



# The Vital Role of Security in Digital Transformation

A strategic approach to IT security and data protection is a critical enabler of digital transformation

RESEARCH REPORT | APRIL 2019

# Digital Transformation: It's a Matter of Survival

Digital Transformation is high on the agenda of nearly every CIO on the planet right now. In fact, it has become an imperative for many businesses because it's nothing short of a survival issue. Every business out there is being pushed to transform by a combination of three key drivers: changing consumer demand, changing technology and changing competition. Some have embraced this reality and surged with new growth—such as Disney, Tesla, Starbucks or even Walmart (named by HBR as a 'digital winner'). Others failed to see the changing dynamics (e.g. Kodak) or were too slow to react to it (e.g. Toys R Us) and have fallen by the wayside.

• *Digital transformation is what closes the gap between what digital customers already expect, and what analog businesses actually deliver.*

## The Paradox of Security

Small wonder then that IDC predicts that enterprises will invest over \$1.7 trillion in digital transformation initiatives in 2019, up 42% from just two years ago. And as senior IT executives move forward with these initiatives, they are faced with an apparent paradox. As platforms become more fluid and infrastructure more virtualized, securing the enterprise can be the biggest challenge to getting started, and an area with the greatest risk of the program stalling or failing. But if done correctly, security can also be one the single biggest enablers of successful transformation.

This sentiment is made clear across two very compelling data points: The CISO Collective reports that 85% of security executives view security as “a major hurdle” for their digital transformation programs, but at the same time, Cisco indicates that nearly two thirds of all executives (64%) also see it as a “significant driver” of their success.

**\$1.7** trillion

estimated total investment by global enterprises in digital transformation initiatives in 2019 (IDC)

**85%**

of security executives view security as “a major hurdle” for digital transformation (CISO Collective)

**64%**

of senior IT executives view security as a “significant driver” of their digital growth strategies (Cisco)

# Seeking the Views of Security Professionals

It is with this paradox in mind that we sought out the opinions of security professionals themselves, seeking to understand their views on security as both a barrier to- and enabler of digital transformation, and looking to gauge their sentiment regarding its role in their digital transformation programs both now and in the future.

**To do so, we conducted a survey with IT decision makers (ITDMs) according to the following scope:**



- ITDMs with direct responsibility for information security and data protection
- Working for an enterprise of 1000+ employees
- Located in North America (US, Canada) and UK
- Online survey of 18 minutes, conducted during November/December 2018

*The survey was conducted with a total of n=608 respondents, and data reported herein has a 4% margin of error at the 95% confidence interval.*

## Digital Transformation Relies on Security and Data Protection

Not surprisingly, the survey showed that a strong majority of ITDMs consider digital transformation to be very important to their growth strategy. But even more interestingly, the same number of ITDMs see a strong causal link between security and digital transformation. Fully 78% believe that the success of their digital transformation relies heavily on strong IT security and data protection, even more than the 64% that see it as a “significant driver” in the research mentioned above.

4 out of 5 ITDMs believe that their digital transformation success relies upon strong security and data protection.

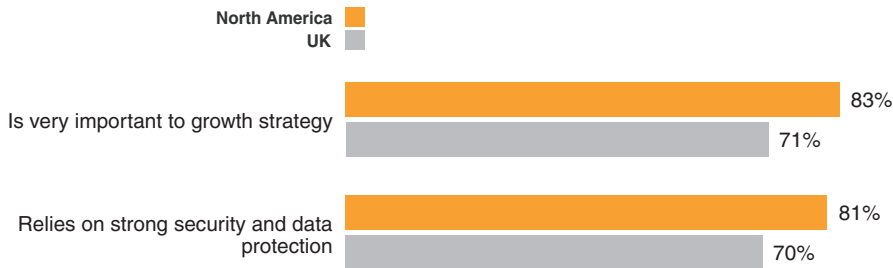
### DIGITAL TRANSFORMATION...



There are some distinct regional differences between North America and the UK on these metrics. While measures in the UK are still high, there is a 12-point gap between the two when it comes to viewing digital transformation as being important to growth, and a similar 11-point gap in the perception that it relies on strong security and data protection.

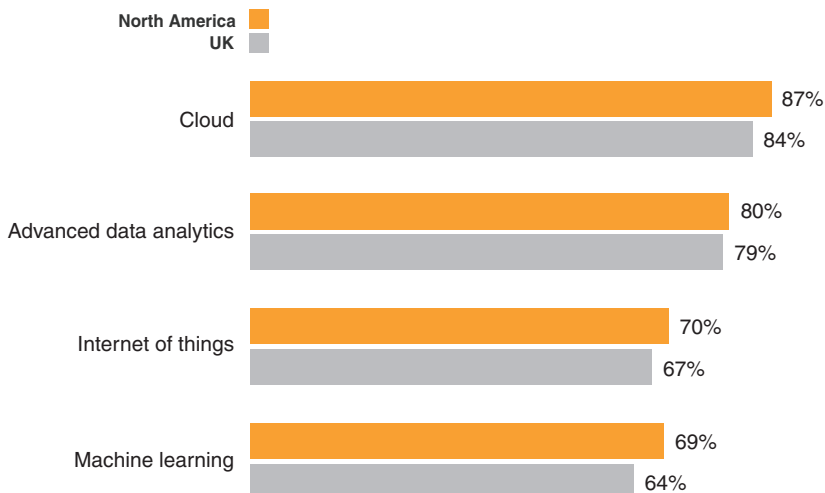
*Regional differences may be rhetorical, with North American ITDMs taking a more assertive stance in their messaging of digital transformation, security and data protection.*

**DIGITAL TRANSFORMATION...**



However, upon closer inspection of the data, it seems that at least part of this gap between North America and the UK is based upon the perceptions and opinions of respondents. For example, North American ITDMs take a more emphatic stance, being significantly more likely to describe themselves as early adopters of technology (62% vs 46%) and preferring “best of breed” providers (58% vs 49%). Moreover, the current deployment of solutions that drive digital transformation, such as cloud, IoT, advanced data analytics and machine learning are very similar across both regions. This suggests that regional differences may be at least partially rhetorical, with North American ITDMs taking a more assertive stance in their messaging of digital transformation, security and data protection.

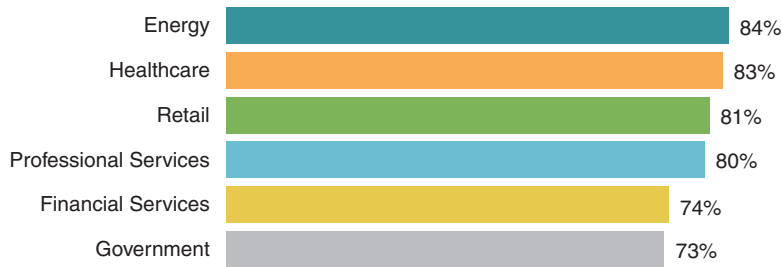
**TECH IN PRODUCTION**



Looking at the different industry sectors, it is notable that strong majorities of ITDMs in all sectors believe that their digital transformation strategies rely on strong security and data protection. While heavily-regulated and industries such as Energy and Healthcare felt this most strongly, even the Government sector, traditionally more of a laggard in tech adoption, had three quarters of its respondents drawing the causal link between security and digital transformation success.

## DIGITAL TRANSFORMATION...

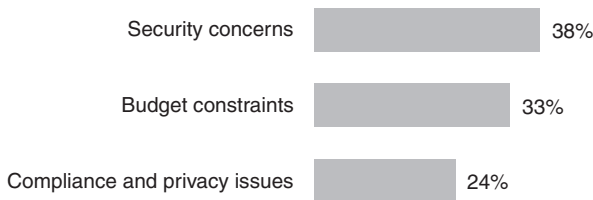
### Relies on strong security and data protection



# Digital Transformation Challenges

Asked about what they saw as the biggest obstacles to achieving their digital transformation ambitions, ITDMs raised security concerns as their number one challenge, greater even than the budgetary constraints that they operate under. This serves to emphasize the perceptual paradox: That while the vast majority see strong security and data protection as a key driver of digital transformation, a significant minority also fear that it is a major barrier to achieving their strategic goals.

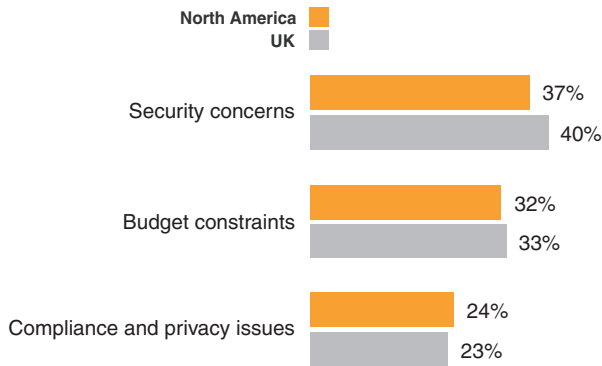
### BIGGEST OBSTACLES TO DIGITAL TRANSFORMATION



There wasn't a lot of separation at a regional level, although ITDMs in the UK are directionally more likely to see security as being their biggest obstacle to digital transformation, which likely explains why they are slightly less positive than their North American counterparts.

*The perceptual paradox: While the vast majority see strong security and data protection as a key driver of digital transformation, a significant minority also fear that it is a major barrier to achieving their strategic goals.*

### BIGGEST OBSTACLES TO DIGITAL TRANSFORMATION

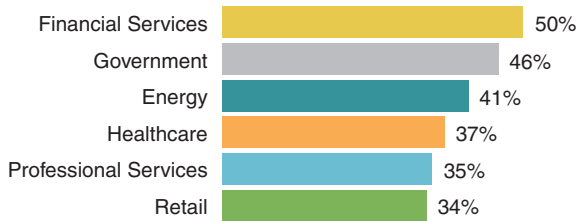


*ITDMs view security concerns as the number one challenge for digital transformation, greater even than the budgetary constraints that they operate under.*

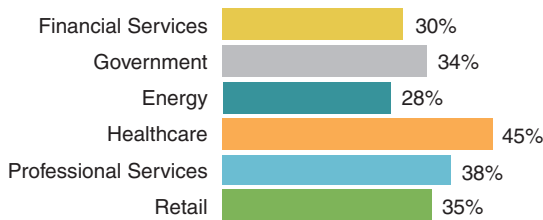
Looking across the different industry sectors, a half of all financial services respondents see security concerns as their biggest obstacle to digital transformation, well above the average. By contrast, retail and professional services respondents are least concerned about security, likely contributing to their greater buoyancy about digital transformation as highlighted previously.

### BIGGEST OBSTACLES TO DIGITAL TRANSFORMATION

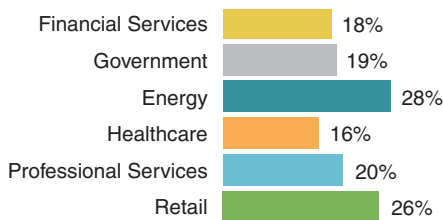
#### Security concerns



#### Budget constraints



#### Compliance and privacy issues



# There Are Two Very Different Security Professional Personas

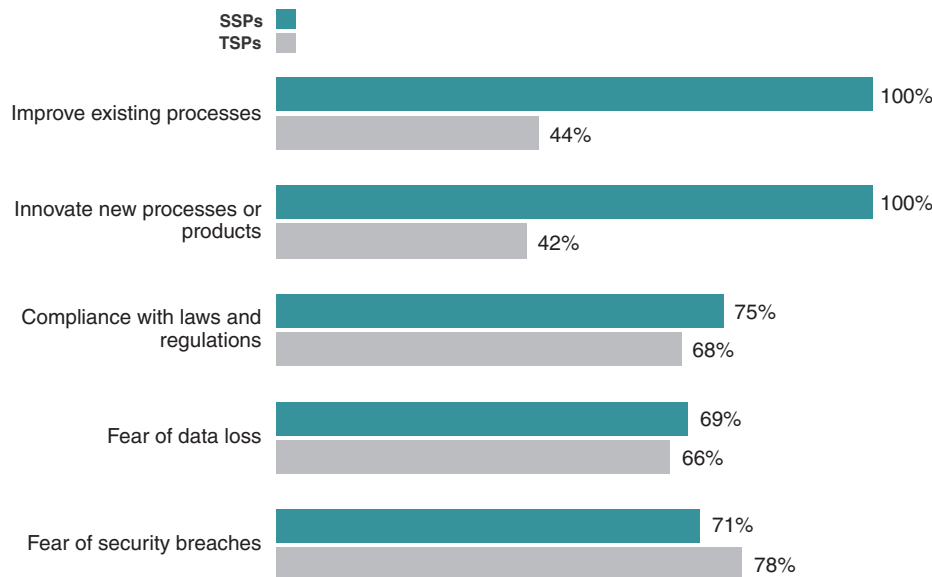
The research also brought to light a polarization in the attitudes and sentiments of ITDMs with responsibility for IT security and data protection. There is a stark difference between those that took a more traditional, conservative stance on security, and those that saw it as a strategic enabler of business growth.

This divide was most clear when respondents indicated what motivated their security strategy, and this data was used point to segment the ITDMs into two key persona types:

- **STRATEGIC SECURITY PROFESSIONALS (SSPs):** View security as a strategic enabler for improving existing business processes and innovating new processes or product. These respondents tend to be more senior compared to TSPs, with nearly half having the title of Chief Information Security Officer (CISO).
- **TRADITIONAL SECURITY PROFESSIONALS (TSPs):** Motivated more by fear of security breaches and data loss than by using security for strategic purposes. These respondents tend to be more junior compared to SSPs, although a quarter of this group was still made up by CISOs.

*There is a stark difference between those that take a more conservative stance on security, and those that see it as a strategic enabler of business growth.*

## MOTIVATORS OF SECURITY STRATEGY



What is notable with this separation of personas is that SSPs and TSPs are similarly motivated by concerns regarding compliance, security breaches and data loss, but SSPs are universal in their motivation for using security for strategic purposes and at more than double the rate of TSPs.

The separation in this segmentation is made even more evident when the ITDMs are asked about their personal and organizational attitudes towards IT security and data protection, and whether it is a strategic advantage or the cost of doing business. More than 9 in 10 SSPs and their organizations view security as a strategic advantage in the digital transformation process, whereas a third or more of TSPs view security simply as the cost of doing business. What is also notable is the close alignment between personal and organizational views for SSPs, whereas even TSPs that do take a more strategic view are more likely to be in a workplace that doesn't align with their personal views.

More than 9 in 10 SSPs and their organizations view security as a strategic advantage in the digital transformation process.

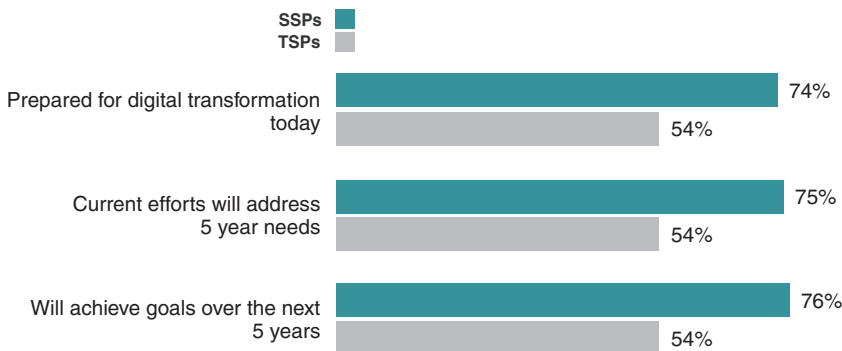
**SECURITY IS A STRATEGIC ADVANTAGE**



# Differing Perceptions of Now and the Future

As a result, SSPs are significantly more confident about their digital transformation initiatives, holding a 20%+ advantage over TSPs in both current sentiment and future perceptions. Three quarters believe that they are well prepared for digital transformation, that their current efforts will address the needs that their business will have in five years' time, and that they will achieve their digital transformation goals over the next five years. By contrast, only half of the TDS segment report the same level of confidence.

**DIGITAL TRANSFORMATION NOW AND IN THE FUTURE**





# What Makes SSPs More Successful?

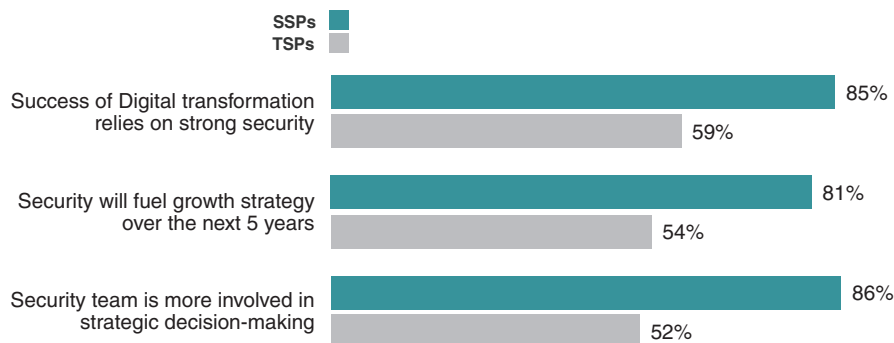
Given that SSPs are significantly more confident in their current and future digital transformation endeavors, one has to ask the obvious question: What makes them different? The research data points to a number of key themes that are consistent with SSPs, where their progressive sentiments and actions increase the likelihood of success with their digital transformation projects.

While SSPs might see security as being one of their more formidable challenges, they have embraced it as an enabler of their success rather than fearing it as a potential roadblock.

## 1 SSPs tie digital transformation and security closely together

It starts with the strategic approach. SSPs have recognized early on that their digital transformation initiatives are reliant on the strength of their IT security and data protection strategies. While they might still see security as being one of their more formidable challenges, they have embraced it as an enabler of their success rather than fearing it as a potential roadblock. This means taking a proactive approach to integrating security within digital transformation programs from the outset, rather than adding it as an input further downstream in the process. Importantly, 86% of the SSPs also indicated that this also meant that their security teams have become much more involved into strategic decision-making, helping to drive things forward from the front end rather than patch things up at the back end.

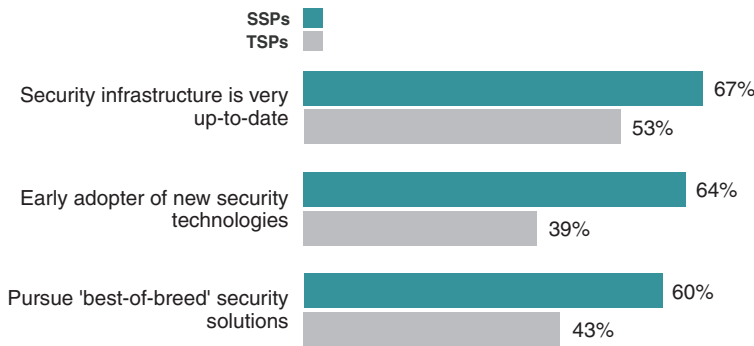
### TYING DIGITAL TRANSFORMATION AND SECURITY TOGETHER



## 2 SSPs aspire to technical excellence across consolidated security vendors/products

SSPs are also distinctive in that they are considerably more likely to aim for technical excellence in all of their endeavors. They are significantly more likely than TSPs to state that their existing security infrastructure is up-to-date, that they are an early adopter of new technologies, and that they pursue best-of-breed security solutions on an ongoing basis. Of course, other organizational priorities and budgetary constraints can still put a dampener on even the most ambitious SSP in this regard. But setting out with an ambition for technical excellence, even if only partially achieved, is indicative of an SSP and a higher likelihood to achieve digital transformation success.

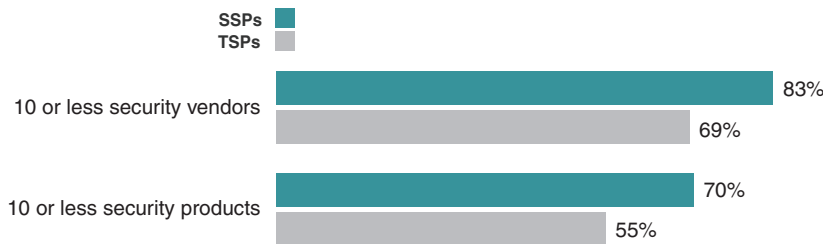
### TECHNICAL EXCELLENCE



SSPs are significantly more likely to have a proactive and strategic approach to data classification as part of their data protection strategy.

SSPs are also considerably more focused when it comes to their security vendors and products. Significantly more SSPs report using 10 or less security vendors compared to TSPs, and similarly, 15% more SSPs indicated that they have 10 or less security products deployed compared TSPs. Rather startlingly, nearly a quarter of TSPs use more than 25 different security products. So as most organizations increasingly seek to purchase security technologies that consolidate products and vendors, it is clear that SSPs have a considerable head start in this regard.

### VENDOR/PRODUCT FOCUS



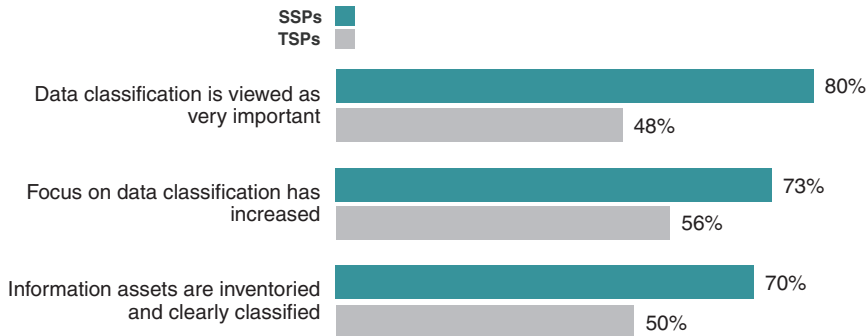
## 3 SSPs view data classification as a key part of their data protection strategy

At the heart of any digital transformation strategy is the imperative of understanding the identity of the organization’s data. Security professionals need to identify where their data is, understand and evaluate the sensitivity of the data, take steps to mitigate leakage, all while minimizing burden on the end users and maximizing value of security investments.

With that in mind, a notable standout is that SSPs are significantly more likely to have a proactive and strategic approach to data classification as part of their data protection strategy. The research showed that 80% of SSPs view data classification as very important, while less than half of TSPs felt the same. Moreover, three quarters of the SSPs feel that their focus on data classification has increased over the past two years, and that as a result their information assets are well managed today, again significantly more than TSPs. This is a particularly notable example of

how the forward-thinking approach of SSPs at the strategic level of data protection filters down to specific components such as data classification.

**DATA CLASSIFICATION**

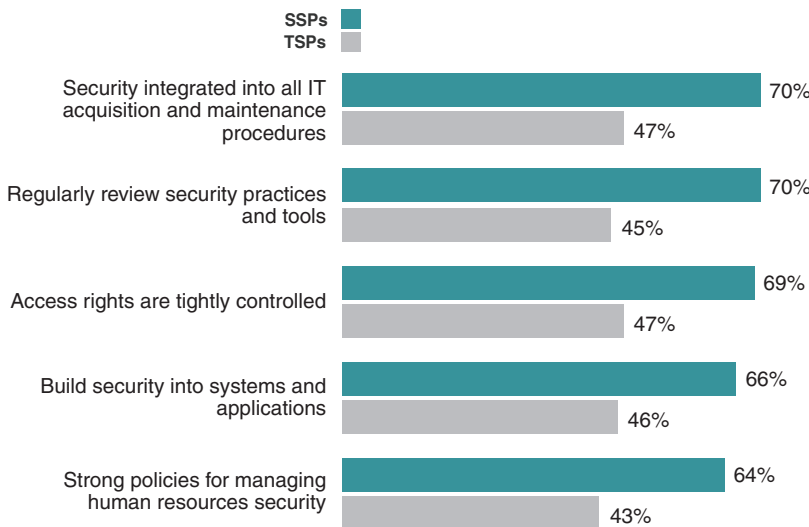


SSPs create a strong security culture by placing a far greater emphasis on security management practices as part of their overall leadership and decision making.

**4 SSPs create a strong security culture through clear policy management**

Perhaps unsurprisingly, SSPs also stand out from TSPs by placing a far greater emphasis on security management practices. More than two thirds of SSPs indicate that management topics such as access rights, security reviews and human resource policies are an important part of their overall leadership and decision-making, while less than half of TSPs make the same claim. This might seem intuitive for day-to-day business, but clearly having these fundamentals in place is going to be a crucial driver of digital transformation success, while gaps in security management can quickly create issues that stall digital transformation programs.

**SECURITY MANAGEMENT PRACTICES**



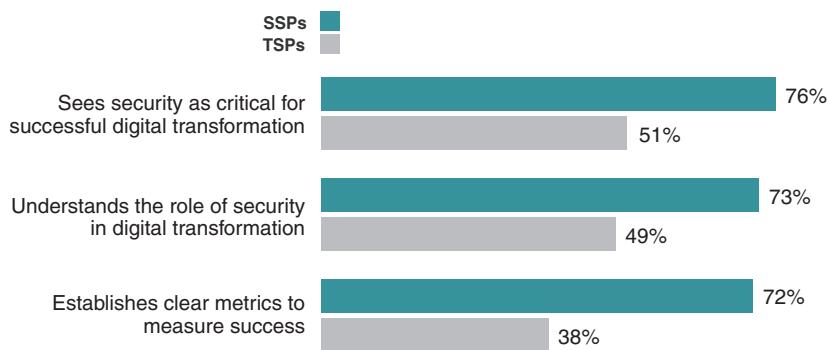
## 5 SSPs benefit from strong executive support

While the SSPs are significantly more prepared and confident of success, it is not all down to their own personal stance. Another key ingredient is the culture and leadership within their workplace. After all, they can have the boldest of ambitions, but if they can't get the IT and business leadership to share in their vision, all of their efforts can end up being for naught.

This is another area where SSPs stand out from the crowd. When asked about the role that executive leadership plays in enabling their strategies, they are significantly more effusive than TSPs. Three quarters have strong buy-in from executive leadership when it comes to prioritization of transformation, understanding its role or seeing security as a critical driver, whereas barely half of TSPs feel the same. Most notably, nearly double the number of SSPs feel that their executive leadership establishes clear metrics to measure success, a vital component of any digital transformation program.

• Three quarters of SSPs have strong buy-in from executive leadership when it comes to prioritization of transformation, understanding its role, or seeing security as a critical driver.

### EXECUTIVE LEADERSHIP...



# Adjusting the ITDM Mindset

Just a few years ago, ITDMs tended to focus on the piece parts of digitization—such as a cloud, e-commerce etc.—and often tackled each in semi or complete isolation. They tended to be more consumed with “nuts and bolts” of virtualizing servers or building and app, and less on the bigger picture. But as the industry and technology has matured, and platforms have become better understood, this digital transformation has become an integrated strategy that is driven by strategic goals such as accelerating innovation or creating competitive advantage, rather than tactical objectives such as delivering cost savings.

The reality is that the industry has changed, and security professionals need to adjust to that change. A “glass half empty” view of digital transformation results in a lot of anxiety over issues such as a more fluid delivery platform, the loss of perimeters, or the loss of control of physical infrastructure. But security leaders now have a chance to rethink their approach to security and data protection as it is needed for successful digital transformation. Getting it right has the potential to transform the security function from being perceived as a “cost of doing business” or even a brake on getting things done, to being a driver of competitive advantage and catalyst to accelerating innovation.

## ABOUT HELPSYSTEMS

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at [www.helpsystems.com](http://www.helpsystems.com).

**titus**  
by HelpSystems

## ABOUT MARKET STRATEGIES INTERNATIONAL-MORPACE

Leading market research firms Market Strategies International and Morpace bring clients closer to their customers through exceptional insights. The firms specialize in brand, customer experience, product development and segmentation research, and are known for blending primary research with data from syndicated, benchmarking and self-funded studies to help clients succeed. They have earned the trust of many of the world's top brands across the automotive, consumer & retail, energy, financial services, health, technology and telecommunications industries. Market Strategies and Morpace are combining into one firm, as part of an acquisition of both firms by STG, and will be rebranded under a new name to be announced in 2019. With more than 450 research professionals, the collective firm is now the 15th largest market research firm in the US and top 25 globally.

**P** +1 734.542.7600 | **E** [info@marketstrategies.com](mailto:info@marketstrategies.com)

Visit our website: [marketstrategies.com](http://marketstrategies.com)

Read our blog: [freshmr.com](http://freshmr.com)

