BLACK & WHITE PAPER

451 Research® | Advisory

Managing Risk through Digital Transformation

How enterprises see the relationship between security issues and their digital transformation initiatives

SEPTEMBER 2017

PREPARED FOR

CenturyLink®

About this paper

A Black & White paper is a study based on primary research survey data that assesses the market dynamics of a key enterprise technology segment through the lens of the "on the ground" experience and opinions of real practitioners – what they are doing, and why they are doing it.

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 207 426 1050

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

INTRODUCTION

This report is part of a global study of more than 1,400 enterprises that is designed to explore the extent of digital transformation playing out in organizations planning or actively applying digitization to strengthen competitive differentiation. Respondents included both IT professionals and line-of-business (LOB) managers across multiple vertical and geographic sectors. In identifying four key organizational pillars (operational efficiency, customer/constituent experience, agility and management of risk) as drivers for digital transformation, we assess how strategies are being shaped by business imperatives and the priorities of different key vertical markets. The objective of this report is to highlight how enterprise strategists and practitioners with a working knowledge of digital transformation perceive the relationship between that process and issues of risk management and security.

KEY FINDINGS

- 40% of respondents said that better management of risk is a key driver in their digital transformation projects.
- Risk management is one of the fundamental, if not foundational, concerns of businesses across the globe.
- Nearly half of respondents (49%) said that securing customer data is one of their main digital transformation objectives.
- Businesses in the Asia-Pacific region are more likely than their peers in Europe or North America to identify risk mitigation when they talk about their imperatives.

Digital Transformation and Risk Management: Thoroughly Entwined

Digital transformation is an important component in the efforts of many businesses to overhaul their technology and processes for a more complex era. As companies wrestle with the fine details of building digital transformation strategies, many report that the issues of risk management and security are front and center in those efforts. Business leaders are increasingly aware of the importance of putting risk mitigation at the forefront of the discussion.

According to the results of a wide-ranging survey of attitudes toward digital transformation conducted by 451 Research, businesses exhibited concern about risk-related issues, and a willingness to consider risk-abatement strategies in tandem with other technological issues. These concerns are apparent among both IT professionals and LOB managers, although not always to the same degree. In general, survey respondents indicated an awareness of the connection between building a successful digital transformation process and the need to bake in specific risk management best practices.

What the survey results uncovered is that the key challenge for business leaders is getting the message out across their organizations that risk management should be seen as a core component of the digital transformation process – not an afterthought or an adjacent effort. Security needs to be built into digital transformation from start to finish, up and down the technology stack, and from datacenter to edge.

The concerns and challenges that emerged among managers all point to the need to approach risk proactively rather than reactively. With a threat landscape that is continually changing and putting multiple parts of the business under constant stress, businesses need to adopt a stance of 24/7 vigilance. To put that aside during a digital transformation planning process is to court unnecessary revamping and retrofitting of security technology later on, at presumably greater expense. Instead, the consensus is emerging that risk is one of the key drivers of digital transformation in the first place, and should be incorporated into the plans every step of the way.

Defining Risk in the Context of Digital Transformation

The 451 Research survey on digital transformation asked respondents across verticals to weigh in on the relationship between their perception of risk and what steps they are taking to develop digital transformation strategies. For example, when asked what the main drivers are for digital transformation, 40% of respondents cited, 'To better manage risk (e.g., cybersecurity, data privacy, systems reliability).' That was the third-most-selected response, behind reducing costs and improving customer experience.

When asked to weigh risk against other important organizational goals, including improving efficiency and agility, risk scored slightly lower overall against the other goals in the broad sample. Select groups within the sample – people in government and financial services firms, for example – rated risk higher. One interpretation of the data is that of the four goals available, three of them are highly aspirational. Risk management, in contrast to customer experience or corporate agility, comes with a set of standards and disciplines already baked into it as a business practice. IT and business leaders are already aware of the compliance and security requirements inherent in a risk management strategy; therefore, the need for digital transformation to swoop in and present a company-wide solution to a standing problem is less urgent.

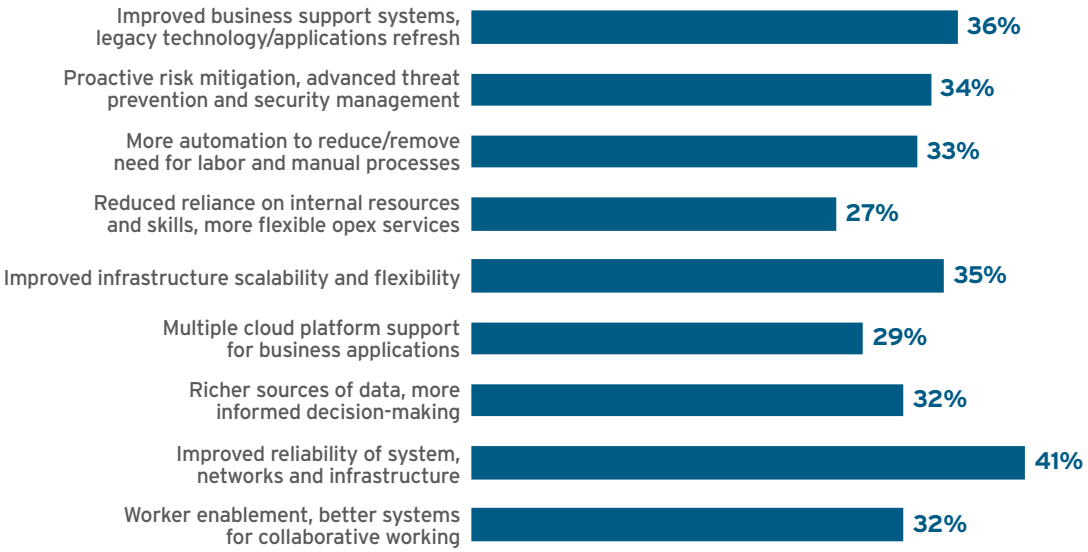
But as Figure 1 illustrates, risk does matter to those who are making digital transformation plans. It may not be the central problem a business is setting out to fix, but it is essential to entwine risk-related thinking into the wider digital transformation strategy planning.

Figure 1: Organizational goal priorities as they relate to the four pillars of digital transformation

Source: 451 Research (n = 1,402)

This is borne out by the expression of priorities that people are seeking when it comes to their IT-related investments in a digital transformation project. When asked, both LOB executives and their IT counterparts highlighted the improved reliability of systems, networks and infrastructure as their top choice (41%). The need for proactive risk mitigation, threat protection and security management was cited by 34% of respondents. In both cases, IT professionals selected those choices at slightly higher rates than their LOB colleagues.

Figure 2: IT-led priorities as they relate to digital transformation



Source: 451 Research (n = 1,402)

When asked more broadly about the main objectives of their digital transformation projects, LOB and IT respondents had very similar risk-related goals. Overall, 49% wanted to secure customer data, 44% to secure internal data, and 36% wanted to foster proactive risk mitigation through digital transformation. Notably, the more concerned respondents were about risk in general, the more they expressed a need to protect customer data in particular: 72% of those who were highly attuned to risk as a core goal cited customer data as a priority.

The survey suggests that when thinking about digital transformation, business leaders think about risk broadly. They interpret risk to encompass three areas:

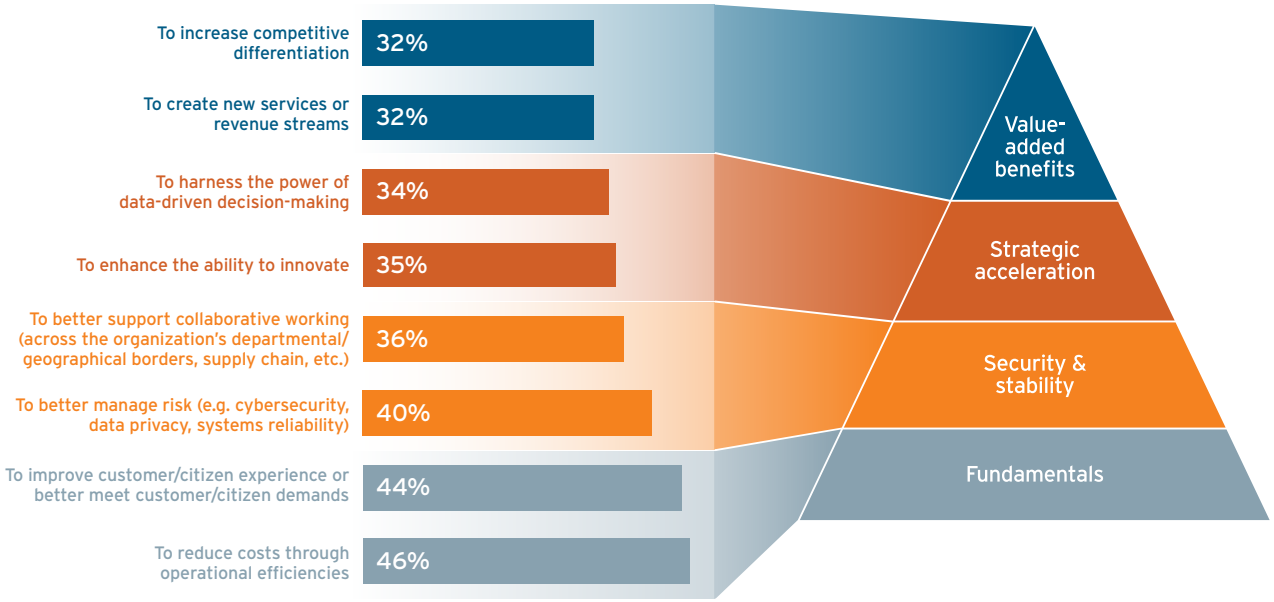
- **Data security**, as applied to both internal datasets and external customer information. This takes into account both data at rest and during transit across public or private networks.
- **Proactive mitigation and threat prevention**, or the ability to see and anticipate security threats and breaches before they occur, and build digital systems to head them off.
- The **impact of system and infrastructure reliability** on the ability of the business to continue to operate in the face of unforeseen events: fire, flood, outages and emergencies. In this case, risk and business continuity are intimately tied to an organization's other core goals – being agile, efficient and customer-friendly.

Clearly, different elements of that risk taxonomy are going to be relevant to different internal constituencies, but the picture that is emerging from the 451 Research survey is that concern about risk management overall is fairly consistent within organizations. There is a consensus that getting buy-in from the executive level requires that risk and security policies be embedded within any digital transformation initiative. Only 18% of respondents cited the inability to gain buy-in from executive leadership as a barrier to transformation. Likely because risk and security are so deeply embedded across business and IT, with specific concerns about data, systems and continuity, companies are already attuned to the need to incorporate them into digital transformation planning, with the blessing of C-level executives.

Every digital strategy is shaped and motivated by business need. As Figure 3 illustrates, in the context of enterprise digital transformation strategies, these needs arrange into a classic Maslow's Hierarchy of Needs format, with cost efficiency and customer satisfaction as the foundational elements needed for an organization to survive and thrive. Just above that layer, close to the fundamental level, sits better management of risk (in myriad forms, but here principally addressing those that are associated with cybersecurity, data privacy and systems reliability). This features on many corporate agendas, and 40% of organizations rated this as a key driver of desired digital transformation outcomes.

With solid foundational steps as an underpinning, and with the lower-order needs of organizational security and stability satisfied, respondents recognize that digital transformation programs will then begin to deliver the more strategic and value-added benefits that provide competitive differentiation. These take all shapes and can exhibit a variety of forms.

Figure 3: The hierarchy of business needs puts risk near the foundation



Source: 451 Research (n = 1,402)

IT and LOB see the landscape differently

People with different roles in an organization sometimes have different notions of what digital transformation will accomplish, and how to get to those goals. Often, the idea of mitigating risk colors the views of decision-makers.

For example, IT managers appear to be see cloud as a higher priority than their LOB counterparts. About 31% of IT professionals cited 'Multiple cloud platform support for business applications' as an investment priority for digital transformation, compared with just 25% of LOB managers. A similar gap appears between the two groups on 'Improved infrastructure scalability and flexibility.'

Business managers, by contrast, are more likely than IT to prioritize systems for worker collaboration (38% to 29%), and to prioritize richer sources of data to assist decision-making (35% to 31%). These priorities put security behind operational efficiency and agility as transformational goals.

These variations in viewpoint and prioritization indicate that IT managers are looking at protecting their organizations from risk by embedding risk mitigation into the entire stack. LOB professionals are aware of risk as an issue, and certainly indicate concern for it, but they are more immediately focused on extending their operational capabilities.

In some ways, this can be explained as the tension between goals and fears. While many business people see risk as a problem to be mitigated or a box to be checked on a plan, others understand it to be fundamental, from the architecture on down.

Regional and vertical variations in risk perception

There are also notable differences in the way people view risk management based on their location. For example, asked about barriers to digital transformation, 35% of respondents in Asia-Pacific cited the failure to secure sensitive data, compared to 29% in North America and 25% in the EU. Similarly, when asked about drivers behind digital transformation, again Asia-Pacific respondents were more attuned to risk; 43% in that region cited the need to better manage risk as a driver, compared to 39% in North America and 36% in the EU, as noted in Figure 4.

The spread between Asia-Pacific and Europe may indicate that European companies have already had to grapple with these issues due to tighter regulatory regimes, privacy regulations and a longer-term focus on protecting customer data. Asian companies may still be in the early stages of incorporating risk management into their planning for digital transformation and, therefore, are more highly attuned to the issues involved.

Generally, across regions, the earlier respondents' firms were in the process of planning their digital transformation strategies, the more likely they were to identify 'securing customer data' as an important risk-related objective. It was cited by 52% of those in the early stages of planning, compared to 46% of those who already had formal plans in place. This may indicate that firms are becoming more mature in their capabilities and management of risk as they progress on their digital transformation journey.

A similar regional disparity appears in financial services firms. When asked what kinds of technologies they expect to be disruptive in their industry, 39% of Asia-Pacific respondents mentioned using analytics to fight fraud and manage risk. Just 27% of EU respondents cited that, with North America again in the middle. Similarly, 40% of Asian respondents cited biometrics as a disruptive technology, compared to 26% in the EU and 32% in North America. Financial technology innovation is likely pushing banks in all regions to accelerate their digital initiatives and investments in technology for better customer experience, agility, and improved efficiency.

Figure 4: Variations in regional views on risk

SNAPSHOT	APAC	NA	EU
Identify potential failure to secure sensitive data as a barrier to digital transformation	35%	29%	25%
Identify better risk management as a digital transformation driver	43%	39%	36%
Identify analytics to fight fraud and manage risk as a disruptor in financial services	39%	32%	27%
Identify biometrics as a disruptor in financial services	40%	32%	26%

Source: 451 Research (n = 1,402)

Compliance and security are not the same

Because risk is such a broad area of concern, differences in approach show up between vertical markets. The 451 Research survey looked at four main industries: consumer retail, financial services, healthcare and government (only federal government responses were represented in Figure 5).

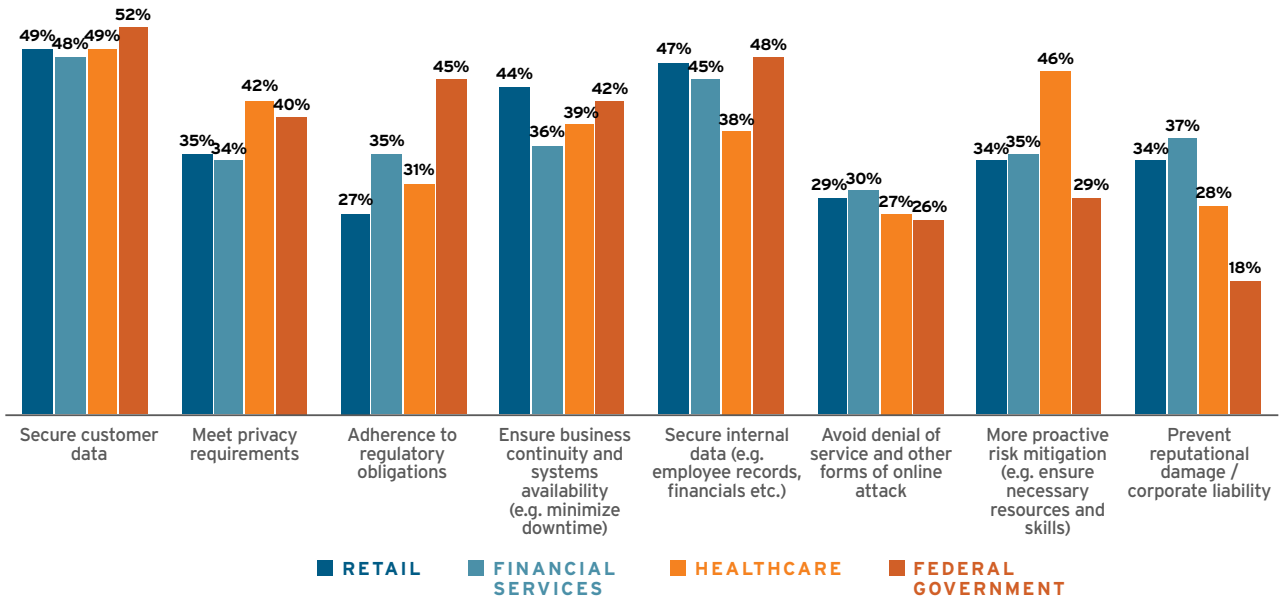
Figure 5 illustrates the differences between those four groups in how they perceive the end point of a digital transformation process with regard to risk management. Not surprisingly, all have a significant interest in securing customer data – this is the top choice for most respondents. Securing internal data was also of major concern across industries.

People who work in healthcare and government exhibited concern about adhering to regulatory obligations and proactive risk mitigation, while their counterparts in retail and financial services expressed concern about the dangers of reputational damage, which is understandable in competitive, customer-facing businesses.

These differences, though, suggest that there is a gray area in risk management between compliance and security, with people tending to favor one or the other depending on their role. Meeting compliance regulations will not cover all security needs because typical results only offer a minimal baseline of protection. Why? Because compliance corresponds to a set of specific requirements that change slowly, not daily as we see in the security landscape. Compliance is simply ensuring that specific requirements are in place (typically only once a year). To truly protect sensitive data, both security and compliance are critical. Without a smart, thorough and active security program coupled with a solid compliance plan, organizations remain at significant risk of being breached.

Survey data suggests that the best approach to risk management overall is to unify the approach up and down the stack, making it central to the digital transformation project, along with achieving efficiency and agility.

Figure 5: Main objectives for better management of risk as they relate to digital transformation



Source: 451 Research (n = 1,402)

Risk as an integral part of the digital transformation process

The fact that there are multiple visions of what risk is, and how to mitigate it, suggests that businesses need to incorporate risk management thinking into the digital transformation process from the start, and through all stages of planning and execution.

One indication of this can be seen in the way perceptions change depending on how far along the digital transformation process organizations are. For example, 34% of respondents at businesses that are in the early stages of their digital transformation programs cited proactive risk mitigation as one of their IT investment priorities. That number increased at organizations further along in the process, implying that as businesses wrestle with competing priorities and the complex demands of ensuring security along with agility and efficiency in operations, they increasingly recognize the importance of embedding risk mitigation into the entire stack. In effect, they pivot from seeing 'protection' as something you do piecemeal toward something that needs to be handled across the board.

The key to risk management is to be proactive rather than reactive: elevate technologies and processes that allow for flexibility in the face of unknown issues and circumstances, rather than acting after the fact, when damage is perhaps already done. In this way, risk is the component of digital transformation that ties together the other three core objectives (agility, efficiency and customer experience).

Survey respondents indicated a willingness to seek outside help for some of their risk-related digital transformation initiatives. Forty-five percent of respondents overall indicated that they would work with an outsourcing partner for their business continuity and disaster recovery services as part of a digital transformation project. A similar number, 46%, expressed willingness to work with partners for threat prevention and managed cybersecurity services. In that case, the figures rose with experience: 45% of those in the early stages of planning digital transformation were interested in working with outside partners, increasing to 52% among those farther along in planning. This indicates that some experience coordinating among internal constituencies and exploring the nuances of technology in the digital transformation stack raises awareness of the need to incorporate proactive risk mitigation more completely into the process.

This suggests that there is a benefit to bringing LOB and IT professionals together as early in the digital transformation process as possible so they can establish common definitions of risk, identify perceptions of security and threats, and establish the need for outside help before resources are committed to the project.

Recommendations

ADAPT AND TRANSFORM CYBERSECURITY

Digital transformation touches all aspects of the business. Every innovation – every upgrade, connection, application or technology added – whether in the cloud or on-premises – will increase complexity, scale and operational risk, which not only creates difficulties for IT teams but potentially results in serious repercussions for the business. One of the key challenges for risk-minded professionals will be adapting company culture, processes and controls to accommodate the changes produced by digital transformation initiatives.

Organizations need to tear down the walls or silos between security and operations and create cross-functional teams focused on securing specific mission-critical assets and reducing security gaps.

Digital transformation often leads to an explosion of connected environments where the traditional, contained enterprise network no longer exists and perimeter protection is no longer enough. The focus of cybersecurity needs to shift from securing network perimeters to safeguarding data spread across systems, devices and the cloud. This means organizations should take a 'security by default' approach where protection is the default posture. Organizations need to tear down the walls or silos between security and operations and create cross-functional teams focused on securing specific mission-critical assets and reducing security gaps. Through digital transformation, security leaders have the potential to transform security into a competitive advantage: security efforts can be aligned with the business, proactively identifying and mitigating risks while being the catalyst for accelerated innovation by enabling the organization to move faster and take bolder steps than it may have otherwise attempted.

EMBRACE RISKS

Not only are complex digital transformation initiatives making it difficult for organizations to fully grasp their entire risk profile, but digital transformation is also resulting in new or unfamiliar risks for enterprises – such as blockchain, IoT and big data. In many cases, the company's view of risk may be the biggest threat to a successful digital transformation program. Organizations with strong risk aversion are in danger of preventing or stifling the innovation and change needed to move digital transformation projects forward. Overcoming aversion to risk is one of the most important characteristics of digitally successful and mature companies.

Organizations must embrace risk and strengthen their understanding and monitoring of each individual risk, as well as the company's complete risk profile. Shifting from being a risk-averse organization to one that embraces risk requires diligence and perseverance. To make this shift, organizations must clearly communicate their vision and new way of thinking and behaving regarding risk – this will often entail pushing people outside their comfort zones and forcing them to think and act more courageously. Embracing risk also requires collaboration across the company – requiring trust and the elimination of the siloed behavior that is typically found in traditional organizations. Organizations that successfully embrace risk have embedded risk management in the company's cultural and organizational foundation to a point that it is often not noticeable as a separate function at either the strategic or tactical level.

However, organizations cannot pause their digital transformation initiatives to wait for their corporate cultures and appetite for risk to catch up. Cultural change and transformation execution must take place simultaneously, with each powering the other. Executives are often risk-averse and do not believe they have the freedom to fail, especially when they are faced with the constant pressure to exceed – not just meet – quarterly expectations. To overcome this fear, organizations need to create a company culture, from the top down, that fosters experimenting and innovation. This means that it is acceptable if projects fail, especially small ones, but it is important to learn from those failures, pivot quickly, and look for the opportunities that digital transformation can bring – such as enhanced intelligence and speed infused into operations, transformation of existing products/services, and completely new business models. Embracing risk is intimidating but, ultimately, can be the key to just how far the organization can go.

INVEST IN SECURITY AND SHOW RESULTS

Digital transformation is not a 'one and done' project. Organizations cannot stop evolving – they must constantly innovate and take advantage of existing and new digital technology, services and business practices. As a result, organizations should carefully consider security investments and ensure those investments can enable the organization to respond to business climate changes, address new competition, adapt to changes in regulations and technology, and adjust quickly to changes in global economic variables.

Investments in external cybersecurity expertise can help address the complex challenges often introduced by many digital transformation initiatives, such as managing and securing applications and data in multiple clouds. By working with cybersecurity service providers, organizations can tap into the shared knowledge and data on existing and emerging threats — acting as an early-warning system to developing threats, especially when it comes to new technologies or platforms. Service providers can leverage the lessons they have learned from other organizations' digital transformation projects to avoid pitfalls, enabling the enterprise to better protect mission-critical assets and data and progress faster.

Organizations making investments in security efforts need confirmation that that the investments are performing according to expectations and are delivering the expected value. Security teams should track and report on the performance of security systems and the impact of security controls. Although providing metrics on security measures can be challenging, effective security metrics share some common characteristics: they support the goals of the business, they are quantitative, they are easy to collect and analyze, and they can show trends.

Having the right security controls in place and having ways to measure their effectiveness can help the enterprise build confidence toward taking on new risks, encouraging innovation and continuous digital transformation.

APPENDIX

Methodology

The survey data used in this report was collected by 451 Research in March and April 2017 using a combination of web-based surveys and telephone-based interviews as part of a global digital transformation enterprise study – commissioned by CenturyLink and conducted in 11 countries across North America, Europe and Asia-Pacific. It is designed to provide insights that will help executives understand how businesses are leveraging the changes and opportunities of digital technologies to serve different stakeholders, manage risk, support continuous improvement in operations, and invent new services and business models.

In taking the pulse of digital transformation across a broad spread of sectors, we have been able to identify which new IT choices are becoming popular, explore service partner preferences, and track investment priorities, as well as establish the state of vertical-specific digital transformation readiness and evolution.

Study Demographics

All respondents have primary responsibility for making purchasing recommendations and influencing decisions and strategy about digital transformation initiatives, or they have significant decision-making authority. About 40% of respondents are responsible for decisions about digital transformation strategy, with 60% providing input. Overall, 60% of respondents work as senior IT executives, and 40% lead line-of-business departments for their organizations. Our business segmentation corresponds with the categories typically used by service providers to identify midmarket and large enterprise customers.

Further Information

This report is one in a series to explore the current state of maturity of enterprise digital transformation strategies representative of organizations in key commercial sectors and government agencies in North America, Europe and Asia-Pacific.

The series comprises a set of reports addressing the analysis of the global picture, as well as three summary regional reports that assess some of the variations identified across geographies.

There are also four vertical-market-focused reports that will help IT and line-of-business executives in financial services, healthcare, retail and government to navigate some of the key issues and considerations specific to digital transformation themes in these sectors.

About CenturyLink

CenturyLink is a global communications and IT services company focused on connecting its customers to the power of the digital world. CenturyLink offers network and data systems management, big data analytics, managed security services, hosting, cloud, and IT consulting services. The company provides broadband, voice, video, advanced data and managed network services over a robust 265,000-route-mile U.S. fiber network and a 360,000-route-mile international transport network. Learn more about how CenturyLink can help you accelerate your digital transformation.

For further information, go to **www.centurylink.com/business/enterprise/it-security/it-risk-mitigation.html**