

opsview 

State of the IT Nation Report

November 2019



Contents

Executive Summary	3
Poor practices hinder system health	5
Call on me – firms still need reassurance of back-up	12
Firms' IT strategies not matching today's digital environment	15
Conclusion	18

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Opsview, and its affiliates (referred to collectively as "Opsview"), and may not be disclosed or copied without prior written consent of Opsview.

Opsview retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Opsview makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit www.opsview.com.

Copyright © 2019, Opsview. All rights reserved.

Executive Summary

IT is the bedrock of any organization, but unlike Finance, Operations or HR, IT is often viewed as a cost-center instead of a strategic hub. This is despite the fact that with the prospect of a global recession looming, IT spending is only set to increase. In fact, Gartner predicts that global spending on IT will reach \$3.88tn in 2020, a 3.7% year-on-year growth.

This growth in IT can be explained because businesses are realizing the incredible value of 'digital' – be it the infrastructure itself (cloud, big data, analytics etc.), or emerging technologies (machine learning, AI and augmented/virtual reality) that can vastly benefit their productivity and profitability. However, despite this vision for a more connected enterprise, and digital transformation encouraging closer business collaboration, it seems that IT and other departments are still not seeing eye-to-eye and business siloes and fragmented systems are still a significant prohibitor to company innovation and growth.

A Financial Times and Apptio report confirmed this, with only 30% of CFOs and CIOs agreeing on issues including new products and services, allocation of IT investment in new digital strategies, and accountability for technology investment decisions. Finance leaders cited that IT needs to develop greater influencing skills in order to deliver the change their business requires. This included CIOs communicating where IT adds a competitive edge – as without this justification the function is sometimes viewed as less strategic than other just as critical business functions.

Organizations need to balance the requirement for digital transformation with IT to ensure that real value can be extracted from such investments. Simply put, organizations need to have the right foundations in place to support both the new breed of digital services and the hodgepodge of disparate and decentralized systems that lie behind these: virtual machines, hybrid cloud accounts, IoT endpoints, physical and virtual networks and much more. In this context, it's difficult to overstate the importance of effective IT Operations and Monitoring. Although the discipline is often viewed as "keeping the lights on", the truth is that without these solid foundations in place, digital transformation projects are doomed to fail.

Clearly a change in approach is needed, with a back to basics best practice the optimal way forward. While our research reveals that organizations are wising up to this (with 2019/2020 roadmaps prioritizing more basic functions over transformation activities), it also highlights worrying gaps in IT strategies. The fact of the matter is that this research shows organizations don't have sufficient visibility into what's happening across their IT estate which open them up to significant risk, IT complexity, tool sprawl and outages. With many enterprises struggling with the issue of legacy systems while bringing new technology into the stack, this buccaneering approach will only lead to failure. It's no wonder that the people we researched are needed on-call so often – because the likelihood of operational failure is so high.

The key takeaway from this research is that organizations aren't adopting a strategic approach to IT. They appear to be investing in day-to-day infrastructure requirements, however are failing to do basic necessities – such as monitoring the entire IT stack. Just 22% of businesses we talked to monitored their whole estate, leaving them exposed. This is because there is no single source of truth for the whole system, meaning tracing issues back to their source becomes increasingly complex. Based on this information, it's not hard to see why IT struggles to shake its reputation as a cost center.

Organizations need to focus on getting the foundations right and implementing an IT monitoring system that provides full system visibility, and can quickly identify problems before they cascade. This makes IT much more profitable and frees up the IT workforce to concentrate on more strategic projects which drive business value.

Unless firms adopt this approach, they will be the 97% which don't see sustained value from transformation projects, and CIOs will forever be resigned to no seat at the top table.

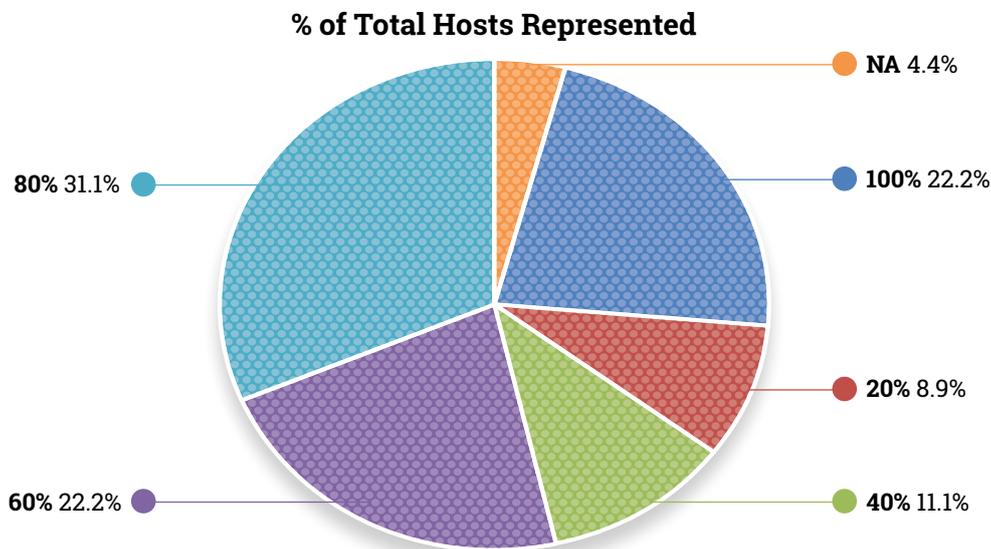
Opsview's research was conducted between April and August 2019, sampling 217 IT professionals working in enterprise environments.

Section one: Poor practices hindering system health

A healthy IT infrastructure is what underpins and drives forward all successful business operations. However, all too often issues arise when IT departments don't have full visibility into what is happening within their IT stack. Take IT outages for example – these are often caused not by one, big disaster (such as a total loss of power), but by smaller, more intricate issues which very quickly snowball into one, amalgamated problem. This impacts the business not only in terms of downtime and lost revenue, but reputation also, with some firms such as TSB and BA forever associated with long, catastrophic outages.

It seems that despite some of the biggest companies suffering outages of late (Amazon, Google, Cloudflare, Instagram to name but a few), other companies are not learning from their mistakes with regards to what precipitates an outage – lack of visibility across their IT estate. The vast majority of businesses we researched (73%) are not monitoring their whole infrastructure, with 60% monitoring less than 1,000 hosts. As explained above, the risk associated with this is vast, and also means that the IT department will spend many hours searching for information on what is the root cause as there is no single version of the truth or a clear picture of what happened, when. For firms looking to maximize productivity, this is a very backwards approach. It is also surprising considering almost half of those researched were responsible for IT estates that spanned three or more physical locations; meaning keeping IT infrastructure healthy for everyone should be of utmost priority, to prevent downtime across multiple locations.

Of hosts you're monitoring, what percentage is this of the total hosts (virtual or physical) in your IT estate?

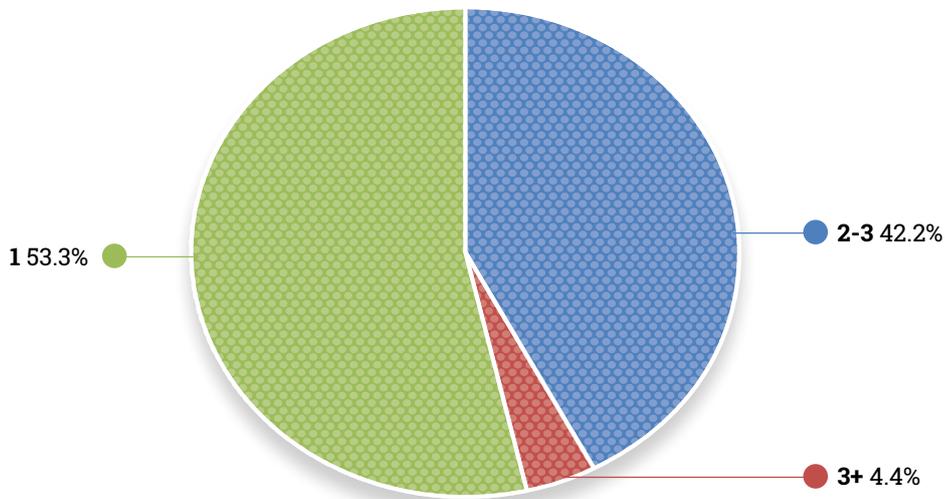


The research also showed that almost half of businesses we talked to are utilizing more than one public cloud region. When operating across jurisdictions, firms need to be aware of potential issues to help avoid downtime, and it's worrying to think that many of the 47% of firms working across numerous cloud regions don't have a single source of truth with regard to IT operations. With such high numbers failing to monitor their entire IT estate, and spanning many public cloud regions, businesses are opening themselves up to a higher degree of risk. In addition, the multiple regions may also be taking matters into their own hands, using their own tools to try and ascertain some level of clarity. This inevitably leads to IT tool sprawl, and high internal costs as tools may be duplicated across the company, auto-renewing across different teams and costing the business for a substandard service.

This theory was confirmed in our research, with 80% confirming they use 2-5 monitoring tools. The fact so many are resorting to multiple tools when one, single solution should suffice, again reiterates how firms are failing to implement the correct digital foundations in IT monitoring. A recent Forrester report painted a more worrying picture, stating that 33% of companies are using over 20 monitoring tools, hindering agility and adding multiple layers of complexity. This approach also stifles future growth, as without the right IT infrastructure in place to support modern tools and older legacy systems, firms will not be able to have a cohesive IT stack – leading to business siloes and stilted operations.

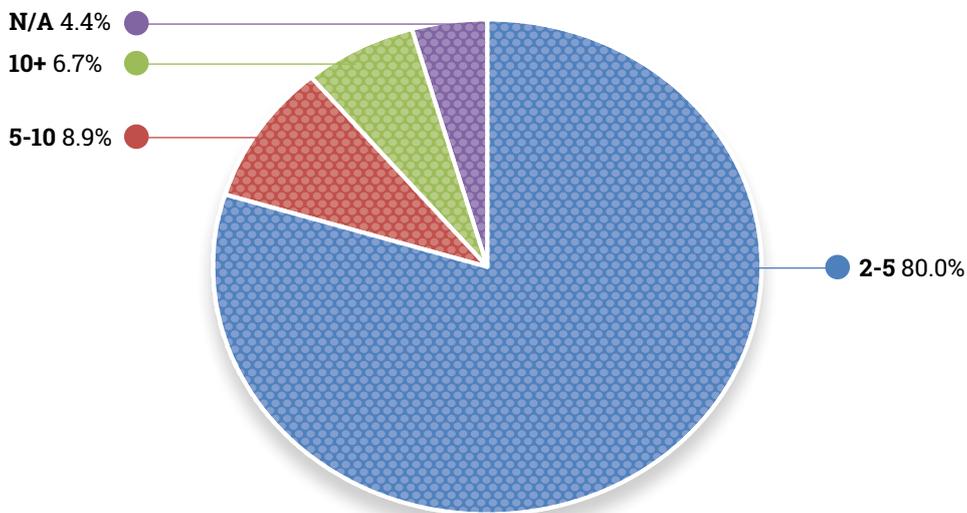
Does your IT estate span one or more public cloud region? If so, how many?

Does your IT estate span one or more public cloud region?



How many different tools (not instances of a single tool) are now in use for monitoring at your organization?

How many different tools are now in use for monitoring?

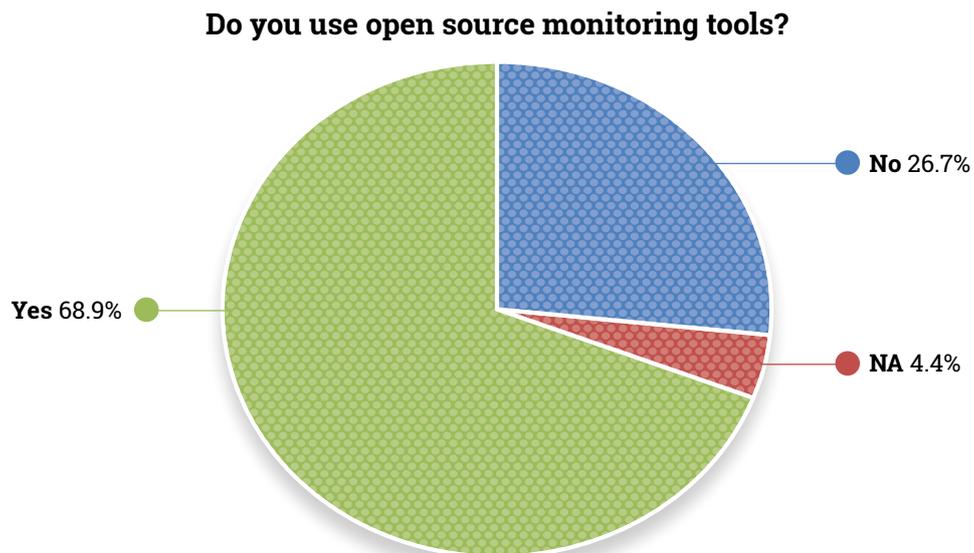


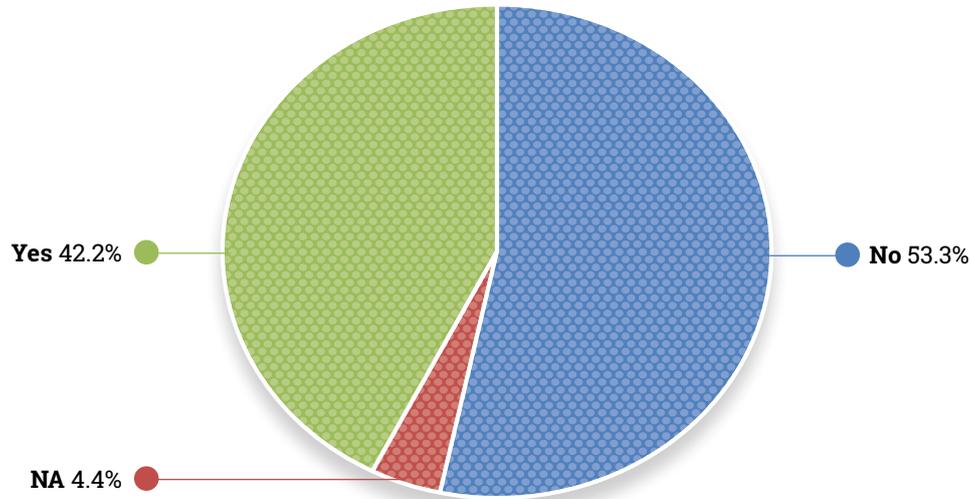
Another key theme that our research highlighted was that nearly three in four corporations (69%) use open source monitoring tools such as Nagios®. While many organizations are initially attracted to open source tools due to the fact they're free, there are other cost considerations which should be evaluated. Ongoing maintenance and support costs (such as increased resource or teams solely dedicated to its upkeep) start to outweigh the lack of annual license fee; meaning Nagios® and other open source tools prove more expensive than often thought. This is because the Nagios® platform requires substantial work to set up, use plugins, and configure – all of which needs to be done by an experienced sysadmin with extensive Nagios® knowledge. It takes a long time to develop this intricate understanding of the technology, meaning businesses will start to rely very heavily on just one or two individuals for their monitoring needs. A monitoring solution with an easier learning curve negates this issue.

Therefore, time and money is used on open source platform upkeep rather than strategic projects which drive more value. Firms should beware of the 'free' price tag as IT functionality should not be sacrificed just to keep costs low – especially when certain features are tied in to subscription requirements such as enterprise packages.

Businesses should also consider the other risks associated with open source IT monitoring – namely security dangers and minimal support. The fact that our research revealed that over two fifths (42%) are using multiple instances of a single source tool to monitor at scale highlights how a high proportion of businesses are taking a very backwards approach to monitoring. Not only are they failing to address all areas of the IT estate, they are also incurring incremental costs across the business by adopting poor IT monitoring practices business-wide simply to 'save' money. Investing in one, single solution which provides a more comprehensive service and single source of truth would surely be the preferable alternative, enabling business agility and the conglomeration of the IT estate.

Do you use open source monitoring tools (e.g. Nagios®)?



Do you use multiple instances of a single open source tool to monitor at scale?

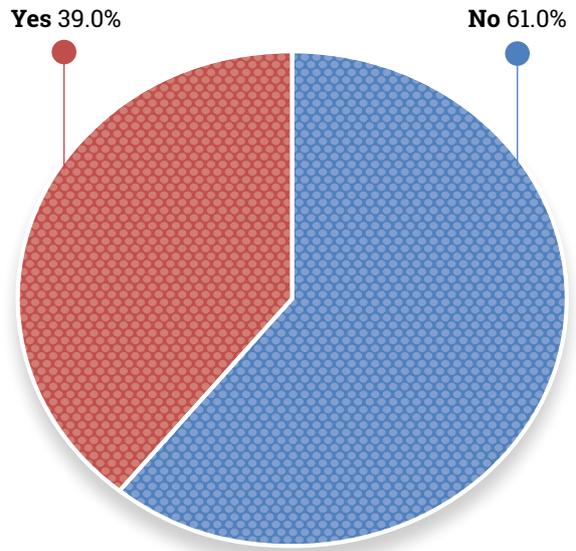
Alongside the preference to use open source monitoring, even at scale, our research also revealed firms' indecision between on-premises and SaaS-based monitoring. Almost two in five (39%) of corporations utilize SaaS monitoring, while a significant 74% of firms still use on-premises monitoring – demonstrating a traditional approach to monitoring, and in some instances, overlap between on-premises and cloud-based operations. While the move to the cloud has operational benefits such as greater agility, clearly concerns remain about control and data security, which on-premises provides. Ultimately, having an overlap shows indecisiveness, and could well be slowing businesses down by duplicating efforts – mainly as both options require upkeep – and organizations would be wise to consider which platform provides most business benefit – now and in the near future; especially if digital transformation is on the horizon.

Despite the split approach, there is a common theme – yet again a large number of hosts remain unmonitored – so for all the benefits firms reap, they are still open to significant and sustained risk as there is no single picture of system health.

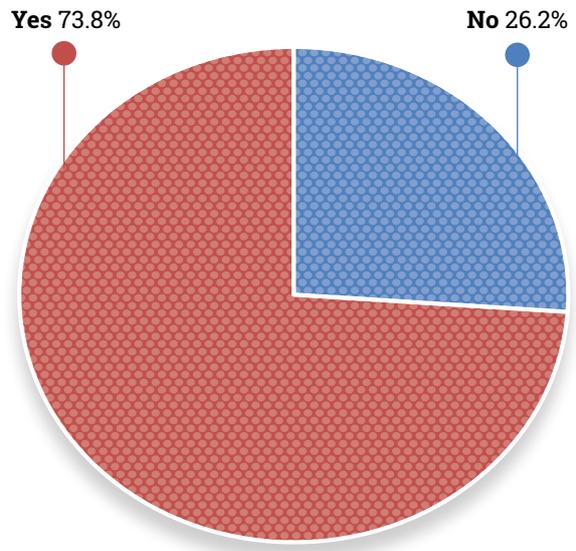
It is no surprise, therefore, that over half (58%) of those researched admitted to not being able to view the entire IT estate under “a single pane of glass”. While we have addressed many of the issues this causes previously, ultimately it will cost firms in multiple ways. Time, duplication of effort, complexity, tool sprawl, delay, increased chance of outages – the list goes on. For all the apparent ‘cost savings’ that open source platforms provide, businesses must wise up to the potential costs they will incur without a more comprehensive monitoring option. Gartner estimates that downtime costs corporations \$300k per hour, which fails to include reputational and internal costs. For many businesses, this number could lead to serious ramifications on its profit and loss, making the outlay on an IT monitoring solution which could ultimately prevent these instances seem less stark in comparison.



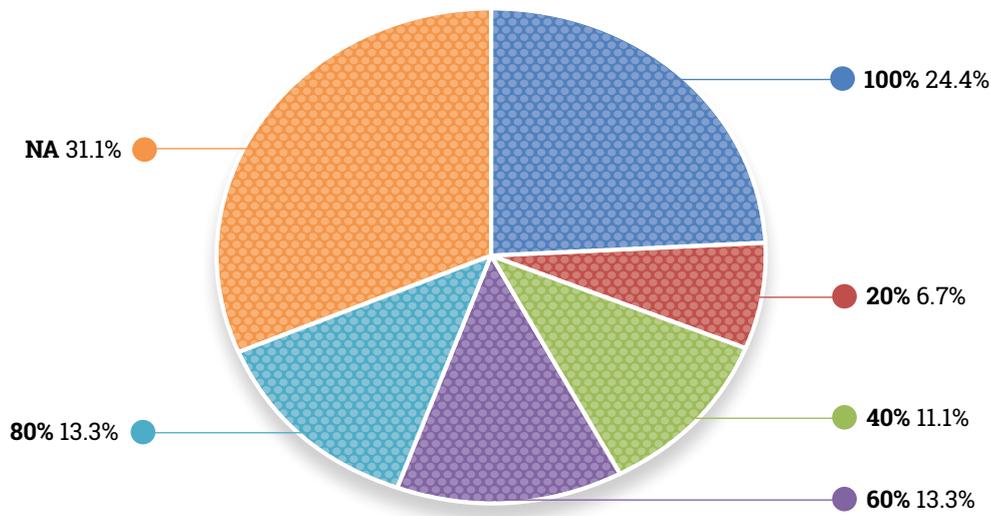
Do you use SaaS-based monitoring?



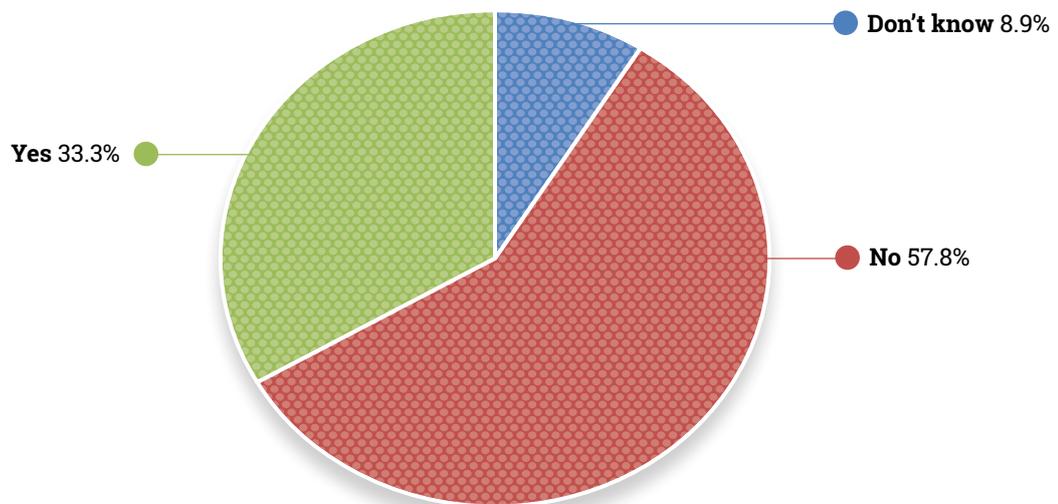
Do you use premise-based monitoring?



What percentage of total hosts do you monitor using on-premises?

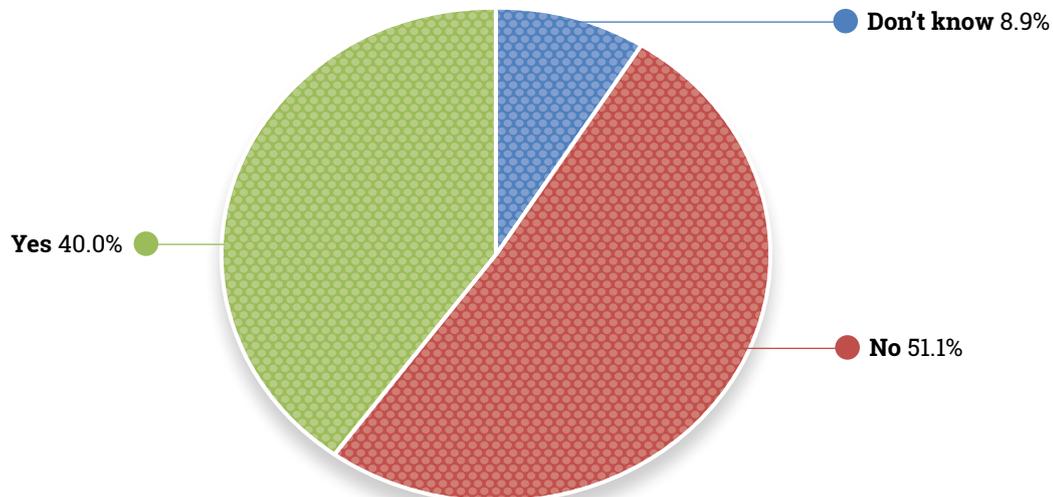


Can you view your entire organization's IT estate under a "single pane of glass"?



This siloed approach to IT also means the department's value is not necessarily felt throughout the business. Over half of firms (51%) don't share dashboards beyond the IT department – perhaps understandably if they don't have the data which can show a positive return. In an ideal world, IT system health should be shared across the C-Suite – informing operations – such as customer uptime and how this is influencing sales, dwell time and website analytics. In today's digitally-orientated world, having online operations working optimally is crucial to success. Just look at the repercussions TSB witnessed following its IT downtime fiasco – not only did it suffer financially, it also lost 12,500 customers, showing how user experience and reputation is crucial to customer acquisition and retention. This potential insight into customer behavior would help position IT as a strategic partner to Sales, Marketing, Operations and Finance, helping augment its influence across the board.

Do you use monitoring to share dashboards beyond the boundaries of IT operations? (e.g., with business stakeholders, to show the current state of critical business-facing and customer-facing services)



Over half of organizations (53%) are failing to automate IT monitoring, and therefore do not benefit from a more agile environment (which in turn reduces manual input). This would enable a sounder virtual infrastructure which in turn allows for a more development orientated environment which drives innovation. Even small integrations, combining monitoring with programs such as ops management, ticketing and Slack are not being taken advantage of, with the majority of firms not able to facilitate this. It's no surprise then that 64% of respondents did not integrate with time and efficiency saving tools like Puppet, showing an apathy to digital enhancements, and thereby missing out on a consistent environment which these tools enable.

For the 'Connected Enterprise' to become a reality, corporations need to drive through this form of automation, as it can save time and money. Almost two in three (64%) are not able to use monitoring as part of a toolchain that automatically mitigates certain kinds of issues – such as redeploying crashed cluster members; and from this research we can deduce it's because they just don't have the right foundations in place. By failing to get their IT estate under control, and a holistic view as part of this, firms are unable to take advantage of basic cost and productivity saving measures – which would benefit not only the balance sheet but the workforce too, as they would be assigned to more engaging, strategic work. Gartner ascertains that the number one cause of IT outages is human error – due to issues such as brain drain or being over-stretched. Automating simple tasks could help eradicate this, providing more fulfilling work than manual checks. Unlike humans, there would also be a clear timeline of activity, with one single source of truth, in turn denoting the original source of failure in the case of a cascade, where it can sometimes be hard to pinpoint the exact factor which caused a crash.

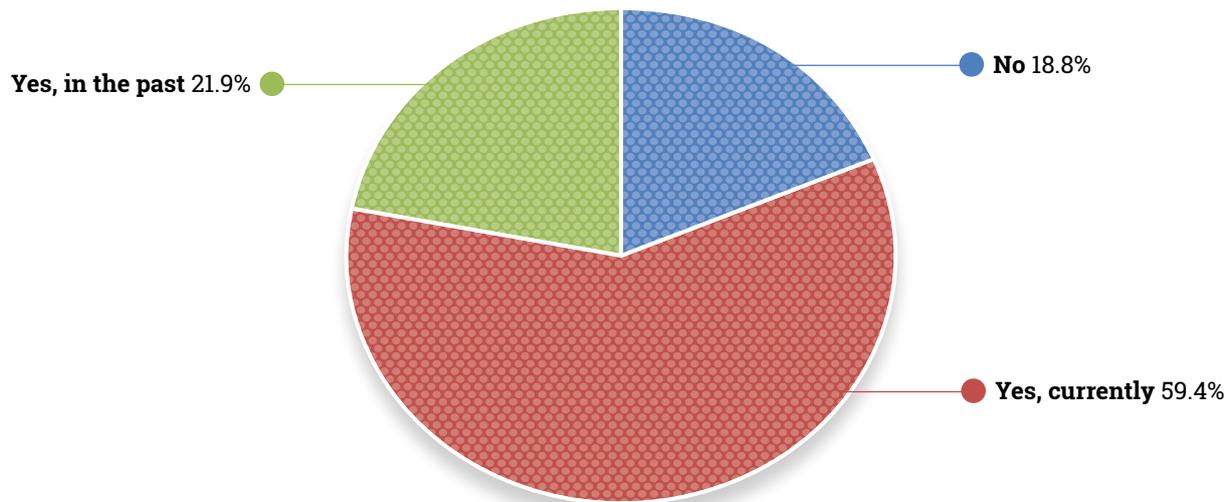
The narrative throughout this report shows that many firms are setting themselves back, perhaps due to a fear of an initial investment or the belief that free tools will help paper over the cracks. However, to help demonstrate its true strategic potential, businesses must implement a better monitoring strategy, underpinned by a single pane of glass approach if they hope to add any business value, and thereby credibility in the boardroom.

Section 2: Call on me – firms still need reassurance of back-up

IT downtime is a scourge on most businesses. Not only is it lost revenue, it's also lost opportunity and the chance to engage existing and new audiences; causing frustration all round. It affects multiple departments – Sales, Marketing, Operations and Finance – and although it's not always the fault of IT, it almost exclusively gets the blame. To try and mitigate this risk, many businesses employ a host of IT technicians on-call to fix any issues that may arise, no matter the time of day.

However, as seen in the previous section, if firms adopted a more strategic approach to IT infrastructure with effective monitoring in place, would they need to invest so heavily in on-call services? While having someone on hand to sort potential issues of course provides a sense of surety, when the cause of an incident is often unclear, does it benefit firms in the long-run? This section will analyze how businesses use their on-call team, and the challenges they face in responding to IT issues.

Are you currently, or have you ever, worked on-call?

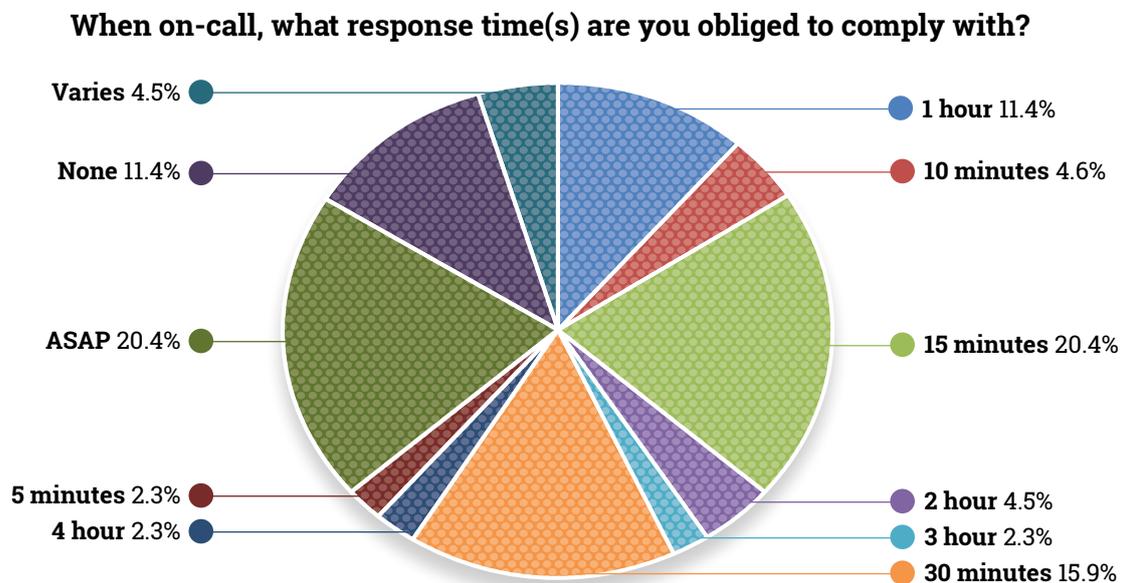


According to the data, over four in five IT professionals have worked on-call – either currently or in the past. This reinforces the concept that firms don't have the right infrastructure and monitoring processes in place, and therefore need additional support on hand, should any IT incident occur. The problem this presents, however, is consistency, as shifts vary in terms of length and commonality. They can differ in terms of lasting just a few hours, through to a couple of months; meaning one business could have several people on-call during the course of an issue – which could lead to a difference of opinion in how to react to warning signs, or overall system response. Overlooking the fact that technology could be used to safeguard against this (such as Opsview Cloud which prevents firefighting and enables time for innovation and projects), it also opens firms up to risk. Inconsistency will make it much harder to trace the initial IT incident and how it occurred, as one person's reaction to a potential issue may differ to another.

Another interesting takeaway the research highlighted was how employees on-call were compensated, and their motivation to do a good job. Just 52% of respondents are compensated for being on-call, with 48% saying it's a job requirement, and therefore they are not able to claim for the overtime hours. Considering under a third of companies routinely compensate for missing SLAs (28%), it appears there is a diminished incentive for those on-call to put their all into fixing the issue. This again is opening up firms to significant risk – as while many employees will act with the professionalism the job requires, in the case of issues which could have been dealt with in working hours, it does mean resentment could creep in, or the failure to deliver full concentration to the task in hand.

There's also the expectation that comes with being on-call. Considering almost half of respondents (48%) were obliged to respond within 15 minutes, it again calls into question why businesses are not giving their workforce the correct tools. Service-centric dashboards and reports should help employees fix what matters, instead of wasting hours trying to locate the source of the issue. Plus, with out-of-the-box support, having employees on-call should soon be a thing of the past.

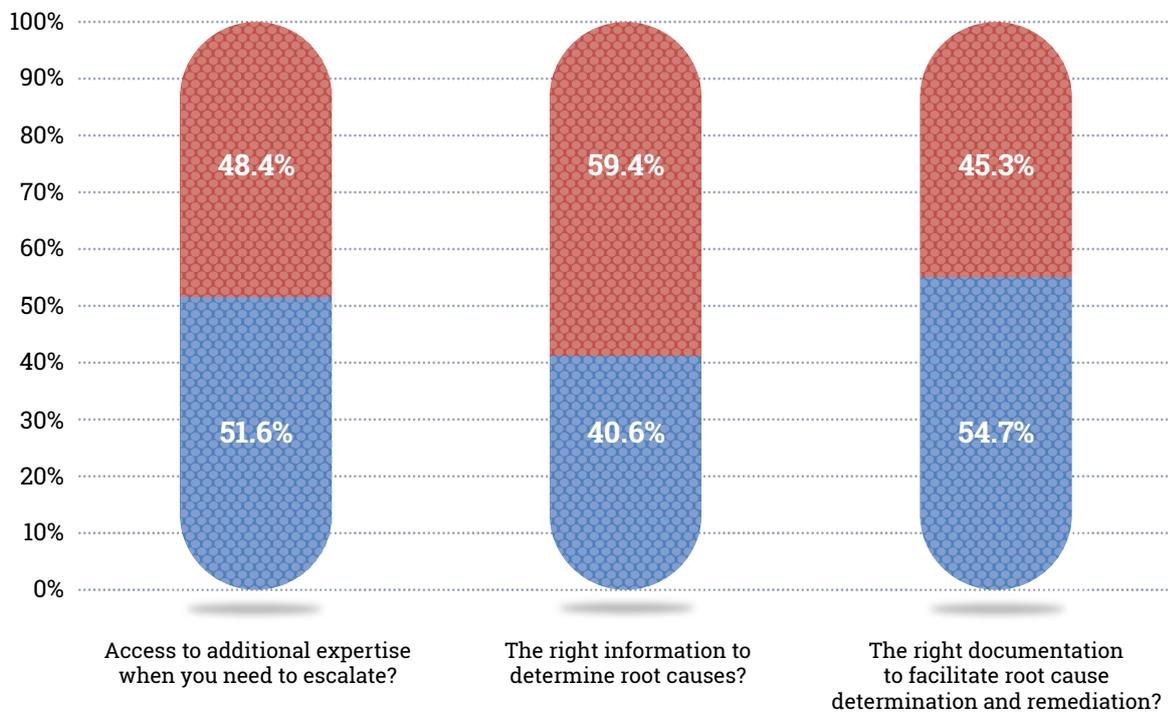
Without a clear activity timeline (which monitoring provides and as per the previous section most firms are failing to implement across the whole IT estate), it will be very hard for those on-call to remediate the issue promptly, even if they respond within the desired timeframe. According to Enterprise Management Associates (EMA), due to the issue of tool sprawl, IT teams can take between three and six hours to pinpoint performance issues; so even if on-call teams are responding quickly, it doesn't necessarily mean the issue is fixed in a similar snappy timeframe.



Our research also reveals that on-call rotations are generally seen as a junior job, despite their grave financial and reputational cost. When asked if managers join in the rotation, two thirds (66%) said no – highlighting how it predominantly falls on the shoulders of more junior employees. This could be a mistake in two respects; first, it implies the job is an easy fix, perhaps degrading the severity of the situation. However, judging by the fact that major companies have fallen foul of IT outages (Google, Amazon, Cloudflare), which cost millions of dollars, it seems perplexing that resolving the issue should fall on junior shoulders. There’s also the job satisfaction issue. In today’s workforce, there is much more churn than previously – making employee retention much harder. By failing to expose more junior team members to strategic work, businesses are perhaps risking job satisfaction by keeping them on-call.

Over two in five cited the fact that when on-call they did not have the right information to determine root causes, and a significant 55% said they did not have access to the right documentation to facilitate determination and remediation. Interestingly, 52% said they did not have access to additional expertise when the issue needed escalating, demonstrating how the issue of IT outages is not taken seriously within businesses. Not only is the necessary infrastructure not in place, but neither is the help when needed, reinforcing the idea that IT is seen as a cost center than a value-add. It again highlights the need for dashboards and reports which give users the information they need in a quick, digestible way – such as via Opsview Cloud.

When alerted to an issue, do you feel you have access to:



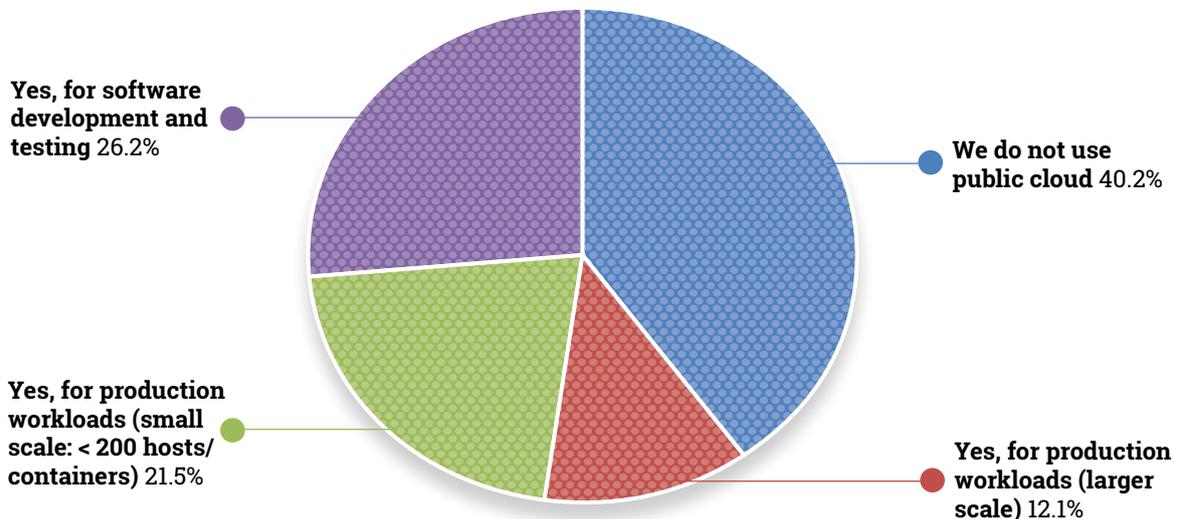
Section 3: Firms' IT strategies not matching today's digital environment

Digital transformation is driving considerable change within the workplace, as firms look to unlock value and move towards becoming connected enterprises. However, not only is it an expensive outlay (insurance giant AXA devoted €950 million over just two years to it), for many firms, it's also a risky investment – as seen by the low success rates. McKinsey's data that over 70% of projects fail should be a warning sign to businesses that they need to get the basics right before they embark on expensive infrastructure overhauls.

An issue many firms encounter and don't plan for is that the pace of technology change management outpaces organizational change, putting pressure on decision making processes and forcing firms to move with greater dexterity. This can cause problems, especially when decisions have been made yet then can't be executed due to legacy or convoluted IT architecture.

This disjointed approach has led to firms needing to prioritize more basic IT estate changes in the first instance, as the bigger, more strategic and technically complicated work is simply not possible with the current architectural environment. McKinsey's data really does emphasize that firms can't run before they can walk, and this section explores the areas businesses are focusing on over the coming months, in order to help drive value.

Does your enterprise use public cloud?



A takeaway from the research is that now over half of businesses are using a public cloud – mainly for software development and testing, thanks to its time saving capabilities. A key aspect of utilizing a public cloud is the ability to free up staff, as they are no longer responsible for maintaining on-premises equipment. This is perhaps reflected in the Cloud's main uses – mainly software development and testing (a test and learn environment), and smaller production workloads – implying a desire to move towards a more innovative environment.

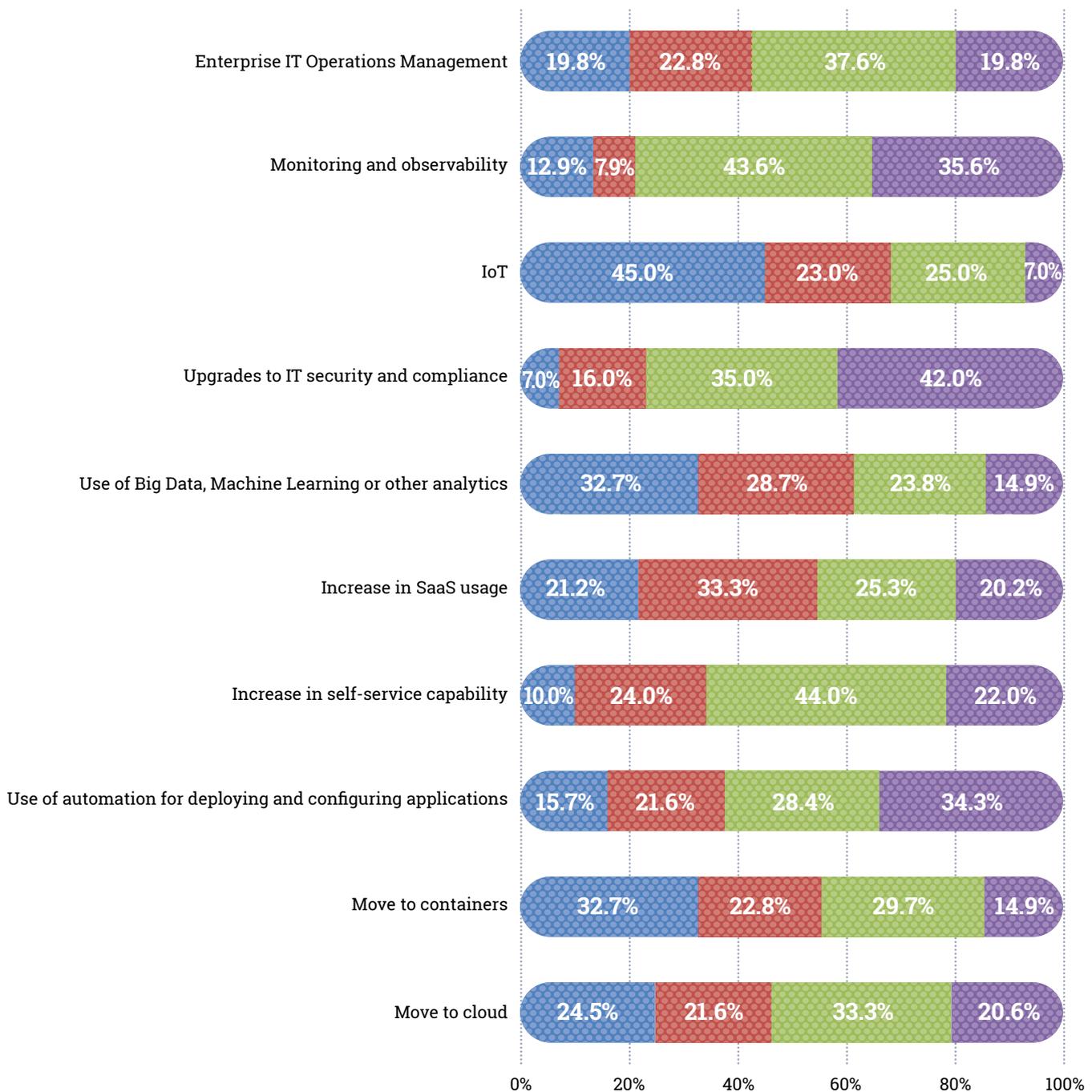
However, when we look at organizations' 2019/2020 roadmaps, the innovative culture portrayed above does not match up. Arguably, the most innovative and technically driven strategies (Internet of Things integration, use of big data/machine learning and move to containers) is not even on a huge proportion of business plans. Instead, priorities include upgrades to IT security and compliance, monitoring and observability, and use of automation – activities which should already be a baseline competence. This yet again brings to the forefront that firms are lacking the necessary IT infrastructure to implement more strategic projects, which is setting them back on their transformation journey.

A step-change is required. While it's good news that firms are finally getting their digital houses in order, it's alarming that it's taken them so long, which baseline, necessary operations such as monitoring and observability should encompass. For organizations to successfully become connected enterprises, they need to live and breathe digital – yet without the right infrastructure – many of which still lack – this will never be possible.



How do you rank the importance of each topic to your organization's IT strategy in 2019/2020?

- 1** = not on our roadmap
- 2** = evaluating
- 3** = proofs-of-concept or small deployments in progress
- 4** = significant money and time will be devoted to this in 2019/2020



Conclusion: Laying the groundwork for future success

As seen by this report, while digitally-driven operations and the connected enterprise is no doubt an aspiration for many businesses, for the time being, that's all it is. Organizations are woefully underprepared for implementing strategic, technical projects as they simply don't have the IT foundations on which to build upon. While organizations are no doubt dealing with a multitude of issues on a daily, if not hourly basis, unless they go back to basics in terms of IT monitoring and operations, they will be one of the 70% of failures that McKinsey cites.

To adequately deal with issues such as legacy IT, system health and downtime, corporations need to prioritize visibility – which means comprehensive IT monitoring. This should be conducted via a single pane of glass, displaying how every node and part of the estate is performing – whether it's on-premises or in the cloud. This will identify any potential issues and can also be used to demonstrate IT's value by providing shareable data for the business (especially when integrated with programs such as Splunk) – helping to dispel the myth that IT is merely a cost center. To achieve this, it's worth paying for solutions which not only integrate with IT estates, but also provide the usability and customer service which businesses are calling for. Whether it's comprehensive reporting, custom views and trend analysis or automation and integration – organizations need to be prioritizing services such as Opsview Cloud to help them demonstrate IT's value and save valuable time.

IT monitoring can also be the bedrock from which manual labor is reduced. When combined with automation, issues can be fixed before they cascade, finally freeing up the workforce to get involved in more strategic or innovative work. This will upskill them more quickly, engage them, and deliver the culture of learning and innovation which many firms so desperately crave, as ultimately this will benefit them in the long run – both in terms of product development and talent acquisition and retention.

We are well and truly in the digital age, and it is true that firms that fail to innovate will most likely cease to exist. Customers are more fickle than ever before, so IT operations must be consistently operating to exceptional standards to help support business strategy. As we've seen from this report, firms are starting to correct the mistakes made in the past, but until these errors are rectified, few will go on to become digital powerhouses or successful connected enterprises. The message is clear – get the foundations right, as they will be the tools which drive your business towards future success.

If you want to explore how modern IT monitoring can help in your digital transformation, call us on



www.opsview.com



EMEA: +44 1183 242 100



sales@opsview.com