SYNTAX

2021 IT TRENDS

A Year of New Industry Benchmarks

The objectives and challenges driving IT in today's enterprise

Executive Summary

2020 was a year of forced transformation for IT leaders. IT teams scrambled at the beginning of the year to enable work-from-home environments in response to the COVID-19 pandemic. Pressing and stretching their capabilities, IT teams onboarded new technologies and migrated business functions to the cloud at unprecedented levels.

The mass shift of employees to work from home resulted in an eruption of cyberattacks. Bad actors feasted on vulnerable endpoints at home offices and cloud deployments. Firewalls and virtual private networks (VPN) were tested and in many cases, found to be ineffective. Since we've never seen such a tumultuous year for the IT industry, Syntax wanted to know: **What's next for IT?**

To answer this important question, Syntax surveyed **500 IT decision-makers** to assess how the global pandemic affected their businesses and what strategic decisions they'll make in 2021.

The result of the survey is an IT trends report that shows what IT leaders plan on doing after 2020 changed their world. We'll examine how they pivoted and explore what challenges still lie ahead in 2021.

Regardless of how much progress it will take to end the global pandemic, 2021 will serve as a canvas for IT decision-makers to optimize best practices like remote work and permanently enabling the cloud.

The industry shift toward remote work increases the responsibilities of companies to protect themselves against hackers and do a better job with cybersecurity. Given the high demand for cybersecurity talent, our data shows that many IT leaders will aim to increase their outsourcing of cybersecurity in 2021, creating a potential boom in third-party cybersecurity support as IT decision-makers try to plug gaps in their organizations' technical IT infrastructure. Security will also be a persistent focus in all areas of IT — including cloud, employee training, and business continuity and disaster recovery — as the success of these initiatives is rooted in business operations and cybersecurity resiliency.

In the end, 2020 was the spark of major change in the IT industry. And 2021 will redefine industry standards for the long term. Let's dive into the IT trends of 2021 based on the survey results.

— **By Marc Caruso, Chief Architect and Matthew Rogers, Chief Information Security Officer (CISO) of Syntax**

2021 IT Trends

01 Cybersecurity to be outsourced at an astonishing rate

02 IT teams will never look the same

03 Expect cloud security to surprisingly be neglected

04 IT leaders to have a rare negotiation opportunity

05 Work-from-home improvements will be unsettling for IT

06 Data analytics to see substantial gains in IT

SECTION 1

Cybersecurity to be outsourced at an astonishing rate

Cyberattacks exploded after the global pandemic started. IT leaders are bolstering their cybersecurity protection by purchasing more tools, but these tools are not enough to protect enterprises. The continued rise in attacks at all hours of the day, combined with a greater need for third-party cybersecurity consultation, will create a new wave of outsourcing to managed service providers (MSPs).

DID YOU KNOW?

83%

of decision-makers with in-house cybersecurity teams are considering outsourcing to an MSP within the next six months

77%

of IT leaders said cyberattacks were more frequent after the COVID-19 pandemic started

Most frequently occurring cyberattack in 2020

58% Phishing/social engineering

Answering the eruption of cyberattacks

More than half (56%) of IT leaders said they will allocate more than 40% of their IT budgets to cybersecurity in 2021. Additionally, **37% listed "improving cybersecurity protections" as their top IT investment initiative for 2021**.

The reason for substantial investment? A major spike in cybersecurity attacks.

Seventy-seven percent of decision-makers reported that cyberattacks became more frequent after the pandemic started, with 40% saying the increase was "significant." To combat the rise in cyberattacks, 90% of IT leaders purchased new cybersecurity tools and 93% said these tools made cybersecurity easier — but they aren't entirely satisfied.

To protect themselves from around the clock attacks, 91% of IT leaders either employ their own security operations center (SOC) team or in-house security talent — only 9% of respondents use a cybersecurity managed services provider (MSP). Of those decision-makers using an in-house solution, **83% said they're considering outsourcing within the next six months**. We expect the use of MSPs to skyrocket and become the new industry standard, similar to the outsourcing movement seen in IT infrastructure management over the past five years.

Top 3 most common cybersecurity purchases

01 Threat intelligence

02 Bot detection

03 Vulnerability scanning

56%

of IT leaders said they will allocate more than 40% of their IT budget to cybersecurity in 2021

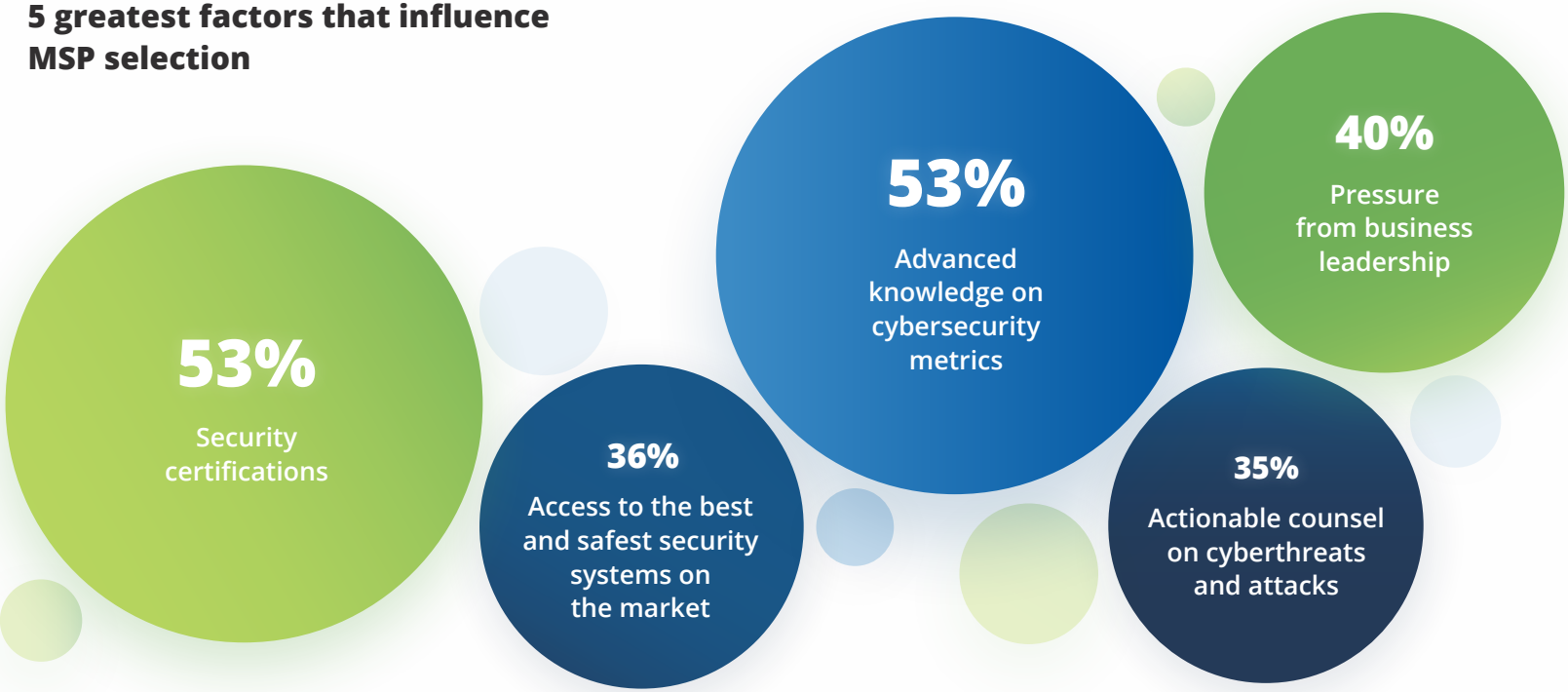
Top 3 most frequently occurring types of cyberattacks in 2020

58% Phishing/social engineering

35% Brute-force password attack

30% Stolen credentials and DoS

5 greatest factors that influence MSP selection



Knowing the problem, but not the solution

The reason behind this boom is **a lack of strategic counsel from existing security software tools** — 45% of IT leaders with in-house security teams considering an MSP cited a lack of strategic counsel from existing tools. Additionally, 41% said existing tools were too expensive. Our team at Syntax encountered this scenario throughout the pandemic. We have seen chief information officers' (CIOs) and chief technology officers' (CTOs) phones light up with security alerts from their cybersecurity tools during meetings — but these security alerts usually offer no real solution to the problem flagged. However, survey respondents did not cite the ability to provide actionable guidance as a top factor when selecting an MSP.

THE SYNTEL

If you're considering a cybersecurity MSP, think beyond your immediate security needs to assess the organization's ability to offer strategic guidance on how to address emerging cyberthreats. Without actionable counsel, you'll be stuck knowing damage is happening, but lack the understanding to stop it.

SECTION 2

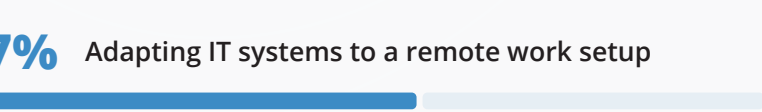
IT teams will never look the same

Decreased IT team headcounts were a significant challenge for IT leaders in 2020. This forced change resulted in a greater reliance on outsourcing and automation to keep IT operations running smoothly. The movement shows no signs of stopping, as IT leaders need to do more with less.

DID YOU KNOW?

Most difficult challenge for IT departments during the pandemic

57% Adapting IT systems to a remote work setup



92%

of enterprises that experienced IT staff cuts said COVID-19 **accelerated their digital transformation** compared to only 71% of businesses that didn't reduce IT staff

Reduced teams result in greater reliance on technology

More than 3 in 4 IT leaders (79%) saw a reduction in headcount at the beginning of the pandemic as enterprises cut costs. Operating with a smaller team presents significant challenges for IT departments tasked with adapting IT systems for remote work and managing an influx of support requests.

Although more than 1 in 4 (28%) decision-makers said "working with fewer IT employees" was a top challenge, teams with reduced headcounts reported a higher rate of accelerated digital transformation. Additionally, 92% of companies that laid off IT staff said COVID-19 accelerated their digital transformation compared to 71% of those that did not experience department cuts. The increased rate of digital transformation reported by companies with reduced IT staff correlated with higher rates of outsourcing and use of automation.

In addition, 89% of companies that laid off staff plan to outsource their internal cybersecurity operations to an MSP compared to 60% of companies that didn't cut IT staff. Furthermore, 17% of IT decision-makers that laid off staff said it was a higher priority to automate tasks with robotic process automation (RPA), machine learning (ML) or artificial intelligence (AI) in response to COVID-19 compared to 10% of decision-makers that didn't make cuts.

More than 3 in 4 IT leaders (79%) saw a reduction in headcount at the beginning of the pandemic as enterprises cut costs

28%

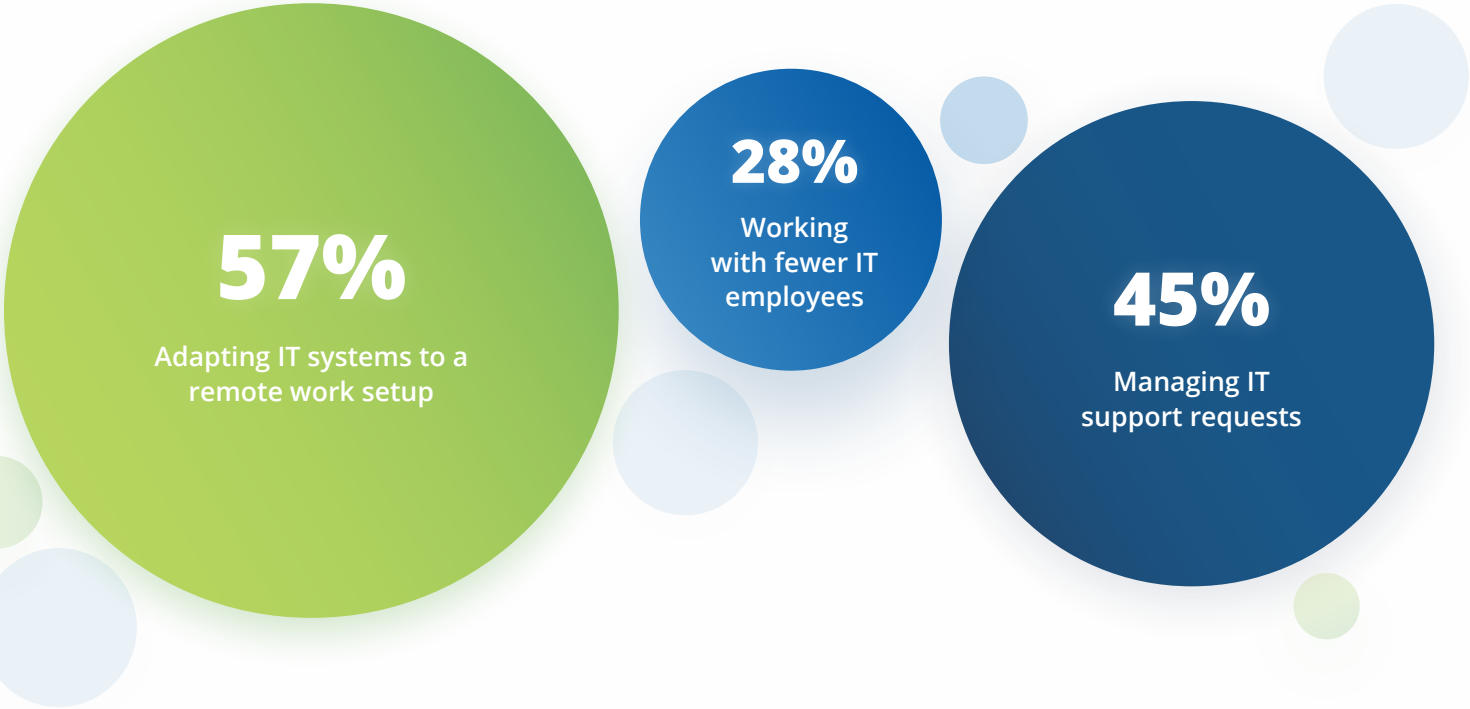
More than 1 in 4 decision-makers said "working with fewer IT employees" was a top challenge

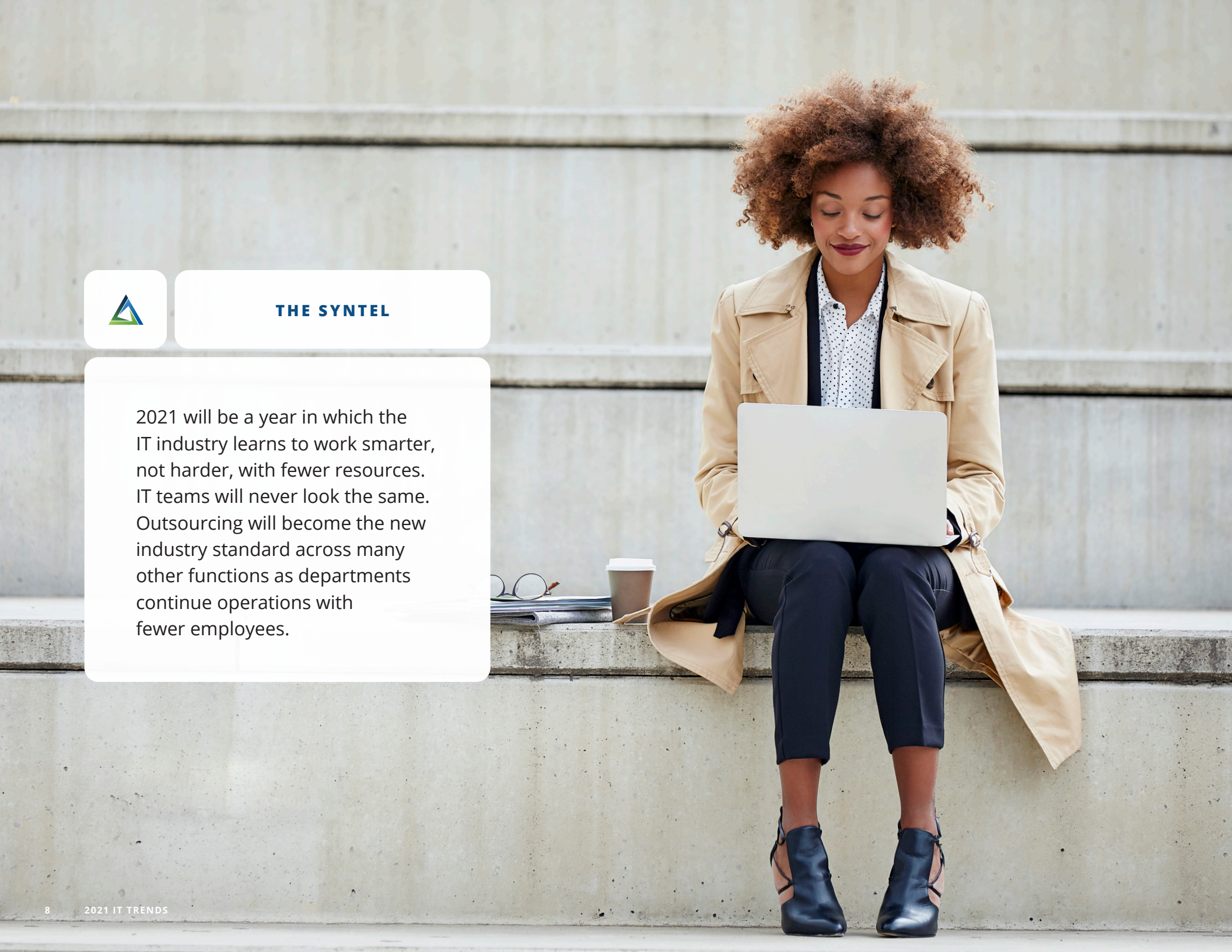
89%

of companies that laid off staff plan to outsource their internal cybersecurity operations to an MSP compared to 60% of companies that didn't cut IT staff

Moreover, 45% of all IT leaders said managing IT support requests was a challenge during the pandemic. With this, we expect more organizations to invest in application managed services (AMS) to fulfill the volume of functional support requests demanded in a remote work environment. AMS teams provide all organizations — regardless of whether or not they made IT cuts — a cost-efficient solution to fulfilling functional support requests in a timely manner.

Top 3 IT department challenges during the pandemic





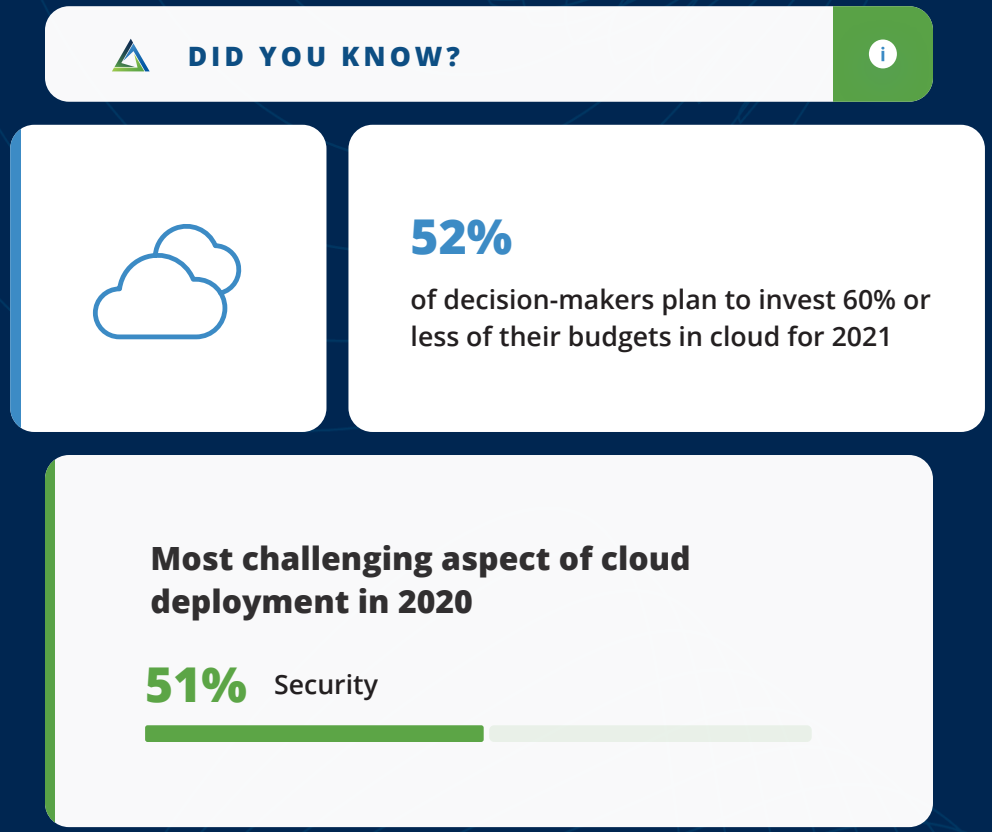
THE SYNTEL

2021 will be a year in which the IT industry learns to work smarter, not harder, with fewer resources. IT teams will never look the same. Outsourcing will become the new industry standard across many other functions as departments continue operations with fewer employees.

SECTION 3

Expect cloud security to surprisingly be neglected

Cloud migration will continue in 2021 as companies refine their remote work capabilities. Decision-makers will prioritize business continuity and disaster recovery (BC/DR) during this migration. However, cloud security is not receiving the focus it requires. As a result, this neglect could have damaging consequences for enterprise cloud systems.



An incomplete formula for cloud migration

Ninety-nine percent of IT leaders said they were satisfied with their cloud deployment during the pandemic — a triumph considering the major shifts many organizations made to their business operations.

Continued cloud migration will be a focus in 2021: 30% of IT leaders said the pandemic deprioritized the migration to cloud, but cloud migration tied with improving cybersecurity protections as the top IT investment initiative for 2021 at 37%. Furthermore, 52% of decision-makers said they plan to invest 60% or less of their budget in cloud next year. Another quarter of decision-makers said they will invest 30% or less.

Leaders are planning a clear investment strategy in the cloud. However, their efforts don't appear to address the cloud's greatest challenge: security. Decision-makers rated security as the most challenging area of the cloud, but didn't rank it in the top areas of cloud investments for 2021. Instead, factors tied to business continuity took greater priority, which is peculiar since the success of BC/DR hinges on adequate security.

99%

of IT leaders said they were satisfied with their cloud deployment during the pandemic

51%

of decision-makers rated security as the most challenging area of the cloud

Data storage opens up many vulnerable endpoints, especially with the expanded use of file-sharing tools in the cloud. And if these endpoints aren't secure, a breach could cripple an organization's cloud system. Hybrid and multi-cloud systems require a seamless integration of multiple platforms, meaning the connections between these systems must be guarded to ensure functionality. And decision-makers' third-place cloud investment for 2021 — system maintenance — can't be executed without security guardrails in place to keep systems running.

It's important to remember that BC/DR and security are two different components. BC/DR doesn't guarantee security. In fact, security is the foundation for BC/DR — the more security vulnerabilities are minimized, the greater chance your business has to continue running or recover from unforeseen events like cyberattacks, IT equipment failures, and natural disasters.

CLOUD CHALLENGES VS. CLOUD INVESTMENT

Top 3 most challenging aspects of cloud deployment

51% Security

44% Migrating on-premise IT infrastructure to cloud

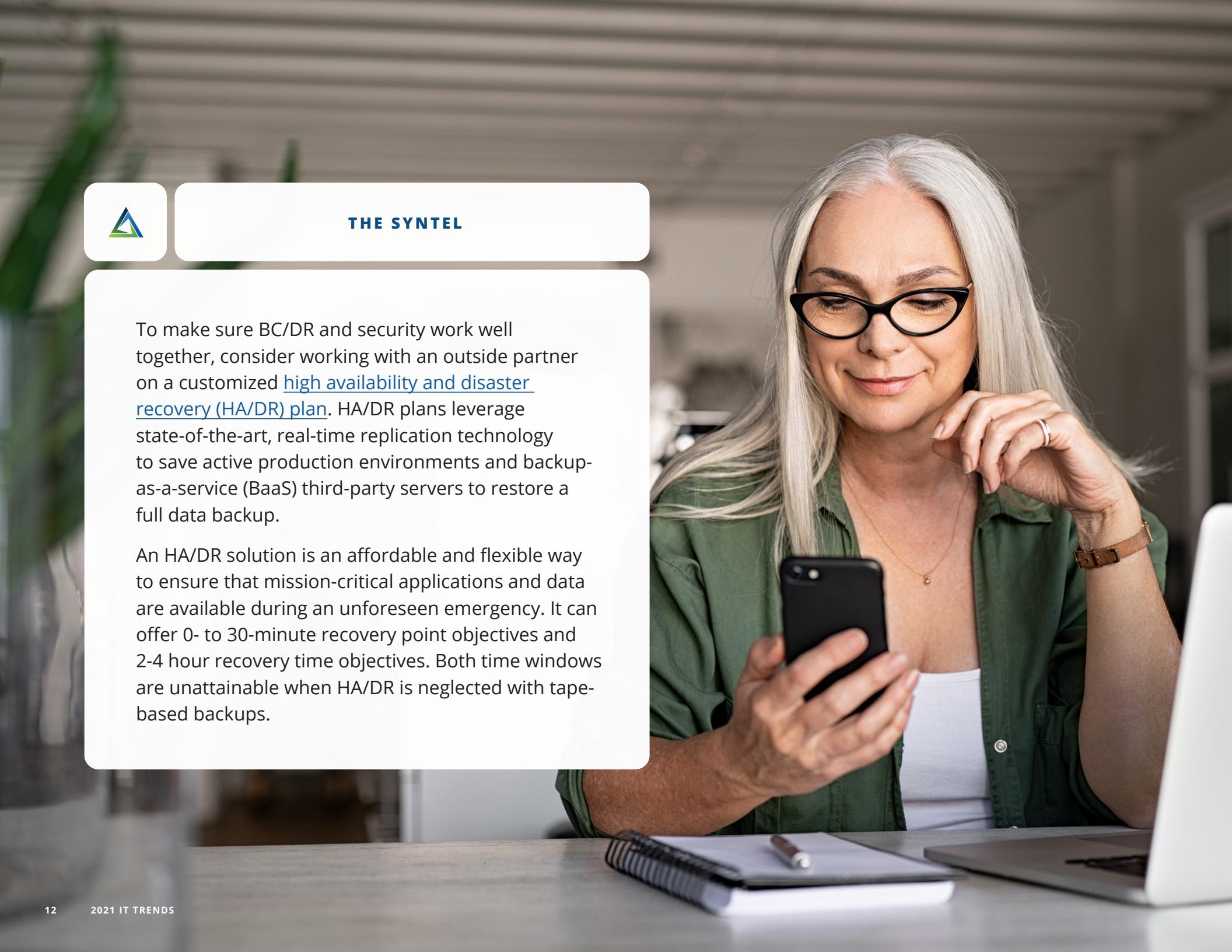
36% Difficulty with employees using cloud tools

Top 3 cloud investments for 2021

62% Increased storage and/or flexibility

48% Multi-cloud and/or hybrid cloud capabilities

47% System maintenance



THE SYNTEL

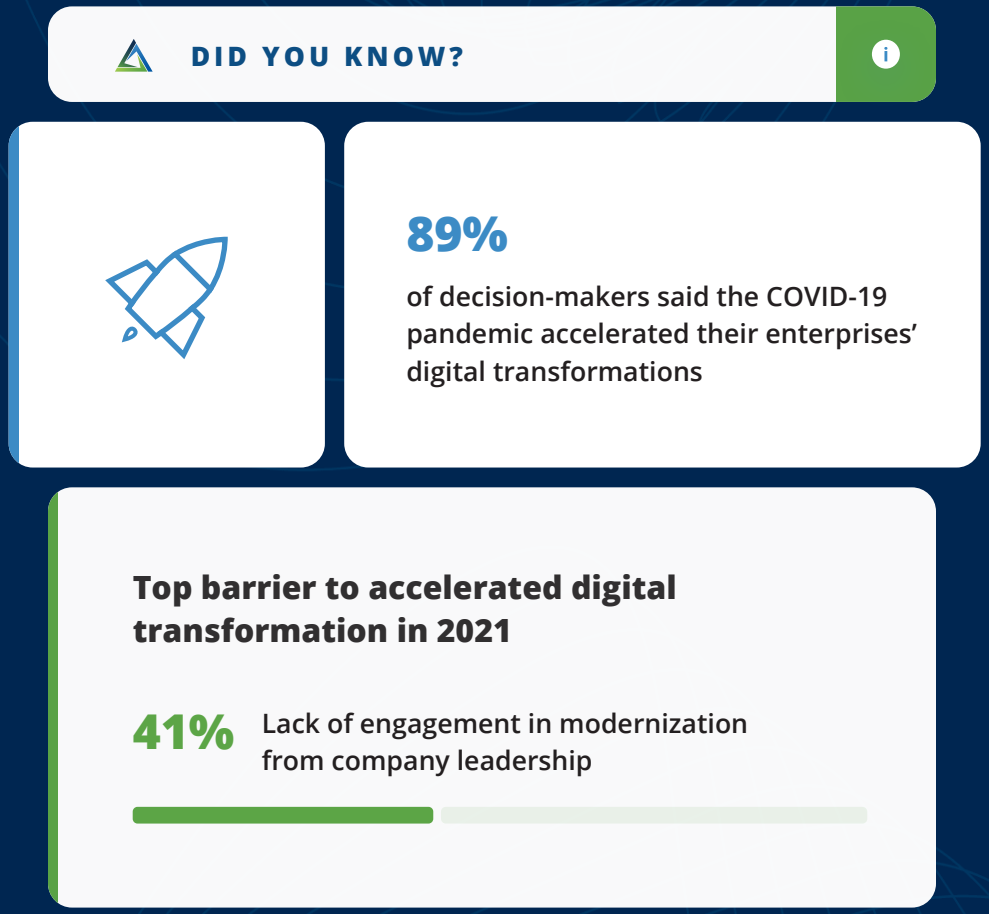
To make sure BC/DR and security work well together, consider working with an outside partner on a customized high availability and disaster recovery (HA/DR) plan. HA/DR plans leverage state-of-the-art, real-time replication technology to save active production environments and backup-as-a-service (BaaS) third-party servers to restore a full data backup.

An HA/DR solution is an affordable and flexible way to ensure that mission-critical applications and data are available during an unforeseen emergency. It can offer 0- to 30-minute recovery point objectives and 2-4 hour recovery time objectives. Both time windows are unattainable when HA/DR is neglected with tape-based backups.

SECTION 4

IT leaders to have a rare negotiation opportunity

The pandemic was a major accelerator of digital transformation. This will continue at a rapid rate over the next year. And while decision-makers expect pushback from non-IT leadership in facilitating digital transformation, IT leaders also have more leverage at the negotiating table to make initiatives come to fruition.



Building the case for digital transformation with data

COVID-19 was a catalyst for rapid organizational change, with 89% of IT leaders saying the pandemic accelerated their enterprise's digital transformation. This acceleration shows no signs of stopping, with 96% of respondents saying their digital transformation will not slow down in 2021.

IT decision-makers said knowledge gaps between multiple generations of workers and slow adoption of digital transformation initiatives by employees were top barriers to accelerated digital transformation. However, their biggest concern lies at the top of the company hierarchy — a lack of modernization engagement from company leadership, which could broadly hinder necessary technological advances for organizations.

C-suite IT leaders appear to feel this same frustration with leadership, with 47% noting a lack of modernization buy-in from fellow company leaders. Chief information officers (CIOs) and chief digital officers (CDOs) have sparred with other leaders over how many resources should be dedicated to digital transformation. However, IT decision-makers will have more leverage in 2021 — if they make their case the right way.

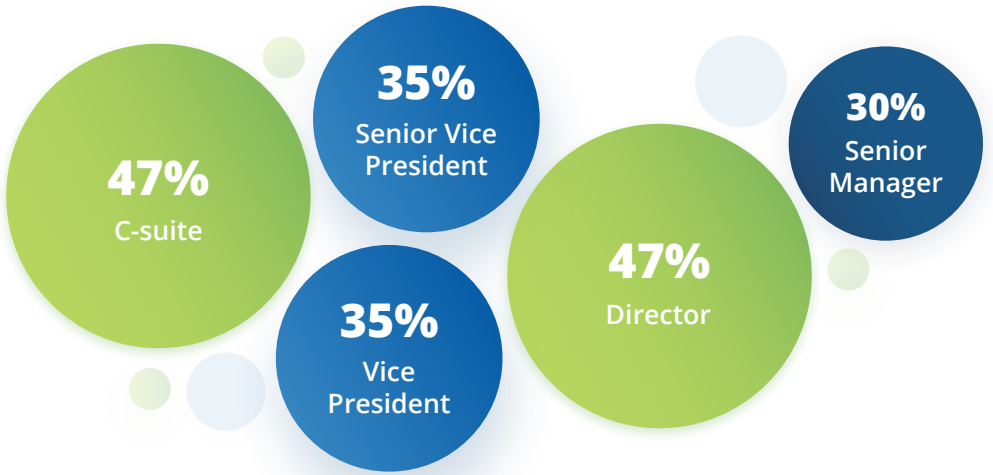
Top 3 potential barriers to accelerated digital transformation

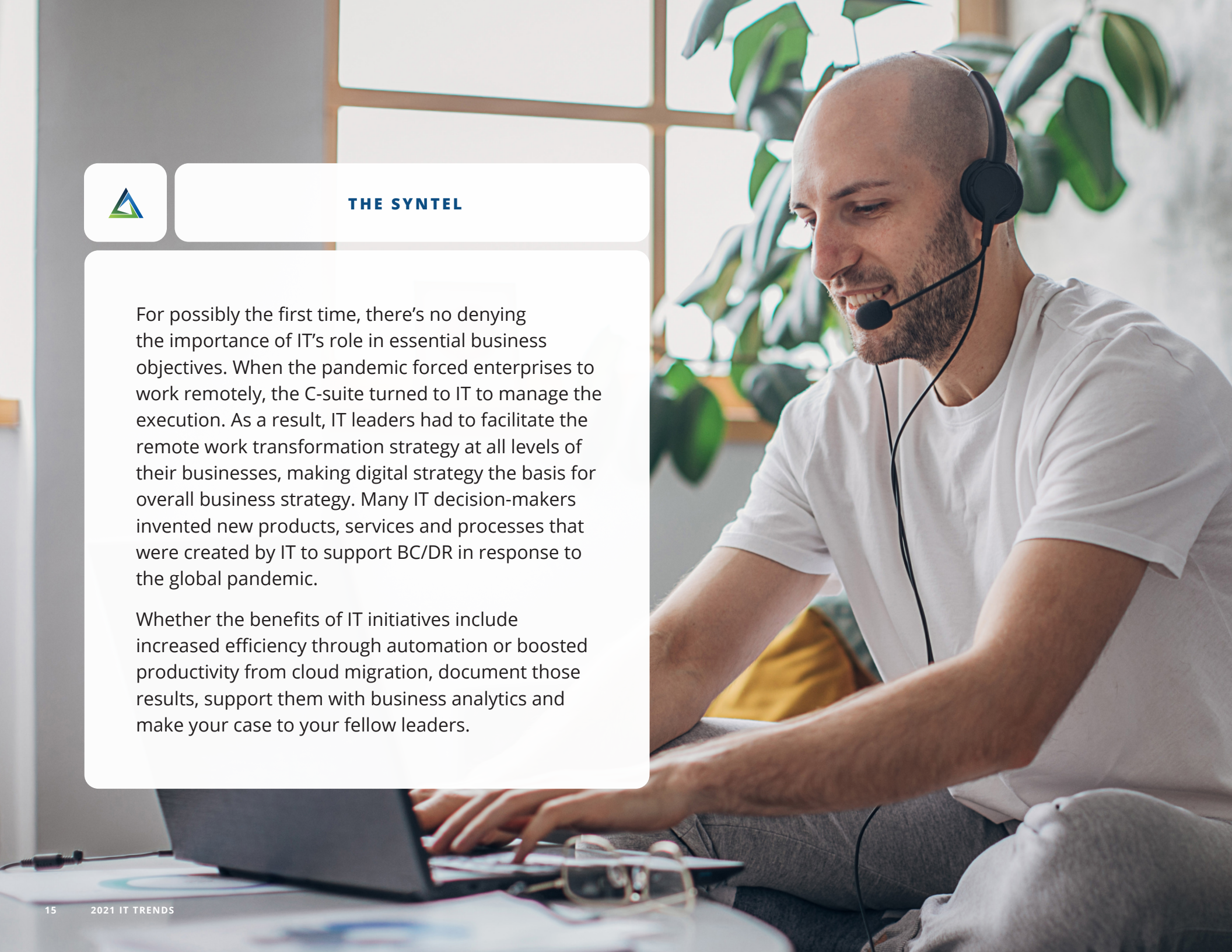
01 Lack of engagement in modernization from company leadership

02 Knowledge gaps between multiple generations (by age) of users within the organization

03 Slow adoption of digital transformation initiatives by employees

IT leaders who said a lack of leadership engagement in modernization was a top barrier to digital transformation, by position level





THE SYNTEL

For possibly the first time, there's no denying the importance of IT's role in essential business objectives. When the pandemic forced enterprises to work remotely, the C-suite turned to IT to manage the execution. As a result, IT leaders had to facilitate the remote work transformation strategy at all levels of their businesses, making digital strategy the basis for overall business strategy. Many IT decision-makers invented new products, services and processes that were created by IT to support BC/DR in response to the global pandemic.

Whether the benefits of IT initiatives include increased efficiency through automation or boosted productivity from cloud migration, document those results, support them with business analytics and make your case to your fellow leaders.

SECTION 5

Work-from-home improvements will be unsettling for IT

IT leaders think employee training will optimize remote work, with security needs driving the initiative as organizations battle phishing attacks and shadow IT. However, decision-makers must remember that the whole is greater than the sum of its parts — training programs are only one piece of the solution to IT challenges.

DID YOU KNOW?

32%

of IT leaders said further building remote work capabilities was a top IT priority for the next year

Top initiative to support remote work in 2021

59% Improving employee training on remote work tools

An incomplete plan to improve remote work

Although the remote work revolution was brought on by necessity, almost two-thirds (63%) of IT leaders said the transition to remote work went "extremely well." Eighty-five percent also expect remote work to continue in 2021, and 32% of respondents said further building remote work capabilities was a top IT priority for 2021.

Working from home is no longer just a perk at progressive businesses — it's the way many of us will work for the foreseeable future. Now that most organizations have spent months working remotely, IT leaders will aim to establish robust employee training programs to better support remote work in 2021.

Given that phishing attacks were the most frequently occuring cyberattack reported by decision-makers in 2020, place security at the forefront of your training initiatives. The 2020 holiday season was also ripe for hackers to use shopping phishing scams to entice end users with fake deals and compromise their networks.

Phishing training provided by an MSP is a viable training solution that bolsters remote work training while further securing your company. These programs send test emails to employees to gauge their instincts and knowledge of possible phishing scams. Forty-seven percent of decision-makers also want to improve employee training on the risks of shadow IT and the reasons why authorized tools must be used. While training is important, it won't eradicate shadow IT alone. Many in the industry think giving end users a large portfolio of approved tools will keep employees from using other third-party services, but some employees will still circumvent IT.

Top 3 initiatives to support remote work in 2021

01 Improving employee training on remote work tools

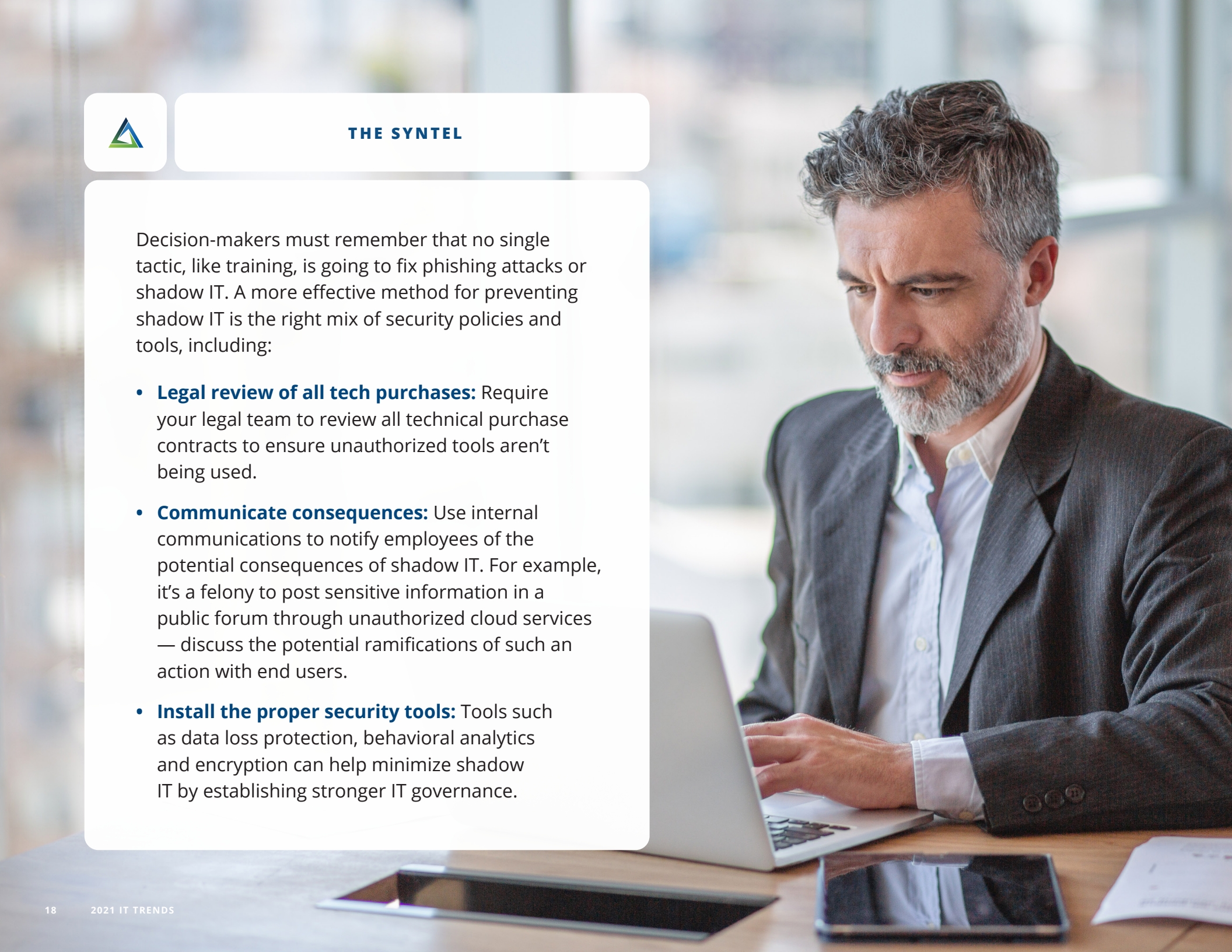
02 Updating our IT infrastructure to support remote access

03 Improving employee training on risks of shadow IT/need to use authorized tools

THE SYNTEL

Decision-makers must remember that no single tactic, like training, is going to fix phishing attacks or shadow IT. A more effective method for preventing shadow IT is the right mix of security policies and tools, including:

- **Legal review of all tech purchases:** Require your legal team to review all technical purchase contracts to ensure unauthorized tools aren't being used.
- **Communicate consequences:** Use internal communications to notify employees of the potential consequences of shadow IT. For example, it's a felony to post sensitive information in a public forum through unauthorized cloud services — discuss the potential ramifications of such an action with end users.
- **Install the proper security tools:** Tools such as data loss protection, behavioral analytics and encryption can help minimize shadow IT by establishing stronger IT governance.



SECTION 6

Data analytics to see substantial gains in IT

Business analytics and intelligence are poised to gain relevance as IT leaders leverage growing repositories of data to drive business decisions. Nevertheless, this endeavor is easier said than done. Decision-makers will need to use the right tools for business analytics and intelligence to make the effort worthwhile.

DID YOU KNOW?

42%

of IT leaders said their data analytics and business intelligence initiatives were deprioritized due to COVID-19

55%

of IT leaders plan to invest in data analytics and business intelligence in 2021

Data analytics and business intelligence will take a step toward industry-wide adoption in 2021

Data analytics capabilities and business intelligence experienced a setback from the pandemic — 42% of IT leaders said these initiatives were deprioritized because of COVID-19. Enterprises with reduced IT headcounts especially felt this deprioritization — 46% had to reduce their data analytics and business intelligence priorities versus only 29% of enterprises that didn't make IT cuts.

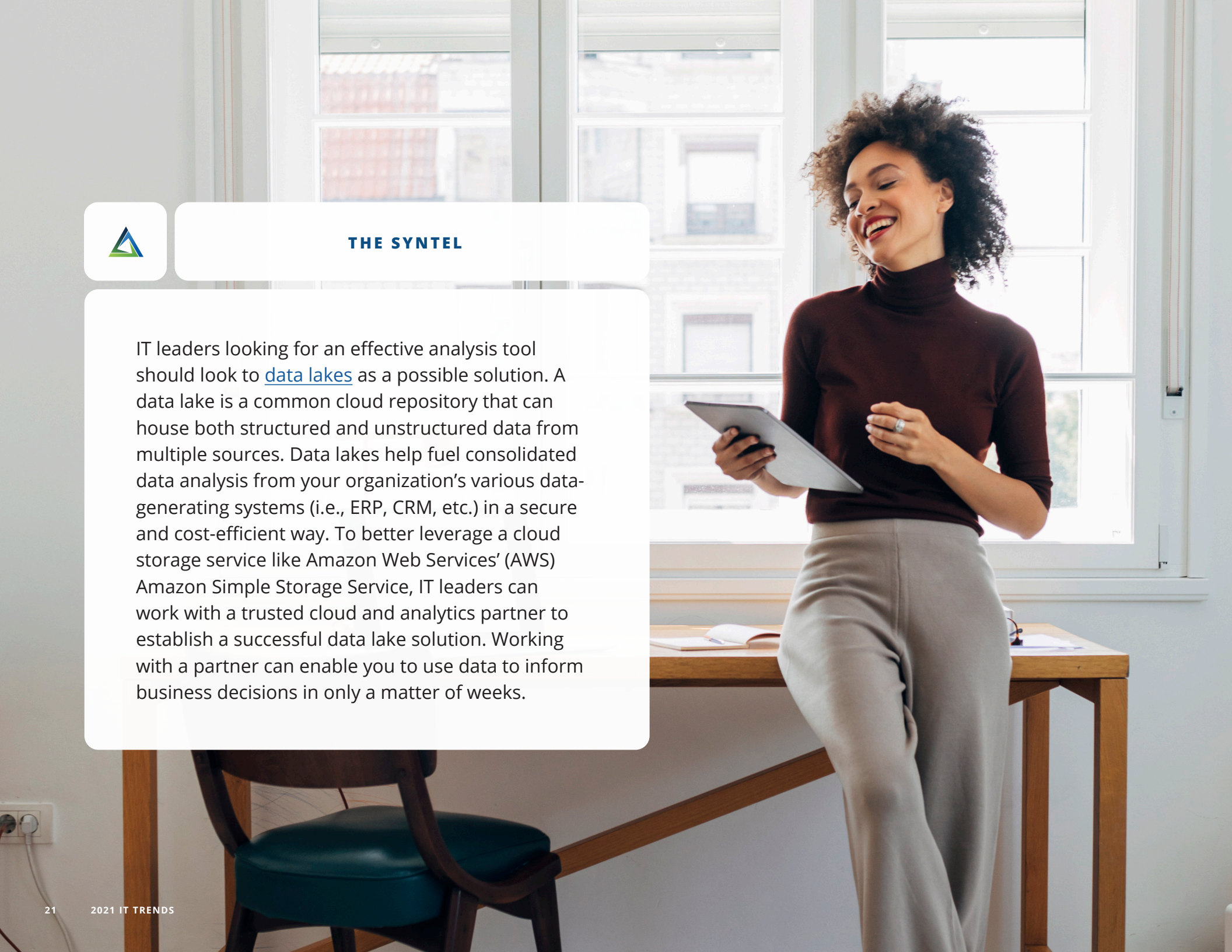
However, 2021 is shaping up to be a bounceback year for these tools with 55% of decision-makers planning on investing in their development over the next year, including teams with and without reduced IT headcounts. IT decision-makers everywhere are under pressure from their organizations to make better-informed, data-driven decisions in the digital business era brought on by COVID-19.

Today's business systems are generating more data than ever before and IT teams must use tools like business analytics software to analyze it. With the average company seeing their data volumes grow by 50% annually from an average of 33 unique data sources, it's no longer workable for an in-house data scientist to manually analyze data in spreadsheets.

While many enterprise resource planning (ERP) systems offer data warehouses with analytics capabilities, most don't allow for cross-analysis against sources like customer relationship management (CRM) data. These data warehouses also require businesses to define exactly what they need from the data upfront, which can add up in cost and time. Companies are left with mounds of data that can inform business decisions without a suitable method for analyzing them.

Prioritization of data analytics and business intelligence in 2020 vs. 2021

	Deprioritized due to COVID-19	Reprioritized in 2021
Building data analytics capabilities	22%	27%
Building business intelligence capabilities	20%	28%



THE SYNTEL

IT leaders looking for an effective analysis tool should look to data lakes as a possible solution. A data lake is a common cloud repository that can house both structured and unstructured data from multiple sources. Data lakes help fuel consolidated data analysis from your organization's various data-generating systems (i.e., ERP, CRM, etc.) in a secure and cost-efficient way. To better leverage a cloud storage service like Amazon Web Services' (AWS) Amazon Simple Storage Service, IT leaders can work with a trusted cloud and analytics partner to establish a successful data lake solution. Working with a partner can enable you to use data to inform business decisions in only a matter of weeks.

An unparalleled opportunity for IT in 2021

2021 will be a benchmark year for the IT industry. The restructuring of team personnel and practices because of the pandemic will redefine how professionals operate — even when businesses eventually return to pre-pandemic environments. The lack of plans from decision-makers to hire more IT staff and the need to execute operations with fewer employees will spur a newfound, increased reliance on MSPs and third-party partners across all IT functions.

Cybersecurity will see the first wave of increased outsourcing as organizations continue fighting a rapid increase of cyberattacks. Other areas primed for more outsourced support include automation of rote responsibilities, AMS for employee support requests and facilitation of training programs. With IT now seen as a critical component of business success, decision-makers have a groundbreaking opportunity to bring digital transformation to new heights across their enterprises.

How will your enterprise use this pivotal moment in 2021?

If you're ready to redefine IT infrastructure and operations, cybersecurity, and business analytics and need a partner to guide your organization's journey, contact us to see how we can help. You can also find more insights from our team at the Syntax Resources page and follow our blog for the latest industry expertise.

METHODOLOGY

Syntax surveyed 500 U.S. IT decision-makers in October 2020. All respondents were at the senior management level or above, worked at companies with 500+ employees and at least $500 million in total annual revenue. Participants were also directly involved in choosing or helping their organization implement new technology and were part of an enterprise that worked for two weeks or more from home during the COVID-19 pandemic.

Respondent breakdown by position level

28%	Senior manager
28%	Director
9%	Vice president
5%	Senior vice president
30%	C-suite

SYNTAX