THE 2019 KASEYA STATE OF IT OPERATIONS REPORT FOR SMALL AND MIDSIZE BUSINESSES

Kaseya®

Introduction

Five years ago, Kaseya surveyed IT professionals from midsize companies to gain a better understanding of the state of IT operations in this market segment, which we define as businesses with up to 5,000 employees. Since then, the Kaseya IT Operations Survey has been conducted annually to gauge IT trends and capabilities among IT professionals in midsize organizations.

The resulting report aims to provide insight into current trends and allow IT teams to see how they compare to their peers.

Like reports in years past, the Kaseya 2019 State of IT Operations Report provides an in-depth view and analysis of the key challenges and priorities those in IT operations management face. The report examines security concerns, compliance challenges, and backup strategies of IT professionals globally.

As you will see, some aspects of IT operations have undergone a seismic shift in recent years, while others have remained static.

Key Findings

1. Improving Security and Service Levels are Paramount Priorities

- As in the previous years, improving security is the topmost priority of most midsize businesses, selected by 57 percent of survey participants. However, cybersecurity and data protection are also major challenges (cited by 62 percent), which we attribute to increasingly sophisticated cyberattacks.
- Delivering higher service levels is among the top priorities in 2019 (stated by 24 percent of respondents) — this is at odds with the decline in percentage of companies that have formal service-level agreements (SLAs) in place.
- Controlling IT costs also holds as a top priority for more than one-third of respondents. This is closely linked to the challenge 35 percent of companies face with budget constraints.

2. Data Breaches and Outages are Strongly Correlated

- 32 percent of respondents experienced a security breach in the past 5 years, down slightly from 35 percent citing a breach in the past 5 years in 2018.
- 10 percent of respondents had at least one breach in the past year.
- 12 percent of respondents had a ransomware attack in the past year, a 10 percent drop from 2018. However, ransomware attacks are increasingly targeting enterprises rather than consumers. Consequently, ransomware is still a considerable threat to midsize businesses.
- The relationship between outages and data breaches is significant. Nearly 61 percent of respondents who had a security breach in the past year had two to four outages. This is an increase of 15 percent compared to 2018, when 45 percent of participants who had a security breach had 2 to 4 outages. This correlation is likely attributable to the IT Operational Maturity Level of the organization. Lower maturity equates to more data breaches and outages.

3. Automated Patch Management yet to be Widely Adopted

- Automated patch management isn't yet standard operating procedure for the majority of small and midsize companies. Only 42 percent of respondents automate or plan to automate patch management. An automated patching process is critical to enabling businesses to keep their systems up to date, as it ensures critical software vulnerabilities are addressed quickly, before an exploit occurs.
- Similarly, only 42 percent monitor third-party software and apply critical patches for these within 30 days, whereas 43 percent said they did so in 2018.
- 65 percent of participants apply critical OS patches within 30 days of release, whereas about 68 percent said they did so in 2018.

4. Backup and Disaster Recovery Strategies Widely Adopted for Servers — but Not SaaS

- 9 out of 10 respondents said they back up their servers.
- Companies seem to have opened the door to cloud data backup. Backup to the cloud in combination with other media is among the top five backup and disaster recovery strategies, adopted by 33 percent of respondents.
- 31 percent of participants have a formal business continuity disaster recovery (BCDR) plan approved by management in place, and 34 percent have the ability to automatically recover to a separate site.
- About one-third of respondents test their disaster recovery plan regularly.
- Only about 29 percent of respondents back up their SaaS application data, the same as in 2018. There continues to be a lack of understanding that SaaS data backup is typically the customer's responsibility for anything longer than 30 days.

Key Findings

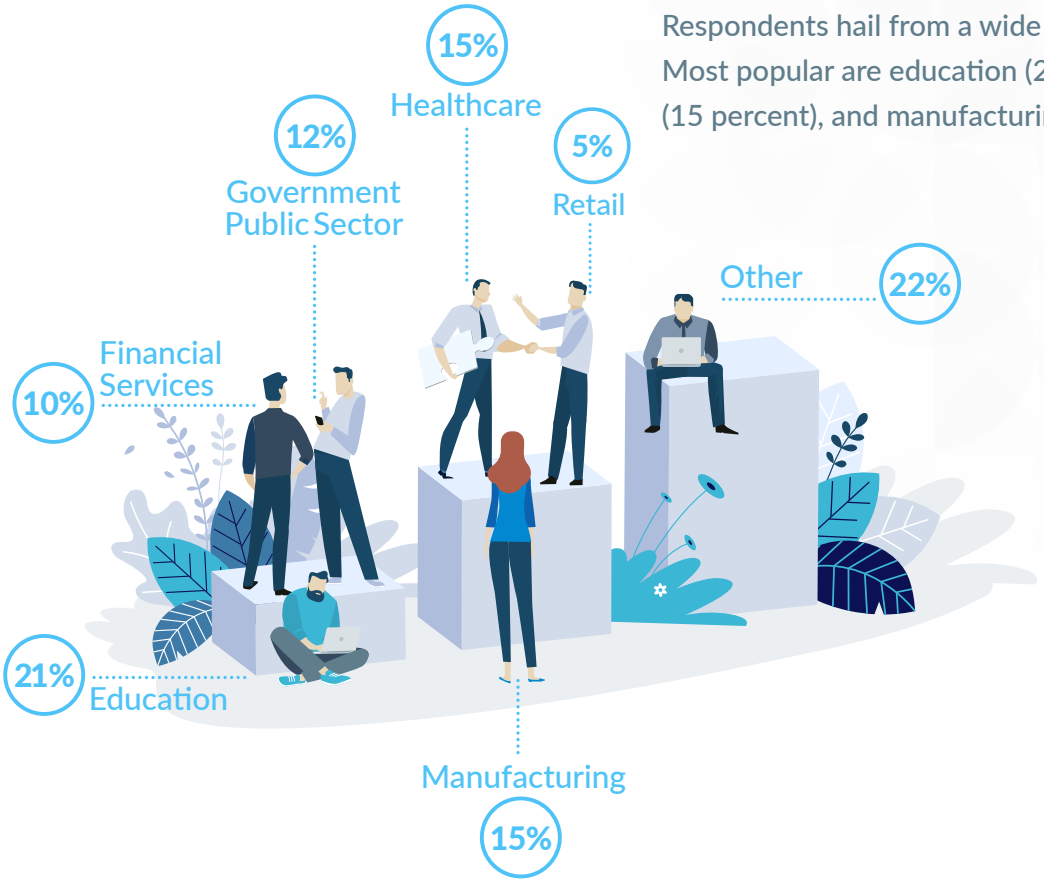
5. HIPAA Rules Regulatory Compliance Requirements, GDPR is Gaining

HIPAA, PCI, and GDPR top the list of compliance regulations impacting respondents in 2019. 31 percent of participants have taken steps to ensure HIPAA compliance, whereas 26 percent adhere to PCI and about 16 percent to GDPR. GDPR moved from No. 6 in 2018 to No. 3 in 2019, not surprising given the regulation took effect in May 2018.

Our Respondents

Although the bulk of respondents come from the United States (83 percent), 17 countries are represented among respondents.

Respondents hail from a wide swath of industries. Most popular are education (21 percent), healthcare (15 percent), and manufacturing (15 percent).

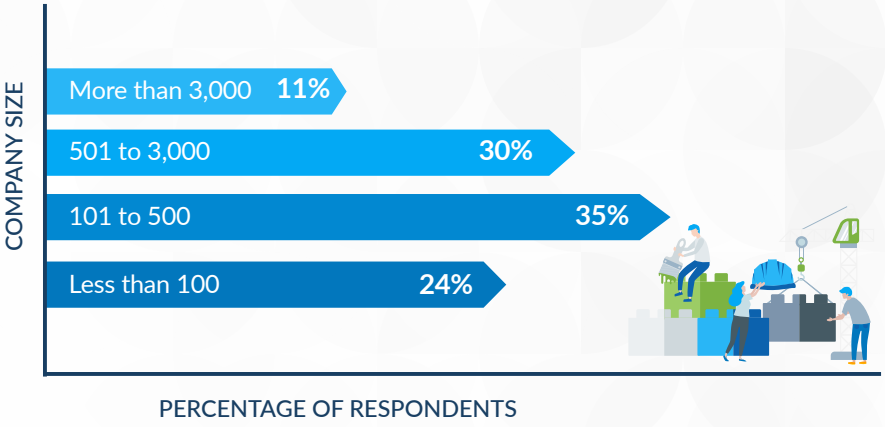


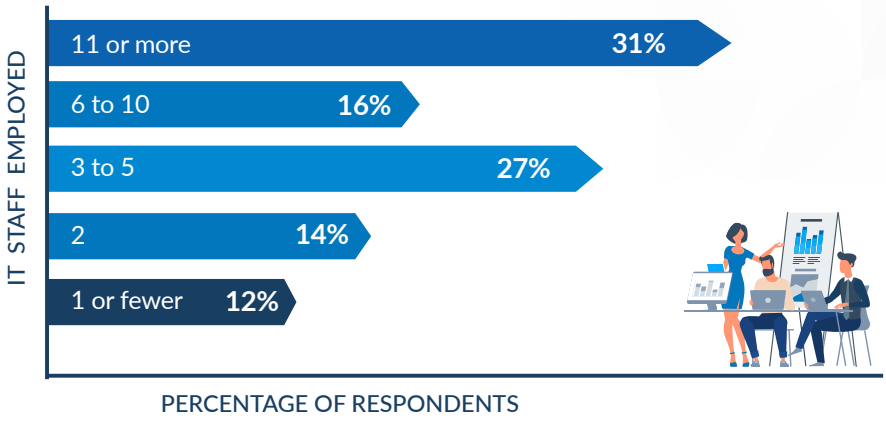
Our respondents are truly in the IT trenches, grappling with day-to-day issues. More than half are IT managers or system administrators.

Director of IT	22%
Head/VP/Chief	9%
IT Manager/Supervisor	30%
Network Engineering /NOC Manager	6%
Project Manager	5%
System Administrator	21%
Other	7%

Over half of our respondents come from companies with fewer than 500 employees.

Not surprisingly, multifunctional IT professionals are prevalent among respondents, as indicated by the size of IT departments. More than half come from organizations with five or fewer IT professionals.



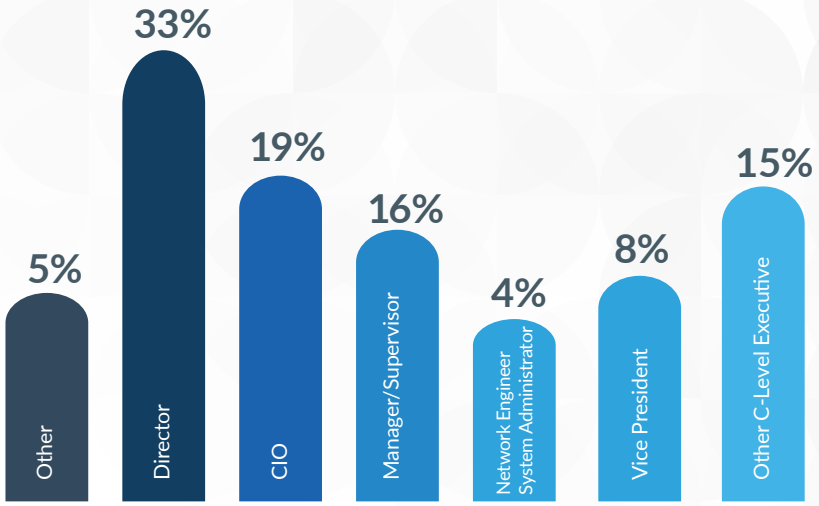


Who are the decision makers?

It's been said that nearly every business decision is also a technology decision. With this in mind, it is important to understand who the decision makers and influencers are.

For IT Decisions

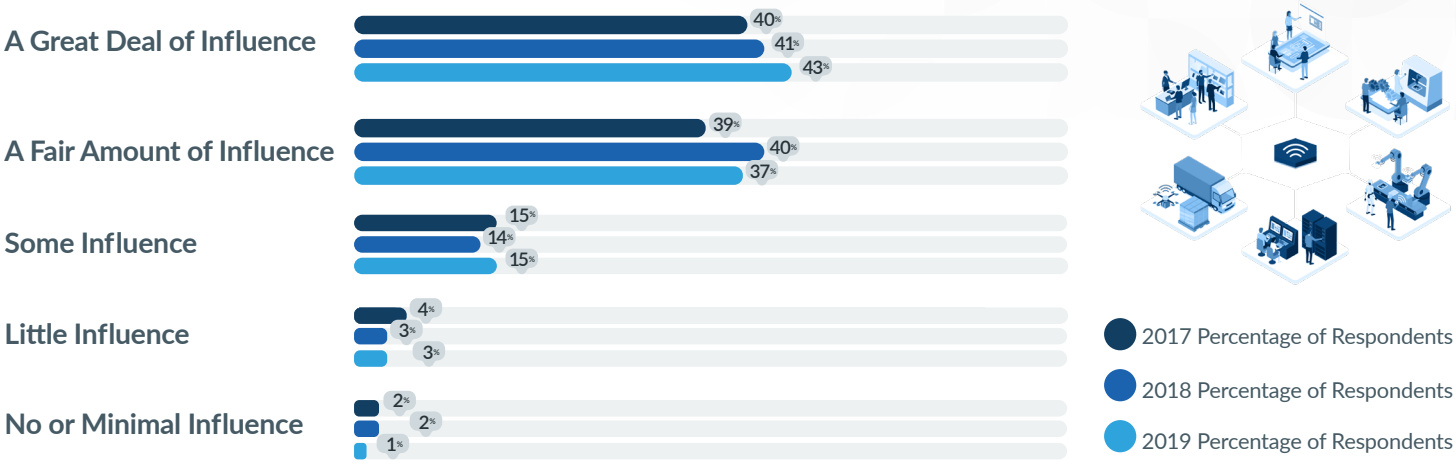
One-third of respondents said the Director of IT is the primary decision maker when it comes to major IT decisions in their company, and for about one-fifth of survey participants, the CIO is the chief IT decision maker.



On C-level Decision Making

Our 2019 results continue to support the idea that IT leadership deserves a "seat at the table" for business decision making. Among survey respondents, the head of the IT department has a significant degree of influence on C-level decision making within the company. This is consistent with the recognition that in today's business environment business decisions are often also technology decisions. IT departments are experiencing tremendous changes as their roles expand to impact customer service, sales, and business strategies of the companies they support. This applies to our respondents as well.

The degree of influence of the head of IT department on company-wide decision making has risen considerably in the past three years. Nearly half (43 percent) of respondents state that the head of the IT department has a great deal of influence on C-level decision making in their company.



The State of IT Operations in Small and Midsize Businesses

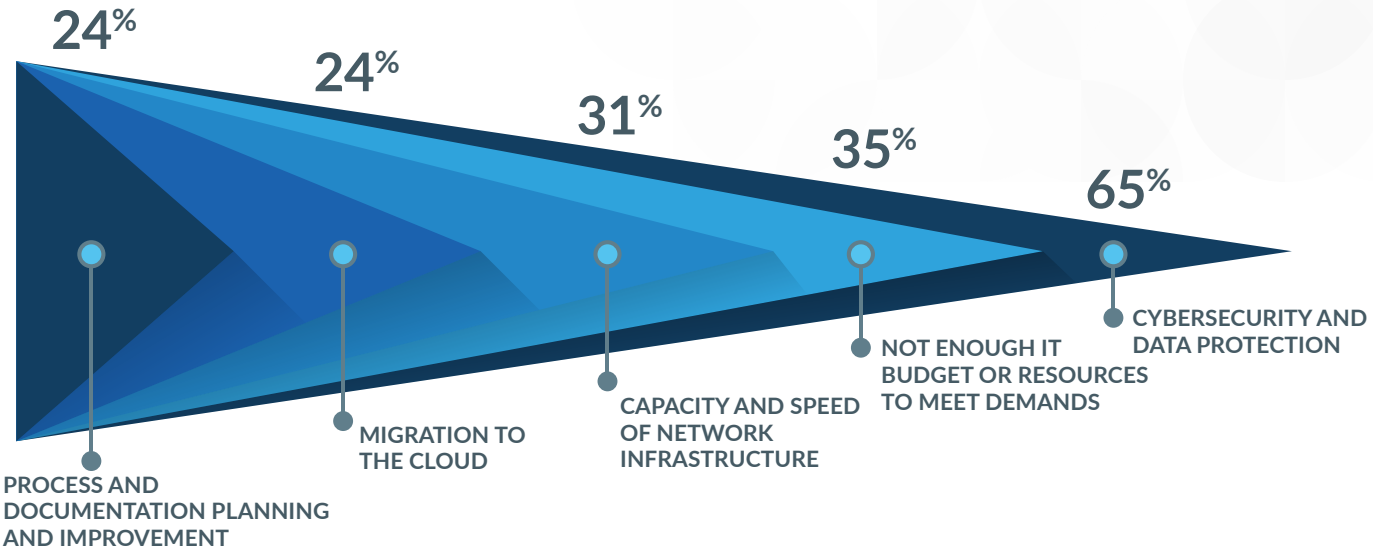
The Present: Top Priorities for 2019

Improving security is once again the top priority for survey respondents on 2019. Owing to limited budgets, reducing IT costs comes in second, and delivering higher service levels takes the third position among top priorities for the year.

The Future: Challenges Companies Anticipate Facing in 2020

Cyberattacks are extremely expensive for midsize business to endure. Measured by cost per employee, organizations with 500 to 10,00 employees had an average security breach cost of $3,533, compared to $204 per employee in larger enterprises, according to the 2019 Ponemon Cost of Data Breach report.[1] Further, according to a joint report by Cisco and the National Center for the Middle Market, about 60 percent of SMBs fold within six months of a cyberattack.[2]

With SMBs increasingly in the cross-hairs, the importance of security will continue to grow. However, a combination of factors that include zero or insufficient increases in IT budget, a growing skill gap in cybersecurity among IT personnel, and increased sophistication of cyberattacks add up to the challenges SMBs face in maintaining their IT infrastructure and data security year after year.



Higher IT Operational Maturity is Aspirational for Many

IT Operational Maturity is defined by a collective set of IT management capabilities and is indicative of what an IT department can do for the growth of a business. Our IT Operations Survey results found more than one-third of IT teams to be consistently at the lowest level of maturity (Reactive), and more than half to be at the two lowest levels (Reactive and Efficient).

In the past several years, small and midsize businesses have not made much progress toward achieving higher levels of Operational Maturity.

At the other end of the spectrum, only 4 percent of respondents indicated they are at the second highest level of Operational Maturity (Aligned), where they are tracking and managing against service-level agreements (SLAs). Further, 11 percent of respondents said they have a strategy in place to add value to their business, thus pinning them at Strategic, the highest level of IT Operational Maturity.

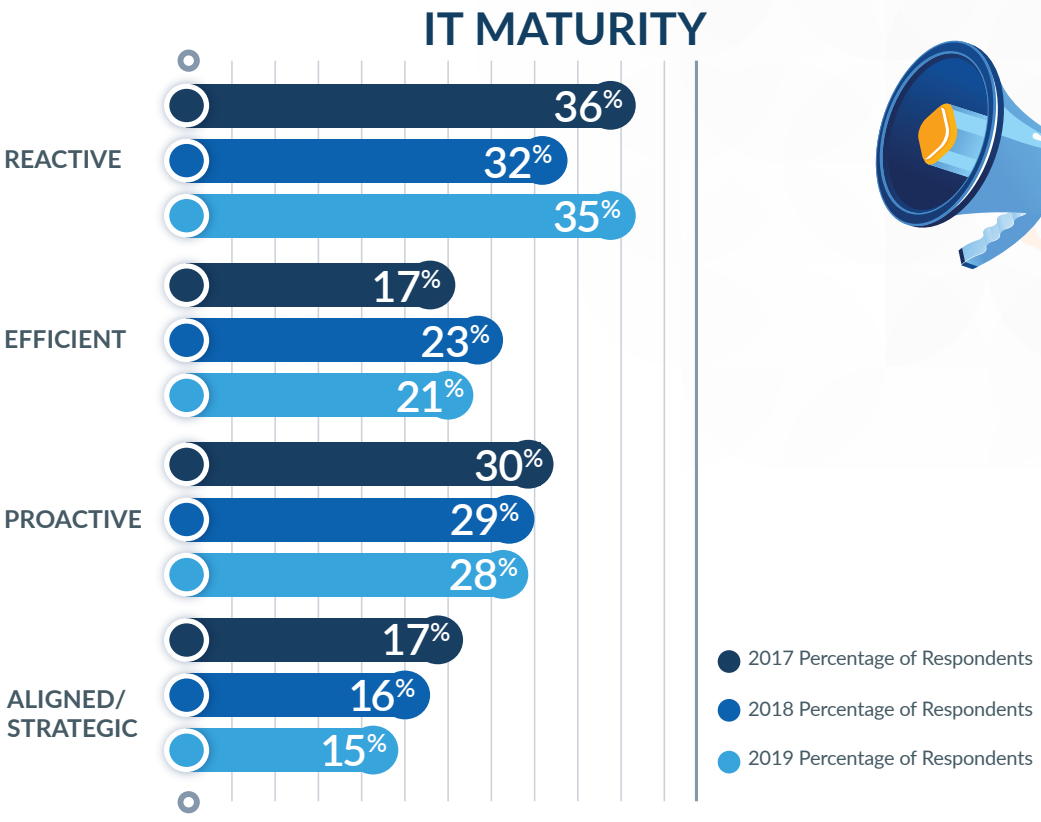
35%
Responsive to individual challenges and requests (Reactive)

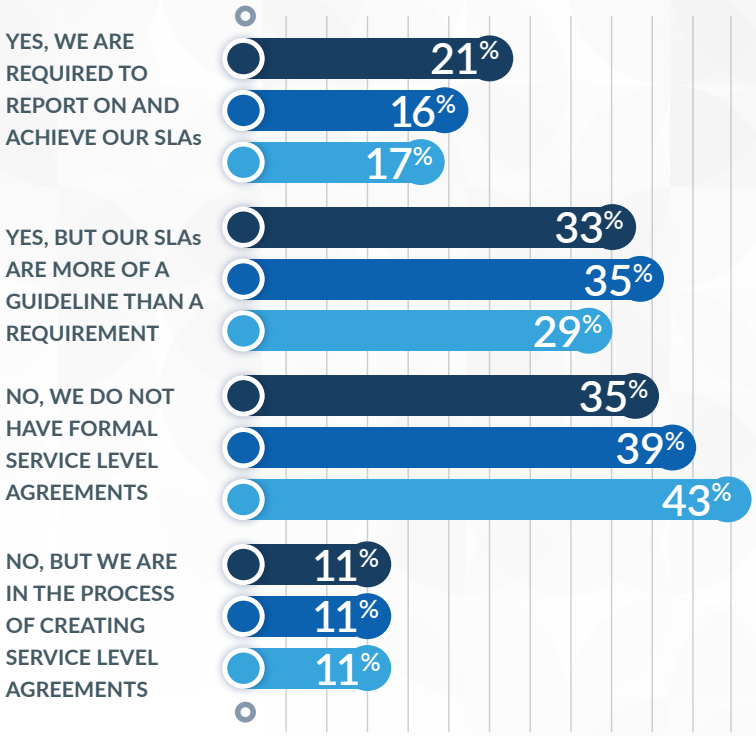
21%
Systematic in our approach to solving known issues and dealing with daily tasks (Efficient)

28%
Proactive in our approach to IT management, automating repetitive tasks and many remedial actions (Proactive)

4%
Tracking and managing against service level agreements (SLAs) or availability/performance expectations (Aligned)

11%
Achieving IT operational excellence and taking a strategic role in driving business innovation (Strategic)

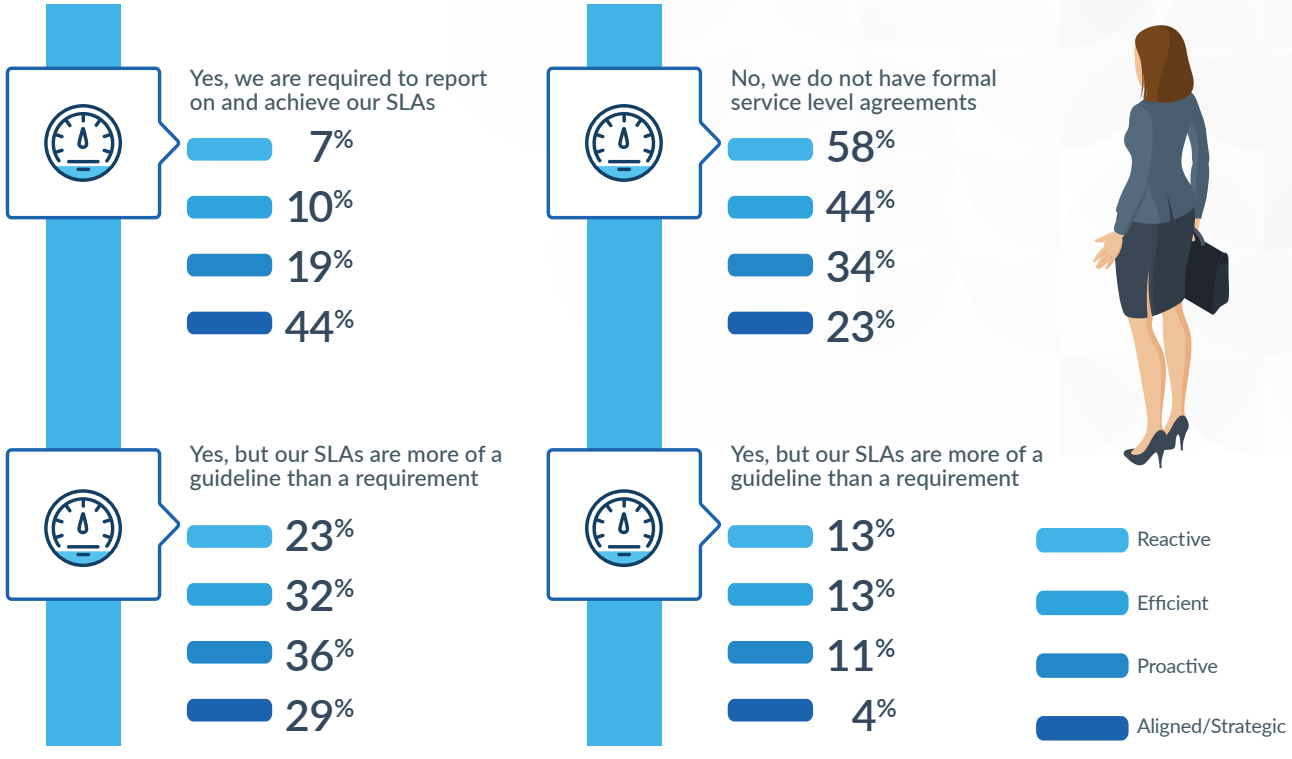




Lack of Formal Processes Goes Hand-in-hand with Lower Maturity

Despite "improving service levels" being a top priority for 2019, the percentage of respondents whose companies do not have formal SLAs in place has risen since 2017. More than 40 percent of respondents to this year's survey lack formal SLAs. This is consistent with being at a lower level of IT Operational Maturity.

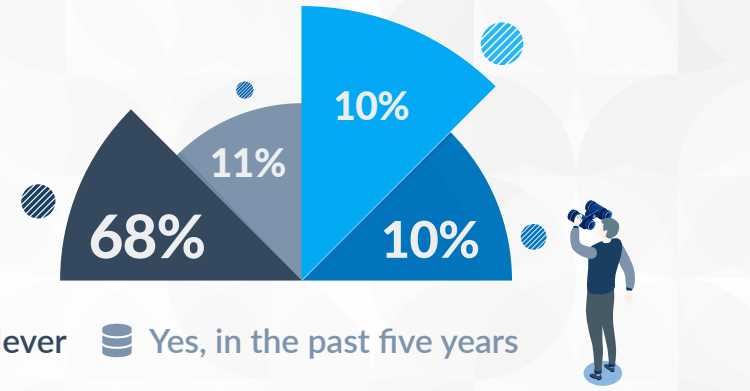
In the survey, **about 58 percent of respondents** whose companies do not have formal SLAs are at the bottom of the IT Operational Maturity ladder (Reactive).



The State of IT Security

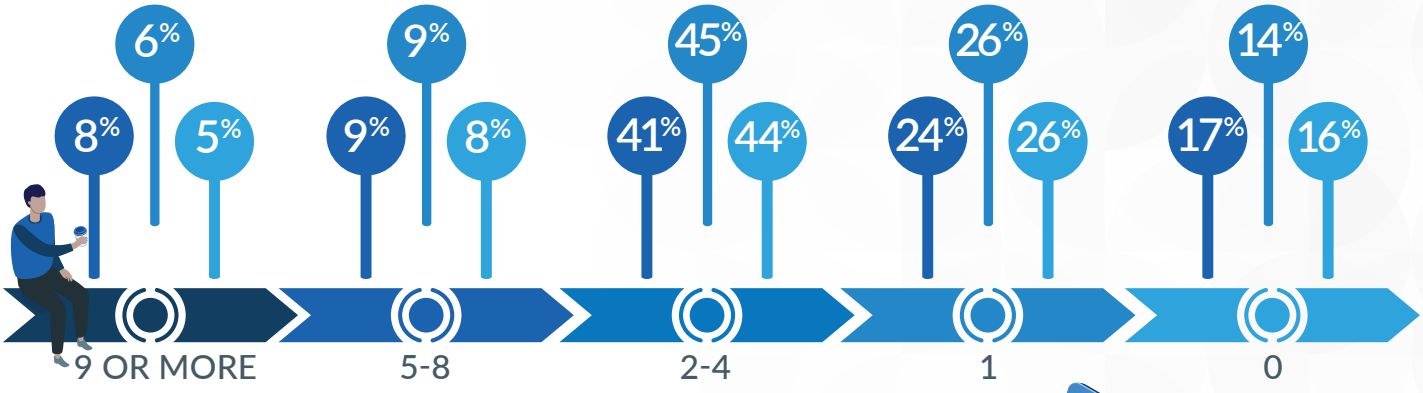
Ransomware attacks and data breaches were constantly in the news over the past year. Cyberattacks are often targeted at large organizations. However, in recent years, cyber-criminals have been increasingly targeting small and midsize businesses. According to the Verizon Data Breach Investigations Report for 2019, 43 percent of breaches affected small and midsize businesses.[3] State and local governments are particularly at risk, with two cities in Florida paying $600,000 and $460,000 in ransom in 2019, for example.

Over 30 percent of respondents experienced a security breach in the past five years, down slightly from 35 percent in 2018. At least 10 percent of our respondents were hit by a breach in the past year.



Outages and Security Breaches are Highly Correlated

About 84 percent of our respondents had at least one network outage lasting longer than five minutes in the past 12 months, and 57 percent of respondents had more than one outage in the past year.

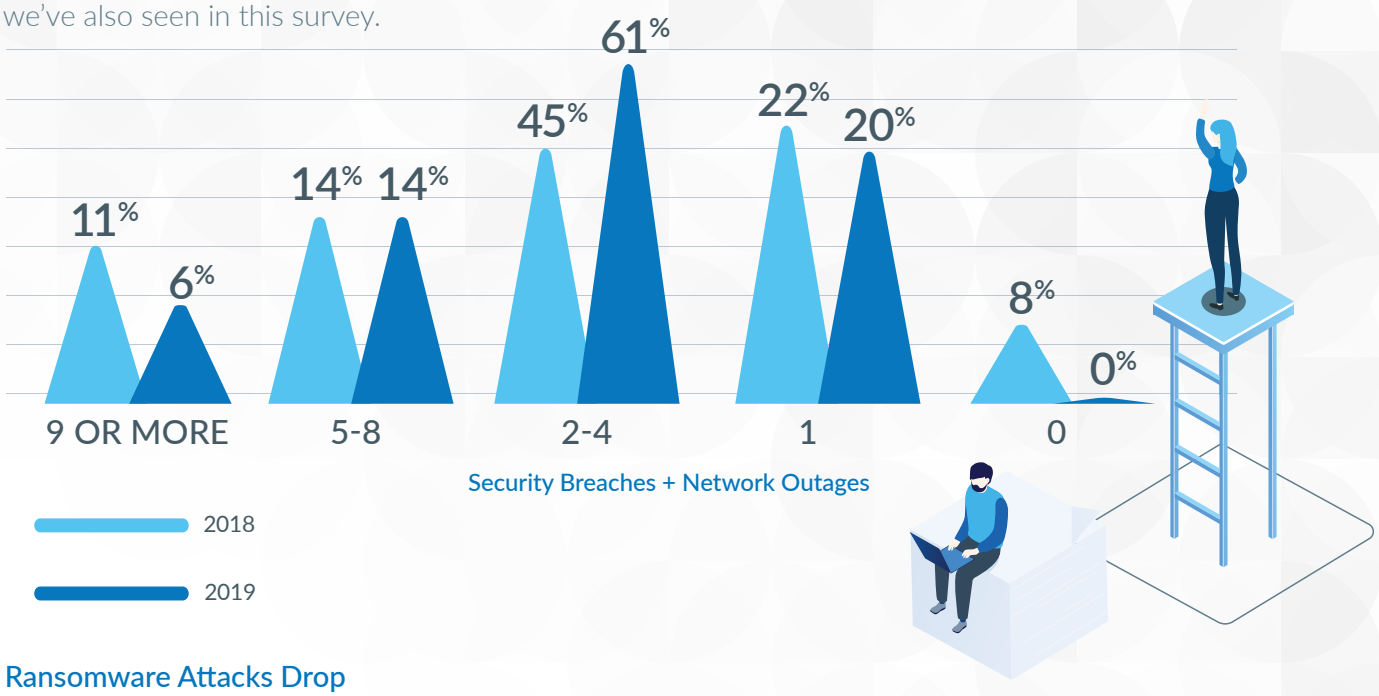


Percentage of Respondents 2017

Percentage of Respondents 2018

Percentage of respondents 2019

Nearly 61 percent of respondents who had a security breach in the past year experienced two to four network outages. This is 15 percent more than in our 2018 survey. The strong correlation between network outages and security breaches is most likely related to the low level of IT Operational Maturity we've also seen in this survey.



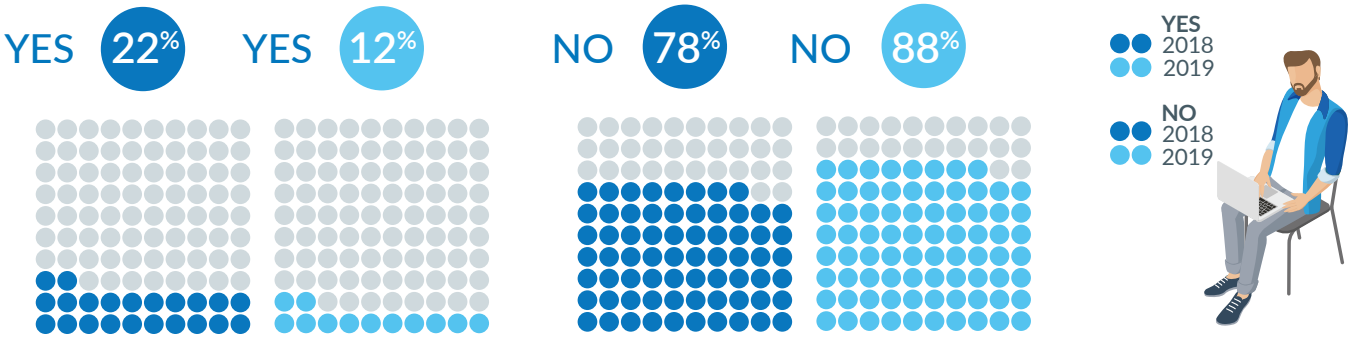
Ransomware Attacks Drop

About 12 percent of respondents experienced a ransomware attack in the past year, a drop of 10 percent from 2018. This is surprising given the increase in number and sophistication of ransomware attacks. According to a report by Cisco, ransomware attacks are growing more than 350 percent annually.[4] The drop in reported ransomware attacks in the Kaseya survey speaks to fact that companies are listening and getting smarter about how they defend against and respond to attacks. The importance of security is an ongoing theme among respondents. A big factor in defending against ransomware is employee education on email phishing scams that lead to ransomware attacks in many cases.

While companies are gearing up to protect themselves from ransomware attacks, a new kind of attack called cryptojacking has entered the domain. Cryptojacking is the unauthorized use of someone's computer to mine cryptocurrency.

Although some data shows that ransomware attacks are on the decline, companies should remain vigilant against these and other types of attacks and arm themselves accordingly.

Have you experienced a ransomeware attack?



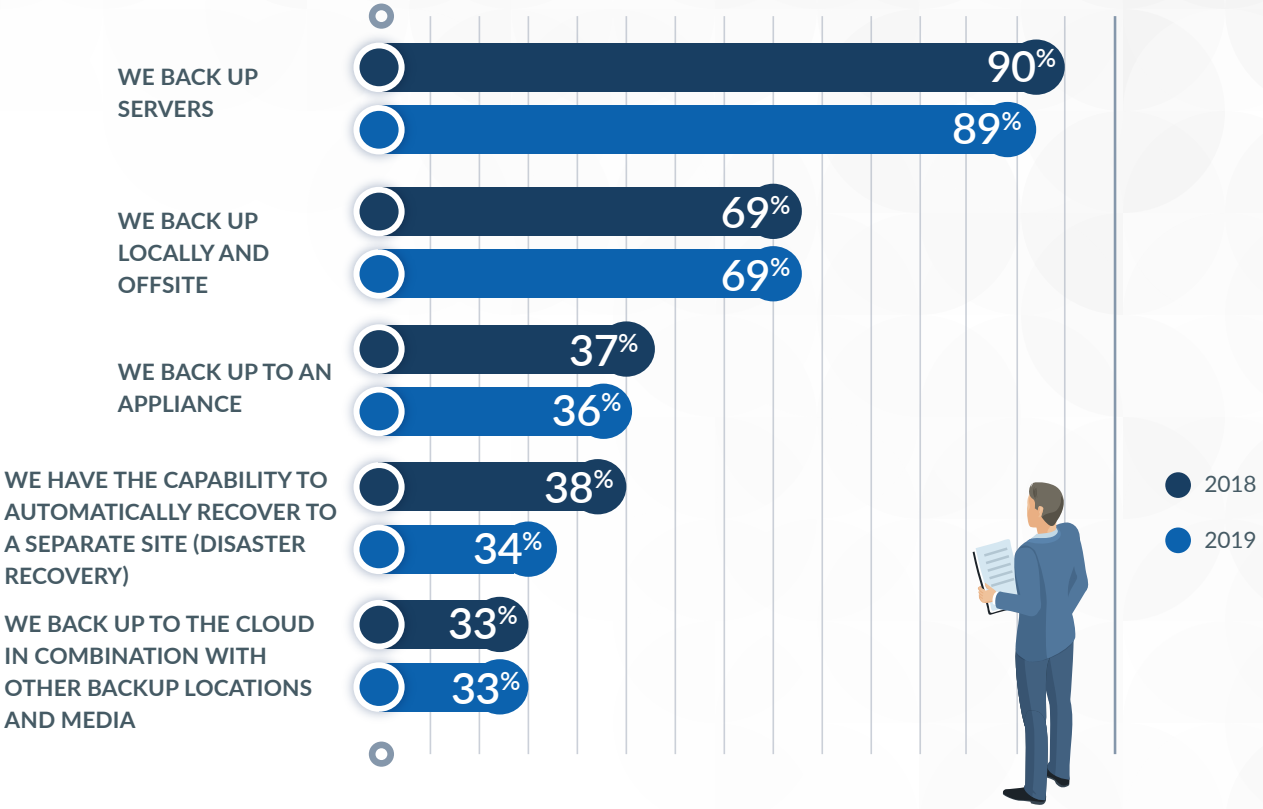
The Cloud is Gaining in Importance for Disaster Recovery

Almost all of our respondents have adopted some type of backup strategy. Backing up servers, backing up locally and offsite, and using an onsite appliance are the three most popular backup strategies.

Backup to cloud in combination with the other media is among the top five business continuity and disaster recovery (BCDR) strategies, adopted by 33 percent of respondents. This result is in line with the information gathered from the most recent Unitrends Cloud and Disaster Recovery Survey, which found that cloud-based data protection is increasing in its importance to reducing data loss. About 60 percent of their responding organizations report using the cloud for backup and disaster recovery.[5]

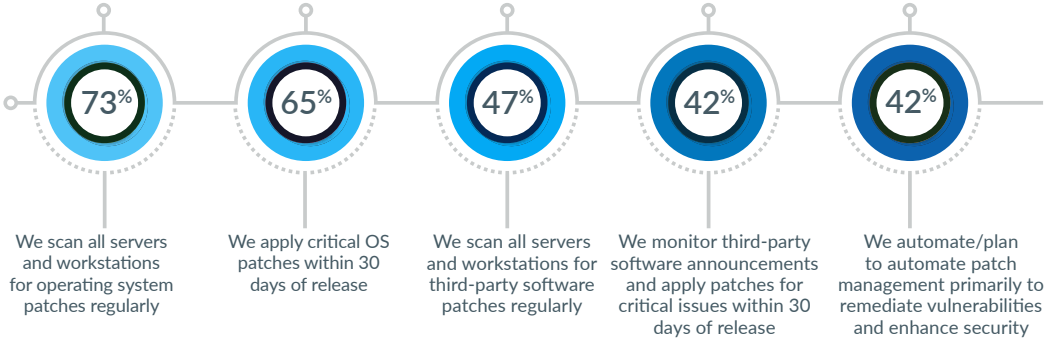
Disaster recovery testing is a vital part of a backup and recovery plan. Without proper testing, you will never know if your backup can be recovered. Among our respondents, only 31 percent test their disaster recovery plan regularly. This shows that businesses are underestimating the importance of recovery testing.

Backup and Recovery Action Plan



Vulnerability Management Policies Selectively Adopted

Nearly three-quarters of respondents scan all servers and workstations for operating system (OS) patches regularly, and 65 percent of respondents apply critical OS patches within 30 days of release.



While automated software patching is a highly cost-effective alternative to the drain of manual patching, it is not widely adopted. Only 42 percent of respondents automate or plan to automate patch management to enhance security. Further, only 42 percent apply critical third-party application patches within 30 days.

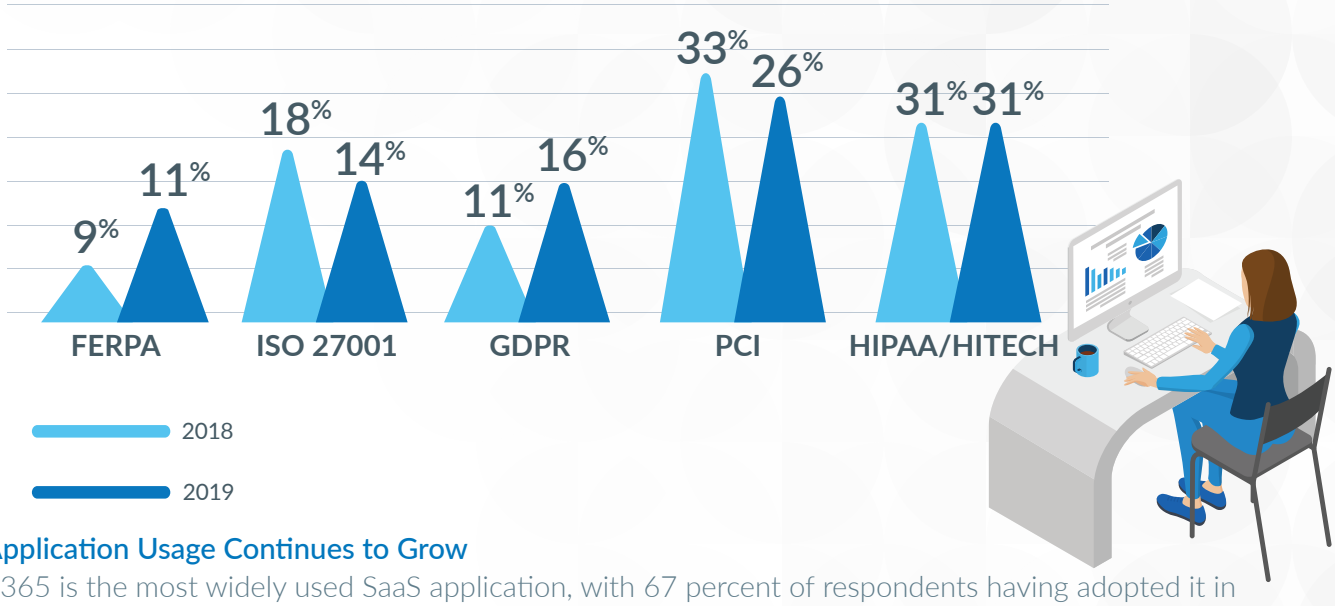
Significant improvements must be made in both of these areas. The vast majority of security breaches are preventable by applying patches in a timely manner. Automation can make this happen.

Compliance Requirements Implemented

As data privacy regulations become increasingly prevalent, complying with industry regulations is a must for every company – regardless of its scale of operations. Fines for non-compliance can be quite costly. HIPAA compliance is a top priority for 31 percent of our respondents. This is followed by 26 percent of respondents complying with PCI.

The percentage of respondents complying with GDPR rose to 16 percent in 2019, compared to 11 percent in 2018. GDPR took effect in May 2018 and affects any organization doing business with customers in the European Union (EU).

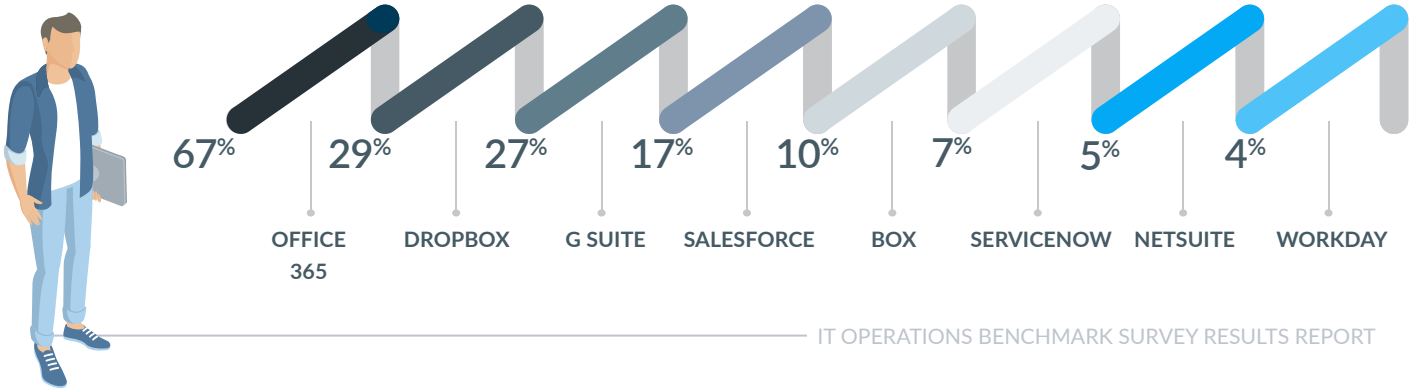
Given the geographic breakdown of respondents, these results are not surprising.



SaaS Application Usage Continues to Grow

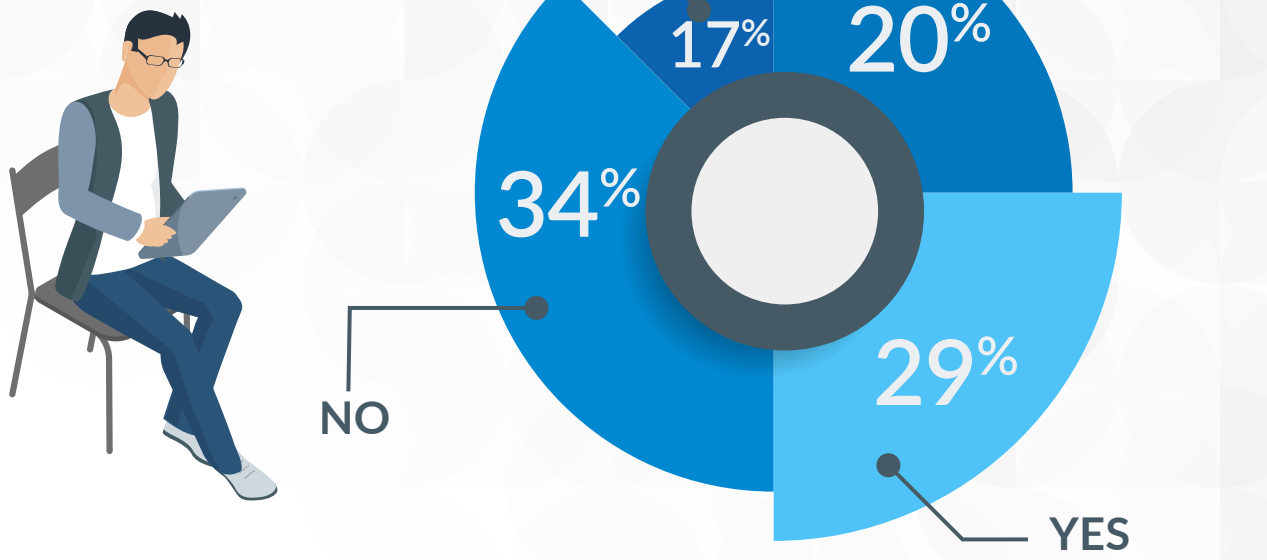
Office 365 is the most widely used SaaS application, with 67 percent of respondents having adopted it in their organizations. Google G Suite moved past Salesforce in the past year to come in third on the list in 2019.

This aligns with general trends. According to Forbes, 30 percent of all IT budgets were allocated to cloud services in 2018. 48 percent of that spend was for SaaS.[6]



Protection for SaaS data is lagging, however. In contrast to backup for server-based applications — for which 90 percent of respondents said they are backing up data — only 29 percent of respondents are using a third-party backup and recovery solution to protect SaaS data. Another 20 percent said they are partially backing up this data.

Are you protecting your SaaS data with a third-party backup and recovery solution?



Inventory Process for Asset Management

When asked about their inventory process, 71 percent of respondents said they inventory endpoints for OS information, while 70 percent of respondents said they inventory endpoints for vendor and serial number or warranty information.

In addition, 60 percent of survey participants collect inventory data on hardware resources, including CPU, RAM, and disk size. This type of data is especially critical when you are planning an OS migration, such as from Windows 7 to Windows 10.

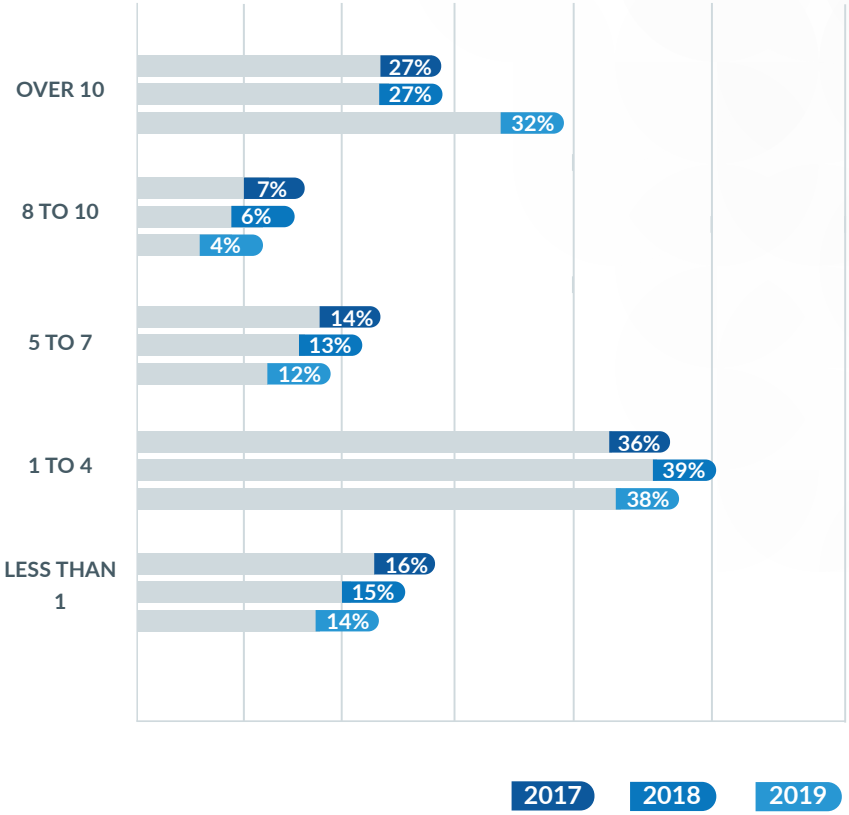
We inventory endpoints for OS information	71%
We inventory endpoints for vendor and serial number/warranty information	70%
We inventory endpoints for installed software	64%
We inventory endpoints for computing information (e.g., CPU, RAM, or disk)	60%
We inventory endpoints for software licensing data	53%
We inventory endpoints for user account information	45%
We do not inventory endpoints	8%

Peer-to-Peer Comparisons

Knowing where you stand in comparison to similar organizations is helpful in setting benchmarks and goes a long way toward more effective decision making. Here's what our respondents reported.

Average Number of Devices per Technician

Nearly half of our respondents stated that one technician supports an average of 100 to 500 endpoint devices.



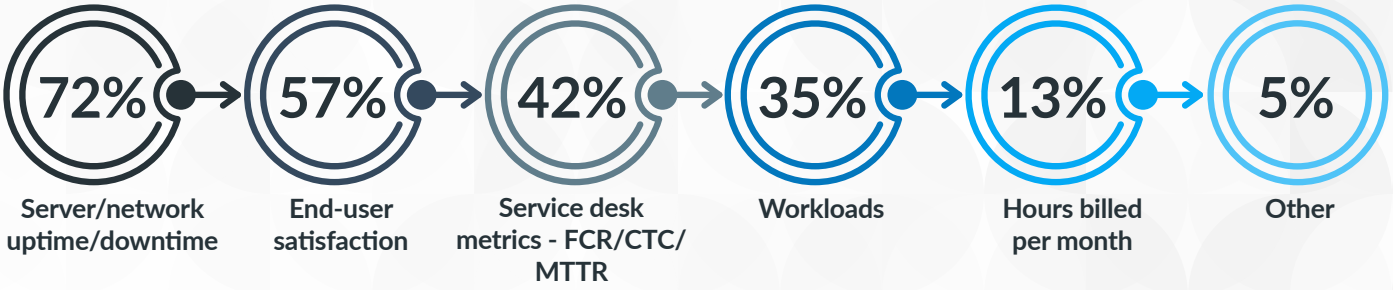
Average Number of Support Tickets per End User

For 38 percent of respondents, the average number of support tickets generated per end user each month in their company ranges from 1 to 4. For 32 percent of respondents, it is over 10.

IT Operations Performance Metrics Used

Server and network uptime/downtime is the performance metric measured the most – by nearly three out of four respondents. This is followed by end-user satisfaction – by 57 percent of respondents.

This indicates that companies aren't underestimating the importance of maintaining high user satisfaction rates.



Top Areas of IT Efficiency

When asked about their effectiveness in optimizing IT efficiency across various technologies and functions, centralized antivirus/antimalware scanning and data storage backup were cited as the top two areas, followed by server monitoring. Remote management came in fourth, tied with help desk and service management.

- Centralized Antivirus/Anti-Malware Scanning 78%
- Data Storage Backup (Daily, Weekly, Monthly) 76%
- Server Monitoring 67%
- Remote Device Access/Control 64%
- Helpdesk and Service Management 64%

IT DEPARTMENTS IN THE FUTURE – A PEAK INSIDE 2020

IT plays an important role in the growth of a business and its path to digital transformation. IT professionals are not only expected to keep the systems running but must also help transform the business. CIOs are constantly working to control costs, increase competitiveness, and, as more companies become heavily regulated, improve compliance.

When asked about how they expect the role of the IT department and the CIO to evolve in 2020, survey participants responded as follows.

65% The primary decision maker and resources for all information technology decisions and support whether internally developed or externally sourced

18% Responsible for maintaining legacy infrastructure and endpoint devices, information management and security – other departments will make their own application and services purchase decisions

15% An information technology broker for the company's business units and functions with responsibility for services procurement and technology standards for information management and security – third party service providers will maintain the infrastructure and deliver applications as (cloud) services

CONCLUSION

Security is understandably the top priority of most small and midsize businesses. The frequency and sophistication of cyberattacks continue to grow at a rapid pace. IT teams need a comprehensive set of IT security management tools to continually improve their security posture. These include antivirus and antimalware, identity and access management, insider threat detection, patch and vulnerability management, and backup and disaster recovery tools.

Another top priority is improving service levels. This requires having more formal processes in place, including formal SLAs. These guide the IT team to deliver higher quality services to the business by meeting specific key performance indicators (KPIs).

IT automation is another key requirement for improved IT service delivery. Automation drives higher IT operational efficiency and can dramatically improve key metrics such as mean time to resolution (MTTR).

Your IT management solution should make it easy to automate common IT processes and remediate incidents without technician involvement.

In some cases, it makes sense to work with an IT service provider to enhance service delivery. Network operations center (NOC) services are one example. The service provider may be able to provide these services at a lower cost than you can achieve on your own.

Kaseya's IT Complete solution for IT management is a comprehensive suite of products that work seamlessly to meet all of your IT needs. **Visit our website to learn more.**

REQUEST A DEMO

OR START A FREE 14-DAY TRIAL TODAY!

Sources

1. 2019 Ponemon Cost of Data Breach Report
2. Cyberthreats and Solutions for Small and Midsize Businesses, Vistage
3. 2019 Verizon Data Breach Investigations Report
4. Cisco Cybersecurity Report: 2019 Threat Report
5. The Disappointing State of Backup and Recovery in 2019, Unitrends
6. State of Enterprise Cloud Computing, 2018, Forbes

OUR METHODOLOGY AT A GLANCE

Kaseya conducted its 2019 IT Operations Benchmark Survey using a structured questionnaire in June 2019. All participants were asked if they were primarily employed in an IT operational role with some responsibility for IT infrastructure or IT services deployment, operation, management, or support. Only responses from those who answered in the affirmative were included in the survey results. Among those, 66 percent of the final respondents identified their primary responsibility as "all of IT." In total, valid responses were received from 496 IT professionals. The focus of the survey was IT operations (individuals and groups) at midsize organizations, which we define as organizations with up to 5,000 employees. Only companies in this range are included in the survey results.

04302020