computing research

RESEARCH PAPER

Getting to the top of your game: how does the modern IT service organisation best serve the enterprise?

June 2020

Sponsored by

ivanti

CONTENTS

Introduction

From security and patch management to asset management to security response management, to application modernisation, IT teams are typically divided into a series of different specialisms, AKA 'silos'. This separation can be viewed positively, as enabling different individuals to play to their strengths and deliver the best service. It could also be viewed through a less positive prism as a barrier to the flexibility needed by a dynamic enterprise.

Computing surveyed 150 technical and business decision makers representing organisations from a wide variety of industries including banking and finance, logistics, manufacturing, retail and the government. The size of organisations varied from those employing 100 people to those employing more than 5000.

This objective of the research was to uncover the challenges facing enterprise IT in the key operational areas of asset, service, endpoint and security management and to discuss the impact these challenges are likely to be having on the agility of the organisation as a whole and the perceptions of IT by the wider enterprise.

The research concludes with a discussion of how Unified IT, comprising integration and automation of these often separated functions, can help modern IT management get to and stay on top of their game with the fastest possible response times to security incidents and the most effective organisation of different teams and resources and budgets.

Key Findings Include:

- 85 per cent of those participating in our survey were at least reasonably confident that their ITSM was serving the business well.
- 82 per cent also reported at least reasonable levels of confidence that their organisations were not under licenced or overspending on licensing.
- There was almost no difference in confidence levels relating to the visibility of tangible physical IT assets as opposed to cloud assets. This is an outlier in terms of usual *Computing* research in this area.
- The most widely cited challenges facing IT services organisations supporting the newly increased levels of remote workers were security, a lack of self-service functionality and compliance concerns.
- 41 per cent of respondents has experienced an increase between 20 and 40 per cent in endpoints in the last year alone. 28 per cent had seen an increase in excess of that.
- 69 per cent expected the total number of endpoints they supported to grow over the next three years.

- 61 per cent of our respondents had automated at least half of their endpoint management and security, with 39 per cent using automation to a much lesser degree.
- 80 per cent agreed to at least some extent that there were still too many repetitive, labour intensive tasks involved in keeping end users patched, secure, and compliant.
- 70 per cent of respondents agreed to at least some extent that it was getting progressively more difficult for IT Services to keep up with the needs of their businesses.

Optimising Assets

Enterprises are transforming to survive. Technology innovation and the personalisation of the delivery of goods and services are driving each other and the businesses who thrive in this climate will be those who embody a flexible, dynamic approach and deliver digital access to goods and services fast. The digital economy is also generating unprecedented quantities of data, and agile businesses are putting data strategy at the centre of their plans. Unlocking the immense value of this data is a pan-organisational challenge, taking in leadership and cultural considerations but also technology. Furthermore, the drive to reduce costs runs through every decision.

IT Service Management (ITSM) as the process and practice of assessing the design, delivery and management of IT services overall is crucial in determining the agility of an organisation. The whole point of ITSM is to ensure that the optimum blend of people, process and technology exists to enable business goals. IT Asset Management (ITAM) is a related process (and technology) used to keep track of an organization's hardware and software inventory, manage asset lifecycle and make buying decisions accordingly. Their centrality to the process of transformation means that both ITAM and ITSM are having to adapt quickly to new digital norms. Are they doing so?

Confidence in ITAM and ITSM is generally high. 85 per cent of those participating in our survey were at least reasonably confident that their ITSM was serving the business well. The extracts shown below illustrate some of the factors for success in this area.

"IT services are delivered effectively with few incidents; assets are registered and well managed."

"Metrics suggest overall positive feedback - plenty of self-service tools and help in place to serve the user base."

"Most issues are dealt with usually same day. Assets are managed with monitoring tools that give us an overview of system health."

"We have a number of tools providing oversight that gives us a fair degree of confidence, coupled with some strategic decisions that have simplified our estate, generally."

However, it is also worth exploring why some 15 per cent of research participants were less confident about their ITSM. The extracts below hints at where challenges are occurring -or might be occurring in the not too distant future.

"a) off-budget purchases of cloud services by individuals b) Items that are not labelled as IT but contain embedded IT."

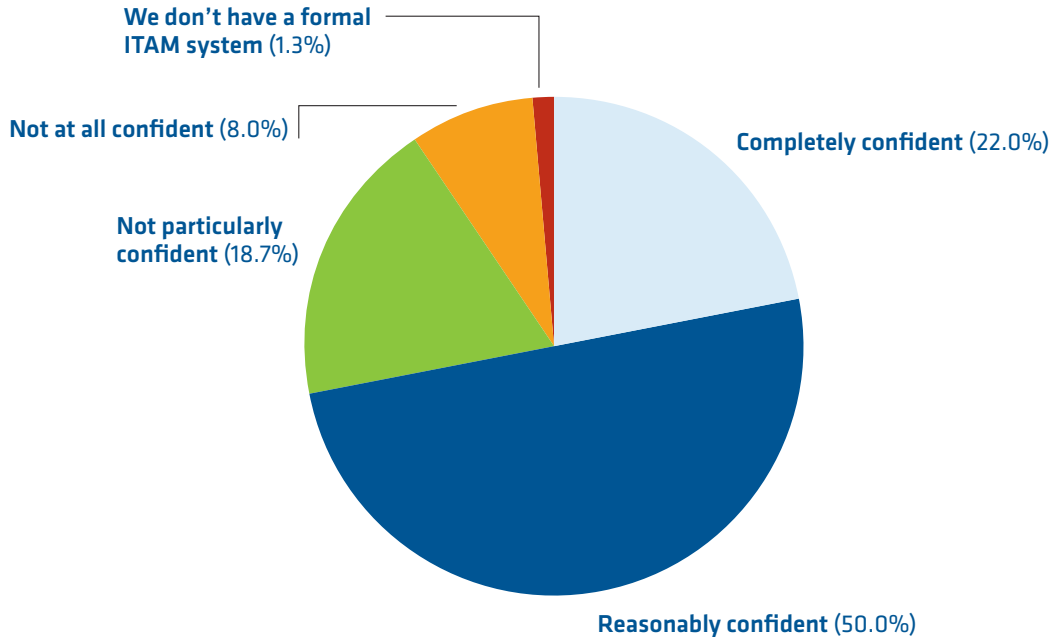
"At the present level of integration, we are not having any serious problems, although problems may arise from a more complete integration."

"There is always the risk of shadow IT - people bringing their own kit to work."

"The fact that the organisation spans multiple sites with a significant minority of staff mobile presents challenges in tracking portable devices."

Figure 1 combines the results of two questions about confidence in ITAM. The first question specifically concerned the visibility of all IT assets from acquisition to disposal and the second cloud management in terms of costs and licencing.

Fig. 1 : How confident are you that your IT Asset Management (ITAM) system is providing visibility of all IT assets from acquisition to disposal?



Not only was the level of confidence high across the board but there was almost no difference in confidence levels relating to the visibility of tangible physical IT assets as opposed to cloud assets. Our respondents were also very confident that their organisation was not under licensed or overspending on licencing with 82 per cent reporting at least reasonable levels of confidence.

These findings are somewhat at odds with a good deal of research conducted over the last six months for *Computing* which has consistently reported concerns from organisations about the visibility of cloud assets and the management of cloud costs, which for many enterprises are coming in significantly higher than was anticipated at the outset of cloud migration.

It is impossible for ITSM and ITAM to be a useful part of the process of digital transformation if the two are working independently of each other. It is impossible to efficiently deliver business services such as deployment and application management, patching etc. and resolving problems relating to assets without also having a clear view of the inventory and management of those assets. On this as well confidence levels were high. 76 per cent were happy that ITAM and ITSM were well integrated.

Remote Control

When it comes to changes in working patterns in the last decade the direction has been one way only. The move to more flexible working as well as a phenomenal leap in the quality of mobile solutions and connectivity in the last decade has led to a massive increase in the numbers of people working remotely for at least some of the time. The Covid-19 pandemic took a trend that already existed, and turbo charged it.

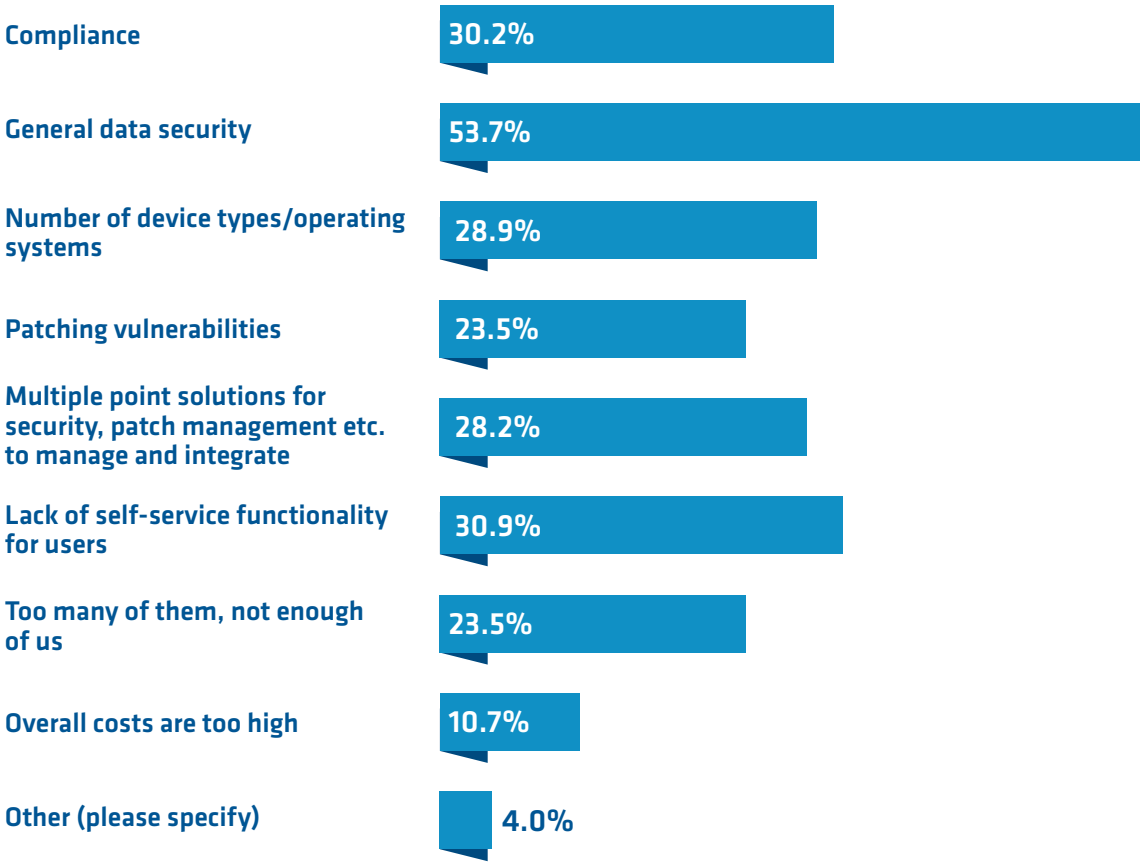
Whilst at the time of writing the lockdown imposed in late March is being eased in the UK, the advice to work from home if possible is still in place – and likely to remain so for quite some time. Many workers who were predominantly office based in the olden days of last year are rather enjoying at least some aspects of home working – notably the greater autonomy and extra time gifted by a lack of commute. That said, many miss the more social aspects of office life, the ability to avoid domestic incursions into the working day and the anchoring effect of a separate place of work. That commute home can also serve more positively as a coda to the working day. It is unlikely that working life will return to the way it was at the end of 2019 but a greater place for remote working in the future seems a pretty safe bet at the time of writing.

The ability to support remote workers is therefore more important now than it has ever been. Figure 2 *(see next page)* illustrates some of the challenges that enterprises face in this area. Survey respondents were asked to select up to three challenges.

The high showing of security in the list of challenges given is not a huge surprise, and recent events will have likely increased the anxiety levels of CISOs. Security companies have been reporting Covid related phishing activity since early in March and attackers are continuing to exploit people both on a personal level in terms of their need for news and information and their need to connect with others and also on a more professional level with phishing attempts related to the financial help being made available for small businesses, Job Retention Scheme etc.

Correlated with security is the issue of compliance, which shows strongly in our list of challenges. This finding shines a spotlight on another issue that businesses managing large sets of freshly minted remote workers are really struggling with, namely that of unauthorised file sharing or collaboration platforms, and the placing of corporate or customer data onto these platforms. Enterprises have been struggling to find a balance on this issue for years. It is not terribly difficult to simply remove administration rights for users, but this tends to have two effects. The first is that the rate of calls to your help desk increases significantly.

Fig. 2 : What are the most common challenges you face supporting remote workers?



The second, probably more damaging response from users is that they work round the problem by simply picking up a separate device not owned or controlled by you, downloading a user-friendly consumer application and carrying on as they were before. This device doesn't need to be connected to a corporate network to present a threat to compliance. What is required is a solution enabling unauthorized code to be blocked on corporate connected devices without user productivity being detrimentally affected. It is necessary to take the end user with you. Remote workers, now more than ever, need to feel that they are empowered and trusted to do their jobs, not feel as if they are being treated like liabilities to be controlled and monitored.

The lack of self-service mentioned by 31 per cent of our survey respondents is knitted into the whole issue of empowering users. Some are struggling to adapt to remote working technologies and home offices won't always be suitably equipped which makes it likely that in many organisations, the volume of calls to helpdesks has increased sharply. Being able to close these tickets with minimal human intervention requires a strong knowledge base that remote workers can access, and high levels of automation so that remote workers get the help that they need to enable them to remain productive.

Never Ending Story

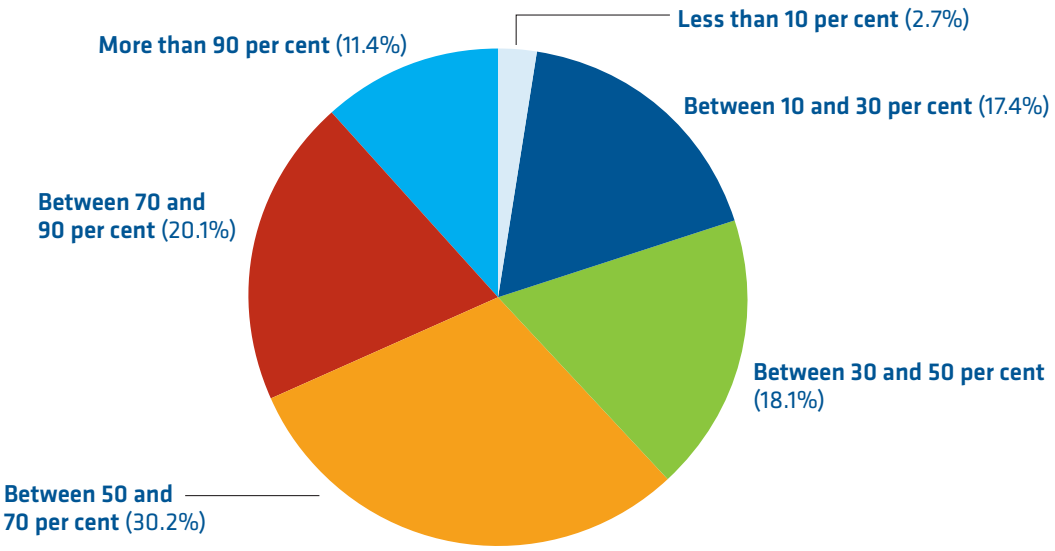
The challenges being faced by our survey respondents in supporting remote workers is part of the much larger overall challenge of endpoint management. The causes of many technology issues are complex, but the cause of much endpoint management difficulty is, for once, straight forward – the number of endpoints has gone through the roof. The variety of devices has also increased significantly. When asked what proportion of endpoints had been added to their organisations in the last year the most popular answer, cited by 41 per cent, was that they had experienced an increase of between 20 and 40 per cent in endpoints. 28 per cent had seen an increase in excess of that. 69 per cent expected that number to grow over the next three years, with only five per cent expecting the number of endpoints to decline.

Managing and securing these endpoints is not a straightforward exercise – and the more devices proliferate the harder it gets. One issue is the number of security tools all serving slightly different but often overlapping functions. Anti-malware, email gateway security, application control, DLP, encryption, etc. Recent research by *Computing* has established that in the event of a security incident, 70 per cent of organisations have to interrogate more than four separate sources of data. It tends not to make for speedy incident resolution. Whilst 32 per cent of our respondents had managed to consolidate their security estate to some degree a further 40 per cent were planning to do so and 21 per cent said it was on their agenda but not at the top. Recent events are likely to have reordered priority lists.

The automation of endpoint management and security as a whole goes a very long way to solving most, if not all, of the challenges outlined above. A platform which automates patch management and access rights/privilege management which can also be integrated with an anti-malware solution frees up IT teams from the tedium and difficulty of managing and integrating multiple solutions for different aspects of security. Management and security can all be managed from one place and for end users it's business as usual.

61 per cent of our respondents had automated at least half of their endpoint management and security, with 39 per cent using automation to a much lesser degree.

Fig. 3 : What proportion of your endpoint management and security is automated?



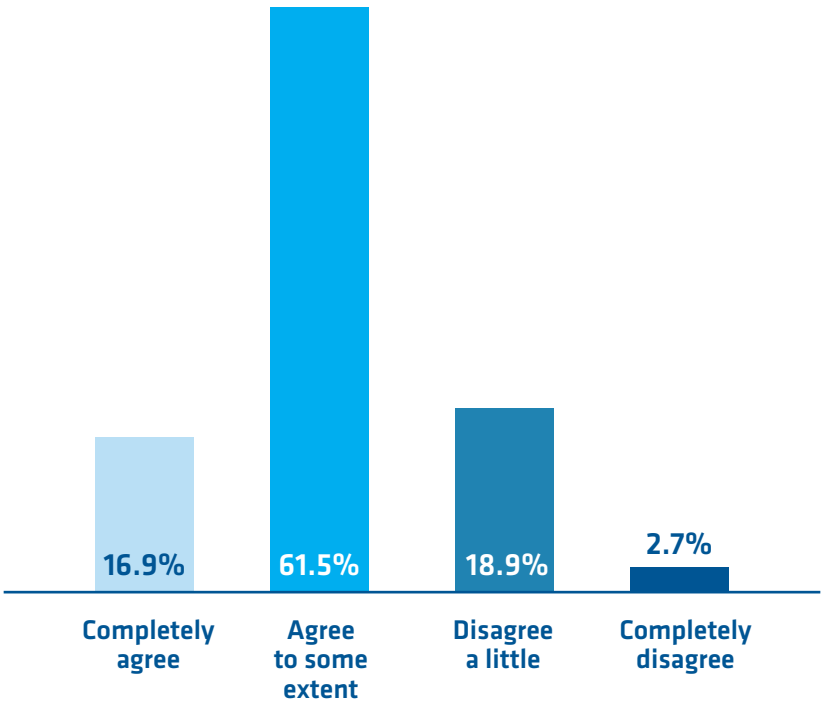
Our survey picked up a strong appetite for a greater scope for automation. When asked to what extent they agreed that, *"There are still too many repetitive, labour intensive tasks involved in keeping end users patched, secure, and compliant,"* almost 80 per cent of respondents agreed to at least some extent.

Conclusions

IT Service organisations, and the ITSM and ITAM processes and tools that they employ are having to adapt sharply to a fast-changing business environment where digital channels are everything. The majority of respondents to our exclusive research are confident that their ITSM was serving their businesses well. There was strong confidence that the systems in place were enabling businesses to stay on top of cloud costs, management and licencing as well as physical IT assets. A majority had their ITAM well integrated into their ITSM process so had a clear view of the inventory and management of assets when delivering business services.

On the surface these seem like very positive findings but findings from other questions call this apparent high level of confidence into question. Figure 4 illustrates responses to a question about how difficult IT Services teams found it to keep up with the needs of their business. With 70 per cent of respondents in agreement the picture becomes more swan like – serene surface level confidence with frantic paddling occurring unseen beneath the surface. The sustainability of this situation is a moot point.

Fig. 4 : To what extent would you agree with the following sentence?
"It's getting progressively more difficult for IT Services to keep up with the needs of the business?"



Getting to the top of your game: how does the modern IT service organisation best serve the enterprise?

We're all remote workers now and it's posing considerable challenges for IT Services. Security and compliance are huge concerns, but these rank alongside the difficulty that a dearth of self-service functionality for users causes for IT Services. The speedy roll out of home working to far greater numbers of users than would regularly be the case has drastically increased call volumes at many IT service desks.

New home working norms are just part of a much larger and longer standing challenge of managing an ever-increasing number and variety of endpoints. For our respondents, a year on year increase of 25 per cent in the number of endpoints they had to manage and secure was quite within the realm of normal. A majority expected that number to grow even more in the next three years, no doubt fuelled at least in part by a big increase in the scope of IoT and edge computing.

The number of solutions in the mix is part of the problem. Although a little fewer than one third of respondents had managed to consolidate their security estate to some degree, a majority are juggling far more individual security solutions than they would wish. Furthermore, whilst 61 per cent of our respondents had automated at least half of their endpoint management and security, nearly 80 per cent agreed that there were still too many repetitive, labour intensive tasks involved in keeping endpoints patched, secure and compliant.

Answers from another question also illustrate the thirst for greater automation in the processes of IT services organisations. We asked what role automation played for our respondents' employers in the on and offboarding of new/departing employees in terms of equipment, licencing, service provisioning etc.? For the largest proportion of respondents (41 per cent) it played only a small role, with a further seven per cent saying there was no automation at all. Only for 18 per cent did automation play the majority role in these processes.

The confidence our research participants have in the visibility and lifecycle management of their cloud and physical assets may not be sustainable in the long term, given the issues that they have told us they are experiencing. In order to best serve their businesses, IT service organisations should consider a more unified approach, merging their enterprise service management with their endpoint management and security – and automating currently manual processes.

This unification allows the enterprise to more efficiently manage and secure their evolving working environment by discovering and tracking assets wherever they happen to be. A single platform approach to automating the often manually managed areas of patching and maintenance along with the deployment of access management and anti-malware solutions removes many of the manual tasks which our respondents told us remained. The top-level confidence that we saw in terms of asset visibility and management can be extended beneath the surface.

Perhaps most importantly of all this unification can make life easier for end users – and significantly improve their perceptions of IT services organisations. This is the essence of best serving the enterprise. End users measure their IT services organisations by the degree to which they enable their productivity. Any impact on the user experience tends to attract poor feedback. A unified approach has the potential to optimise the user experience and allow IT services organisations to enable, manage and secure their enterprise in a the most cost effective, sustainable manner.

About the Sponsor, Ivanti

Ivanti: The Power of Unified IT.

Ivanti unifies IT and Security Operations to better manage and secure the digital workplace. From PCs to mobile devices, VDI, and the data center, Ivanti discovers IT assets on-premises and in the cloud, improves IT service delivery, and reduces risk with insights and automation. The company also helps organizations leverage modern technology in the warehouse and across the supply chain to improve delivery without modifying backend systems. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world.

For more information:

Visit: www.ivanti.co.uk

Follow: @GoIvanti on Twitter