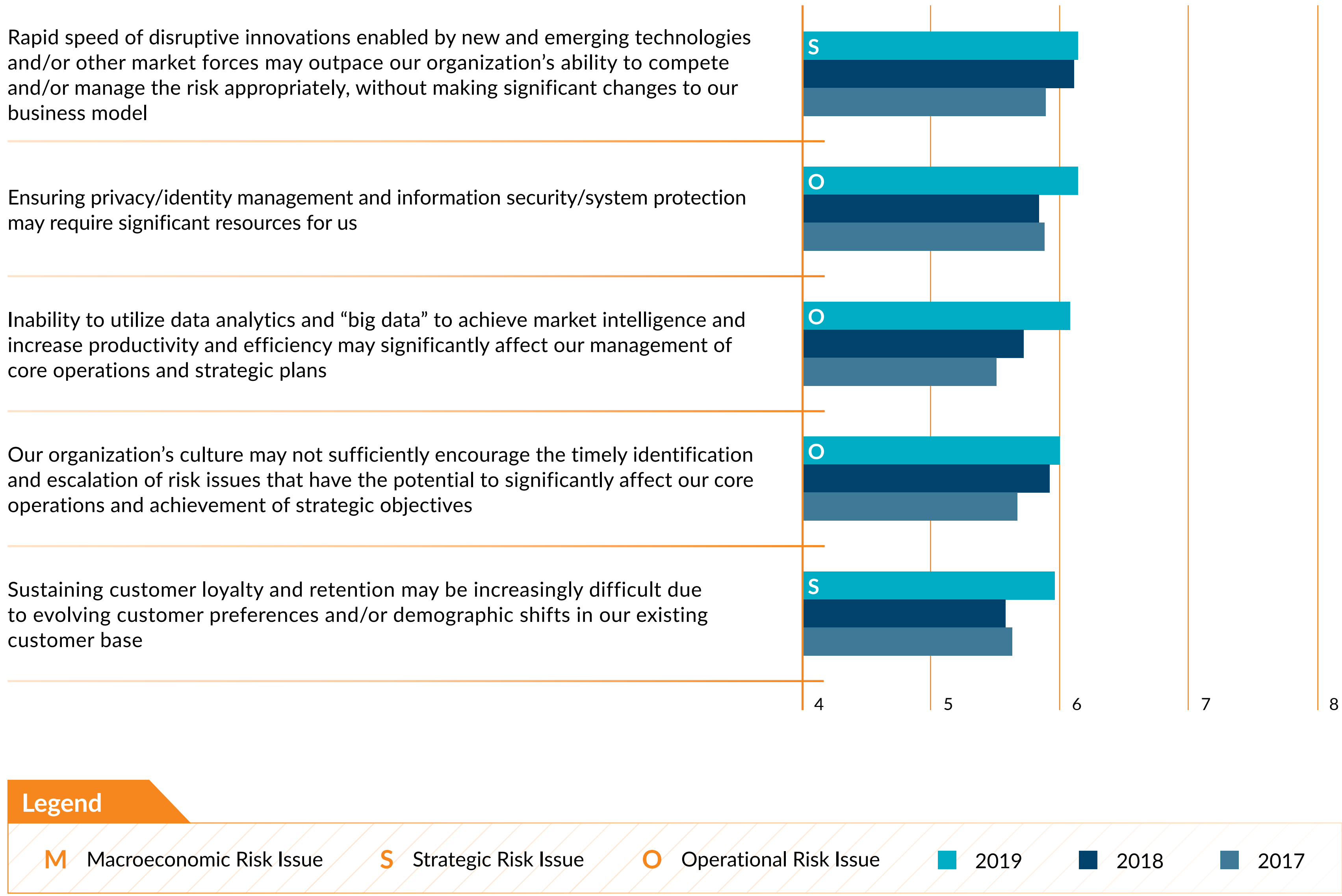


TABLE OF CONTENTS

FIGURE 1 (CONTINUED)



In addition to providing a summary of the overall risk findings across the entire set of 825 respondents, we also provide sub-analyses to compare risk perspectives across respondents from different sized organizations, different C-suite and board positions, industry groupings, and geographic location of the entity, among other groups. Some of the most notable key findings from that sub-analysis include the following:

- **Executives have differing views about the magnitude and severity of risks expected in the coming year —** There is variation in views among boards and C-suite executives regarding the magnitude and severity of risks for 2019 relative to prior years. Interestingly, board members report the highest overall score about their impression regarding the magnitude and severity of risk for 2019 relative to CEOs, CFOs and CROs. Out of the 30 risks examined, board members rate 26 of the 30 risks as "Significant Impact" risks. In contrast, CEOs only rated six of the 30 risks at that level. So board members seem to be substantially more concerned about risks than the C-suite. However, when comparing overall scores for magnitude and severity of risks for 2019 to 2018, the most noticeable increase in risk scores among specific executive groups (other than the "Other C-Suite" group) was for CEOs, suggesting that CEOs perceive a noticeable upward shift in risks for 2019 relative to 2018. In fact, in the prior year, CEOs did not rate any of the 30 risks as "Significant Impact" risks, while for 2019 they rated six of 30 risks at that level. These findings suggest there is a strong need for discussion and dialogue to ensure everyone is in agreement at the highest level of the organization as to what the most important risk exposures are and whether the organization is focused on them appropriately.

- **Dominance of concern about operational capabilities —** Respondents are noticeably focused on risks related to their organization's infrastructure and core operations. Advancements in technologies, the ability for organizations that were "born digital" to quickly adjust to market conditions faster than larger, more established organizations, and threats to their IT systems and concerns about ensuring the privacy of data in those systems are creating challenges for organizational leaders to manage. Seven of the top 10 risks for the full sample reflect operational risks, with the remaining three risks related to strategic risk concerns. The dominance of concern related to the capabilities of the operations, systems, personnel and infrastructure from within the organization is overshadowing risks on the horizon driven by external factors. While the strength of the overall economy is fueling growth, in some organizations that growth may be outpacing the entity's investment in strengthening core operations. These concerns are consistent across all four size categories of organizations we examined. In fact, in all size categories except the very largest organizations, four of the top five risk issues reflect operational risk concerns. For the very largest organizations, three of the top five risk concerns are of an operational risk nature.

- **Risks vary noticeably across different regions of the world —** While organizations operate in a global business environment, the risks that they may face can differ widely across different geographic regions. This year we are able to analyze the results across eight different regions of the world. That analysis finds that the nature of risks varies significantly depending on geography. Respondents in Latin America/South America and in India-based operations rated the magnitude and severity of risks for 2019 at the highest levels. And, the nature of risks differs across the regions, with five of the eight regions mostly concerned about operational risks, while the remaining three regions are most concerned about macroeconomic risks. In particular, respondents in Europe, Latin America/South America, the Middle East and Africa rated risks related to economic conditions in the top five list of risks. As organizations explore doing business in different parts of the globe, it will be important for them to understand how risks may differ depending on where those operations are based.

- **Concerns about cyber risks and succession planning and talent acquisition/retention are very common —** Most organizations, except those in the largest size category, identified concerns about their organization's ability to manage cyber threats and the related potential for reputation damage as a top five risk concern. As organizations continue to embrace the benefits of technology, automation and digital transformation, it is likely that this concern will remain high for years to come. In fact, cyber concerns have been in the top 10 list of risks all seven years that we have conducted this survey. Succession challenges and the ability to attract and retain top talent appears in the top five list of risks for all four organizational size categories we examine. Record low unemployment and the tightening labor market are creating challenges for organizations to scale their operations as demand continues to grow in the current strong economy. Interestingly, risks related to cyber and succession planning were deemed as "Significant Risks" by all C-suite positions, including board members, for 2019. Clearly, both are top of mind issues.

- **Most industries sense a heightened risk concern for 2019 —** Our sub-analyses of results across six different industry groups finds that every group, with the exception of the Technology, Media and Telecommunications industry group, perceived that the magnitude and severity of risks affecting their organizations are greater in 2019 than in the prior year. The Healthcare and Life Sciences industry group reflects the highest overall concern related to the magnitude and severity of risks. Not surprisingly, cyber risk is rated as a "Significant Impact" risk concern across all six industry groups we examined. That risk is the only one of the 30 risks identified at that level for all industries. All of the top five risks increased over 2018 for each of the industry groups, with the exception of two of the top five risks for the Energy and Utilities industry group and one of the top five risks for the Technology, Media and Telecommunications industry group.

Table 2 lists the top 10 risks with the percentage responses for the three risk classifications (Significant Impact, Potential Impact, Less Significant Impact) we employ in this report.

Top 10 Risks (With Percentages of Responses by "Impact" Level)[2]

TABLE 2

RISK DESCRIPTION	Significant Impact (6 — 10)	Potential Impact (5)	Less Significant Impact (1 — 4)
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low-cost base for their operations, or established competitors with superior operations	71%	12%	17%
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets	71%	11%	18%
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered	69%	11%	20%
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand	68%	12%	20%

[2] The risks presented in Table 2 are in the same top 10 risk order as reported in Figure 1. That list is based on each risk's overall average score (using our 10-point scale). Table 2 merely reflects the percentage of respondents selecting a particular point on the 10-point scale. For example, 71% of respondents selected either "6," "7," "8," "9" or "10" as their response (using our 10-point scale) for the risk related to the organization's existing operations and legacy IT infrastructure, whereas only 69% of respondents chose one of those responses for the risk related to regulatory change and scrutiny.

TABLE 2 (CONTINUED)

RISK DESCRIPTION (CONTINUED)	Significant Impact (6 — 10)	Potential Impact (5)	Less Significant Impact (1 — 4)
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations	68%	11%	21%
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model	68%	11%	21%
Ensuring privacy/identity management and information security/system protection may require significant resources for us	66%	12%	22%
Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans	66%	12%	22%
Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives	65%	11%	24%
Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base	65%	13%	22%

In addition to our Key Findings, other notable findings this year regarding those risks making the top 10 include the following:

- **Rapid speed of disruptive innovation —** This strategic risk soared to the top for 2018 and it remains a top 10 concern for 2019. Sixty-eight percent of our respondents rated this risk as a "Significant Impact" risk for 2019. This top risk reflects respondent concerns regarding the specter of disruptive innovation or new technologies outpacing an organization's ability to keep up and remain competitive. With advancements in digital technologies and rapidly changing business models, respondents are focused on whether their organizations are agile enough to respond to sudden developments that alter customer expectations and change their core business model. This risk is especially a concern for board members, CEOs and CROs, with these groups of respondents rating it as a top five risk concern.
- **Privacy and identity management —** Concerns related to privacy and identity protection continue to be among the top 10 risk concerns for 2019. The presence of this risk in the top 10 is somewhat expected given the increasing number of reports of hacking and other forms of cyber intrusion that compromise sensitive customer and personal information. Two-thirds of our respondents rated this risk as "Significant Impact" for their organization. This concern is likely linked to the proliferation of legislation to protect the privacy of personal information. Initiated in the European Union and spreading to the United States and elsewhere, that legislation has created enormous complexities for business with the teeth of potential fines, penalties and reputation loss that cannot be ignored. As the expanding digital economy enables businesses and third-party organizations to house sensitive information obtained in many ways, fresh exposures to that information and identity theft present themselves.
- **Inability to use big data and data analytics —** There is continued concern among respondents about their ability to utilize data analytics and big data to achieve competitive advantage and to manage operations and strategic plans. They sense that other organizations may be able to capture intelligence that allows them to be nimbler and more responsive to market shifts and changing customer preferences. In the digital age, knowledge wins and advanced analytics is the key to unlocking the gate to insights that can differentiate in the market.
- **Culture may not encourage timely escalation of risk issues —** Interestingly, respondents continue to highlight the need for attention to be given to the overall culture of the organization to ensure it is sufficient to encourage the timely identification and escalation of risk issues. This risk issue was added to our 2015 risk survey, and it has been ranked in the top 10 risks each year since then. Sixty-five percent of respondents rated this risk as a "Significant Impact" risk. The effectiveness of formal and ad hoc upward communications processes is of vital importance to keeping an organization's leaders in touch with business realities. Coupled with concerns over resistance to change, the presence of this risk reflects on the state of the organization's culture.

- **Sustaining customer loyalty and retention may be becoming increasingly difficult —** Concern about the organization's ability to sustain its existing customer base considering changing demographics made the top 10 list of risks for 2019 after dropping out of the top 10 in 2018. This risk is important because companies with high churn rates incur significant costs in replacing lost customers. Sustaining customer loyalty and retention is about increasing profitability through superior top-line performance and reduced marketing costs and other costs associated with educating new customers. Younger generations who have grown up in a technology-centric world are rapidly embracing digital technologies that are transforming all kinds of ways organizations have historically delivered their products and services. The growing presence of app-based platforms, digital marketing and other online ordering delivery services is shocking many of the traditional forms of customer interactions. If organizations cannot adjust their operations and legacy IT infrastructures (see risk #1 in the top 10 list), they may not meet the expectations of their core customers in a manner sufficient to retain their loyalty.

Additional insights about the overall risk environment for 2019 can be gleaned from these analyses, which we highlight in a number of charts and tables later in this report. Following are some additional significant findings:

> One of the most surprising findings this year was the complete absence of macroeconomic risk concerns in the top 10 for 2019. Concerns over economic conditions have been highly ranked in all six prior years of our survey, but that perception has shifted in a substantial way looking forward to 2019. However, as we note, economic concerns do exist in certain areas around the world, including Europe.
>
> — Mark Beasley, Professor of Enterprise Risk Management and Director of the ERM Initiative, Poole College of Management, NC State University

- **Less concern about macroeconomic risk issues for most, but with some exceptions —** Interestingly, respondents are not as concerned about economic conditions in domestic and international markets relative to prior years. In the six prior years we have conducted this study, economic concerns were rated high, placing this risk near or at the top of our top 10 risks in most years. Last year, economic concern dropped several positions and for 2019 that concern did not make the top 10 list of risks overall. In fact, no macroeconomic risk made the overall top 10 list of risks for 2019 and no macroeconomic risk made the top five risk concerns for each of the four organization size categories we examine. This suggests that respondents seem more positive about macroeconomic issues for 2019 relative to the past several years. However, it is important to note that concerns about the economy are in the top five list of risks for certain regions of the world, including Europe, Latin America/South America, the Middle East and Africa.

- **Risks differ widely depending on region of the world —** In addition to receiving 371 responses from individuals in organizations headquartered in North America, this year we were fortunate to also receive 454 responses from individuals in other parts of the world. This allows us to provide more detailed analyses of responses across different regions of the world than we have been able to do in prior year surveys. This year we provide a detailed breakdown of the results across eight different geographic regions. It is interesting to note the differences in viewpoints about risks for 2019 between organizations located in North America and those from the rest of the world. For North American respondents, only two of their top five risks were rated as "Significant Impact" risks for 2019; however, for every other region of the world, all of the top five risks in each region were rated as "Significant Impact" risks. Similarly, when asked about their views regarding the overall magnitude and severity of risks for 2019, respondents from organizations located in North America had the lowest score (tied with respondents from Africa). Respondents from Latin America/South America and India had the highest concern about the magnitude and severity of risks for 2019. There are some consistencies in risk concerns across certain regions of the world. For example, respondents in North America, Europe, Australia/New Zealand and Asia are all concerned about their organizations' existing operations and legacy IT infrastructure, succession and talent acquisition/retention challenges, and exposure to regulatory change. In contrast, respondents in the Middle East and India are concerned about geopolitical shifts and instability in governmental regimes. Those same respondents, in addition to those from organizations in Africa, selected macroeconomic risk concerns as the majority of their top five risk issues for 2019.

- **Most risks are higher for 2019 —** We added two new risks to our list of 30 risks for 2019. Out of the 28 risks that we also examined in the prior year, all but three of the risks increased in score for 2019 relative to 2018. Three of the top five risks with the greatest increase in risk ratings from 2018 relate to operational risk concerns. Interestingly, two of those risks made the top 10 list of risks — concerns about existing operations and legacy IT infrastructure and concerns about succession and talent acquisition/retention challenges. While concern over risks related to outsourcing and other forms of joint ventures and partnerships did not make the top 10 list of risks, that concern increased noticeably for 2019 from 2018 — indicating that this is a risk that is being watched more closely.

- **Concerns about ease of entrance of new competitors and shifts in consumer preferences affect most organizations —** All organizations signaled an increased concern about the ease of entrance of new competitors into the industry and marketplace for 2019. With advancements in technologies enabling improved operational efficiencies and the hyperscalability of business models to accommodate rapid growth, there are opportunities for organizations to enter new markets like never before. For example, new entrants can leverage technology in ways that avoid the costly investments in physical infrastructures that have traditionally provided the platform for offering products and services. Respondents are also increasingly concerned about their ability to identify and respond to unexpected shifts in social, environmental and other customer preferences. For certain demographic shifts, such as an aging population and increased urbanization, organizations are concerned that they may not recognize those and other shifts on a timely basis, or they are concerned that their existing business models may not be sustainable under new conditions.

- **Boards perceive a much riskier environment —** Surprisingly, board members, CEOs, chief risk officers, and other individuals in C-suite positions perceive that the magnitude and severity of risks may be higher for 2019 relative to 2018. Only CFOs, chief audit executives and chief information/technology officers sense a slightly less risky business environment for 2019 in comparison to prior years. These findings suggest that there are noticeable differences in viewpoints among board members and C-suite executives about the nature of the overall risk environment and the need to invest more time and resources in risk management for 2019. What is most striking is that board members are much more concerned about the overall magnitude and severity of risks relative to senior management. Board members ranked 26 of the 30 risks as "Significant Impact" risks. In contrast, CEOs ranked only six of the 30 risks at that level, while CFOs only ranked five at that level. These differences are more pronounced than in our prior year results. The top five risk concerns of board members and individuals representing the various C-suite positions are all "Significant Impact" risks. This contrasts with 2018, when none of the top five risks of CEOs were "Significant Impact" risks.

- **Boards see risks differently than the C-suite —** Board members are most concerned about the ease of entrance of competitors into the industry and marketplace. That represents their number one risk concern. None of the C-suite executives identified that as a top five risk concern for 2019. Board members are also concerned about the potential for increased regulatory scrutiny and change, while that did not make the top five list of risks for CEOs or CFOs. Of particular interest, they are concerned about economic conditions, as are CEOs. Respondents in most of the other C-suite positions did not include that concern as a top five risk issue, except for chief information/technology officers. These differences in views highlight the critical importance of boards and senior management engaging in robust conversations about the critical enterprise risks and emerging risks. It also suggests that board members may not be as fully engaged as management with the digital revolution and its implications to the companies they serve, creating greater uncertainty on their part with respect to these issues.

- **Bigger organizations perceive greater uncertainty —** The three largest size categories of organizations rated all of their top five risks as "Significant Impact" risks for 2019. The smallest organizations (those with revenues under $100 million) rated only one of their top five risks as "Significant Impact." Thus, the environment for most organizations appears to be risky, even though respondents from smaller organizations do not sense the same overall level of risk concern. Unease over operational risks is common among all sizes of organizations (although the specific operational risks differ), and concerns about those risks are generally higher for 2019 relative to 2018. These findings emphasize the reality that there is no "one size fits all" list of risk exposures across all organizations, warranting a careful assessment by each organization of its risk profile.
- **For-profit entities view risks differently than not-for-profit and governmental organizations —** Succession challenges and the ability to attract and retain talent is a top five risk concern for all types of organizational structures — publicly traded companies; private, for-profit entities; and non-profit organizations. For-profit entities — both publicly traded and privately held — are concerned about limitations they may face due to their existing operations and legacy IT infrastructure, changes in regulatory scrutiny, and the potential for disruptive innovations to rapidly emerge and disrupt their business models and core operations. Non-profit and governmental organizations face a different set of top risk issues. They are particularly concerned about an internal culture that may be resistant to change as well as about protecting the privacy and identity of sensitive information they possess within their organizations.

The remainder of this report includes our in-depth analysis of perceptions about specific risk concerns. We identify and discuss variances in the responses when viewed by organization size, type, industry and geography, as well as by respondent role. In addition, on page 121 we pose key questions as a call to action for board members and executive management to consider that can serve as a diagnostic to evaluate and improve their organization's risk assessment and management process.

Our plan is to continue conducting this risk survey annually so we can stay abreast of key risk issues on the minds of executives and observe trends in risk concerns over time.

Overall Risk Concerns for 2019

Before asking respondents to assess the importance of each of the 30 risks, we asked them to provide their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months. We provided them with a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive." The data above shows there appears to be a slightly higher concern about the overall risk environment relative to 2018 returning to the level observed two years ago.

	2019	2018	2017
Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	6.2	6.0	6.2

Figure 1 (shown earlier) summarizes the top 10 risks for 2019. Nine of the top 10 risk concerns for 2019 were also included in the top 10 list of risks for 2018. While respondents continue to be concerned about similar issues, the overall level of concern about each of the top 10 risks is higher than in 2018, signaling a consistently stronger concern about those same risk issues in 2019 relative to 2018. The 2019 average risk scores are also higher than those in 2017, except for one risk. These results suggest that there is an overall greater risk concern for 2019 relative to the prior two years. None of the top 10 risk issues for 2019 relates to macroeconomic concerns, while three relate to strategic risk issues. Thus, operational risks once again dominate the 2019 top 10 risk challenges.

For 2019, respondents are especially focused on the risks associated with the ability of their organizations to adjust their **existing operations and legacy IT infrastructures** to meet performance expectations of their key stakeholders. They are concerned that "born digital" competitors with a lower investment in brick-and-mortar infrastructure and capability to deploy hyperscalable business models that reduce dependence on human resources are more capable of transforming the customer experience and responding to rapidly changing market conditions. Further, the lower entry costs to enter some markets may allow new forms of competition to threaten more established, traditional businesses. While this risk made the top 10 list of risks in

2018, it was in the number 10 spot. This year, respondents rated this concern significantly higher, moving it to the number one position in the list of risks for 2019.

Succession planning and acquiring and retaining talent remains a top risk concern for 2019, moving up four positions to the number two spot for 2019. For the past six surveys, this risk has appeared in the list of top 10 risks. With changing demographics in the workplace due to an aging population and the increasing influence of millennials, record low unemployment, strong economic growth, increasingly demanding customers, increasingly sophisticated business models, and growing complexity in the global marketplace, organizations must up their game to acquire, develop and retain the right talent. Multiple trends are transforming the global talent landscape as well as creating the need for altering talent management strategies. These trends include globalization, digitalization, increasing mobility, worker shortfalls over the long term in many developed countries, and growing opportunities in emerging markets. To illustrate, digital technology raises the bar in the war for talent. To thrive in the digital age, organizations need to think and act digital and this requires a different set of capabilities, knowledge and skills. As boundaryless organizations expand their global reach, they must "think digital" as well as "think global" as they build the culturally aware, diverse and collaborative teams needed to be agile and resilient so they can innovate and face the future confidently. For example, companies in some industries must now access talent pools globally to obtain the specialized knowledge and technical know-how they need. The survey results likely indicate that executives recognize the need for talented people with the requisite knowledge, skills and core values to execute innovative and challenging growth strategies in a rapidly changing world. And such talent lacks abundance.

Anxiety continues over how **regulatory changes and heightened regulatory scrutiny** may affect the manner in which an organization's products and services are produced or delivered. This risk concern remains high on the top 10 risks list for 2019, consistent with what we have observed in all seven years we have conducted this study.

In four of the six prior risk surveys we have conducted, regulatory risk was the number one risk concern, falling to the number four position last year. This year, this risk increased by one position, suggesting an increasing concern about the impact of regulatory change relative to the other top 10 risks. While discussions among political leaders in the United States about reducing some of the regulatory burden may have provided some a sense that potential relief may be on the horizon, the impact on policy change as a result of the midterm elections in the United States and changing policies in Europe due to potential key leadership changes in Germany and the United Kingdom's anticipated settlement of its separation from the European Union may be creating some uncertainty about how all of those changes might impact regulations and government policies. This risk is included in the top five list of risks for all sizes of organizations except the smallest (those with revenues less than $100 million). Four of our six industry groups rated this risk as a "Significant Impact" risk (i.e., a risk with an average score of 6.0 or higher on our 10-point scale). The stakes are high since, without effective management of regulatory risks, organizations are reactive, at best, and noncompliant, at worst, with all of the attendant consequences.

It should come as no surprise to see that concerns about the risk of **cyber threats disrupting core operations** for organizations remained in the top five. Cyber risks have evolved into a moving target, with digitization advances, cloud computing adoption, mobile device usage, creative applications of exponential increases in computing power, and innovative digital transformation initiatives constantly outpacing the security protections companies have in place. Given publicity about data breaches, ransomware attacks and failures to patch known vulnerabilities, along with the growing presence of state-sponsored cyber terrorism and advanced persistent threats and their devastating drain on intellectual property and reputation, the stakes for effective cybersecurity spiral upward. As they do, more executives and directors are recognizing the need for "cyber resiliency." The old thinking of "it is not a matter of if a cyber risk event might occur, but more a matter of when it will occur" is dated. It's happening — now. For most companies, cyber risk events have already taken place and continue to take place, yet many companies do not have the detection and response capabilities they need to reduce the impact and frequency of such events. With the increasing sophistication of perpetrators and the significant impact of a breach, more organizations are recognizing that this risk is an enterprise security issue, not just an IT security issue.

> "Risks associated with heightened regulatory oversight and new limits on how organizations may conduct business have been front-of-mind in all seven years we have conducted this survey, never falling below the fourth highest-ranked risk. We have no doubt this will continue as we observe significant changes in governmental leadership around the globe.
>
> — Bruce Branson, Professor of Accounting, Associate Director, Enterprise Risk Management Initiative, Poole College of Management, NC State University

In addition to issues related to existing operations and legacy IT infrastructures impeding an organization's ability to respond to shifting market conditions, respondents also continue to indicate that **resistance to change** restricting necessary adjustments to their business model and core operations is a top 10 risk for 2019. In these uncertain times, it makes sense to enhance the organization's ability and discipline to act decisively on revisions to strategic and business plans in response to changing market realities, particularly in light of the potential for significant disruptive innovation. To that end, organizations committed to continuous improvement along with breakthrough, disruptive change and innovation to processes, products and services are more apt to be early movers in exploiting market opportunities and responding to emerging risks. The rules of the game are disrupt or be disrupted. Interestingly, this risk concern made the top five list of risks for all sizes of organizations, except for the largest category (i.e., revenues greater than $10 billion). This risk was rated as a "Significant Impact" risk by the largest organizations, but was rated eighth in their overall ranking. More importantly, board members and all members of the C-suite — except for CEOs — rated this as a "Significant Impact" risk for 2019.

Respondents continue to be concerned about the **rapid speed of disruptive innovations** and dramatic changes that new technologies may have in the marketplace. This risk concern is rated sixth in 2019, after rising significantly to the top risk concern in the prior year. Innovations in traditional forms of conducting business may quickly interrupt what has been a core way of doing business. If organizations are not proactively thinking about how they might respond, they may be too late to deal with the impact. Further complexity arises from the nature of innovative, market-changing organizations; these companies are built differently, not because they have a "digital strategy," but because they "think and behave digitally" in setting and executing strategy. With the accelerating speed of change and advancement of digital technologies, rapid response to changing market expectations is a significant competitive advantage for organizations that are nimble as an early mover and able to avoid bureaucratic "command and control" processes that slow down the ability to change in the face of market opportunities and emerging threats. This risk is a particular concern for board members and members of the C-suite, with all of them rating it as a "Significant Impact" risk for 2019, except for those in the CFO and CAE positions. It is also a top five risk issue for organizations in the Financial Services and the Technology, Media and Telecommunications industry groups.

Along with concerns about cyber threats are challenges related to **privacy/identity management and information security/system protection**. Technological innovation is a powerful source of disruptive change, and no one wants to be on the wrong side of it. Cloud computing, social media, mobile technologies and other initiatives to use technology as a source of innovation and an enabler to strengthen the customer experience present new challenges for managing privacy, information and system security risks. With the spread of the European Union data protection legislation requirements to the United States and elsewhere, the realities of this growing risk concern are highlighted by the continued coverage of hacking attacks exposing tremendous amounts of sensitive information involving a number of large companies, the federal government and high-profile political campaigns. The continued advances of technology disruptors in the form of digitization to harvest new sources of value through business model innovation require continued progress in maturing security and privacy capabilities across the enterprise. Achieving this maturation requires improved collaboration between IT and the core business as well as improvements to the human perimeter.

Respondents recognize the growing volume of data that may be available to them, but they are concerned that they may not have the **ability to utilize data analytics and "big data"** as effectively as others. Many are observing how some major players in the marketplace are leveraging knowledge gleaned from structured and unstructured data to improve operational efficiency and effectiveness and target products and services more sharply to the most appropriate market segments. Respondents are concerned that they may be falling behind some of their key competitors with these capabilities and that may limit their ability to manage core operations and strategic plans. This is particularly a concern for the largest organizations that included this risk concern as a top five risk issue for 2019. Those who serve as chief information officers also included this as one of their top five risk concerns.

Respondents expressed concern that their **organization's culture may not encourage the timely identification and escalation of risk issues** that might significantly affect core operations. Despite the recognition that there are several significant top risk concerns along operational, strategic and macroeconomic dimensions, there appears to be an overall lack of confidence that effective processes are in place for individuals to elevate risk issues to the leadership of the organization. The collective impact of the tone at the top, tone in the middle and tone at the bottom on risk management, compliance and responsible business behavior has a huge effect on timely escalation of risk issues. The timely identification and escalation of key risks is not easy, which is likely why this risk was ranked highly. Given the overall levels of risk impact scores for all risks in 2019, this cultural issue may be especially concerning to senior management and boards. Board members, CIOs/CTOs and Other C-Suite executives (see our position analysis section for how this group is defined) rated this risk as a "Significant Impact" risk for 2019.

A risk re-entering the top 10 list for 2019 relates to the concern that the organization may not be able to **sustain and retain customer loyalty** as existing customer preferences and demographics evolve. This risk was consistently a top 10 risk in 2015-2017 but did not appear in our 2018 ranking. Over time, as consumers become more accustomed and comfortable with emerging technologies, they are more likely to do business with organizations that leverage those technologies to better deliver products and services. This dynamic positions new competitors to lure loyal customers away from traditional businesses by appealing to their shifting preferences. Younger generations may be more willing to explore new options and innovations, and may be less inclined to remain loyal customers to a particular provider. This is particularly a concern for CEOs who rated this as their top risk concern for 2019, and the increase in their concern relative to 2018 is noticeable. Interestingly, they were the only executive category to include this risk in their top five risk concerns for 2019 and this reflects their focus on the top line.

We also compared the average scores for 2019 for the total population of 30 risks that we examined in 2018 to identify those risks with the largest changes in scores from 2018 to 2019. The five risks with the greatest increases in risk scores are shown in Table 3. Three of the five risks with the biggest year-over-year increases relate to operational risks. Among the increasing risk issues, respondents are concerned that competitors may enter their markets and as a result, they may also face difficulty in sustaining and retaining existing core customers.

The Five Risks with Highest Level of Increase

TABLE 3

RISK DESCRIPTION	Type of Risk	2019	2018	Increase
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low-cost base for their operations, or established competitors with superior operations	Operational	6.35	5.67	0.68
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets	Operational	6.34	5.88	0.46
Risks arising from our reliance on outsourcing and strategic sourcing arrangements, IT vendor contracts, and other partnerships/joint ventures to achieve operational goals may prevent us from meeting organizational targets or impact our brand image	Operational	5.70	5.29	0.41
Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share	Strategic	5.56	5.18	0.38
Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base	Strategic	5.95	5.57	0.38

We also examined those risks with the greatest reduction in risk impact scores from 2018 to 2019 (see Table 4). Note that only three risks actually decreased in magnitude in 2019. The final two risks are those with the smallest *increases* from 2018 to 2019. That highlights the overall heightened level of risk concern, given the overall risk scores of only three of the 30 risks we examined reflected a decrease between 2018 and 2019.

The Five Risks with Highest Level of Decrease (or Smallest Increase)

TABLE 4

RISK DESCRIPTION	Type of Risk	2019	2018	Decrease/ Smallest Increase
Shifts in environmental, social and governance (ESG) preferences as well as expectations of key stakeholders may be difficult for us to identify and address on a timely basis	Strategic	5.23	5.57	-0.34
Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities	Macroeconomic	5.12	5.45	-0.33
Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address	Macroeconomic	5.25	5.37	-0.12
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model	Strategic	6.13	6.10	0.03
Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives	Operational	5.99	5.91	0.08

Two of the three risks that fell in 2019 from 2018 involve macroeconomic risks. While in prior years respondents have consistently indicated notable concerns about overall **economic conditions restricting growth** in markets their organizations serve, that risk issue fell out of the top 10 list of risk issues for 2019 after being in the number one spot in 2017 and the eighth position in our top 10 list for 2018. Strong capital markets, rising consumer confidence and regulatory relief are creating more overall optimism about the economy for 2019 relative to prior years. Despite the overall drop in this risk concern, it is interesting to note that board members, CEOs and CIOs/CTOs identified economic concerns as a top five risk issue for 2019. Additionally, respondents in the European, Latin American/South American, Middle Eastern and African regions included economic conditions in their top five list of risks. That is not too surprising given the ongoing focus on operationalizing Brexit, recent elections in Brazil, the announcements of leadership changes in Germany, and overall concerns about nationalistic trends and trade policies. Collectively, these results suggest economic concerns remain a significant issue in the boardroom and in certain regions.

> "Overall, seven of the top 10 risks for 2019 are operational risks. Six of these are rated as "Significant Impact" risks — a major increase from 2018 (only one risk rated at this level) and 2017 (no risks rated as "Significant Impact" risks). These results indicate that a heightened focus on operations will be observed in the coming year.
>
> — Don Pagach, Professor of Accounting, Director of Research, Enterprise Risk Management Initiative, Poole College of Management, NC State University

Three-Year Comparison of Risks

We provide an analysis of the overall three-year trends for the 30 risks surveyed this year. As discussed previously, to help identify differences in risk concerns across respondent type, we group all the risks based on their average scores into one of three classifications. Consistent with our prior studies, we use the following color-coding scheme to highlight risks visually using these three categories. Table 5 summarizes the impact assessments for each of the 30 risks for the full sample, and it shows the color code for the 28 risks examined in all three years. Recall that we added two new risks to the 2019 study. Thus, we only show results for this year for these two risks.

- Significant Impact — Rating of 6.0 or higher
- Potential Impact — Rating of 4.5 — 5.99
- Less Significant Impact — Rating of 4.49 or lower

Twenty-five of the 28 risks we examined in both 2018 and 2019 increased in 2019 based on their average risk scores. Eight of the 30 risks were rated as "Significant Impact" risks for 2019, which is noticeably more than both 2018 and 2017, when only two of the 30 risks were rated at that level. This is consistent with the overall finding that respondents are more concerned about the magnitude and severity of risks for 2019 relative to the two prior years. None of the 30 risks had an overall score that fell into the "Less Significant Impact" category. Only three risks saw lower average scores for 2019 relative to 2018. Among the three risks that saw a decrease in risk score from 2018 to 2019, two represent macroeconomic risks, suggesting that respondents are noticeably less concerned about these issues for 2019.

For the most part, the relative significance of all the risks in the macroeconomic and strategic categories has remained consistent for all years, as observed by the consistency in color reflected for most risks across the three years reported. We do observe a marked change in the operational risk category, however. Here, we see six of the 10 risk concerns rated as "Significant Impact," a dramatic increase from 2018 (one risk in this category) and 2017 (no risks rated in this manner).

TABLE OF CONTENTS

Perceived Impact for 2019 Relative to Prior Years — Full Sample

TABLE 5

MACROECONOMIC RISK ISSUES	2019 Rank	2019	2018	2017
Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization	11	●	●	●
Unexpected change in the current interest rate environment may have a significant effect on the organization's operations	18	●	●	●
Anticipated increases in labor costs may affect our opportunity to meet profitability targets	19	●	●	●
Geopolitical shifts and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives	22	●	●	●
Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address	23	●	●	●
Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organization	26	●	●	●
Evolving changes in global trade policies may limit our ability to operate effectively and efficiently in international markets	28	●	●	●
Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities	29	●	●	●
Demands made by activist investors and other key stakeholders may significantly affect how we do business in the marketplace (new in 2019)	30	●	N/A	N/A

TABLE OF CONTENTS

TABLE 5 (CONTINUED)

STRATEGIC RISK ISSUES	2019 Rank	2019	2018	2017
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered	3	●	●	●
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model	6	●	●	●
Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base	10	●	●	●
Our organization may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation	12	●	●	●
Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business	13	●	●	●
Opportunities for organic growth through customer acquisition and/or enhancement may be significantly limited for our organization	14	●	●	●
Substitute products and services may arise that affect the viability of our current business model and planned strategic initiatives	16	●	●	●
Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share	17	●	●	●

TABLE OF CONTENTS

TABLE 5 (CONTINUED)

STRATEGIC RISK ISSUES (CONTINUED)	2019 Rank	2019	2018	2017
Growth through acquisitions, joint ventures and other partnership activities may be difficult to identify and implement	21	🟡	🟡	🟡
Shifts in environmental, social and governance (ESG) preferences as well as expectations of key stakeholders may be difficult for us to identify and address on a timely basis	24	🟡	🟡	🟡
Performance vulnerabilities may trigger shareholder activism against our organization that may significantly impact our organization's strategic plan and vision	27	🟡	🟡	🟡

OPERATIONAL RISK ISSUES	2019 Rank	2019	2018	2017
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations	1	🔴	🟡	🟡
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets	2	🔴	🟡	🟡
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand	4	🔴	🟡	🟡
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations	5	🔴	🔴	🟡

TABLE 5 (CONTINUED)

OPERATIONAL RISK ISSUES (CONTINUED)	2019 Rank	2019	2018	2017
Ensuring privacy/identity management and information security/system protection may require significant resources for us	7	●	●	●
Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans	8	●	●	●
Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives	9	●	●	●
Risks arising from our reliance on outsourcing and strategic sourcing arrangements, IT vendor contracts, and other partnerships/joint ventures to achieve operational goals may prevent us from meeting organizational targets or impact our brand image	15	●	●	●
The cultural behaviors and personal interactions with others exhibited by the organization's management team and other key representatives — as manifested through day-to-day decision-making, attitudes and conduct — may not be aligned with the long-term interests of shareholders, the board's risk appetite, compliance with laws and regulations, and/or the core values most accepted and rewarded by the marketplace (new in 2019)	20	●	N/A	N/A
Uncertainty surrounding the viability of key suppliers, scarcity of supply, or stable supply prices may make it difficult to deliver our products or services at acceptable margins	25	●	●	●

TABLE OF CONTENTS

Analysis Across Different Sizes of Organizations

The sizes of organizations, as measured by total revenues, vary across our 825 respondents, as shown below. The mix of sizes of organizations represented by respondents is relatively similar to the mix of respondents in our prior years' surveys. Almost 70 percent of our respondents are in organizations with revenues between $100 million and $10 billion.

MOST RECENT REVENUES	NUMBER OF RESPONDENTS
Revenues $10 billion or greater	150
Revenues $1 billion to $9.99 billion	348
Revenues $100 million to $999 million	226
Revenues less than $100 million	101
Total Number of Respondents	**825**

The overall outlook about risk conditions differs across sizes of organizations. We asked respondents to provide their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months, using a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive." The three largest size categories of organizations (those with revenues above $100 million) all perceive an increase in the magnitude and severity of risks for their organizations, while the smallest organizations indicated that the magnitude and severity of risks has been relatively stable over the three-year period. The smallest-sized organizations are also the least concerned relative to organizations in the other size categories.

The overall magnitude and severity of risks is believed to be highest among the largest organizations and declines in step with the size strata we explore. There was a significant increase in the perception of the magnitude and severity of risks from 2018 to 2019 for our largest firms.

Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	**2019**	**2018**	**2017**
Organizations with revenues $10 billion or greater	6.5	5.9	6.5
Organizations with revenues between $1 billion and $9.99 billion	6.3	6.1	6.6
Organizations with revenues between $100 million and $999 million	6.2	6.1	5.8
Organizations with revenues less than $100 million	5.5	5.5	5.4

Consistent with our findings related to the overall top 10 risks for 2019 for the full sample, operational risks dominate the top five risks for each of the size categories of organizations. For all but the largest group, four of the top five risks are operational in nature, while for those organizations with revenues in excess of $10 billion, three of the top five are in this category. Succession challenges and the ability to attract and retain top talent appears on all four top five lists. This makes sense given the tightening labor market as the economy continues to expand and strengthen and creates new opportunities for these organizations' workforces.

Regulatory change and regulatory scrutiny continue to be a top five concern for most organizations, except those with revenues less than $100 million. This is a significant change from 2018, when this was the highest-rated risk for the smallest organizations in our sample. Similarly, the three largest size groups share a concern over their legacy IT infrastructure and their ability to keep pace with new competitors who likely have lower cost structures and are more resilient in embracing the new digital landscape.

All organizations, except those in the largest category (those with revenues of $10 billion or more), rated concerns about their organization's ability to manage cyber threats and related damage to operations and brand as a top five risk concern. Interestingly, the largest organizations rated this risk as 13th overall, suggesting that they may be in a leadership position in mitigating exposure to this particular risk event. Indeed, they have more capacity to invest in cybersecurity measures.

Except for the smallest organizations (those with revenues less than $100 million), all other sizes of organizations rated all of their top five risks as "Significant Impact" risks. The largest organizations (those with revenues of $10 billion or more) rated all five above 6.50. For the smallest organizations, only their top-rated risk — concern about cyber threats — was rated as a "Significant Impact" risk.

The sense that core business models may be altered by competitors that introduce new and innovative ways of doing business is on the minds of respondents from both our largest and smallest organizations. The accompanying charts summarize the top-rated risks by size of organization. Only the top five risks are reported.

Rev $10B or Greater

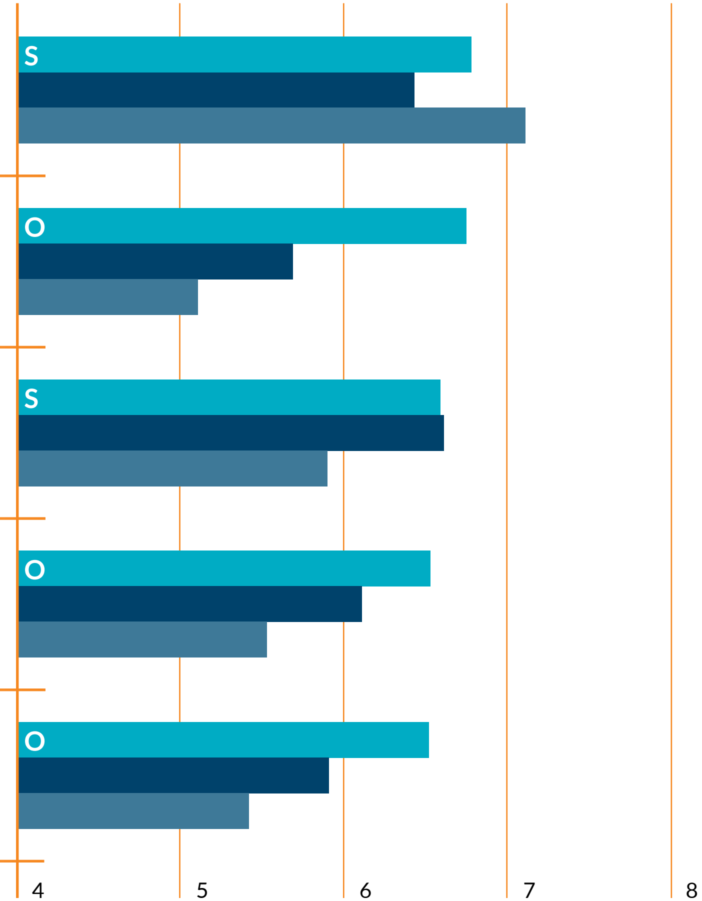
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans

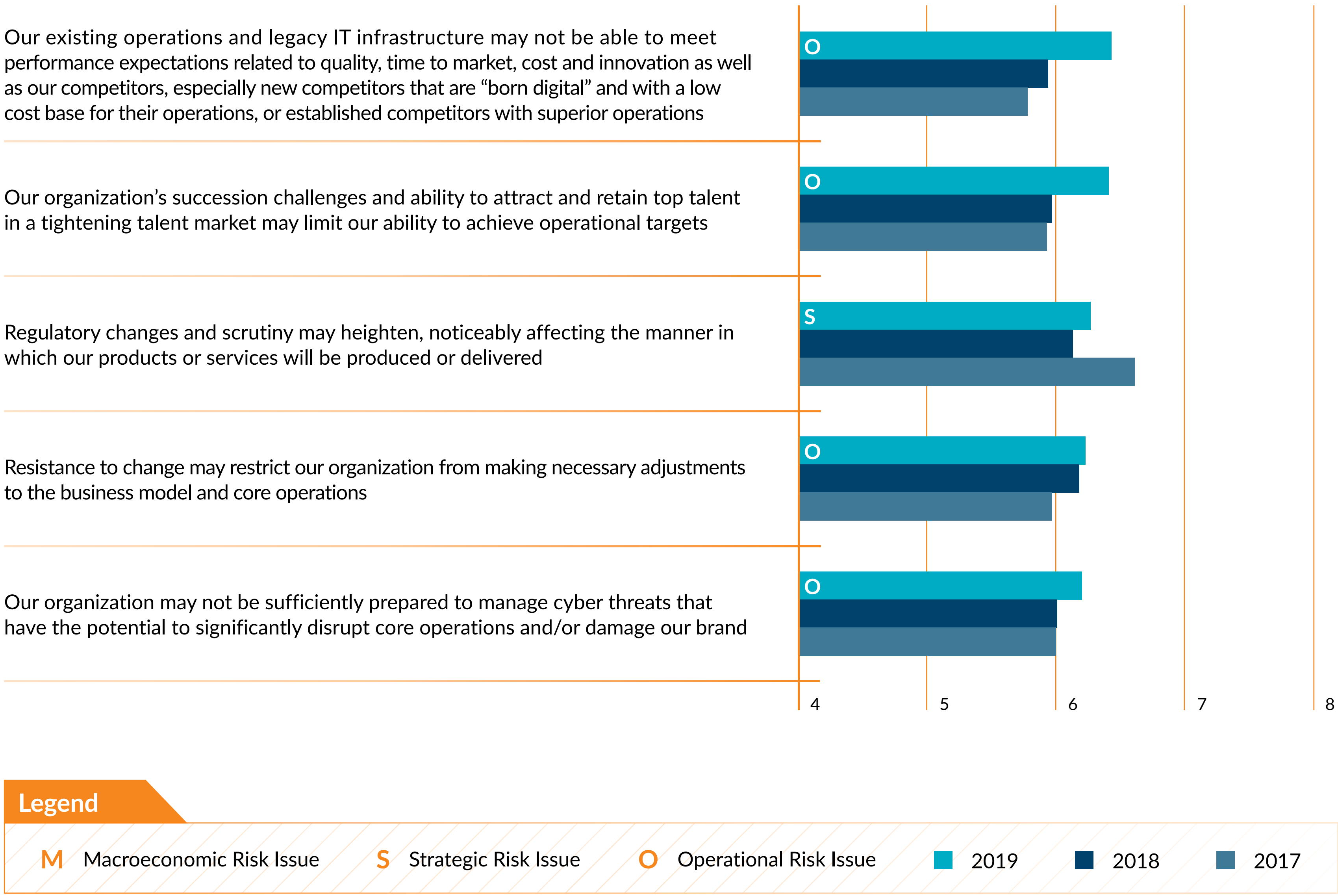


Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue ■ 2019 ■ 2018 ■ 2017

TABLE OF CONTENTS

Rev $1B to $9.9B



Rev $100M to $999M

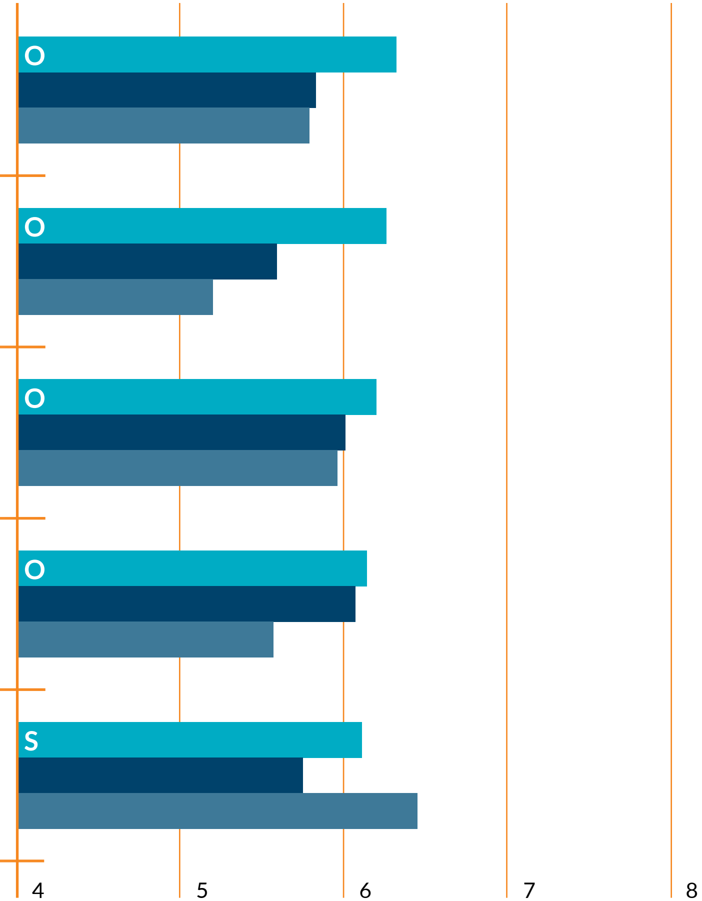
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

Rev Less than $100M

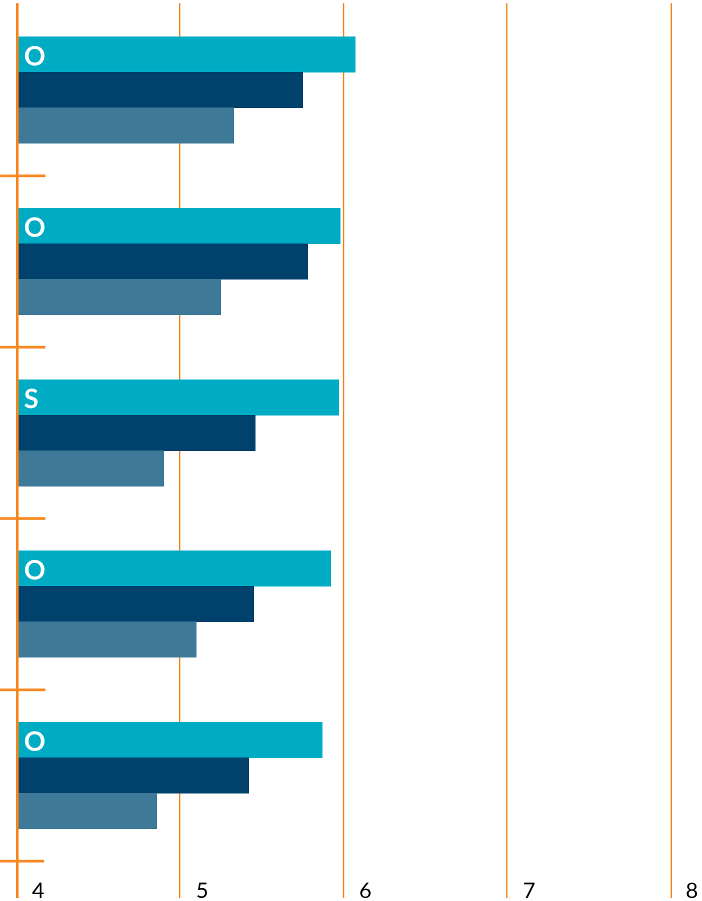
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations



Legend

M Macroeconomic Risk Issue | S Strategic Risk Issue | O Operational Risk Issue | 2019 | 2018 | 2017

Analysis Across Executive Positions Represented

We targeted our survey to individuals currently serving on the board of directors or in senior executive positions so that we could capture C-suite and board perspectives about risks on the horizon for 2019. Respondents to the survey serve in a number of different board and executive positions. The remaining respondents represent individuals currently serving in a variety of executive positions. We received responses from 90 members of a board of directors, and it is reasonable to expect that some CEOs and perhaps other C-level executives also serve on a board.

EXECUTIVE POSITION	NUMBER OF RESPONDENTS
Board of Directors	90
Chief Executive Officer	47
Chief Financial Officer	35
Chief Risk Officer	210
Chief Audit Executive	192
Chief Information/Technology Officer	55
Other C-Suite[3]	100
All other[4]	96
Total Number of Respondents	**825**

[3] This category includes titles such as chief operating officer, general counsel and chief compliance officer.

[4] These 96 respondents either did not provide a response or are best described as middle management or business advisers/consultants. We do not provide a separate analysis for this category.

To determine if perspectives about top risks differ across executive positions, we also analyzed key findings for boards of directors and the six executive positions with the greatest number of respondents: chief executive officer (CEO), chief financial officer (CFO), chief risk officer (CRO), chief audit executive (CAE), chief information/technology officer (CIO/CTO), and Other C-Suite executives.[5]

Similar to our analysis of the full sample and across the different sizes of organizations, we analyzed responses about overall impressions of the magnitude and severity of risks across the above types of respondents. Again, the scores in the table below reflect responses to the question about their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months, using a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive."

Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	**2019**	**2018**	**2017**
Board of Directors	6.7	6.4	5.5
Chief Executive Officer	6.4	5.9	6.0
Chief Financial Officer	6.0	6.3	6.3
Chief Risk Officer	5.9	5.5	6.3
Chief Audit Executive	6.0	6.4	6.1
Chief Information/Technology Officer	6.2	6.3	6.6
Other C-Suite	6.8	6.0	6.4

[5] We grouped individuals with equivalent but different executive titles into these positions when appropriate. For example, we included "Vice President — Risk Management" in the CRO grouping and we included "Director of Finance" in the CFO grouping.

The overall impression among executives with respect to the magnitude and severity of risks in the environment is decidedly mixed. Board members, CEOs and Other C-Suite executives have significantly increased their 2019 risk expectations relative to 2018. These respondents rated the magnitude and severity of risks for 2019 at the highest level among all executives. This increase in risk expectations may be the result of overall concern about how quickly business conditions and expectations for oversight are changing, as well as how quickly it could change going forward. Only CFOs, CAEs and CIOs/CTOs lowered their future impressions of the risk environment.

Interestingly, CIOs/CTOs lowered their 2019 impressions below not only their 2018 ratings but also their 2017 ratings, and CROs, while increasing from 2018, report the lowest level of concern across the variety of positions we surveyed. This contrast in perspectives suggests there may be value in explicitly discussing and analyzing factors that might be influencing overall impressions about the risk environment among key leaders, especially at the highest level of the organization. Thus, enterprise risk assessments would benefit from the influx of multiple perspectives.

As discussed previously, to help identify differences in risk concerns across respondent type, we group all the risks based on their average scores into one of three classifications. Consistent with prior studies, we use the following color-coding scheme to highlight risks visually using these three categories. Below, Table 6 summarizes the impact assessments for each of the 30 risks for the full sample and for each category of executive using the following color code scheme:

- Significant Impact — Rating of 6.0 or higher
- Potential Impact — Rating of 4.5 — 5.99
- Less Significant Impact — Rating of 4.49 or lower

Role

TABLE 6

MACROECONOMIC RISK ISSUES	Board	CEO	CFO	CRO	CAE	CIO/ CTO	Other C-Suite
Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization	🔴	🔴	🟡	🟡	🟡	🔴	🔴
Anticipated increases in labor costs may affect our opportunity to meet profitability targets	🔴	🟡	🔴	🟡	🟡	🔴	🔴
Unexpected change in the current interest rate environment may have a significant effect on the organization's operations	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organization	🔴	🟡	🟡	🟡	🟡	🟡	🔴
Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address	🟡	🟡	🟡	🟡	🟡	🟡	🔴
Geopolitical shifts and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives	🔴	🟡	🟡	🟡	🟡	🟡	🔴
Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities	🟡	🟡	🟡	🟢	🟡	🔴	🟡
Demands made by activist investors and other key stakeholders may significantly affect how we do business in the marketplace (new in 2019)	🟡	🟡	🟡	🟡	🟢	🟡	🔴
Evolving changes in global trade policies may limit our ability to operate effectively and efficiently in international markets	🟡	🟡	🟡	🟢	🟡	🟡	🟡

TABLE 6 (CONTINUED)

STRATEGIC RISK ISSUES	Board	CEO	CFO	CRO	CAE	CIO/ CTO	Other C-Suite
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model	🔴	🔴	🟡	🔴	🟡	🔴	🔴
Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base	🔴	🔴	🟡	🔴	🟡	🔴	🔴
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered	🔴	🟡	🟡	🔴	🟡	🔴	🔴
Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Our organization may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Opportunities for organic growth through customer acquisition and/or enhancement may be significantly limited for our organization	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Shifts in environmental, social and governance (ESG) preferences as well as expectations of key stakeholders may be difficult for us to identify and address on a timely basis	🔴	🟡	🟡	🟡	🟡	🟡	🔴
Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share	🔴	🟡	🟡	🟡	🟡	🟡	🔴

TABLE 6 (CONTINUED)

STRATEGIC RISK ISSUES (CONTINUED)	Board	CEO	CFO	CRO	CAE	CIO/ CTO	Other C-Suite
Substitute products and services may arise that affect the viability of our current business model and planned strategic initiatives	🔴	🟡	🟡	🟡	🟡	🟡	🔴
Growth through acquisitions, joint ventures and other partnership activities may be difficult to identify and implement	🔴	🟡	🟡	🟡	🟡	🟡	🟡
Performance vulnerabilities may trigger shareholder activism against our organization that may significantly impact our organization's strategic plan and vision	🔴	🟡	🟡	🟢	🟢	🟡	🔴

OPERATIONAL RISK ISSUES	Board	CEO	CFO	CRO	CAE	CIO/ CTO	Other C-Suite
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand	🔴	🔴	🔴	🔴	🔴	🔴	🔴
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations	🔴	🟡	🔴	🔴	🔴	🔴	🔴

TABLE OF CONTENTS

TABLE 6 (CONTINUED)

OPERATIONAL RISK ISSUES (CONTINUED)	Board	CEO	CFO	CRO	CAE	CIO/ CTO	Other C-Suite
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations	🔴	🟡	🔴	🔴	🔴	🔴	🔴
Ensuring privacy/identity management and information security/system protection may require significant resources for us	🔴	🟡	🟡	🔴	🔴	🔴	🔴
Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans	🔴	🔴	🟡	🟡	🟡	🔴	🔴
Risks arising from our reliance on outsourcing and strategic sourcing arrangements, IT vendor contracts, and other partnerships/joint ventures to achieve operational goals may prevent us from meeting organizational targets or impact our brand image	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives	🔴	🟡	🟡	🟡	🟡	🔴	🔴
Uncertainty surrounding the viability of key suppliers, scarcity of supply, or stable supply prices may make it difficult to deliver our products or services at acceptable margins	🔴	🟡	🟡	🟡	🟡	🔴	🟡
The cultural behaviors and personal interactions with others exhibited by the organization's management team and other key representatives — as manifested through day-to-day decision-making, attitudes and conduct — may not be aligned with the long-term interests of shareholders, the board's risk appetite, compliance with laws and regulations, and/or the core values most accepted and rewarded by the marketplace (new in 2019)	🔴	🟡	🟡	🟡	🟡	🟡	🟡

Board members and Other C-Suite executives overwhelmingly exhibit the most significant concern about risk issues, as reflected by their ratings of the 30 risks at the highest impact level (red circles). Board members rate 26 of the 30 risks at the highest level, followed closely by the Other C-Suite executives, who rate 25 of the 30 in this manner. CIOs/CTOs were not far behind, identifying 19 of the 30 risks at the highest impact level. At the other end of the spectrum, CFOs identified only five of the 30 risks at the highest level and CEOs were not much different, pegging six of the 30 at the highest level.

The charts on the following pages highlight the top five risks identified by each position.

Of particular note is the observation that three of the top five risks for board members relate to strategic risk concerns, which are more than any other position. CEOs, CROs and the group of executives in our Other C-Suite category identify two of their top five risks in this category. CAEs and CFOs almost exclusively pinpointed operational issues in their top five risks (all five for CAEs and four of five for CFOs). In contrast, board members took a broader view and did not include a single operational risk in their top five list this year.

This disparity in viewpoints emphasizes the critical importance of both the board and the management team engaging in risk discussions, given the different perspectives each brings to the table and the potential for a lack of consensus about the organization's most significant risks. Without clarity of focus, the executive team may be unaligned with the board on what the top risks are. Worse, they may not be appropriately addressing the most important risks facing the organization, thereby leaving the organization potentially vulnerable to certain risk events. The disparity reflected above may also reflect CEOs and board members taking more of a "big picture" view as other executives focus more on operational issues.

> With the disparity of views regarding risk in today's complex business environment, companies can best differentiate themselves with a properly structured risk-informed approach that considers the impact of risk on strategy and performance, measures both risks and opportunities, is integrated with strategy-setting and business planning and execution, and addresses the business needs, expectations and cultural attributes of the organization.
>
> — Emma Marcandalli, Managing Director, Protiviti

Board Members

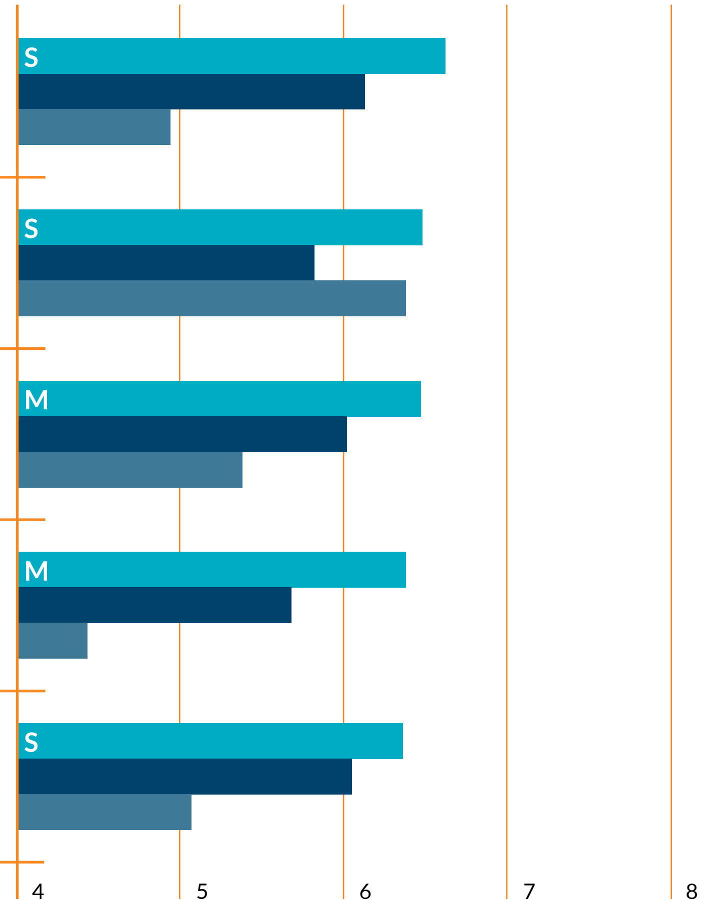
Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization

Anticipated increases in labor costs may affect our opportunity to meet profitability targets

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

CEOs

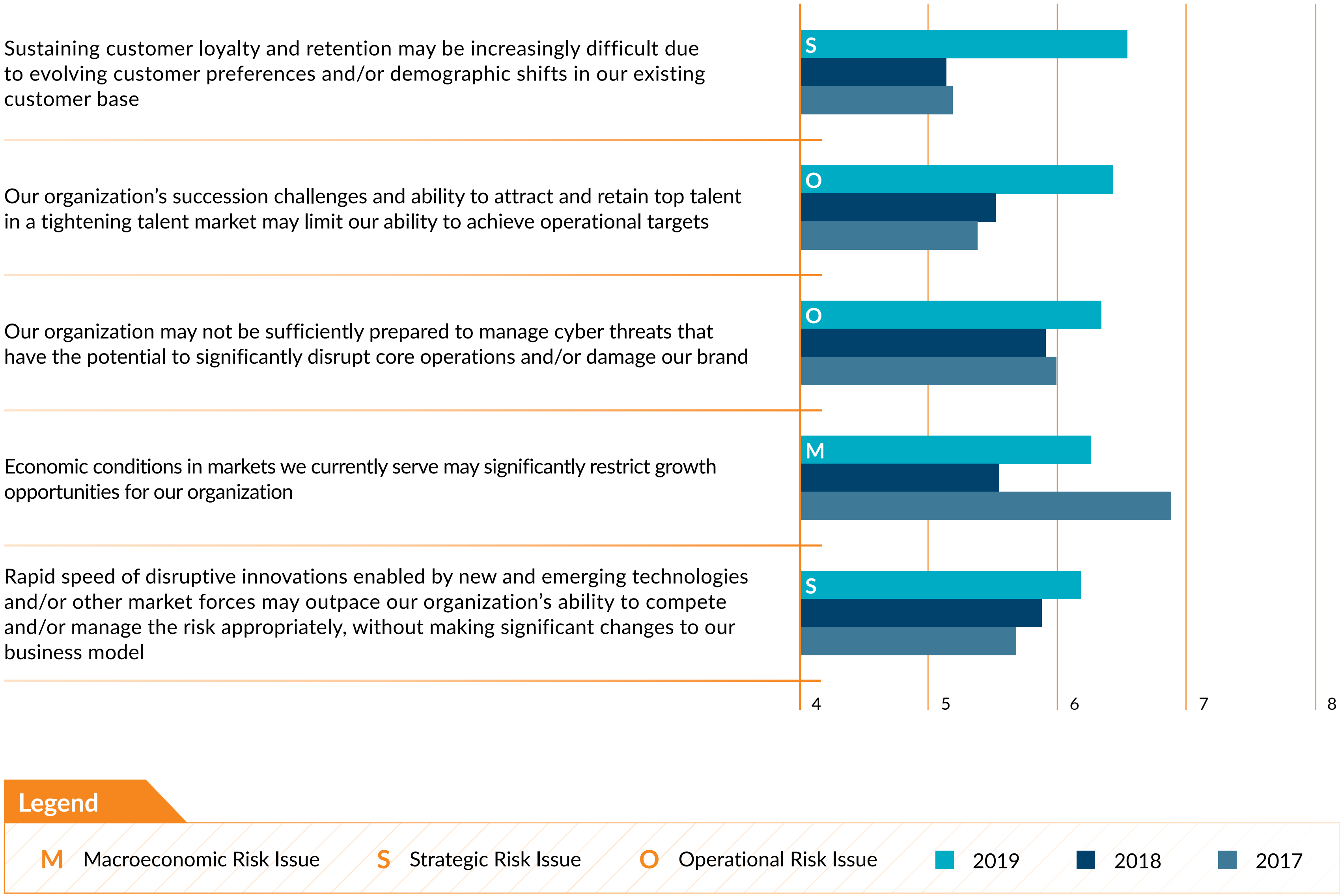

Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base
S
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets
O
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand
O
Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization
M
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model
S
4
5
6
7
8
Legend
M Macroeconomic Risk Issue
S Strategic Risk Issue
O Operational Risk Issue
2019
2018
2017

TABLE OF CONTENTS

CFOs

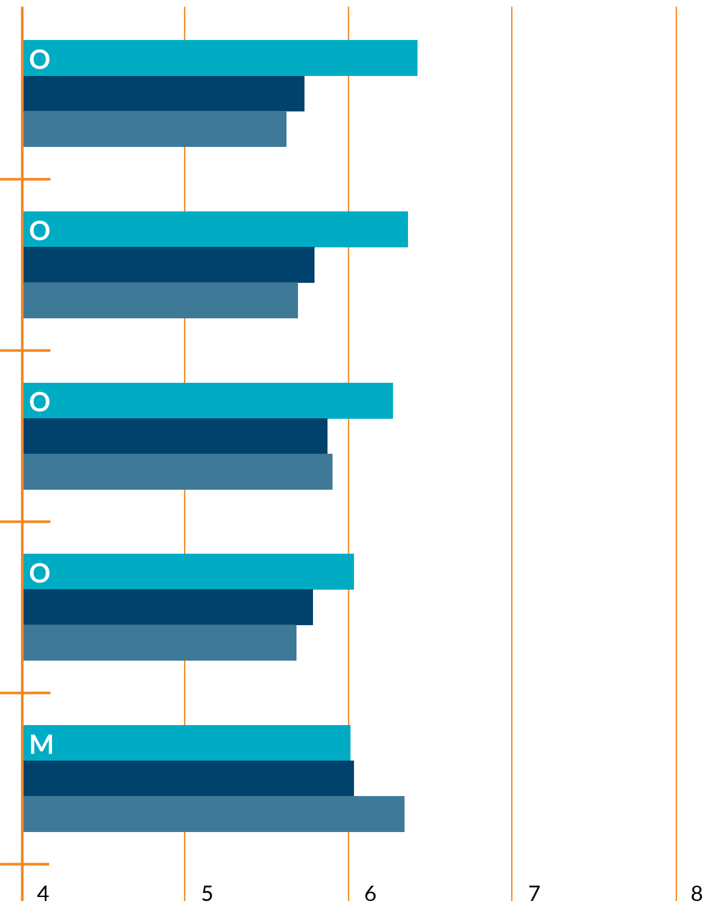
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Anticipated increases in labor costs may affect our opportunity to meet profitability targets



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

CROs

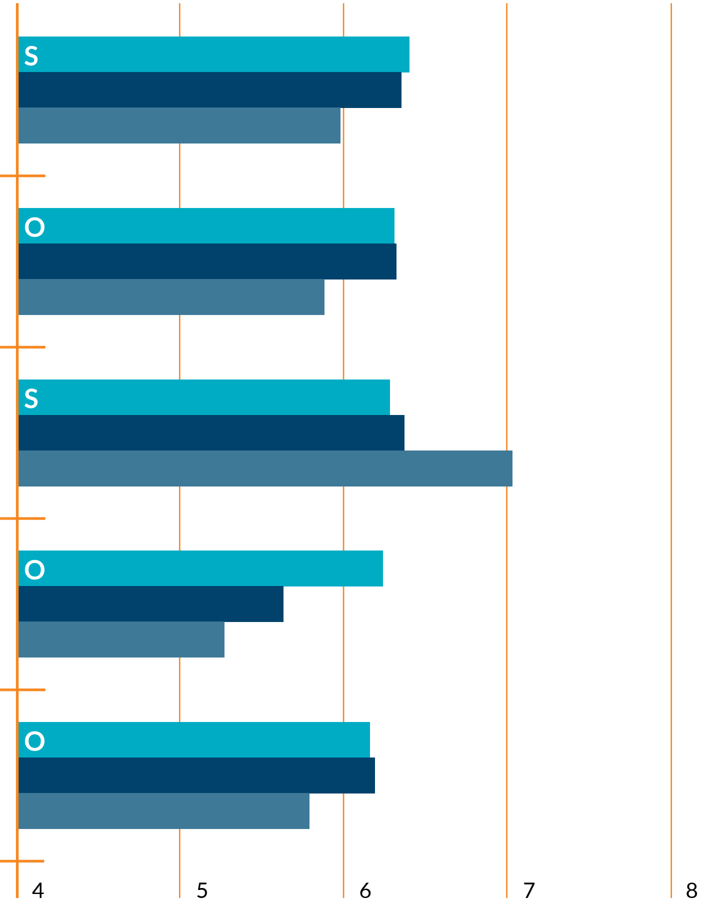
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

CAEs

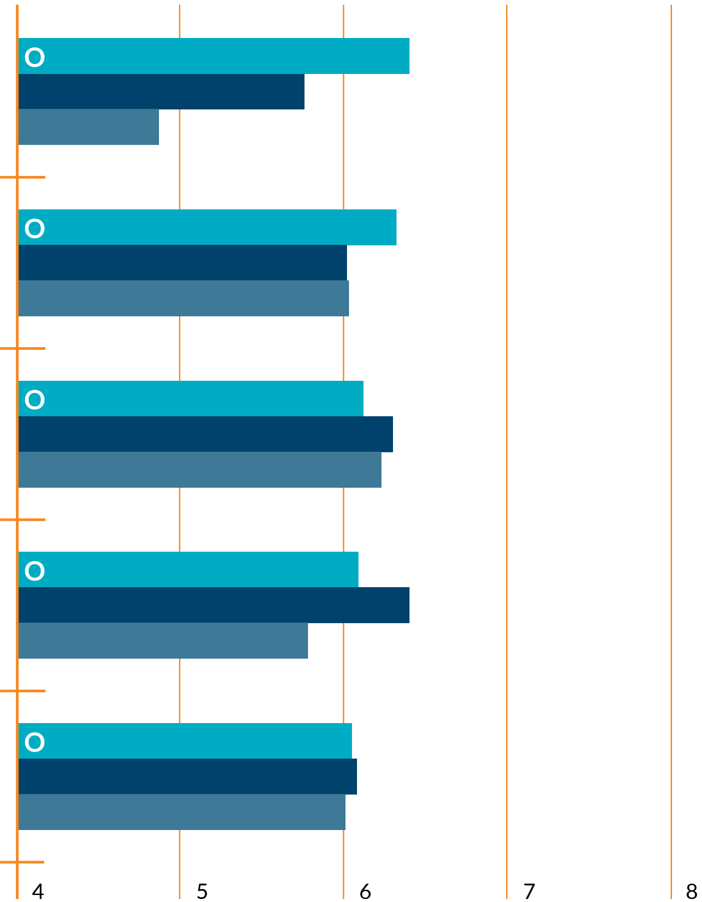
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Ensuring privacy/identity management and information security/system protection may require significant resources for us



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

CIOs/CTOs

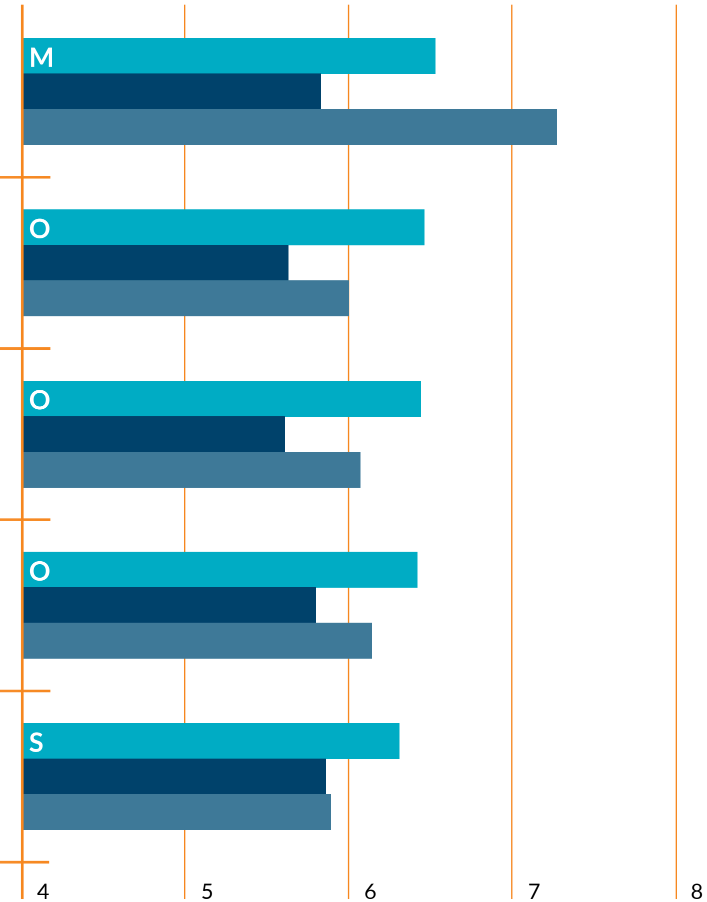
Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Our organization may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

Other C-Suite

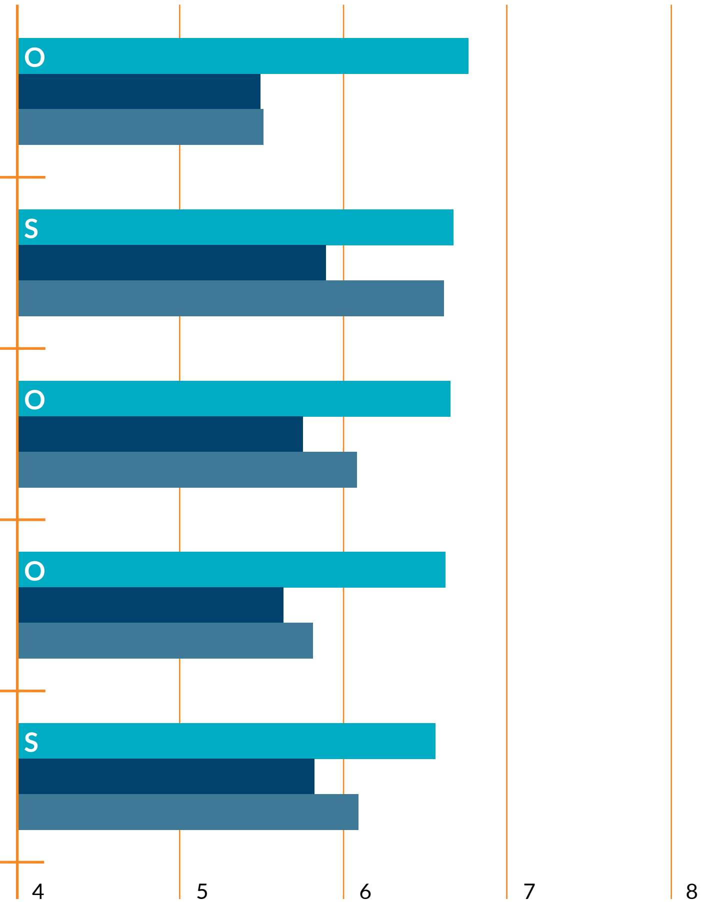
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model



Legend

M Macroeconomic Risk Issue | S Strategic Risk Issue | O Operational Risk Issue | 2019 | 2018 | 2017

Industry Analysis

Respondents to our survey represent organizations in a number of industry groupings, as shown below:

INDUSTRY	NUMBER OF RESPONDENTS
Financial Services (FS)	230
Consumer Products and Services (CPS)	185
Manufacturing and Distribution (MD)	129
Technology, Media and Telecommunications (TMT)	63
Healthcare and Life Sciences (HLS)	93
Energy and Utilities (EU)	72
Other industries (not separately reported)	53
Total Number of Respondents	**825**

We analyzed responses across the six industry groups to determine whether industries rank-order risks differently. Similar to our analysis of the full sample and across the different sizes of organizations and types of respondents, we analyzed responses about overall impressions of the magnitude and severity of risks across the above industry grouping categories. Again, the scores in the table below reflect responses to the question about their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months, using a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive."

Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	**2019**	**2018**	**2017**
Financial Services (FS)	6.0	5.8	6.5
Consumer Products and Services (CPS)	6.1	5.8	5.9
Manufacturing and Distribution (MD)	6.3	6.2	6.1
Technology, Media and Telecommunications (TMT)	6.2	6.5	6.5
Healthcare and Life Sciences (HLS)	6.7	6.2	6.2
Energy and Utilities (EU)	6.1	5.7	6.5

Respondents from every industry group, with the exception of the Technology, Media and Telecommunications industry group, perceived that the magnitude and severity of risks affecting their organization are greater in 2019 than in the prior year. This increase was felt most significantly by the Healthcare and Life Sciences, Consumer Products and Services, and Energy and Utilities industry groups. This is due to increased concerns in a variety of areas affecting different industry groups in different ways. These areas include regulatory matters, disruptive technologies, ability to compete with more nimble competitors, talent management, cyber threats, sustaining customer loyalty and cultural issues. For example, take regulatory concerns. Healthcare reform and regulation of drug prices continue to be a significant political issue affecting the Healthcare and Life Sciences industry group, particularly in the United States. Tariffs and trade continue to roil the Consumer Products and Services industry group, while Middle East politics weighing on energy prices create volatility and environmental issues add to the uncertainty in the Energy and Utilities industry group.

The Healthcare and Life Sciences industry group reflects the highest overall concern related to the magnitude and severity of risks overall. Given technological advancements that continue to occur at a rapid pace as well as significant regulatory uncertainty, this industry group continues to experience significant change relative to the other industry groups.

Respondents in the Energy and Utilities industry group reflect the most volatility in overall risk concerns across the three years. After this industry group saw a significant decrease in the overall risk environment from 2017 to 2018, the 2019 survey results reflect a significant increase in the level of overall risk concern. These changes may be a result of the volatility of oil prices. Oil markets saw a significant decrease in prices in late 2017 and early 2018. In addition, there was a significant drop in volatility for energy companies during 2018. However, in mid-to-late 2018 energy prices again started increasing along with Middle East tensions resulting in an overall increase in uncertainty and volatility.

The 2019 levels of overall risk concern are mostly tracking in line with 2018 levels for the Financial Services and Manufacturing and Distribution industry groups. Surprisingly, we observe a decrease in the overall impression of the magnitude and severity of risks affecting the Technology, Media and Telecommunications industry group, even though the industry's top risks mostly increased.

Table 7 provides an overview of the significance and differences across industries in executive perspectives about each of the 30 risks rated in this study (categorized as macroeconomic, strategic and operational risk issues).

> To no one's surprise, the dynamics in each industry group we examine are different. We see regulatory matters, the effects of disruptive technologies, the war for talent, the persistence of cyber threats, the criticality of preserving customer loyalty, and the all-too-important issue of organizational culture rear their respective heads in different ways, depending on the industry group.
>
> — Pat Scott, Executive Vice President, Global Industry Program, Protiviti

- Significant Impact — Rating of 6.0 or higher
- Potential Impact — Rating of 4.5 — 5.99
- Less Significant Impact — Rating of 4.49 or lower

Industry

TABLE 7

MACROECONOMIC RISK ISSUES	FS	CPS	MD	TMT	HLS	EU
Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization	🟡	🟡	🔴	🔴	🔴	🔴
Evolving changes in global trade policies may limit our ability to operate effectively and efficiently in international markets	🟡	🟡	🔴	🟡	🟡	🟡
Anticipated increases in labor costs may affect our opportunity to meet profitability targets	🟡	🟡	🔴	🟡	🟡	🟡
Unexpected change in the current interest rate environment may have a significant effect on the organization's operations	🔴	🟡	🟡	🟡	🟡	🟡
Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address	🟡	🟡	🟡	🟡	🟡	🟡
Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities	🟡	🟡	🟡	🟡	🟡	🟡
Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organization	🟡	🟡	🟡	🟡	🟡	🟡
Demands made by activist investors and other key stakeholders may significantly affect how we do business in the marketplace (new in 2019)	🟡	🟡	🟡	🟡	🟡	🟡
Geopolitical shifts and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives	🟡	🟡	🟡	🟡	🟡	🟡

TABLE 7 (CONTINUED)

STRATEGIC RISK ISSUES	FS	CPS	MD	TMT	HLS	EU
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model	●	○	●	●	●	○
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered	●	○	○	●	●	●
Sustaining customer loyalty and retention may be increasingly difficult due to evolving customer preferences and/or demographic shifts in our existing customer base	●	●	○	●	●	○
Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share	○	○	○	●	○	○
Our organization may not be sufficiently prepared to manage an unexpected crisis significantly impacting our reputation	○	○	○	○	●	○
Opportunities for organic growth through customer acquisition and/or enhancement may be significantly limited for our organization	○	○	○	○	●	○
Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business	○	○	○	○	○	○
Shifts in environmental, social and governance (ESG) preferences as well as expectations of key stakeholders may be difficult for us to identify and address on a timely basis	○	○	○	○	○	○

TABLE 7 (CONTINUED)

STRATEGIC RISK ISSUES (CONTINUED)	FS	CPS	MD	TMT	HLS	EU
Growth through acquisitions, joint ventures and other partnership activities may be difficult to identify and implement	🟡	🟡	🟡	🟡	🟡	🟡
Substitute products and services may arise that affect the viability of our current business model and planned strategic initiatives	🟡	🟡	🟡	🟡	🟡	🟡
Performance vulnerabilities may trigger shareholder activism against our organization that may significantly impact our organization's strategic plan and vision	🟡	🟡	🟡	🟡	🟡	🟡

OPERATIONAL RISK ISSUES	FS	CPS	MD	TMT	HLS	EU
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand	🔴	🔴	🔴	🔴	🔴	🔴
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets	🔴	🔴	🔴	🔴	🔴	🟡
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations	🔴	🔴	🔴	🔴	🔴	🟡
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations	🔴	🔴	🔴	🟡	🔴	🔴

TABLE OF CONTENTS

TABLE 7 (CONTINUED)

OPERATIONAL RISK ISSUES (CONTINUED)	FS	CPS	MD	TMT	HLS	EU
Ensuring privacy/identity management and information security/system protection may require significant resources for us	🔴	🟡	🟡	🔴	🔴	🟡
Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives	🟡	🟡	🔴	🟡	🔴	🔴
Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans	🔴	🟡	🟡	🟡	🔴	🟡
Uncertainty surrounding the viability of key suppliers, scarcity of supply, or stable supply prices may make it difficult to deliver our products or services at acceptable margins	🟡	🟡	🔴	🟡	🟡	🟡
Risks arising from our reliance on outsourcing and strategic sourcing arrangements, IT vendor contracts, and other partnerships/joint ventures to achieve operational goals may prevent us from meeting organizational targets or impact our brand image	🟡	🟡	🟡	🟡	🔴	🟡
The cultural behaviors and personal interactions with others exhibited by the organization's management team and other key representatives — as manifested through day-to-day decision-making, attitudes and conduct — may not be aligned with the long-term interests of shareholders, the board's risk appetite, compliance with laws and regulations, and/or the core values most accepted and rewarded by the marketplace (new in 2019)	🟡	🟡	🟡	🟡	🟡	🟡

Across the different industries, operational risks seem to be of greatest concern for 2019. Out of the 10 operational risks included in our survey, four of those risks were rated as "Significant Impact" risks for at least five of the six industry groups. In contrast, three of the 11 strategic risks and only one of the nine macroeconomic risks were rated as "Significant Impact" risks by four of the six industries.

For 2019, operational risks related to concerns about succession challenges and the ability to attract and retain talent and concerns about existing infrastructure and legacy IT systems made the top five list of risks for each of the industry groups examined, except for Energy and Utilities. Concerns about the ability to manage cyber threats was rated as a top five risk issue for four of the six industry groups — the exceptions are Financial Services and Technology, Media and Telecommunications. Concerns about the inability to utilize analytics and "big data" increased for every industry group and is seen as a "Significant Impact" risk for the Financial Services and Healthcare and Life Sciences industry groups.

Examining macroeconomic risks more closely, two industry groups stand out: Manufacturing and Distribution, and Energy and Utilities. The Manufacturing and Distribution industry group has three of the macroeconomic risks rated as "Significant Impact" risks versus zero rated at that level in 2018. The Energy and Utilities industry group went from having three macroeconomic risks rated as "Less Significant Impact" in 2018 to none rated that low in 2019. Overall, four of the six industry groups now rate the macroeconomic risk that economic conditions in markets we currently serve may significantly restrict growth opportunities as "Significant Impact."

At the strategic risk level, we see more consistency among the industry groups. However, one change clearly stands out for 2019 — the risk that sustaining customer loyalty and retention may be difficult due to evolving customer preferences. In 2018, only the Healthcare and Life Sciences industry group listed this as a "Significant Impact" risk, whereas in 2019 it is joined by the Financial Services, Consumer Products and Services, and Technology, Media and Telecommunications industry groups.

The Healthcare and Life Sciences industry group has the highest level of risk concerns. Respondents in that industry group identified 14 of the 30 risks as "Significant Impact" risks, with all other risks rated in the middle category of "Potential Impact" risks. The Manufacturing and Distribution industry group has the largest increase in risk concerns. After rating zero risks as "Significant Impact" in 2018, the number of "Significant Impact" risks increased to 10 risks in 2019. The Financial Services industry group also saw a notable increase in the overall concern about the magnitude and severity of risks, with respondents in that industry group rating 10 of the 30 risks as "Significant Impact" risks for 2019 versus only four in 2018. The only industry group that rated fewer risks as "Significant Impact" in 2019 versus 2018 was Energy and Utilities; however, in 2018 it rated three risks as "Less Significant Impact," whereas zero were given that rating in 2019.

The bar charts on the following pages report the top five risk exposures in rank order for each of the six industry groups. The 2019 results are presented in light blue.

Recall that a risk with an average score of 6.0 or higher is considered a "Significant Impact" risk, while risks with average scores between 4.5 and 5.99 are "Potential Impact" risks and risks with average scores below 4.5 are "Less Significant Impact" risks. In addition, the bar charts provide the risk rating for the previous two years with 2018 in red and 2017 in green.

One noticeable observation from these charts is that every industry group rated all of their top five risks as "Significant Impact" risks for 2019, whereas only the Technology, Media and Telecommunications, Healthcare and Life Sciences, and Energy and Utilities industry groups did so in 2018. In addition, while respondents in almost every industry group have the overall impression that the magnitude and severity of risks is higher in 2019 relative to 2018, respondents also generally rate their top five risk concerns as higher in 2019 relative to 2017, as reflected by the bar graphs on the pages that follow.

In 2019, no industry group has a risk with an average score that exceeds 7.0 on our 10-point scale. This is in contrast to 2017, when a number of industry groups had risks ranked above 7.0. However, the increases in almost every risk from 2018 to 2019 are concerning, with four industry groups (Financial Services, Consumer Products and Services, Manufacturing and Distribution, and Technology, Media and Telecommunications) all seeing a significant increase in the number of "Significant Impact" risks in their top five.

There are also differences in categories for the top five risks across the six industry groups examined. The Financial Services, Manufacturing and Distribution, and Energy and Utilities industry groups are the only ones to include a macroeconomic risk in their top five risk concerns. The Consumer Products and Services and the Healthcare and Life Sciences industry groups are mostly concerned about operational risks, given four of their top five risk concerns are in that category. In contrast, only the Financial Services and Technology, Media and Telecommunications industry groups ranked more than one strategic risk among their top five risk concerns.

These noted differences in risk issues across the different industry groups highlight the importance of understanding industry drivers and emerging developments to effectively identify the most significant enterprise risks and emerging risk concerns. Following each bar chart by industry, we provide additional commentary about industry-specific risk drivers.

Financial Services

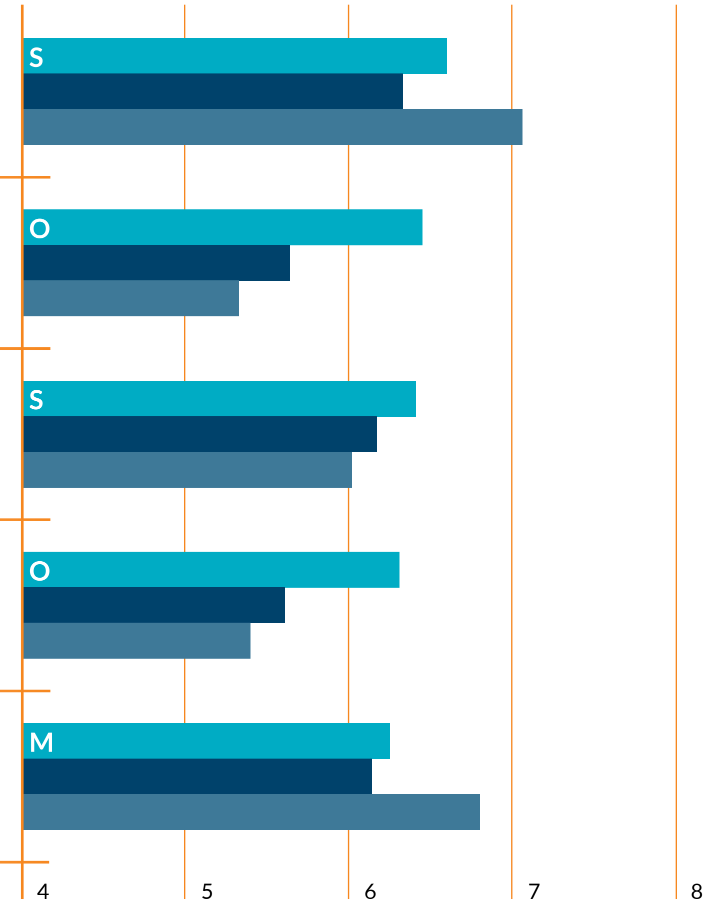
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Unexpected change in the current interest rate environment may have a significant effect on the organization's operations



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Commentary — Financial Services Industry Group

For financial services organizations globally, the years since the global financial crisis that began in 2008 were marked by an unusually intensive and, for many firms, almost exclusive focus on risk management and regulatory compliance matters. Last year, the results of our survey marked an initial shift away from those trends, in that while regulatory compliance matters remained a significant source of risk, digital disruption and other threats to business competitiveness began to be viewed as increasing sources of concern. Our 2019 results show this shift is continuing and, in many areas, accelerating.

> "For Financial Services globally, our top risks surveys conducted for 2018 and 2019 marked a shift away from an intensive and, for many firms, almost exclusive focus on risk management and regulatory compliance matters that transpired since the global financial crisis. While regulatory compliance matters remain a significant source of risk, digital disruption and other threats to business competitiveness are being viewed with increasing concern. The results for 2019 show this shift not only is continuing but is, in many areas, accelerating.
>
> — Michael Brauneis, Managing Director, Americas Financial Services Industry Leader, Protiviti

Regulatory compliance concerns remain elevated but stable

Although regulatory change and regulatory scrutiny remained the highest scoring risk issue this year, scores for this attribute increased only 4 percent year over year. Moreover, perceptions of regulatory risk diverged significantly by geography in this year's survey. Concern for this risk issue actually decreased in North America, reflecting the deregulatory agenda of the Trump administration and Republican-held Congress, as well as what has generally been perceived to be a more balanced, growth-friendly supervisory environment promoted by the new leaders of the major federal regulatory agencies within the United States.

Conversely, the perception of regulatory risk increased significantly among financial institutions in the European Union, as well as those in Asia-Pacific and Australia/New Zealand. European institutions face ongoing efforts to fully implement and optimize controls related to the General Data Protection Regulation (GDPR) that became initially effective in May 2018.[6] Additionally, significant concerns and uncertainty exist regarding the ultimate outcome and impact of the United Kingdom's looming exit from the European Union in light of London's historical prominence as a financial services hub.[7] Financial institutions might face myriad change-management tasks should they need to relocate people and operations out of the United Kingdom and into financial services centers that will remain in the European Union, such as Dublin, Frankfurt and Paris, and obtain the necessary licenses to reflect their new footprints. In the meantime, they also are attempting to develop contingency plans in the event that a failure in negotiations leads to a "no deal" or "hard Brexit" scenario by March 2019.

The Asia-Pacific region continues to experience increasing regulatory scrutiny in areas in which U.S. and European financial institutions have spent the past decade in remediation activities, notably financial crimes misconduct and overall strengthening of the risk and compliance management framework.

Concerns about keeping pace with technological change increase

Although regulatory compliance matters remain important, as described above, we continue to see an accelerating shift in financial institutions' attention toward business growth and innovation objectives. Notably, the attribute that saw the largest year-over-year increase in the current survey was:

> *Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low-cost base for their operations, or established competitors with superior operations.*

This risk issue also increased in significance from 2017 to 2018; however, the rate of increase from 2018 to 2019 was nearly three times that of last year, indicating a strong and accelerating degree of concern about the ability of financial institutions to keep pace with disruptive technology change.

[6] For more information, read *Understanding the General Data Protection Regulation: Frequently Asked Questions*, available at www.protiviti.com/gdpr.

[7] www.bankingsupervision.europa.eu/press/publications/newsletter/2018/html/ssm.nl180815_3.en.html.

Going into 2018, for example, 82 percent of U.S. commercial banks surveyed expected to increase FinTech investments over the next three years, and 86 percent of those expected to begin investing immediately.[8] These expectations were strongly borne out in practice. According to FinTech Global, total financial technology venture investments in the first half of 2018 alone ($41.7B) exceeded those made throughout all of 2017 ($39.4B).[9] Additionally, 2018 continued to see the total number of investments shrink, while average investment size increased significantly and investments continued to shift more to late stage startups. All of these data points indicate a maturing and consolidating market for FinTech capabilities as traditional financial institutions increase investments designed to ward off competition from non-traditional startups.

In practice, we have observed several specific areas of investment, including:

- **Use of technologies such as robotics and other workflow automation tools, natural language processing, and artificial intelligence/machine learning to dramatically increase the efficiency of and reduce costs associated with operational, risk management and compliance activities.** In particular, we are seeing that anti-financial crime and fraud risk management functions are at the center of significant innovation and cost reduction efforts.
- **Modernizing legacy technology platforms and data storage infrastructure to reduce the competitive advantage that "born digital" competitors have in these areas, and enable greater use of big data-driven solutions such as AI-supported digital customer service assistants.** Over the past year, global money center banks such as HSBC (piloting its "Pepper" robot in branches[10]) and Bank of America (with its "Erica" digital assistant[11]) have made headlines for their innovations in these areas. In 2019, we expect to see these trends continue and increasingly trickle down to smaller organizations, as well.
- **Consolidating platforms and providing a more efficient and user-friendly customer-facing digital experience across internet and mobile platforms as well as in physical locations.**
- **Evaluating the feasibility of and beginning to launch initial use cases for distributed ledger technology, particularly in areas such as global payments, trade clearing, and custody operations.**

[8] www.americanbanker.com/news/bank-fintech-investment-will-focus-on-blockchain-and-ai.
[9] http://fintech.global/2018-is-already-a-record-year-for-global-fintech-investment/.
[10] www.cnbc.com/2018/06/26/this-bank-is-staffing-branches-with-humanoid-robots-that-dance-take-s.html.
[11] https://promo.bankofamerica.com/erica/.

Concerns about talent on the rise

In addition to attention shifting to the risk of technology-driven disruption discussed above, the other risk issue that saw the most significant increase between the 2018 and 2019 surveys was:

> *Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets*

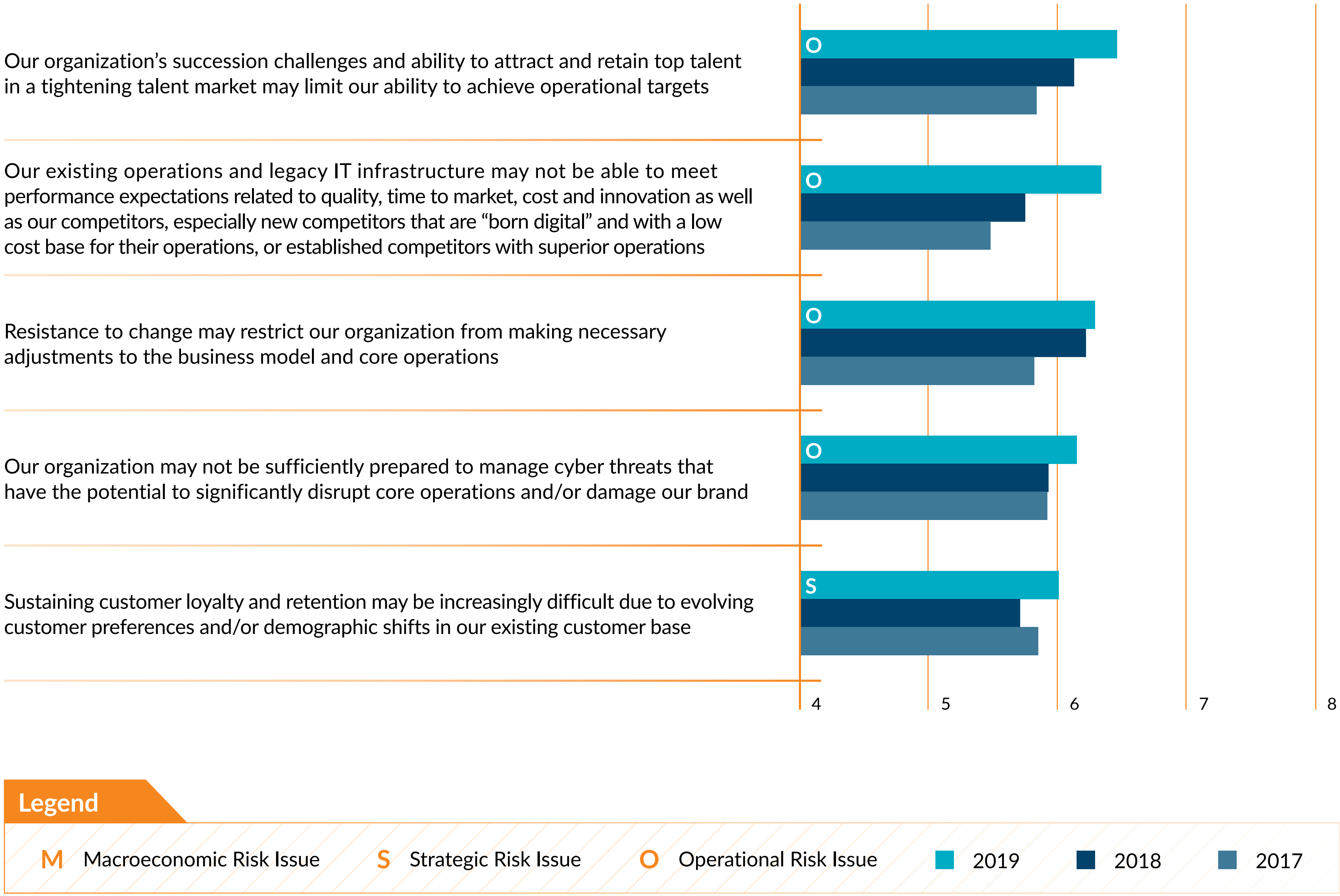
We believe heightened focus on this risk stems from multiple factors. First, at this point in the economic cycle, markets such as the United States have essentially reached full employment and costs to attract and retain specialized talent have increased. For example, while the overall U.S. unemployment rate stood at 4.4 percent as of October 2018, unemployment for the "financial activities" sector was less than half that rate, at 2 percent.[12]

In addition to a broad-based war for talent, this risk issue is strongly coupled with concerns about technological disruption as described above. Financial institutions of all types and sizes are struggling to meet the vastly increased need for data scientists, quantitative resources, information security professionals and other technical specialists. Unlike other positions for which financial services firms must recruit, in these areas they must compete not only with one another, but also with "FAANG"-type tech companies (Facebook, Amazon, Apple, Netflix and Google) that often are viewed as the premier employers in these fields.

Beyond the demand within CIO and chief data officer-type functions for specialized talent, we also are seeing concerns on this front across the second and third lines of defense. For example, as financial institutions increasingly use more complex AI/ML-driven models in place of traditional rules-based programs in areas such as credit underwriting and fraud risk management, chief audit executives worry about how they will be able to find and retain the audit talent with the right technical skills to evaluate these models. In addition, we have had multiple conversations with regulatory agency leadership who share these concerns with respect to their own supervisory teams. Given all of the above, we expect these risks to continue to remain elevated in the years ahead.

[12] www.statista.com/statistics/217787/unemployment-rate-in-the-united-states-by-industry-and-class-of-worker/.

Consumer Products and Services



Commentary — Consumer Products and Services Industry Group

With many baby boomers retiring in the foreseeable future and ongoing industry disruption, Consumer Products and Services organizations are clearly concerned about the competition for talent and succession planning. Increasing in significance notably from the prior year, succession challenges and the ability to attract and retain top talent is at the top of risk issues on the minds of Consumer Products and Services industry leaders for 2019. This continues a trend revealed last year, which also showed a significant jump for this risk issue. In fact, while it was a "Potential Impact" risk issue in 2017, it has been a “Significant Impact” risk issue the past two years.

This issue relates closely to an ongoing interest among these organizations to enhance corporate culture and focus on building and enhancing customer experience. It has been well-documented that consumer products organizations, and retailers in particular, must think and operate differently to be successful in an ever-changing digital business environment.

Consumers have increasingly high expectations for superior customer experience, from near real-time delivery of products ordered online to offering beneficial on-site expertise in retail stores.

Sustaining customer loyalty and retention also ranks as a top five risk for the industry group, as retailers, in particular, explore new and innovative ways to keep their customers engaged and loyal. Bottom line, the status quo is no longer sufficient.

In light of this, succession challenges, and especially the ability to attract and retain top talent, is a key issue as Consumer Products and Services organizations seek to put in place the right leadership and talent to bring in innovative ways of thinking to cultivate and manage their organizations in this new landscape.

This risk issue and resistance to change (another top five risk for this industry group) reflect what is being called the ongoing “retail apocalypse.” Some retailers are thriving in this dynamic environment, delivering high levels of service and capabilities — both online and in their physical stores. Others are struggling and have yet to figure out the right formula for innovation and driving revenue and sales. Here again, the right leadership and new ways of thinking are of paramount importance, requiring strong succession planning as well as recruiting and fostering the talent needed to move the organization forward rather than resist changes to dated strategies and practices.

This landscape is also reflected in our top five list of risk issues, all of which are considered “Significant Impact” risks by industry board members and executives, and all of which have increased year-over-year in significance.

Competing against “born digital” companies, the second-highest rank risk issue for 2019, has been a simmering challenge for several years, but has now become a critical matter for leadership in the Consumer Products and Services industry group to address. With numerous factors at play, “born digital” companies have an obvious big advantage when it comes to competing for market share. For instance, the cost of upgrading or replacing aging legacy systems is considerable, as is offering customers a seamless omnichannel experience to keep them coming back for more and excited about the brand.

> Consumer Products and Services companies are undergoing a sea change made possible with disruptive digital technologies. But at the root of this change is the old adage updated to today's optics – customers are, and always will be, kings and queens! They want it all and industry players who are determined to survive and thrive in this brave new world must adapt to shifting customer preferences, wherever they lead.
>
> — Richard Childs, Managing Director, Consumer Products and Services Industry Leader, Protiviti

It doesn't help matters that more Consumer Products and Services organizations are becoming wary of making seemingly open-ended investments that may not achieve the desired results. They believe that at some point there will be an economic slowdown, possibly limiting their ability to move quickly to make necessary infrastructure improvements. They also are concerned that they may not be able to make these investments fast enough to compete with born-digital organizations that already operate in digital and innovative ways on a daily basis. These organizations do not need to transform — they already are digital. It's very possible that as this dynamic continues to unfold, so-called legacy organizations that continue to fall behind in market share, technology and innovations will become acquisition targets.

Yet for these legacy, or traditional, organizations, competing against born-digital players is not a "no win" proposition. There are long-established companies that are ramping up their technology infrastructure and online services, as well as acquiring digital assets to compete in the digital world. There is a strategy for success, but it needs to be planned and executed well.

With regard to cyber threats, the only surprise in this finding is that this risk issue has not been ranked higher in prior years. Looking at the history of cyber attacks, consumer products and retail organizations were among the first entities to be considered primary targets. Whereas today organizations in virtually any industry should consider themselves targets for hackers, early on it was retailers that were attacked on a regular basis. And for the foreseeable future, consumer products and retail organizations remain a top, if not the top, target for cyber attacks. As evidence of this, look no further than the recent breach announced by a major hotel chain, in which 500 million customer records containing highly personal information were breached.

Consumer products and retail companies cannot thrive without customer loyalty and retention. This strategic risk issue is at the core of why the other top five risks — all operational — are top of mind for these companies. The potential cost of reputational damage due to a cyber attack is a more critical issue than ever before — far more than, for example, actual dollar losses, or costs for credit monitoring services for customers affected by a data breach. A data breach can permanently and irreparably damage the customer's trust and brand loyalty the organization worked so hard to build. Board members and executives throughout the industry recognize that cyber risk can cripple their organizations and scare away their customers.

TABLE OF CONTENTS

Manufacturing and Distribution

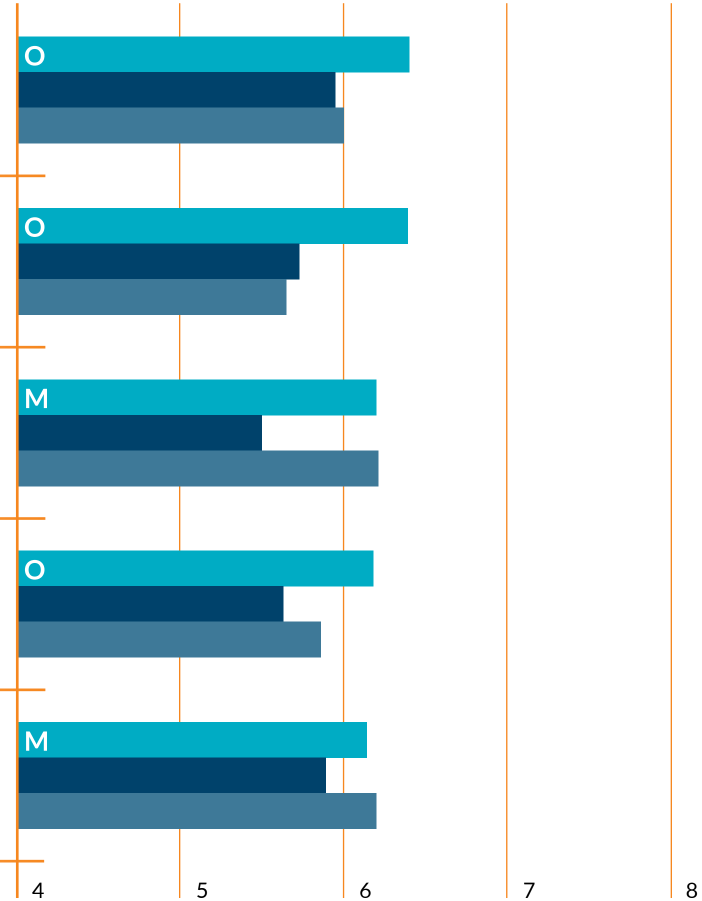
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Evolving changes in global trade policies may limit our ability to operate effectively and efficiently in international markets

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Anticipated increases in labor costs may affect our opportunity to meet profitability targets



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

Commentary — Manufacturing and Distribution Industry Group

Boards and executive management in manufacturing and distribution organizations view a substantially different risk landscape in 2019 versus the prior year, with four of the five top risk issues changing year over year. However, our results indicate that last year's top risk issues for the industry group did not drop in significance — in fact, the risk ratings for each of them actually rose. What we do find is that the scores for the 2019 top risks increased substantially, suggesting manufacturing and distribution organizations are focusing on more tactical operational areas to ensure they can prosper over the long term.

Succession challenges and the ability to attract and retain top talent has been a consistent top five risk issue for manufacturing and distribution organizations for the past several years. However, its risk score and ranking as a "Significant Impact" risk issue indicate it is being viewed with more urgency for 2019.

The U.S. unemployment rate was 3.7 percent for October 2018 (a 49-year low), versus 4.1 percent a year ago and 4.9 percent two years ago. It is no wonder that this risk is top-of-mind for board members and executive management in this industry group. In fact, the unemployment rate is even lower (an estimated 3.2 percent) in the manufacturing sector, making it tougher to find skilled workers, especially for today's automated and technologically advanced processes. In certain geographies, manufacturing industry retirements are exacerbating the challenge, causing companies to look closely into incentives that may draw more candidates. And closely related to these challenges, another top five risk issue for the Manufacturing and Distribution industry group involves anticipated increases in labor costs — potentially affecting the ability to meet profitability targets.

With regard to addressing existing operations and legacy IT infrastructure, this risk issue has steadily crept up over the past two years, finally landing in the top five for 2019. While last year's top five risk regarding the rapid speed of disruptive innovations and new technologies is not ranked as high this year, the broader issues of business and digital transformation and innovation still reflects the impact of that reality on the current state: Outdated legacy systems and/or disconnected/decentralized systems may put manufacturing companies behind their peers, considering the pace of IT change and competitor migrations to next-generation systems to better support the business. Organizations recognize the significant efforts (and costs) to update and upgrade. So the question is not if, but when, to make these improvements to keep pace with the competition and, in particular, born-digital companies that think and operate innovatively at their core.

Not surprisingly, changes in global trade policies potentially limiting the ability to operate effectively and efficiently in international markets remains a top five risk issue. The severity of this risk's rating, once again at the "Significant Impact" level, is consistent with two years ago, when manufacturing organizations were apprehensive about which direction a new U.S. administration might take with economic policy and global trade relationships. Early on, the Trump administration was more focused on healthcare, a new tax code and border protection rather than trade, likely driving down the anticipated significance

> People, trade, cyber and efficiency issues are top-of-mind for Manufacturing and Distribution organizations, but digital innovation opportunities are, as well. Deploying digital capabilities to transform customer fulfillment, quality management, decision-making velocity, cybersecurity, asset management, predictive maintenance, energy usage optimization and resource conservation can improve the business model, sustain competitive advantage and reduce risks.
>
> — Sharon Lindstrom, Managing Director, Manufacturing and Distribution Industry Leader, Protiviti

of this risk issue last year. But throughout 2018, near weekly headlines about new trade agreements, tariffs and trade wars has brought this risk back to the forefront. This makes sense, given that certain sectors, including those reliant on aluminum and steel, are experiencing the impact of the tariffs on their operations. Given the current uncertainty of how the trade wars will play out, we expect this risk to remain high heading into 2019. But longer term, this risk is likely to moderate as nations reach agreements on trade policies and practices.

Board members and executive management in the Manufacturing and Distribution industry group also see cyber threats as a "Significant Impact" risk issue. Although historically considered a lower-priority target industry for cyber attackers, manufacturing organizations increasingly present a broader risk to cyber threats due to Industry 4.0 and the Industrial Internet of Things. In addition, the higher risk rating this year likely reflects the fact that many manufacturers fall short in their cybersecurity planning. Furthermore, the above-mentioned risk regarding existing operations and legacy IT infrastructure possibly not meeting performance expectations leaves them more vulnerable to cyber attacks.

Overall, board members and executive management in the industry believe the magnitude and severity of risks their organizations will face in 2019, with respect to reaching or exceeding profitability or funding targets, are slightly higher than 2018. Since three of the top five risk issues are operational in nature, with potential direct impact to the bottom line, these results explain why these risks are growing concerns.

Technology, Media and Telecommunications

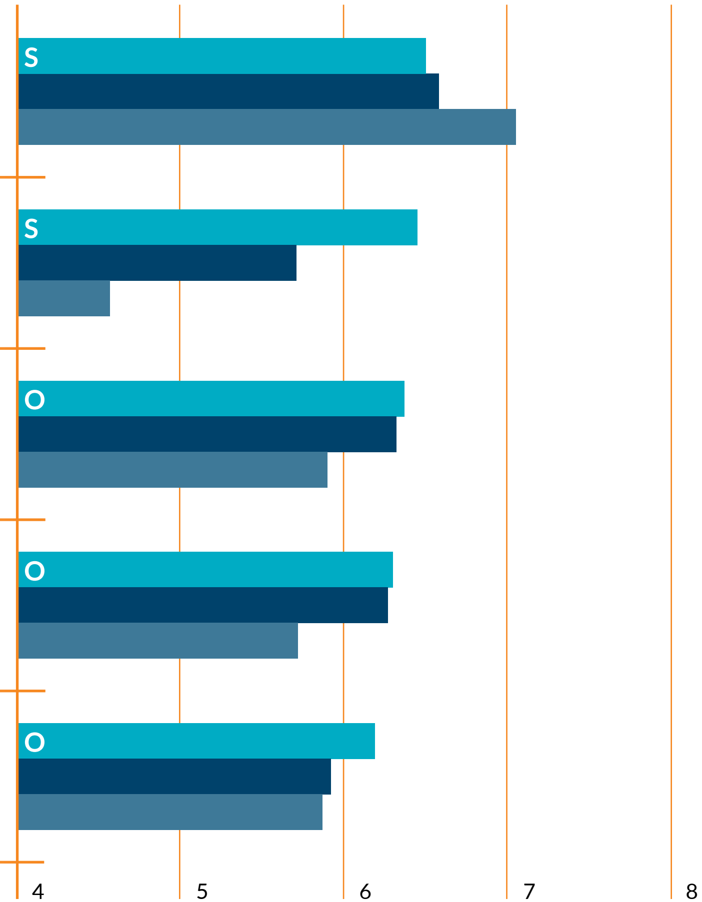
Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Ease of entrance of new competitors into the industry and marketplace or other significant changes in the competitive environment (such as major market concentrations due to M&A activity) may threaten our market share

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

Commentary — Technology, Media and Telecommunications Industry Group

The rapid speed of disruptive innovations remains the top risk for the Technology, Media and Telecommunications (TMT) industry group for the third consecutive year. This is understandable given the rapid pace of change and innovation in the industry and the significantly reduced half-life for dated, legacy business models that can be disrupted and become obsolete quickly.

If anything, it is a bit surprising to find the significance of this risk issue to be moderating, particularly compared to two years ago. It is possible that while the rapid speed of disruptive innovations remains a critically important area for board members and executive management in the industry to address and manage, there is a higher level of awareness about it than ever before, and organizations arguably have become more knowledgeable of strategies to address it effectively. We see many organizations in the industry focusing intently on research, development and ongoing innovation. Most have been facing the risk of disruptive innovations for years and are proactively changing business models and adjusting long-term strategies to avoid being disrupted. That said, we continue to see emerging markets and technologies come into play — another reason why this remains the top risk issue for the industry.

With regard to the ease of entrance of new competitors into the industry (a new top five risk for the industry group in 2019), this has always been a relatively significant risk to TMT organizations. Historically, the barriers to entry in the industry have been low, with few regulatory hurdles. The industry embodies the example of startup companies — with potentially disruptive business models — launching their business from a garage or apartment. However, it is noteworthy to see the rapid increase in significance for this risk issue over the past three years. This also may be perceived as a more pressing risk issue today because, more than ever before, new companies, rather than seeking to obtain and then maintain a relatively small slice of the market, are intentionally becoming acquisition targets for larger companies that subsequently strategize to gain a greater market share for themselves. Organizations — large and small — face potential threats from new entrants in the market that can be acquired by competitors and leveraged to grab market share from them.

Ensuring privacy and identity management and information security/system protection remains a critical risk issue for the industry. Threats continue to grow from multiple bad actors, including rogue individual hackers and global hacking groups as well as nation states. Technology organizations continue to maintain a vast amount of personal data of users and customers. Considering how the brands and reputations of several well-known companies in the industry group continue to be affected by data breaches — and with no end in sight — it is evident why reputational risk is a top concern.

Succession challenges and the ability to attract and retain talent goes hand-in-hand with broader corporate culture issues that remain key areas of focus for TMT organizations. Building a healthy company culture and becoming a responsible firm that demonstrates strong corporate governance, social responsibility and ethical business practices deliver far-reaching benefits that promote attracting and retaining top talent. In today's highly competitive landscape for talent in many different functional areas, having a strong culture can be the difference between keeping and losing your best people.

As part of this concern, more organizations in the industry group are also assessing their diversity and inclusion practices, which will help them address long-term succession and talent retention challenges. As discussed in Protiviti's *Responsible Technology Firm of the Future* white paper series, gender imbalance in the science, technology, engineering and mathematics (STEM) fields will have technology companies struggling to fill millions of these jobs that will be created over the next decade. The implication for technology organizations is there may not be enough qualified employees to drive innovation. By extension, these organizations will be hampered significantly in their leadership succession planning.[13]

Addressing these challenges will not be easy. In addition to a marked gender disparity in entry-level STEM jobs, there are staggering imbalances at the executive level. The fraction of startups owned by women and the percentage of women holding executive positions at technology companies are abysmally low. The number of women occupying board seats also requires attention. This is important in solving the entry-level challenge because there are those who believe that the issue can only be resolved by starting at the top of the company. To make matters worse, attrition is more than twice as high for women as it is for men.[14] These figures suggest that a sea change is needed before gender disparity in STEM fields is no longer a glaring issue.

> "Technology, Media and Telecommunications companies have long focused on creating enterprise value; however, the changing risk landscape is altering conversations in C-suites and boardrooms across the industry, necessitating a more balanced focus on governance and regulatory concerns, a more risk-informed corporate culture, a stronger commitment to social responsibility — including gender diversity — and other matters germane to preserving enterprise value.
>
> — Gordon Tucker, Managing Director, Technology, Media and Telecommunications Industry Leader, Protiviti

[13] *The Responsible Technology Firm of the Future: Corporate Social Responsibility*, Protiviti: www.protiviti.com/US-en/insights/responsible-tech-series-part-4.

[14] Ibid.

Healthcare and Life Sciences

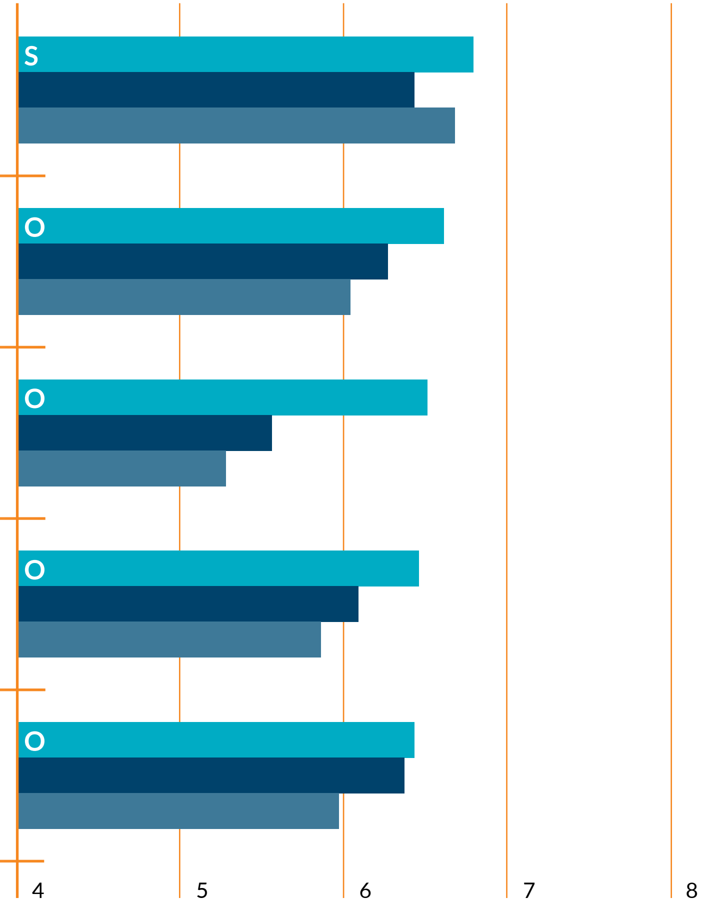
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand



Legend

M Macroeconomic Risk Issue   S Strategic Risk Issue   O Operational Risk Issue   2019   2018   2017

Commentary — Healthcare and Life Sciences Industry Group

Regulatory changes and regulatory scrutiny

The healthcare landscape continues to evolve, with regulatory changes and scrutiny on the rise. This trend continues due to pressure to reduce regulations, control regulatory costs, and increase public engagement for more transparency, public notice and due process in rulemaking. The cost of staying on top of regulatory changes has increased, in part, by imposing significant fines and take-backs for fraud, waste and abuse violations. The collaboration between various government agencies (e.g., Office of Inspector General (OIG), Centers for Medicare and Medicaid Services (CMS), Office of Civil Rights (OCR), and Department of Justice (DOJ)) has exposed the largest healthcare fraud takedown in history — sending a strong message that fraud and abuse will not be tolerated.[15]

The Affordable Care Act remains on uncertain ground as tax reform promises to end the individual mandate, which will mean fewer Americans with health insurance, and likely fewer doctor visits and hospital stays. Additionally, this will result in a decrease in the amount of drugs and medical devices sold. Constraints to access to healthcare will be eased with the growth of telemedicine. The opioid crisis will continue to take center stage, resulting in an increase in mental health and treatment facilities. Additionally, enforcement agencies will increase focus on physician prescribing patterns in the coming year, as elevated scrutiny of the 340B Drug Pricing Program is already being felt across the industry. Specific examples include increased Human Resources and Services Administration (HRSA) audits and the need for annual independent audits of contract pharmacy arrangements. Ultimately, implementing robust and effective compliance programs will be key to understanding and mitigating risk and managing the complex regulatory landscape.

Key compliance areas of focus manifest themselves in the provider revenue cycle terrain, as well. For example, the OIG is focusing on appropriate and compliant coding and billing practices in the post-acute care environment. Additionally, billing and collection policies remain under scrutiny to ensure providers adhere to 501(r) requirements for fair collection protocols, as well as timely identification, quantification and refunding of government overpayments. Also, 2019 will be the first year that home health organizations will be subjected to potential civil monetary penalties for not adhering to new CMS regulations surrounding documentation of the patient's care plan and utilizing data to ensure continuous improvement of patient care and patient outcomes.

Privacy/identity management and information security

A major theme in 2019 will continue to be data privacy and security. The European Union has led the charge with the General Data Protection Regulation (GDPR), which is intended to protect the privacy of individuals within the European Union and the European Economic Area. For healthcare organizations in the United States, the GDPR

[15] "National Health Care Fraud Takedown Results in Charges Against 601 Individuals Responsible for Over $2 Billion in Fraud Losses," U.S. Department of Justice press release, June 28, 2018, www.justice.gov/opa/pr/national-health-care-fraud-takedown-results-charges-against-601-individuals-responsible-over.

carries implications that have yet to be truly understood and enforced. The California Consumer Privacy Act is a new state law that imposes GDPR-like privacy protections. It is set to affect the privacy landscape in the next few years as it gives consumers unprecedented control over their personal data. Other states are following suit with their own legislative initiatives. The Health Insurance Portability and Accountability Act (HIPAA) continues to be a major headache for healthcare-covered entities, with penalties for HIPAA violations that have surpassed the $100 million mark. Clearly, the data privacy movement is in full force and organizations will need to increase their resources to meet the demand of complying with regulations and also to prevent penalties as well as reputational damage, as privacy compliance has become required table stakes in the industry.

Identity management continues to be a source of struggle for the healthcare industry. Managing hundreds or even thousands of users that have been introduced into the environment through numerous means (many of whom are not employees, have non-standard roles, etc.) would place a strain on even the most established and formalized user access management teams. Many healthcare organizations are moving to role-based access, assigning business owners to monitor non-employees, and implementing requirements for more frequent (e.g., quarterly) review of assigned access rights by supervisors or business owners. However, even with those controls, effectively managing access continues to be of concern.

Healthcare organizations leading in this space are focusing on:

- Understanding all areas in which users could be introduced to the environment;
- Assigning business ownership for user access;
- Utilizing role-based access with specific approval requirements for any standard access deviations;
- Moving away from the use of “set up user A like user B”;
- Rolling out multi-factor authentication for remote access and cloud applications;
- Enabling additional authentication functionality for local workstation access; and
- Securing vendor access.

As healthcare continues to become more digital and with more third-party vendors playing a part in the patient/consumer service arena, the need for defined processes with appropriate user access technologies will only grow in importance.

Existing operations meeting performance expectations, competing against “born digital” firms

In 2017, the Health Care Industry Cybersecurity Task Force, established by Congress, issued its *Report on Improving Cybersecurity in the Health Care Industry*, which represented an analysis of the state of healthcare cybersecurity in the increasingly interconnected world of today.[16] What was perhaps most troublesome about the findings outlined in this report were the 38 references to patient safety compared to 19 references to patient privacy. It is clear that change is needed as the industry continues to rely more heavily on technology.

[16] *Report on Improving Cybersecurity in the Health Care Industry*, Health Care Industry Cybersecurity Task Force, June 2017, www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

One theme identified in the report is that legacy devices are a significant problem in the healthcare industry. The Task Force recommended that the industry take action to "phase out legacy and insecure health care technologies."[17] In today's digital world, existing operations and legacy IT infrastructure are a common source of pain and frustration as organizations try to keep up with the competition. Many strategies to further embrace digital transformation die in their infancy because legacy operations and infrastructure are incapable of supporting those initiatives. In resource-constrained organizations, the need to advance and evolve is, all too often, overruled by the desire to cut costs and limit spend.

Recent years have also seen an increase in the opening of virtual care centers. We've seen growth in the use of telehealth, resulting in a consumer-friendly level of convenience that patients are seeking. Furthermore, a truly new business threat is emerging as "born digital" companies such as Amazon, Apple and Google see healthcare as an industry ripe for disruption. These firms are aggressively seeking opportunities to upend healthcare with radical new approaches. Keeping up with these competitors is a reality that will force many healthcare organizations to take a hard look at increasing their appetite for risk. The need to replace legacy operations and IT infrastructure may soon be a harsh reality that comes along with that cultural shift.

> "A look at the top healthcare industry risks for 2019 presents a sobering picture, as each risk represents a significant issue for any player in the industry group. Each organization's strategy, business and risk management plans must take these risks into consideration. For example, regulatory changes and scrutiny are on the rise and well up at the top of the list. The cost of staying on top of and responding to regulatory developments continues to increase. Proactive and effective risk management across the identified top risks will be key to maintaining or enhancing enterprise value.
>
> — Richard Williams, Managing Director, Healthcare Industry Leader, Protiviti

[17] Ibid.

Succession challenges and ability to attract and retain top talent

Attracting and retaining top talent remains a key concern for organizations seeking to appropriately plan succession and configure future operational targets. This is particularly true in the healthcare provider space, with expected nursing and physician shortages in the coming years caused primarily by an aging population on the demand side and an anticipated reduction of interest in the medical profession due to increased regulatory scrutiny on the supply side. An aging workforce, especially at top executive levels, and difficulty for non-profit systems to offer competitive compensation for specialized talent in areas such as cybersecurity also add to the complexity of this issue.

With an increasingly diverse workforce and tightening talent market, understanding what driving factors directly attribute to employee attrition should be top priority. One of the first steps in understanding these factors is the development and deployment of a holistic employee retention strategy and program. In tandem, these items not only should seek to determine employees' top priorities, but also fully engage them in the processes that influence the trajectory of their careers. Effective strategies aid in reducing potential attrition and can also serve as an effective tool in recruiting top-tier talent.

Cyber threats

The healthcare industry continues to undergo significant change due to the frequency and variety of new technologies being utilized across the care continuum, including devices, applications (on-premises and in the cloud), interfaces, etc. As a result, cyber threats are continuously evolving. But when this technology explosion is coupled with the need for seemingly instant access to sensitive information to provide care and the push for interoperability among many healthcare organizations, the resulting potential exposure expands at a rate with which even the most mature organizations struggle to keep pace. Healthcare organizations are also hindered in dealing with applications and devices that may have known security flaws that cannot be patched, updated or fully retired. Many of these may be the only technology on the market to meet specific healthcare delivery needs for certain care specialties or may have required large capital outlays. They also may involve vendors that have failed to provide and allow for ongoing security updates (as is the case with many medical devices).

Those healthcare organizations that are more mature in addressing cyber threats have had success in addressing the technology expansion, with formal governance and assessment processes for new technologies to include connectivity, control and security aspects. Additionally, these organizations are performing ongoing risk analyses, including regular vulnerability scanning and multifaceted penetration testing efforts to identify new areas of vulnerability to be addressed, and have implemented processes and controls to allow for proper incident response and contingency planning should key incidents occur. Healthcare organizations must continue to address the threat landscape presented by the influx of technology from today and tomorrow in order to properly care for patients.

Energy and Utilities

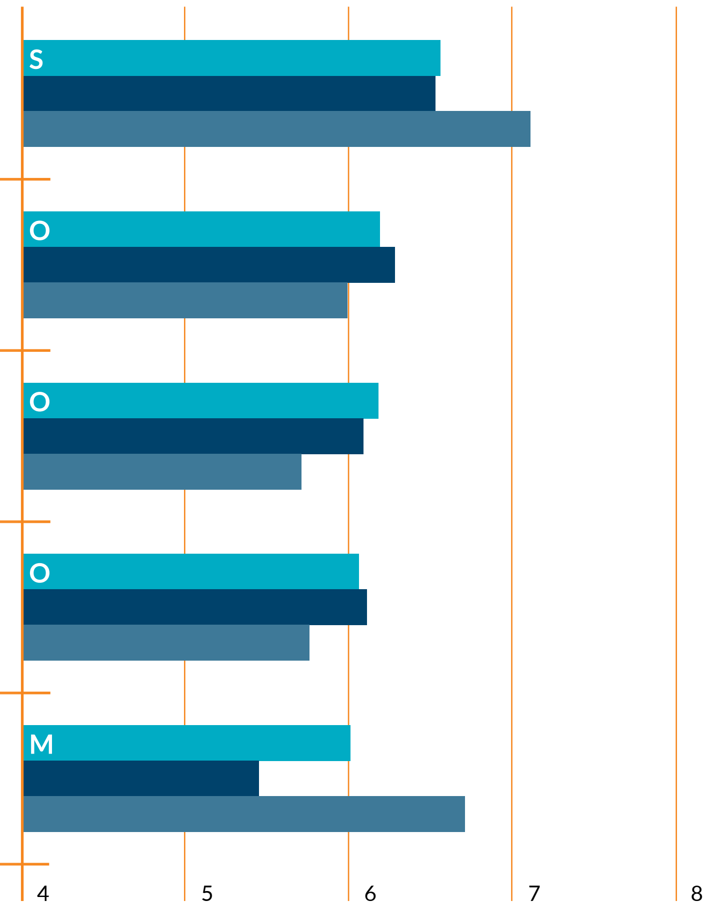
Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Commentary — Energy and Utilities Industry Group

Despite an annual risk outlook that has been volatile over the past three years, the overall view for the Energy and Utilities industry group in 2019 appears to be more optimistic than in the recent past, buoyed by stability in commodity prices, efficiencies realized in operations, and a renewed sense that potentially disruptive forces (geopolitical or technological) have not had sustained momentum. Nevertheless, as outlooks from prior years of our study have shown, there remains an awareness that organizations in the industry group are often blindsided, and board members and C-level executives must continue to be prepared to shift with market trends. As Energy and Utilities industry executives look to formulate their strategies going forward, there are some interesting observations of the risks that lie ahead.

In comparing to last year's results, there are a couple of risks that fell just outside of the top five this year: succession and talent recruiting and retention challenges, and the risks around disruptive technologies. Succession and talent acquisition/retention challenges in the industry are still a priority, but we have seen an increased focus in energy and utility organizations on leadership development programs and human capital management initiatives to ensure there are replacements for the aging workforce. The disruptive technology topic is still an interesting trend that executives need to monitor, but their concerns appear to be easing a bit, as many believe the necessary advancements in various technologies that could disrupt the industry are still several years away from becoming a broader risk issue. Therefore, the risk remains an important issue but is an emerging one to be monitored over time rather than an immediate concern.

Supplanting these two risk issues for 2019 are two risks that historically have been in the top five for the industry group and are closely tied to the ever-changing geopolitical environment: cybersecurity and the risks around economic conditions in various markets. As operations become more "digital," the cybersecurity threat will continue to be an evolving risk for which the industry needs to stay vigilant. When viewed across the current geopolitical landscape, organizations have an elevated awareness for "bad actors" looking to cause harm, such as hacktivists targeting systems and data or, worse yet, adversaries that seek to obtain access to industrial control systems and create a disruptive event. There is also a realization that, with regard to cybersecurity, there is only so much the organization can control, as the enemy is constantly learning new ways to exploit vulnerabilities — particularly the people perimeter. But it is good to see

> Stability in commodity prices, efficiencies realized in operations, and a perception that disruptive geopolitical or technological forces have not had sustained momentum have improved the overall 2019 outlook for the Energy and Utilities industry group. With this more optimistic view (as compared to the recent past), there remains an awareness that the uncertainty of emerging risks and significant disruptive change lies ahead beyond 2019.
>
> — Tyler Chase, Managing Director, Energy and Utilities Industry Leader, Protiviti

that this risk issue has been elevated and should continue to garner the attention and investment necessary to be mitigated.

Organizations are also increasingly reactive to global political decisions that create widespread impacts to markets across the industry. Just a few examples in 2018 that forced energy and utility organizations to be nimble are decisions regarding Iran crude oil, the trade war between the United States and China, and continued tensions in the Middle East. These geopolitical events often "come out of the blue" and result in emergency board-level discussions to quickly evaluate the organizational impact and strategize on steps that should be taken to mitigate any enterprise and operational risks in the various affected markets. While the U.S. government continues to be viewed as favorable for the industry, the macroeconomic and geopolitical environment appears to be volatile enough to warrant the increased level for this risk.

Closely tied is the risk that the organization's culture may not encourage the timely identification and escalation of emerging enterprise risks. With the evolving geopolitics and increased regulations and reporting requirements, organizations within the industry group are being forced to review their risk environment from a broader perspective and ensure that mechanisms are in place to identify and evaluate emerging risks. Additionally, as seen in the top five

TABLE OF CONTENTS

risk issues and discussed below, energy and utility organizations historically have focused on proven business models and are slower to adopt changes. When considering this historical reality, anything that may bring about a need to rethink the business model due to a newly identified risk issue may receive initial pushback within the organization and not receive the attention it warrants.

The two top risk issues for 2019 have been mainstays in the Energy and Utilities industry group for many years of our study, which is not surprising given the evolving regulatory environment and an industry that values traditional operational practices and thus is reluctant to change.

Regulatory scrutiny and the overall regulatory environment remain a high-risk area for the industry group, particularly considering the recent midterm elections in the United States, as varying restrictions on drilling were on the ballot in many states. Additionally, continued pressure from environmental, social and governance (ESG) activists on operational areas such as hydraulic fracturing, emissions and reducing carbon footprints remain a consistent challenge for the industry group. Other concerns include increased tariffs on many products, such as steel, and resulting trade wars that may impact the geopolitical arena for the industry group around the world. Additionally, many leaders in the industry group are focusing on appeasing their stakeholders as investor momentum shifts toward social responsibility and emission/carbon reduction actions, both of which have broad impacts to the organization's operations and internal processes as they look to comply and report. Case in point: The recent announcement that Royal Dutch Shell is setting carbon emission targets and linking them to long-term executive compensation illustrates the dynamic environment that players in oil and gas face.

Tying this all together is the view that energy and utility organizations tend to operate on "tried and true" strategies and thus have been slower than other industries to adopt changes. We have seen a shift in recent years as these organizations desire to be more efficient in their operations and back office, yet there is still a sentiment that the industry group is based on an infrastructure of mechanical plants and equipment that have a history of predictable performance and is expensive to change. While this might be true today, with a focus from the public on social responsibility and increased demands to be operationally efficient, energy and utility companies need to continue to step outside of their comfort zone and look for ways to decrease costs and adopt emerging technologies.

Analysis of Differences Between Public and Non-Public Entities

Participants in the survey represent three types of organizations: publicly traded companies (401 respondents), privately held for-profit entities (270 respondents), and not-for-profit and governmental organizations (154 respondents).

We analyzed responses across these three types of entities to determine whether organizational types rank-order risks differently. Similar to our analysis summarized earlier in this report, we analyzed responses about overall impressions of the magnitude and severity of risks across the three organizational type categories. Again, the scores in the table below reflect responses to the question about their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months, using a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive."

Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	**2019**	**2018**	**2017**
Public Companies	6.2	6.1	6.6
Privately Held For-Profit Companies	6.3	6.0	6.1
Not-for-Profit and Governmental Organizations	5.9	5.5	5.8

Overall, the magnitude and severity of risks for all three organization types increased from 2018 and are generally consistent with the 2017 results (although public companies remain a little less concerned than in 2017). Not-for-profit and governmental organizations saw the largest increase in overall risk levels for 2019, although they still view 2019 overall as slightly below the "Significant Impact" (above 6.0) level. However, looking at the responses in total, we see a slight pickup in overall risk concerns for the full sample in 2019.

Surprisingly, even though overall impressions of the magnitude and severity of risks increased from 2018, each of the three types of organizations rated all their top five risks for 2019 at the "Significant Impact" level. Most importantly, privately held for-profit companies rated all the top five at that level, whereas in 2018 they rated none of their top five risks as "Significant Impact" risks. Public companies and not-for-profit and governmental organizations also rated all five of their top risks as having a "Significant Impact."

Privately held for-profit companies were the only organizations to identify a macroeconomic risk (economic conditions in markets we currently serve may restrict growth opportunities) as one of the top five risks; in addition, privately held companies had two operational risks and two strategic risks in the top five. All five of the top risks identified by not-for-profit and governmental organizations are operational risks. Public companies recognized three operational risks and two strategic risks.

All of the organizations are concerned about succession and talent challenges, with that risk in the top five risks for each of the organization types. Public companies and privately held for-profit organizations shared four of their top five risks: existing operations and legacy IT may not be able to meet performance challenges, succession and talent challenges, regulatory changes and scrutiny may heighten, and rapid speed of disruptive innovations. Public companies also included concerns about cyber risks in their top five risks, while private for-profit companies ranked concerns about economic conditions as part of the top five. Not-for-profit and governmental organizations rated two risks related to culture in their top five list of risks: concerns about resistance to change and concerns regarding the timely escalation of risk issues.

TABLE OF CONTENTS

Public Companies

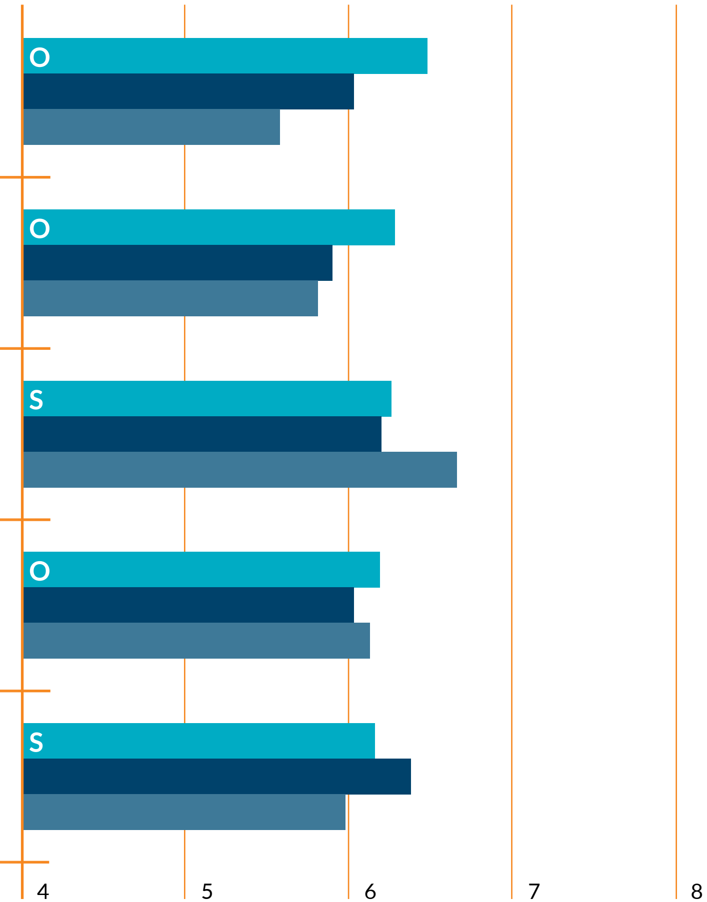
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Privately Held For-Profit Companies

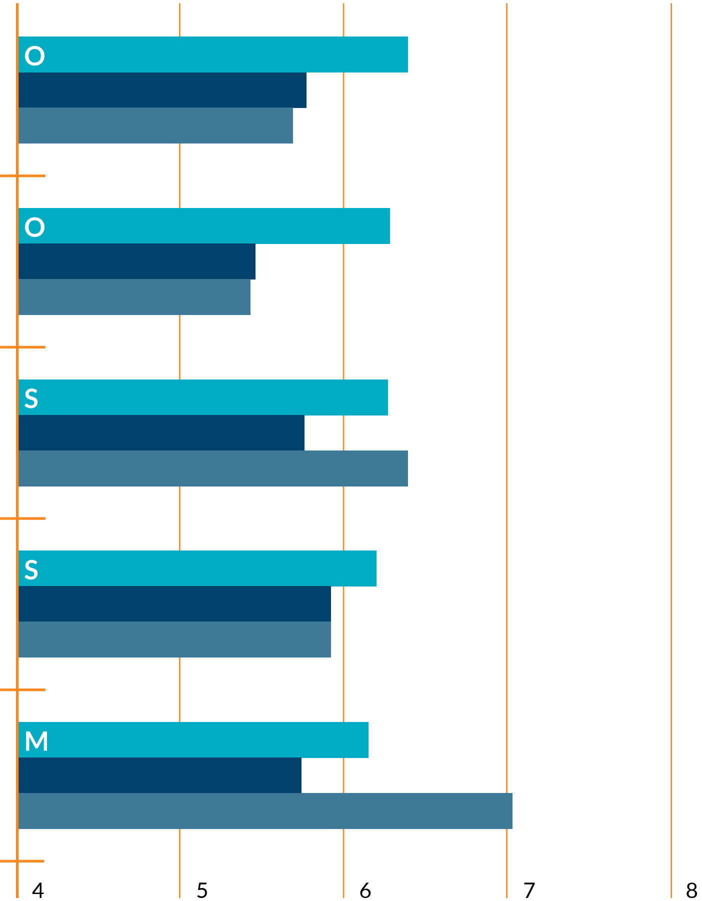
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization



Legend

M Macroeconomic Risk Issue | S Strategic Risk Issue | O Operational Risk Issue | 2019 | 2018 | 2017

Not-For-Profit and Governmental Organizations

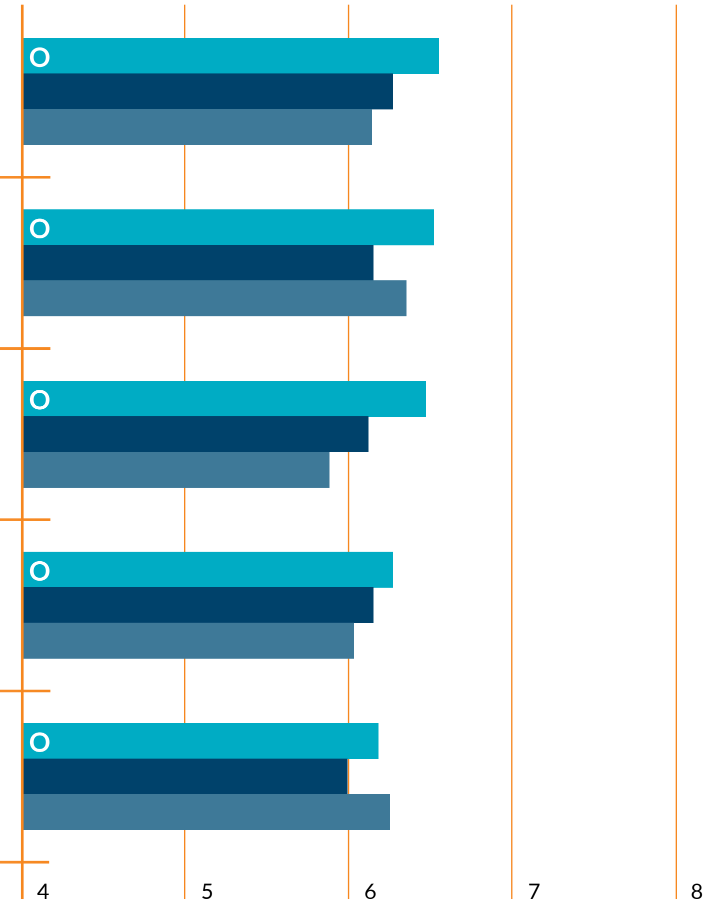
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Ensuring privacy/identity management and information security/system protection may require significant resources for us

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Our organization's culture may not sufficiently encourage the timely identification and escalation of risk issues that have the potential to significantly affect our core operations and achievement of strategic objectives



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Analysis of Differences Among Geographic Regions

For this year's report, we obtained a sufficient number of non-U.S.-based organizations to split the sample into eight distinct groups: 371 North America-based organizations (NA), 120 organizations based in Europe or the United Kingdom (EUR), 86 organizations from Australia/New Zealand (ANZ), 82 organizations from Asia (A), 72 organizations based in Latin America/South America (LASA), 40 organizations from the Middle East (ME), 33 organizations from India (IND), and 21 organizations based in Africa (AFR).

We analyzed responses across the eight groups to determine whether respondents across different geographic locations rank-order risks differently. Similar to our analysis summarized earlier in this report, we analyzed responses about overall impressions of the magnitude and severity of risks across the three categories. Again, the scores in the table below reflect responses to the question about their overall impression of the magnitude and severity of risks their organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months, using a 10-point scale where 1 = "Extremely Low" and 10 = "Extensive."

> We're excited about the global participation in this year's top risks survey and the interesting results across different regions. There are some similarities but also a number of distinctive differences. This year's survey offers a baseline for comparison in the years to come.
>
> — Andrew Clinton, Executive Vice President, International Operations, Protiviti

Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	**2019**	**2018**	**2017**
North America-based Organizations	5.6	5.7	6.0
Europe-based Organizations	6.4	6.4	6.7
Australia/New Zealand-based Organizations	6.7	N/A	N/A
Asia-based Organizations	6.6	N/A	N/A
Latin America/South America-based Organizations	7.1	N/A	N/A
Middle East-based Organizations	6.8	N/A	N/A
India-based Organizations	7.0	N/A	N/A
Africa-based Organizations	5.6	5.3	N/A

Globally, organizations from six of the eight geographic regions agree that the overall magnitude and severity of risks are of a "Significant Impact" level in 2019. Except for North America-based organizations, all regions rate all of their top five risks at the "Significant Impact" level; in contrast, North America only rates two of its top five risks at that level.

Across the eight regions, the similarities and differences are interesting. Five regions are most focused on operational risks, whereas three regions are most focused on macroeconomic risks. Organizations based in North America, Europe, Australia/New Zealand, Asia and Latin America/South America all have at least three operational risks in their top five risks. The threat that existing operations and legacy IT systems may not be able to meet performance expectations appears in each of those five regions' top five lists. In addition, threats related to succession challenges and the ability to attract and retain talent and the threat that regulatory changes may heighten appear in four of the five geographic regions. Only organizations from Europe and Latin America/South America rate risks related to macroeconomic conditions in their top five, with both reporting the threat of economic conditions restricting growth opportunities. Latin America/South America organizations also expressed concern about increasing labor costs.

On the other hand, three geographic regions are more focused on macroeconomic risks. Organizations based in the Middle East, India and Africa all have at least three macroeconomic risks in their top five risks. The Middle East region rated concern about geopolitical shifts and instability in government regimes as its number one risk, while organizations in India rated this third. Organizations in both the Middle East and Africa were significantly concerned with the macroeconomic risks that economic conditions in markets that they currently serve may restrict growth opportunities. In addition, organizations in these two regions also shared the strategic risk that social media and internet applications may threaten how they do business.

Organizations in India and Africa placed the threat that their ability to access sufficient capital would restrict growth opportunities as one of their top five risks. Surprisingly, concerns about cyber threats only appear in the top five risks of organizations based in North America and Europe; perhaps that is because both regions have strong disclosure requirements and include many high-profile cyber targets. Respondents from the Asia-Pacific region were the only group to identify the risk of uncertainty surrounding key suppliers as a top five risk, likely because supply chains in many Asian companies are based on a low-cost model that does not support present-day growth imperatives. In addition, only organizations in Latin America/South America ranked the risk of anticipated increases in labor costs as a top five risk. This could be due to the trade and tariff uncertainties during the latter part of 2018 as well as higher inflationary pressures in many countries in that region.

North America HQ Organizations

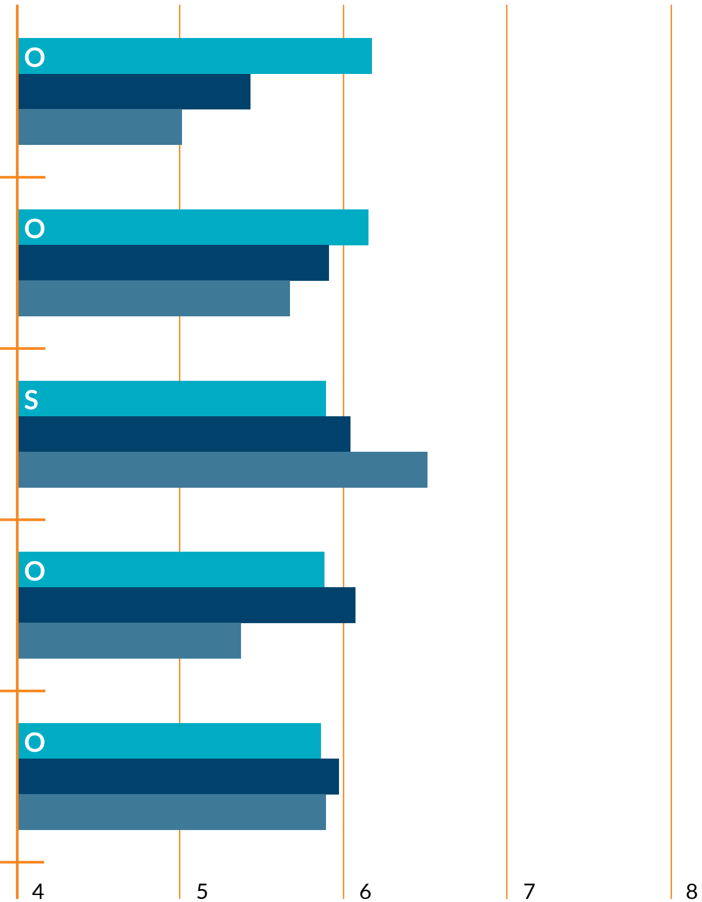
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

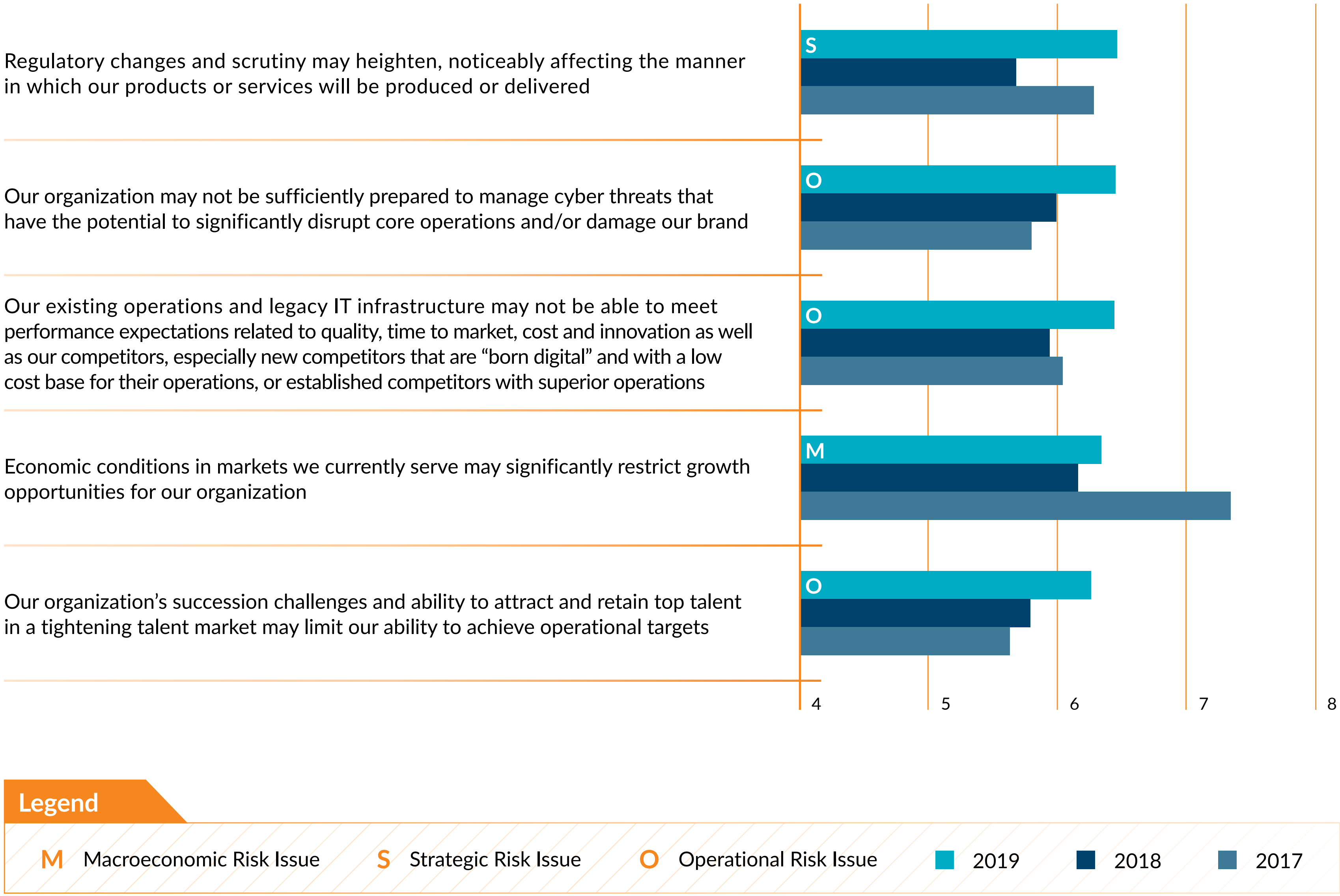
Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Europe HQ Organizations



Australia/New Zealand HQ Organizations

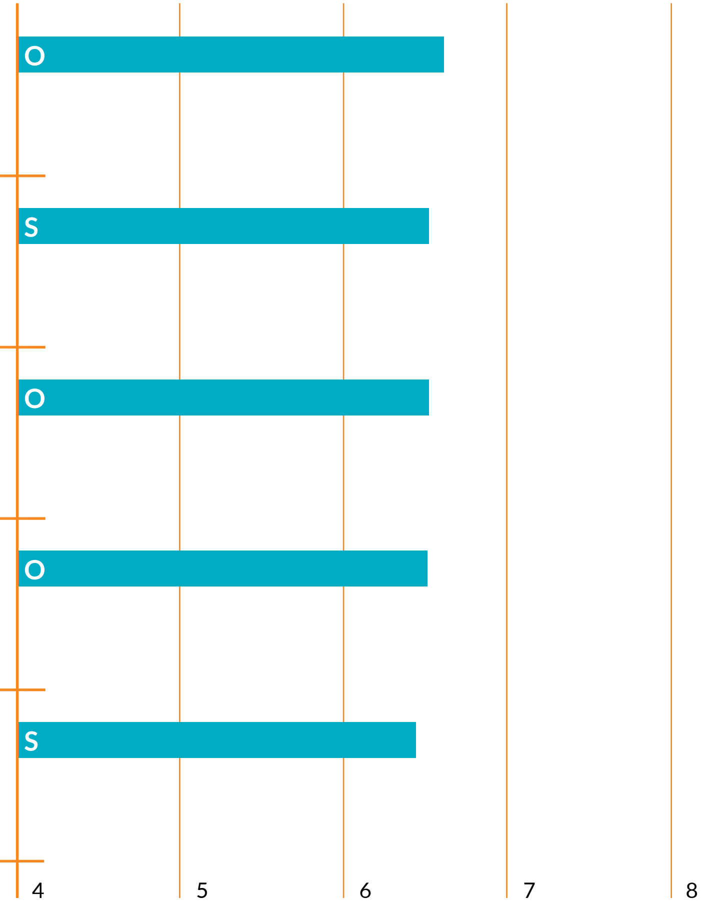
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Asia HQ Organizations

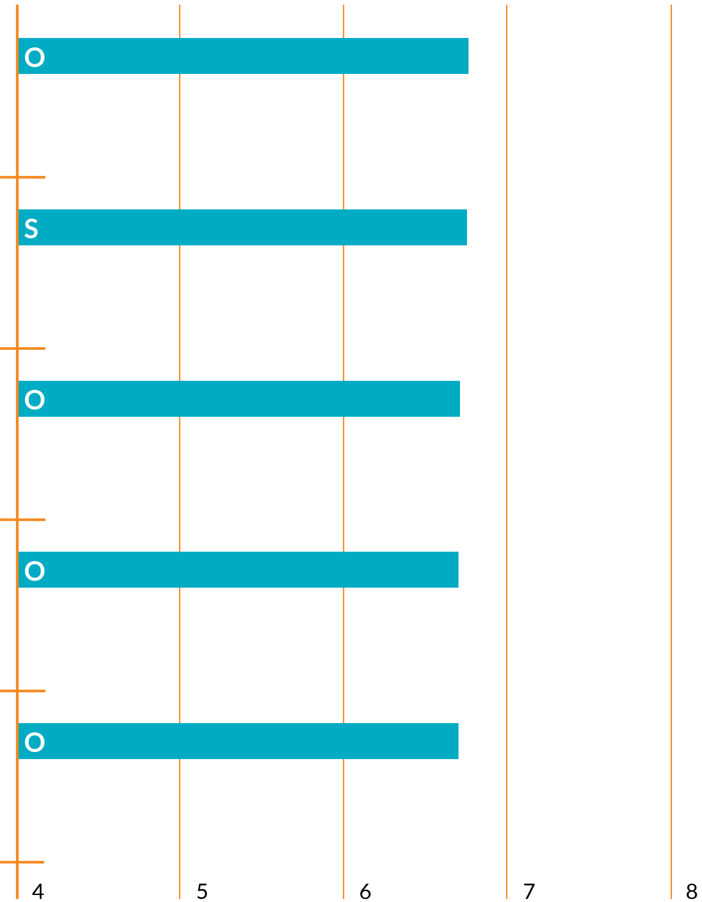
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Inability to utilize data analytics and "big data" to achieve market intelligence and increase productivity and efficiency may significantly affect our management of core operations and strategic plans

Uncertainty surrounding the viability of key suppliers, scarcity of supply, or stable supply prices may make it difficult to deliver our products or services at acceptable margins

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations



Legend

M Macroeconomic Risk Issue　S Strategic Risk Issue　O Operational Risk Issue　2019　2018　2017

Latin America/South America HQ Organizations

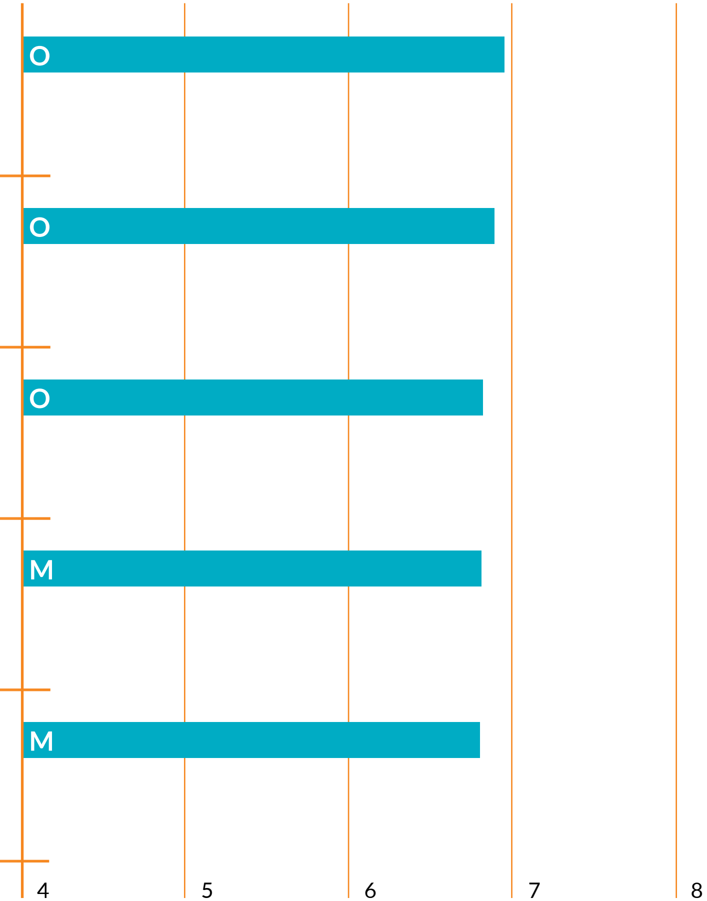
Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations

Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization

Anticipated increases in labor costs may affect our opportunity to meet profitability targets



Legend

M Macroeconomic Risk Issue — S Strategic Risk Issue — O Operational Risk Issue — 2019 — 2018 — 2017

Middle East HQ Organizations

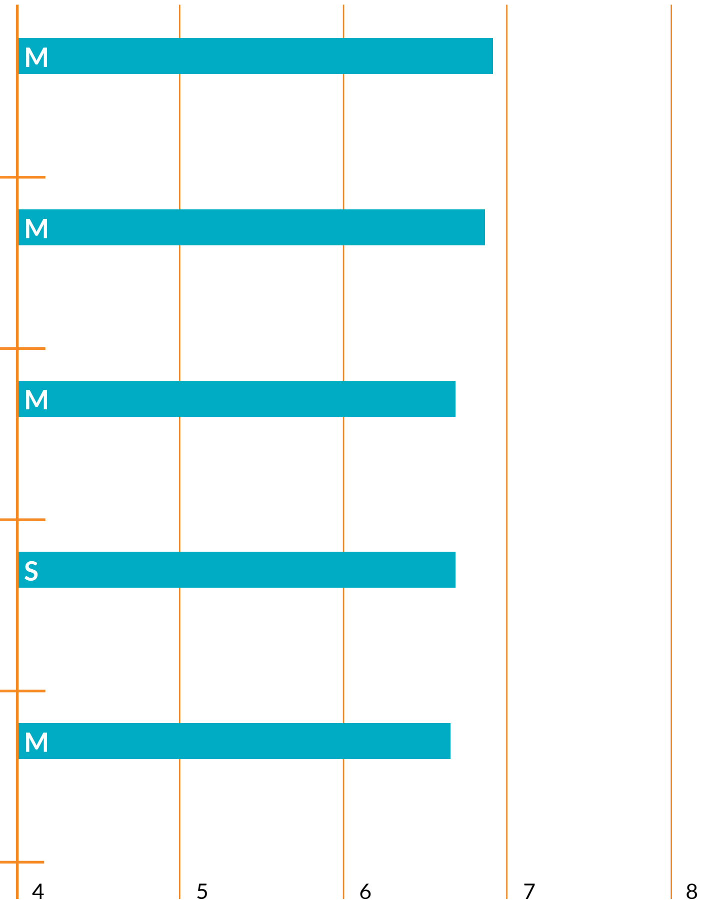
Geopolitical shifts and instability in governmental regimes or expansion of global terrorism may restrict the achievement of our global growth and profitability objectives

Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization

Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business

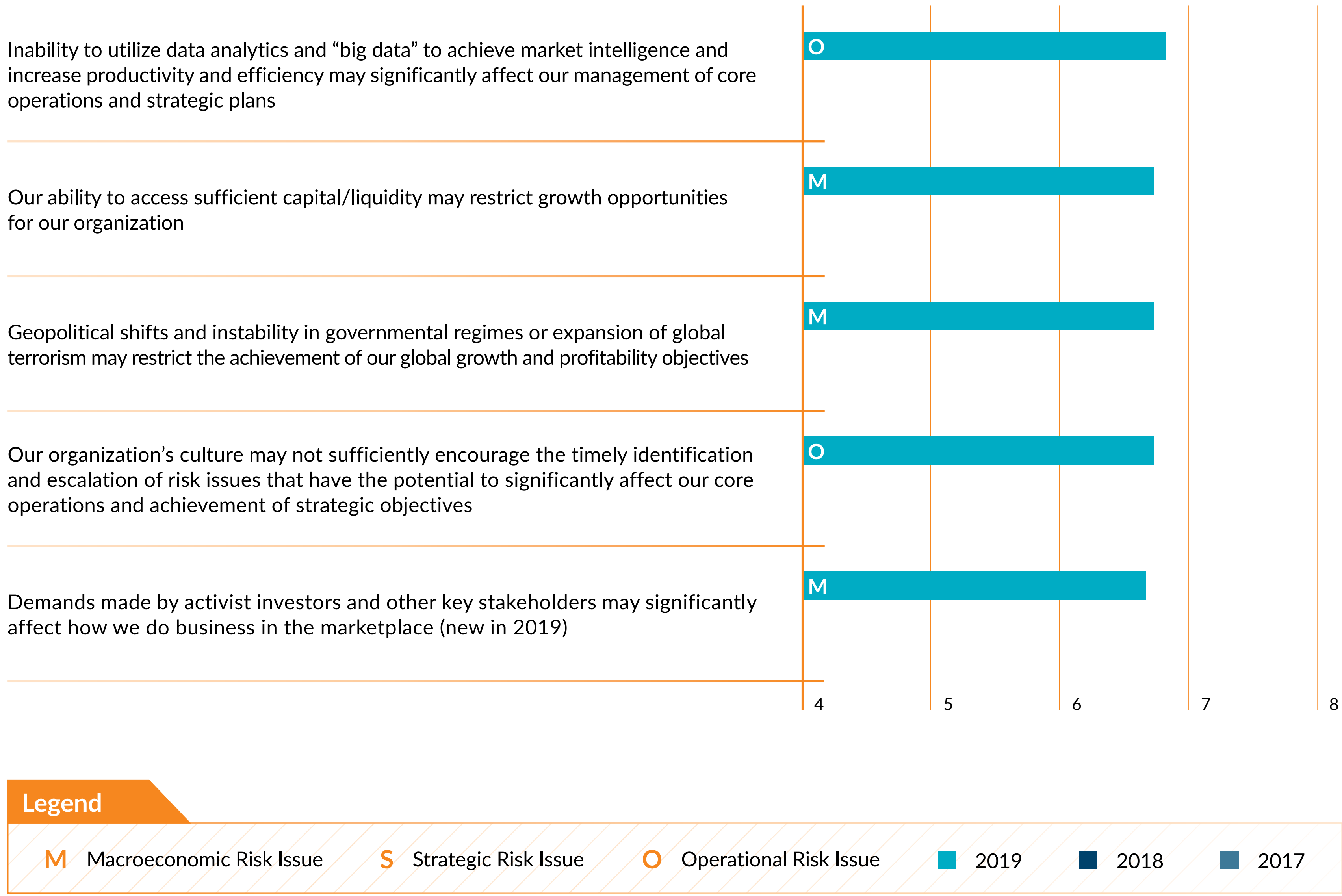
Uncertainty surrounding the influence and continued tenure of key global leaders may impact national and international markets to the point of significantly limiting our growth opportunities



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

India HQ Organizations



Africa HQ Organizations

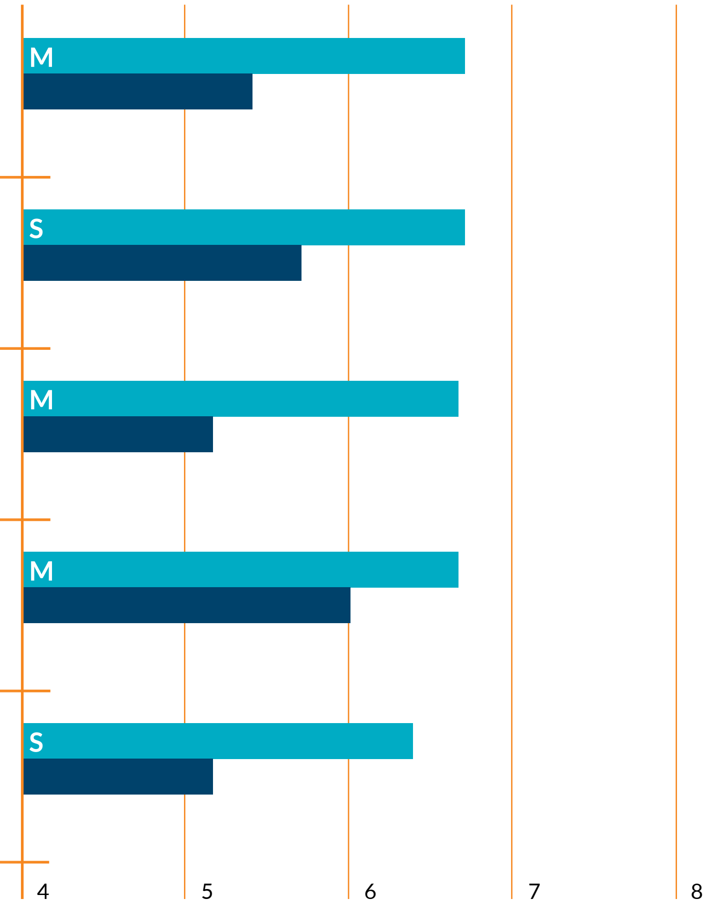
Our ability to access sufficient capital/liquidity may restrict growth opportunities for our organization

Social media, mobile applications and other Internet-based applications may significantly impact our brand, customer relationships, regulatory compliance processes and/or how we do business

Anticipated volatility in global financial markets and currency exchange rates may create significantly challenging issues for our organization to address

Economic conditions in markets we currently serve may significantly restrict growth opportunities for our organization

Rapid speed of disruptive innovations enabled by new and emerging technologies and/or other market forces may outpace our organization's ability to compete and/or manage the risk appropriately, without making significant changes to our business model



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue 2019 2018 2017

Analysis of Differences Between Organizations With and Without Rated Debt

We also asked participants to indicate whether their organizations have rated debt outstanding, whereby the major credit rating agencies may evaluate the overall riskiness of the enterprise and, implicitly, the organization's risk oversight processes as part of the entity's overall credit score. We are particularly interested in observing how organizations with rated debt perceive their overall risk environment in light of the explicit focus of rating agencies on their management and governance processes, including enterprise-wide risk management.

Two hundred ninety-eight participants in the survey represent organizations with rated debt outstanding, while 473 respondents represent organizations without rated debt.

Fifty-four respondents indicated "I'm not sure" in response to this question for 2019.

The 298 organizations in our study with rated debt outstanding include 164 public companies, 78 private companies, and 56 governmental or not-for-profit organizations. For the 473 organizations without rated debt, 213 are public companies, 169 are private, and 91 are governmental or not-for-profit organizations. We report the survey results for 2019 and the two prior years for rated debt outstanding organizations and those without rated debt in the bar charts on the following pages.

The top five risks are the same for both types of organizations, but the ordering of the top five is different among the organizations.

Organizations with rated debt are most concerned about the risk of existing operations and legacy IT infrastructure being able to meet performance expectations, whereas that risk was ranked second for organizations with non-rated debt. In contrast, organizations without rated debt are most concerned about succession challenges and the ability to recruit and retain talent, whereas that was ranked second by organizations with rated debt. Concerns about regulatory changes and cyber threats rank as the third and fourth rated risks for organizations with rated debt and are switched for organizations without rated debt. Both organizations list the risk of resistance to change restricting the ability to make changes to the business model and core operations as their fifth most impactful risk.

Overall, while there is no marked difference between these two groups with respect to 2019 risk concerns, there is a change from 2018. In 2018, concerns about the organization's culture not encouraging the timely identification and escalation of risk issues represented a top five risk issue. In 2019, organizations with rated debt rated concerns about existing operations and legacy IT infrastructure being able to meet performance expectations and the ability to manage succession challenges and to recruit and retain talent as new top five risks. New 2019 risks for organizations without rated debt included concerns with existing operations and concerns about regulatory changes.

> We believe that the increased scrutiny that debt ratings agencies bring to those organizations with rated debt may help mitigate risk concerns. Investments in risk management processes are expected by these agencies, and these investments may serve to lower threat levels for those organizations.
>
> — Bruce Branson, Professor of Accounting, Associate Director, Enterprise Risk Management Initiative, Poole College of Management, NC State University

With Rated Debt

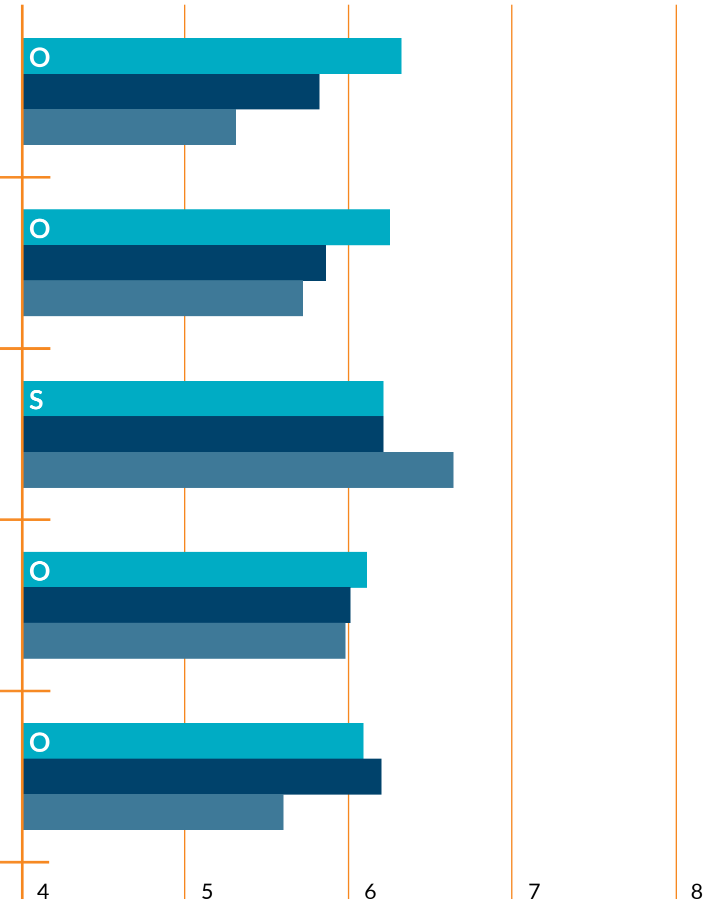
Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are “born digital” and with a low cost base for their operations, or established competitors with superior operations

Our organization’s succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue ■ 2019 ■ 2018 ■ 2017

Without Rated Debt

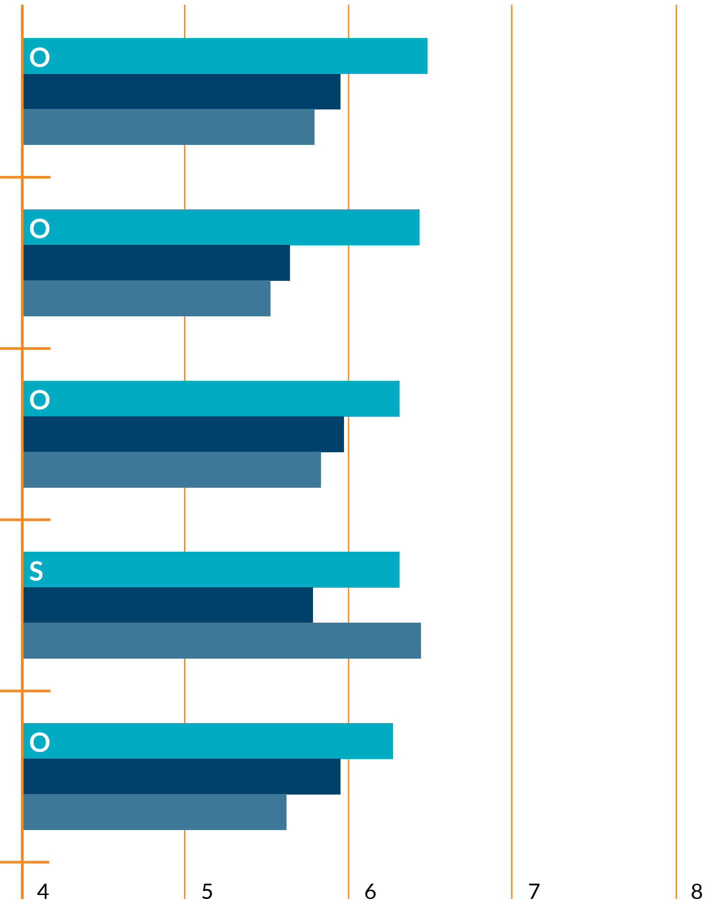
Our organization's succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

Resistance to change may restrict our organization from making necessary adjustments to the business model and core operations



Legend

M Macroeconomic Risk Issue S Strategic Risk Issue O Operational Risk Issue ■ 2019 ■ 2018 ■ 2017

Plans to Deploy Resources to Enhance Risk Management Capabilities

Recall that we asked respondents about their overall impression of the perceived magnitude and severity of risks to be faced and the likelihood of investing additional resources in risk management efforts. The respondents' overall response suggests an increase in the nature of the overall risk environment, with an average score of 6.2 in 2019 relative to 6.0 in 2018.

	2019	2018	2017
Overall, what is your impression of the magnitude and severity of risks your organization will be facing with respect to reaching or exceeding profitability (or funding) targets over the next 12 months?	6.2	6.0	6.2

In light of the risk environment, we asked executives to provide insights about whether the organization plans to devote additional resources to improve risk management over the next 12 months. We used a 10-point scale whereby 1 signifies "Unlikely to Make Changes" and 10 signifies "Extremely Likely to Make Changes."

Consistent with the finding that respondents noted an increase in their impression about the magnitude and severity of overall risks for 2019 relative to the prior year, they also indicate a higher likelihood of deploying more resources to risk management in 2019 relative to 2018 and 2017. This may be due to an overall realization that the world continues to grow in complexity and that there continues to be a need to invest in more robust risk management capabilities.

	2019	2018	2017
How likely is it that your organization will devote additional time and/or resources to risk identification and management over the next 12 months?	6.4	6.1	6.0

We also asked respondents a new question in 2019. Specifically, we asked "Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?" On a scale of 1 to 10, the average score for this question was 6.2. Challenges seem to be highest for organizations in the Healthcare and Life Sciences and Manufacturing and Distribution industry groups, which have average scores of 6.7 and 6.4, respectively.

	2019	2018	2017
Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?	6.2	N/A	N/A

The Financial Services industry group expressed the greatest likelihood to devote additional time and resources toward risk management in 2019, followed by the Technology, Media and Telecommunications and Healthcare and Life Sciences industry groups.

The Energy and Utilities industry group shows the greatest increase in likelihood to invest more in risk management capabilities in 2019 relative to 2018, increasing from 5.2 in 2018 to 6.1 in 2019. That finding is not surprising given that this industry group had the largest number of risks (14 out of 30 risks) rated at the "Significant Impact" level (i.e., an average risk rating of 6.0 or higher on our 10-point scale) and indicate that they anticipate significant challenges to sustaining and/or strengthening their risk management processes in the coming year (with a score of 6.7).

Likelihood that the organization plans to devote additional resources to risk management over the next 12 months

Full Sample			Financial Services			Consumer Products and Services			Manufacturing and Distribution			Technology, Media and Telecommunications			Healthcare and Life Sciences			Energy and Utilities		
2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017
6.4	6.1	6.0	6.7	6.4	6.3	6.1	6.0	5.8	6.3	6.3	6.3	6.4	6.3	5.9	6.4	5.9	5.5	6.1	5.2	5.9

Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?

	2019
Full Sample	6.2
Financial Services	6.2
Consumer Products and Services	6.0
Manufacturing and Distribution	6.4
Technology, Media and Telecommunications	6.1
Healthcare and Life Sciences	6.7
Energy and Utilities	6.0

> In improving risk management capabilities, companies must focus on how they can better anticipate, adapt and respond to change, as well as focus management efforts and resources on the risks and opportunities that truly matter in terms of their impact on achieving their strategic objectives and performance goals. This is what a risk-informed approach is all about.
>
> — Dolores Atallo, Managing Director, Protiviti

We also analyzed responses to these questions across different sizes of organizations — the largest organizations (those with revenues greater than $10 billion) exhibited the greatest increase in the likelihood that they plan to deploy additional resources to risk management (increasing from 6.4 to 6.9). These organizations are likely to be most exposed to the overall risk environment that is growing in complexity. Interestingly, only the smallest organizations expressed a decreased likelihood that they will be investing in more robust risk identification and management over the next 12 months. All other size categories of organizations indicate a higher level of risk management investment for 2019. Larger organizations also believe that they may face higher levels of challenges in sustaining or strengthening their risk management processes.

Likelihood that the organization plans to devote additional resources to risk management over the next 12 months

Full Sample			Revenues Less than $100M			Revenues $100M — $999M			Revenues $1B — $9.9B			Revenues $10B or Higher		
2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017
6.4	6.1	6.0	5.6	6.0	4.9	6.4	6.2	5.9	6.3	6.0	6.4	6.9	6.4	6.1

Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?

	2019
Full Sample	6.2
Revenues less than $100M	5.4
Revenues $100M — $999M	6.2
Revenues $1B — $9.9B	6.3
Revenues $10B or Higher	6.6

Public companies and privately held for-profit enterprises expressed similar levels of likelihood that they plan to invest more time and resources in building out their risk management infrastructure in 2019 relative to 2018. In addition, for-profit enterprises reflected a greater increase in the levels of likelihood to invest than the slight increase in not-for-profit and governmental organizations. The level of interest in improving risk management capabilities across all types of organizations signals a realization that risks affect all types of entities and that no one organization is immune to that fact. Therefore, no entity can afford to ignore the importance of risk management thinking.

Likelihood that the organization plans to devote additional resources to risk management over the next 12 months

Full Sample			Publicly Traded Companies			Privately Held For-Profit Enterprises			Not-for-Profit and Governmental Organizations		
2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017
6.4	6.1	6.0	6.5	6.2	5.9	6.5	6.3	6.4	5.9	5.8	5.5

Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?

	2019
Full Sample	6.2
Publicly Traded Companies	6.2
Privately Held For-Profit Enterprises	6.3
Not-for-Profit and Governmental Organizations	6.0

Interestingly, board members and all of the C-suite executives except for chief audit executives signal that their organizations are likely to invest additional resources in risk management over the next 12 months relative to the prior year. Board respondents appear to be most interested in seeing additional investment in risk management, as reflected by their average overall likelihood score of 7.1 for 2019, which reflects the largest increase in scores from 2018 among all respondent positions. CIOs/CTOs and Other C-Suite executives indicate similar high levels of likelihood for additional investments in risk management, likely intending investments in infrastructure modernization and cybersecurity.

Likelihood that the organization plans to devote additional resources to risk management over the next 12 months

Full Sample			Board Members			CEOs			CFOs			CROs			CAEs			CIO/CTOs			Other C-Suite		
2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017	2019	2018	2017
6.4	6.1	6.0	7.1	6.3	5.3	6.2	5.9	5.9	6.5	6.3	6.4	6.2	5.8	6.0	5.6	6.2	5.5	7.0	6.5	6.7	7.0	6.4	6.4

In addition, board members and respondents in the CIO/CTO and Other C-Suite categories sense the greatest level of challenges in sustaining and strengthening the coordination and exchange of risk information among senior executives.

Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?

	2019
Full Sample	6.2
Board Members	6.5
CEOs	5.9
CFOs	5.8
CROs	5.7
CAEs	6.2
CIO/CTOs	6.7
Other C-Suite	6.8

Recall that for this year, we had a sufficient number of respondents from different parts of the world to perform separate analysis across eight different regions around the globe. As a result, we are only able to show responses for all three years for respondents in North America, Europe and Africa, as shown in the table below.

Organizations with headquarters based in Australia/New Zealand, Latin America/South America and India indicate the greatest likelihood that they will devote additional resources to risk management over the next 12 months. Organizations based in North America and Africa reflected the smallest level of likelihood for that kind of investment in risk management.

Likelihood that the organization plans to devote additional resources to risk management over the next twelve months

	2019	2018	2017
Full Sample	6.4	6.1	6.0
North America	5.8	5.9	5.7
Europe	6.7	6.4	6.7
Australia/New Zealand	7.0	N/A	N/A
Asia	6.9	N/A	N/A
Latin America/South America	7.2	N/A	N/A
Middle East	6.6	N/A	N/A
India	7.1	N/A	N/A
Africa	5.7	6.5	N/A

Organizations based in Latin America/South America, India and Asia seem to face the greatest level of challenges in sustaining and strengthening the coordination and exchange of risk information among senior management.

Over the next 12 months, to what degree do you believe your organization will experience challenges to sustaining and/or strengthening the coordination and exchange of risk information among senior management, front-line business unit and process owners, second-line risk management leaders, and relevant subject-matter experts within the organization?

	2019
Full Sample	6.2
North America	5.6
Europe	6.5
Australia/New Zealand	6.6
Asia	6.8
Latin America/South America	7.0
Middle East	6.7
India	6.9
Africa	5.4

A Call to Action: Questions to Consider

This report provides insights from 825 board members and executives about risks that are likely to affect their organizations over the next 12 months. Overall, most rate the business environment as significantly risky, and on an overall basis, respondents rated 25 of the 28 risks included in prior year surveys as higher in 2019 relative to 2018, suggesting that there continues to be a number of uncertainties in the marketplace for 2019.

The ever-changing risk landscape and the overall perceived increase in the magnitude and severity of risks should prompt boards and senior executives to closely scrutinize the approaches they use to keep an eye on emerging risks. Unfortunately, many organizations continue to manage risks the way they have for many years, even though the profile of risks is changing as the way business is conducted evolves. Their risk profile is most certainly not yesterday's risks, and a focus on financial and compliance risks using static analog age tools and without any conception of the organization's risk appetite leaves decision makers to their own devices. Soon those organizations may realize, once it's too late, that the level of investment in risk thinking and their willingness to engage in robust risk management tools and dialogue is inadequate. Now is the time for boards and C-suites to closely examine how their organization approaches risk management and oversight in the digital age to pinpoint aspects requiring significant improvement. Managing today's risks using outdated techniques and tools may leave the organization exposed to significant, undesirable risk events that could threaten its brand and reputation, and even its very survival.

> In the digital economy, enterprise risk management can be a real difference maker if it contributes to reshaping strategy in advance of disruptive change. When the fundamentals of the business are about to change, executive management must be positioned to secure "early mover" positioning in the marketplace to capitalize on market opportunities and emerging risks.
>
> — Jim DeLoach, Managing Director, Protiviti

Accordingly, in the interest of evaluating and improving the risk assessment process in light of the findings in this report, we offer executives and directors the following diagnostic questions to consider when evaluating their organization's risk assessment process:

Assess impact of leadership and culture on risk management

Because culture and leadership significantly impact the organization's approach to risk oversight:

- Is the board's and the C-suite's support for more robust risk management processes evident to key stakeholders across the organization?
- Do we have an accurate read on how our organization's culture is impacting how employees engage in risk management processes and conversations? If so, how do we know?
- Do we have a "speak up" culture that encourages transparency and sharing of contrarian information and bad news? Are our employees convinced they can "speak up" without fear of repercussions to their careers or to their compensation? For example, does the process:
  - Encourage an open, positive dialogue for identifying and evaluating opportunities and risks?
  - Focus on reducing the risk of undue bias and groupthink?
  - Give adequate attention to differences in viewpoints that may exist across different executives and different global jurisdictions?
- Is adequate attention given to red flags indicating signs of a dysfunctional culture that suppresses escalation of important risk information or encourages unacceptable risk taking? Are warning signs posted by the risk management function or internal audit addressed timely by executive management?

Evaluate the scope of risk focus

Given the pace of change experienced in the industry and the relative riskiness and nature of the organization's operations:

- To what extent are we centering our focus on risks in the context of our organization's strategy, business objectives and operations?
- Does the process consider a sufficient time horizon to pick up strategic risks, e.g., the longer the horizon, the more likely new issues will present themselves? Does the process consider extreme as well as plausible scenarios?
- Is our focus on the identification of risks mostly on internal operations, people and processes with minimal focus on external risks linked to geopolitical shifts, emerging innovations, and changes in macroeconomic factors?
- Are we encouraging the identification of opportunities to take on more risk on a managed basis?

Ensure the robustness of risk assessment across the organization

Because risks are constantly changing, the risk management process needs to be definable and repeatable to ensure business leaders are staying abreast of emerging issues:

- Would most describe our organization's approach to risk management as one that is siloed across disparate functions in the organization or one that is more ad hoc than structured?
- Is the process supported by an effective methodology that is definable, repeatable and understood by key stakeholders?
- Do we engage all the right stakeholders in the risk identification process?
- How often are we engaging in a formal or an informal risk assessment process? Is it frequent enough?
- Does the process delineate the critical enterprise risks from the day-to-day risks of managing the business so as to focus the dialogue in the C-suite and boardroom on the risks that matter?
- Is there a process for identifying emerging risks? Does the risk-identification process allow the board and management enough time to adequately consider response plans to these risks?

Nail down accountabilities for managing risks following a risk assessment

Following completion of a formal or informal risk assessment:

- Are risk owners assigned for newly identified risks?
- Is there an effort to source the root causes of certain risks that warrant a better understanding? Does the process look for patterns that connect potential interrelated risk events?
- Are effective risk response action plans developed to address the risk at the source? Are the risk owners accountable for the design and execution of those responses?
- Are significant risks related to the execution of the strategy and business model monitored over time to consider whether changes have occurred requiring corrective action, and the organization operates within established risk tolerances in meeting key business objectives?
- Are we monitoring the business environment over time for evidence of changes that may invalidate one or more critical assumptions underlying the organization's strategy? If so, when there is evidence that one or more critical assumptions underlying the strategy are becoming, or have become, invalid, does management act timely on that knowledge to revisit the strategy and undertake necessary mid-course adjustments?
- Do decision-making processes consider the impact of a decision on the organization's risk profile?
  - Have we sufficiently communicated the relative value and importance of considering risk in decision making across the enterprise?
  - Is the board sufficiently involved in the decision-making process, particularly when it involves acquisition of new

businesses, entry into new markets, the introduction of innovative technologies or alteration of key assumptions underlying the strategy?

- Is there actionable, current risk information that is widely shared to enable more informed decision making?

Communicate an enterprise view of top risks and board risk oversight

With respect to communicating and overseeing the risk profile:

- Is the board informed of the results of management's risk assessment on a timely basis? Do directors agree with management's determination of the significant risks?
- Are significant risk issues warranting attention by executive management and the board escalated to their attention on a timely basis? Does management apprise the board in a timely manner of significant emerging risks or significant changes in the organization's risk profile?
- With respect to the most critical risks facing the organization, do directors understand at a high level the organization's responses to these risks? Is there an enterprisewide process in place that directors can point to that answers these questions and is that process informing the board's risk oversight effectively?
- Is there a periodic board-level dialogue regarding management's appetite for risk and whether the organization's risk profile is consistent with that risk appetite? Is the board satisfied that the strategy-setting process appropriately considers a substantive assessment of the risks the enterprise is taking on as strategic alternatives are considered, and the selected strategy is executed?
- Given the organization's risk profile, does the board periodically consider whether it has access to the diverse expertise and experience needed — either on the board itself or through access to external advisers — to provide the necessary oversight and advice to management?

These and other questions can assist organizations in defining their specific risks and assessing the adequacy of the processes informing their risk management and board risk oversight. We hope the important insights about the perceived risks on the horizon for 2019 provided in this report prove useful. We also hope that the insights serve as a catalyst for an updated assessment of risks and the risk management capabilities in place within all organizations, as well as improvement in their risk assessment processes and risk management capabilities.

Research Team

This research project was conducted in partnership between Protiviti and North Carolina State University's Enterprise Risk Management Initiative. Individuals participating in this project include:

NORTH CAROLINA STATE UNIVERSITY'S ERM INITIATIVE

- **Mark Beasley**
- **Bruce Branson**
- **Don Pagach**

PROTIVITI

- **Pat Scott**
- **Jim DeLoach**
- **Kevin Donahue**
- **Brian Christensen**
- **Emma Marcandalli**
- **Dolores Atallo**
- **Matthew Moore**

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 75 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

ABOUT NORTH CAROLINA STATE UNIVERSITY'S ERM INITIATIVE

The Enterprise Risk Management (ERM) Initiative in the Poole College of Management at North Carolina State University provides thought leadership about ERM practices and their integration with strategy and corporate governance. Faculty in the ERM Initiative frequently work with boards of directors and senior management teams helping them link ERM to strategy and governance, host executive workshops and educational training sessions, and issue research and thought papers on practical approaches to implementing more effective risk oversight techniques (www.erm.ncsu.edu).

NC STATE Poole College of Management
Enterprise Risk Management Initiative

www.erm.ncsu.edu

protiviti®

www.protiviti.com