



2020 Global Managed Services Report

How organizations are adopting smart sourcing to navigate with confidence



Foreword

If there is one constant in life – it's change. Change is inevitable; it's how we adapt, develop and move forward. Nowhere has this been more apparent than in recent events surrounding COVID-19. The impacts have been dramatic and life changing. It's changed the way businesses operate, how we view the world, and how we work. This has fundamentally altered and driven the need to rethink strategies and redeploy workforces. Remote working is the new normal.

The role of the CIO is also constantly changing. Previously responsible for controlling end-to-end decision making around the IT estate, CIO's have evolved into business enablers. And now in these unprecedented times, the entire organization turns to them and their teams to lean in and deliver the seemingly impossible - to keep the business running.

Business continuity and security are front and center of the

enterprise, working to survive. Yet, as we venture forward, the coming together of people from across the organization, partners and service providers, determines the recovery success.

While siloes will always exist, the bigger picture is more important. The relationships with those outside our normal scope will deliver far reaching outcomes to help restore organizations, albeit in a different, but equally effective state. Now more than ever is the time to leverage the trusted, flexible partnerships you've built, turning to those partners who have prepared for such events so that your operations can continue uninterrupted. Those flexible and agile enough to provide the services you need, and who can protect you from threat actors taking unspeakable advantage of dire circumstances.

All of these trends and more have come to light in our 2020 Global Managed Services Report. Conducted by IDG Research (and supplemented with other Global NTT Ltd. Reports), we've lifted the lid on the importance of smart sourcing for organizations and the service providers they partner with. All seen through the light of security, transformation reimaged and technical expertise.

Afterall, tough times will pass. But it's the leaders focused on recovery and restoration, as well as ensuring any future

disruptions have minimal impact, who will make certain their teams and organizations come through in the best possible shape.



Damian Skendrovic
Executive Vice President,
Managed Services
Go-to-market, NTT Ltd.

Damian currently has a dual role covering the Go-to-market organization for NTT Ltd.'s Transformation and Platform Services Business, as well as CEO of NTT Com Managed Services. He is responsible for transforming our global managed services capabilities and go-to-market to drive customer satisfaction and growth, responding to client's changing business requirements. Damian's career spans over 25 years in IT, 20 years in IT Services, 14 of those within NTT Ltd. He holds several board positions including NTT Europe Ltd., Gyron Internet, NTT Com Managed Services, Secure-24 and Capside.

Follow Damian on [LinkedIn](#).

Key Findings

The rise of smart sourcing



NTT Ltd's 2020 Global Managed Services Report, conducted by IDG Research, covers the challenges and opportunities felt by over 1,250 business and IT leaders across the world. And from that, a move from what has historically been termed outsourcing, to **smart sourcing**.

At its simplest, smart sourcing is an approach to the selection and prioritization of those service providers that go above and beyond the delivery of tactical IT solutions. It's about nurturing long-lasting relationships with providers who can deliver

Expanding further, it's about the following:

1. Having the relevant expertise to augment the gaps in your own in-house IT team.
2. Providing the widest services portfolio enabling you to consolidate the number of partners you need to manage on a daily basis.
3. Not only running your daily business, but also taking you forward on your IT transformation journey to deliver business agility.
4. **Financial** stability, plus a global footprint of ICT infrastructure and being secure by design.

business outcomes aligned to the goals of the entire organization.

Organizations need to be selective about the service providers they work with and the relationships they build and rely on.

Our study uncovered three core insights:

Insight #1

Identify and secure your assets

'Reducing security risks is the top reason for considering a managed service provider.'

Security is a prime factor in the value service providers bring. As organizations adjust to new ways of working and IT teams restore operations in new environments, both security and governance play a vital role in the ability of service providers to meet client requirements.

Insight #2

Transformation reimaged

'48% of business leaders acknowledge a need to optimize the workplace environment to meet the demands of an evolving workforce.'

Organizations should reconsider what IT transformation currently is. While they get to grips with a new look business, there's also a need to redevelop and have one eye on the future too.

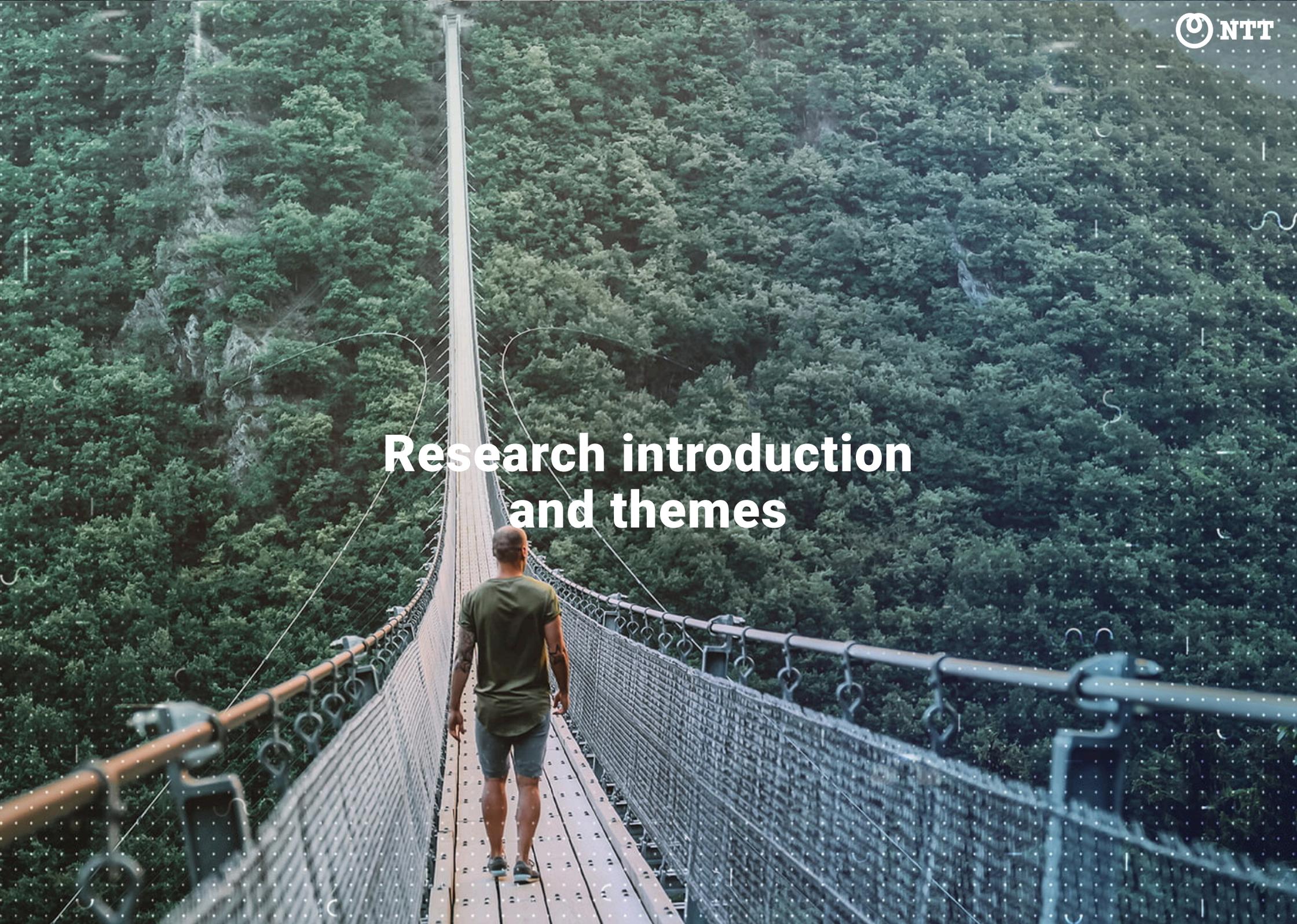
Insight #3

Technical expertise and strong service provision builds trust and strong relationships

'Organizations feel MSPs will provide the most value over the next 3-5 years through their security capabilities (44%), financial stability, trust and reputation (43%), and automation (43%).'

Now more than ever is IT's time to demonstrate value. IT keeps core business applications, processes and the network not just alive and well, but dynamic to shift under the new ways.

¹*NTT Ltd. CX Benchmarking Report 2020

A person in a green t-shirt and shorts is walking away from the camera on a suspension bridge. The bridge has a wooden deck and metal railings. Below the bridge is a vast, dense green forest. The scene is captured from a high angle, looking down the length of the bridge.

Research introduction and themes



NTT Ltd.'s 2020 Global Managed Services Report is a comprehensive, in-depth view of managed services. Conducted by IDG Research on behalf of NTT Ltd., respondents came from a cross-section of IT and business leadership positions, totaling over 1,250 people in 29 countries across the USA, Europe, MEA, APAC and Australia, and in a range of sectors.

As the relevance of a smart sourcing service model increases, it's important to outline the challenges currently experienced by business and IT leaders as we enter a new phase of continuity and restoration:

- The way in which we work has shifted - in most cases - forever. Remote working and the rise of bring your own device (BYOD) has hastened the need for proactive security alerts and fixes before issues even arise. With rapidly changing situations, organizations expect partners to

quickly provide new services to enable them to cope with, or fast track, additional requirements.

- Previously, organizations sought to quickly scale to meet increased customer demand. Now, scale is focused on secure networks and remote workers, digital platforms and collaboration tools.
- Solutions need to be delivered with continuity, agility and scalability. And it needs to be done almost instantly. Speed of execution is critical and even more so in current times. The ability to simplify and automate the organization through platform-based services remains an ongoing focus, regardless of macroeconomic forces.
- Growth aspirations have been completely challenged. Transformation was for the most part, focused on customer experience and new revenue streams. Now, end-user transformation sits front and center on the CIO agenda.

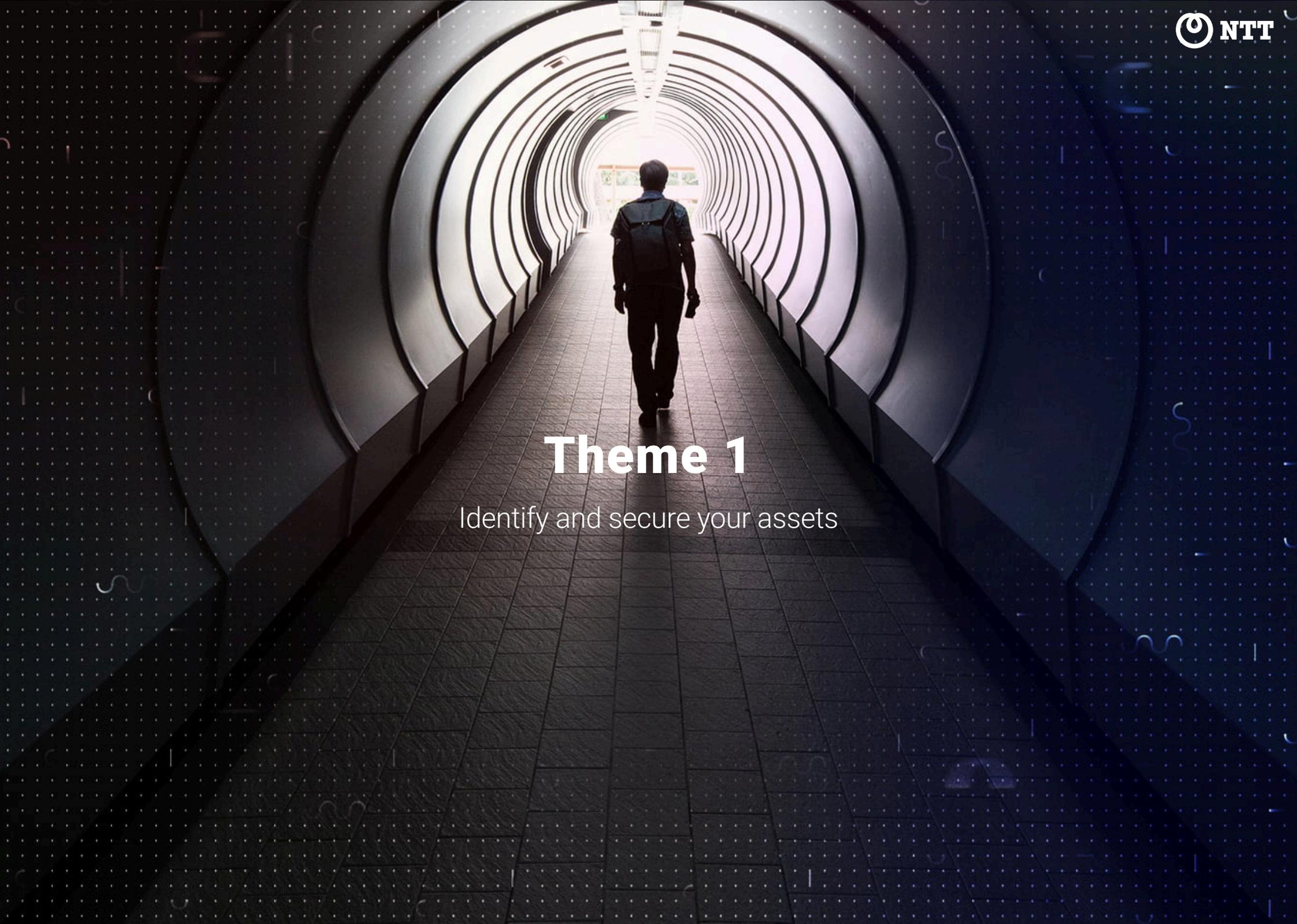
All of this points to greater demand in how service providers can play a larger, more intelligent role in enterprise

development. Large global organizations with centralized, standardized and automated systems and processes are now fundamental to continued business operations. Organizations need to know their service partner will support them to pivot their focus onto business continuity, processes and tools to keep their employees safe and productive. All while still managing their fundamental IT ecosystems.

In the following sections we analyse the core components of those relationships in more detail, based on the findings of the IDG study. Additionally, it will draw insights from a number of other studies conducted by NTT Ltd.

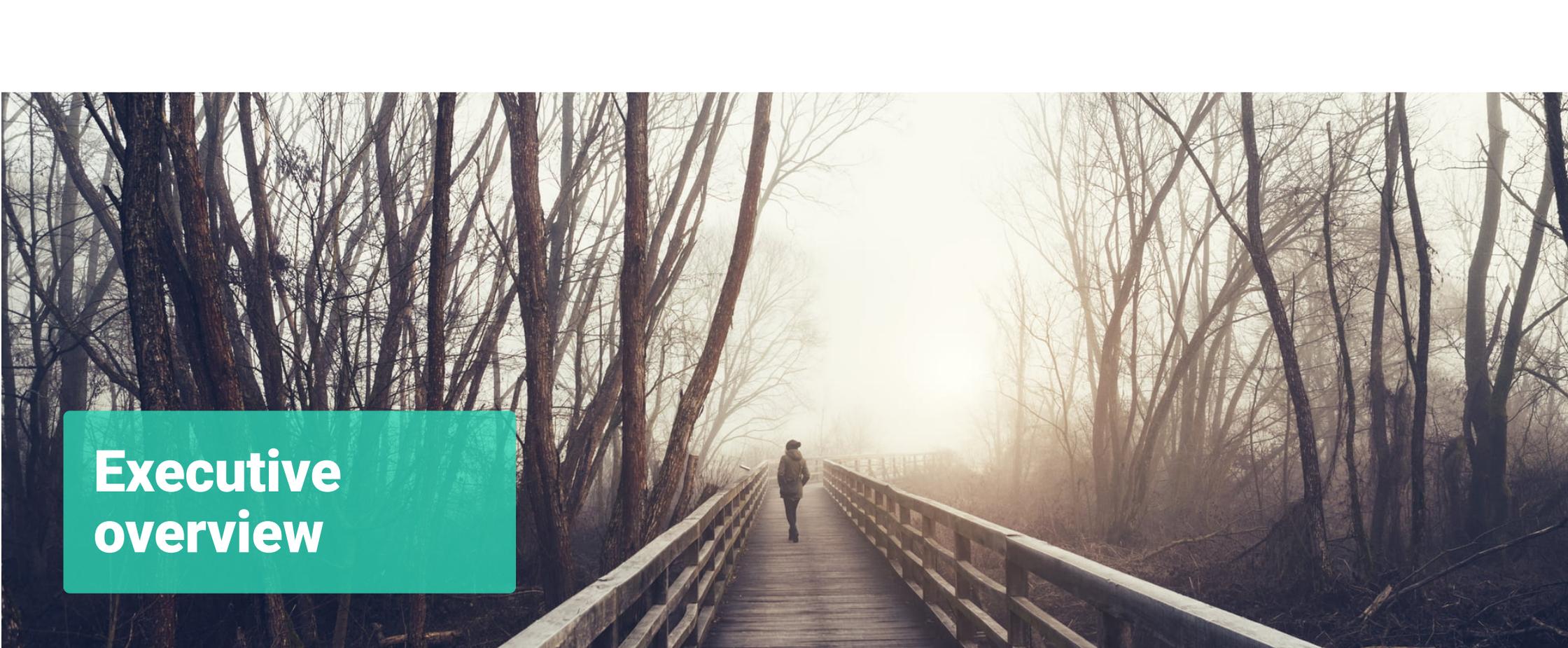
The themes covered in detail are:

1. Identify and secure your assets.
2. Transformation reimaged.
3. Expertise and service provision.

A person is walking away from the camera down a long, brightly lit tunnel. The tunnel has a tiled floor and curved walls with a grid of lights. The person is wearing a dark jacket and a backpack. The tunnel leads to a bright opening at the end.

Theme 1

Identify and secure your assets



Executive overview

Security is a global necessity, pervasive throughout every aspect of organizations and escalates with technological advances. As enterprises restore their operations, in what for some are unfamiliar operating environments, increased security is essential.

There are also implications around the potential lack of sufficiently resourced IT teams to meet the challenge of integrating legacy and new technologies securely; a necessity given the need to enable workforces and ensure their productivity with the right tools, regardless of location.

If not, organizations tend to see a rise in shadow IT. That is, the line of business stakeholders (and their end-users) taking matters into their own hands to implement technology to

better perform their roles. And, while that may benefit them in one sense, the lack of consistent security protocols and tools, via the vital missing input from IT, could have disastrous impacts on the security of the entire organization.

But while continuity currently headlines conversations, IT leaders should consider flexibility, agility and user experience as part of their overall security posture; positioning themselves positively when uneasy times pass.



Security and continuity

Evaluating security postures and dealing with security risks is a perennial challenge.

The IDG study found 57% cited 'reducing security risks' as a common challenge, rating the highest among all factors considered. This trend continues to show that organizations struggle to defend themselves against a complex and worsening threat landscape; mirroring findings from NTT's Risk: Value 2019 report.

It's no surprise therefore to see a majority of organizations (55%) turn to service providers for their ability to help 'reduce security risks', as the most popular value-added service they offer.

Recent events have resulted in a dramatic increase in remote working, which in turn, has placed even greater demands on IT and security teams. They must have visibility across all endpoints and are tasked with keeping the corporate network,

information assets, data and devices both operational and secure to ensure business continuity. And, looking ahead, need to update and patch critical systems where required. Endpoint detection, web content filters, and VPN clients for example, all require careful planning too.

For those who already have a remote working or BYOD program and respective policies in place, the focus is likely on how to quickly scale and shift security operations from on-premises activities to remote support – and how to do so with limited resources. User security profiles would have changed, and the cybersecurity posture would need to shift to address that with the introduction of, for example, remote vulnerability management, end-point protection and incident response services to ensure the security of people working from home.

Do you have multi-factor authentication (MFA) across all your devices? (BYOD and corporate)

- Yes – we have MFA across all our devices, both corporate and BYOD
- Yes – But partially across only corporate devices, not BYOD
- No
- I don't know

POST ANSWER —

Top challenges areas supported by service providers

Security is the most commonly cited IT challenge; it's also the top area IT departments call upon service providers to support.

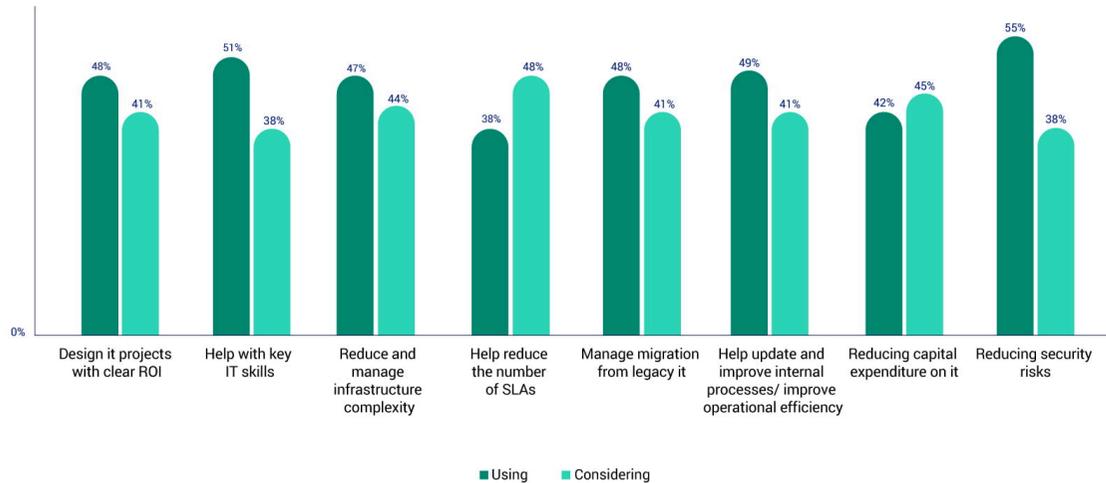


Fig. 1: Are you using or would you consider using a Managed Service Provider (MSP) to help your IT department and if so for which particular challenge?

Source: IDG Research for NTT Ltd on managed services

For those without a remote working or BYOD security program, the challenge is amplified. There are a wide variety of issues to consider, including whether the employee has an internet connection capable of supporting access. And subsequently, how to manage, engage and properly enable employees who have not previously worked from home let alone how the

organization supports and secures that remote workstation with, for example, VPN, encryption and privacy. In this case, security teams are fundamentally rethinking their security posture and operations, and requiring a drastic culture change in order to enable business resiliency.

Further to this, threat actors are exploiting the fact that more people are working from home, potentially, on inadequately secured devices and networks. NTT Ltd.'s April 2020 Monthly Threat Report noted an increase in spam, phishing and malware campaigns specifically taking advantage of the COVID-19 crisis.

Matt Gyde, President and Chief Executive Officer, Security division at NTT Ltd. comments, 'Organization's digital journey has fundamentally changed how security is deployed, configured and managed. The traditional perimeter security model is being questioned as we see the proliferation of end point devices. The rapidly growing digital footprint needs to be secured and is protected from a rise in malicious activity targeting the remote worker. Our Managed Security Services can be deployed rapidly. It can flex and scale to support already stretched security teams, enabling employees to work securely from anywhere and on any device, to ensure business continuity.'

Security was also rated the important factor for supporting the business case for using a service provider. Thirty-two percent of respondents rated it as the most important factor, compared to 30% for improved operational efficiency and 29% for better performance / availability. And, the trend for utilizing the skills of service providers for security looks set to grow over the coming 18 months. Sixty-four percent said they expected to outsource their security needs over the coming year and a half, compared to 53% who do so currently.

The ability to flex, scale and turn data into knowledge is one of the core benefits of a platform-based approach to delivering security services. Instead of merely seeing isolated events, a service provider focused on smart sourcing will provide you with your entire security picture. Feeding threat intelligence and advanced analytics into the platform delivery, ensures not only consistent, repeatable services, but capabilities to prevent advanced threats, and at speed. It also provides insight and metrics into future trends and methods to remain one step ahead of attackers, giving your organization the balance you need in your security posture.

Outcomes drive the business case

Managed services will be measured by their ability to drive outcomes related to cost, performance, agility; the most important business factors include security improvements (32%), improved operational efficiency (30%) and better performance/availability (29%).



Fig 2: Which of the following factors are most important in supporting the business case for your organization's use of managed IT services?

Source: 451 Research for NTT Ltd on Managed Services

Lack of security skills and resources

The array of change and pressures placed on IT and security teams through the coming months is further compounded by a lack of resources and skills.

An average of 42% of organizations to NTT Ltd.'s 2019 Risk:Value Report state they did not have adequate resources or skills in-house to cope with the number of security threats they face. Additionally, a high proportion of organizations in the technology, finance and public sector industries expect a skills impact – and are among the top five sectors globally to face cyberattacks.

There's no easy answer to filling the skills and resources gap. Yet, it does highlight the large reliance organizations place on using managed service providers to guide them through challenging situations; particularly those related to security. Technical expertise was rated the most important feature by 44% of respondents when considering a managed services provider, according to research conducted 451 Research for NTT Ltd. in 2019.

The impact of skills and security skills shortages

An average of 42% of organizations do not have adequate resources/skills in-house to cope with the number of security threats; an average of 46% indicate a more general IT skills shortage.

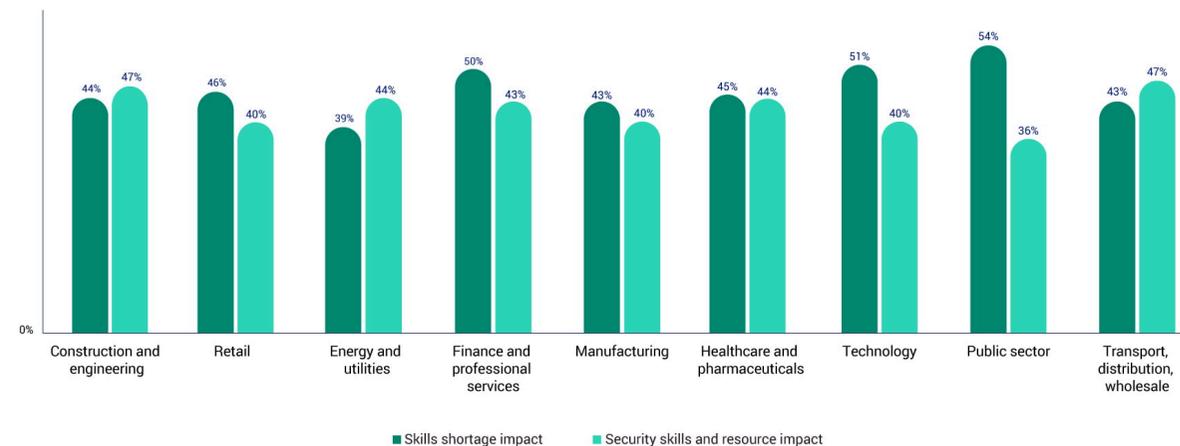


Fig. 3: What are the changes you envisage impacting your IT decision making in the next 18 months? Answers provided for 'Skills shortages'

Source: 2019 Risk:Value Report, NTT Ltd

Supporting this, NTT Ltd.'s Global Customer Experience Benchmarking Report 2020 uncovered that 62% of organizations said they expected an increased need for cybersecurity/IT support skills over the next two years.

Organizations are caught in a quandary over skills and resources. While the need to rely on specialist partners becomes even greater post a major event, pressures from the business can dictate cost reduction. As such, a broad range of capabilities from a service provider with platform-delivered services pays huge dividends.

Platform-delivered services allow organizations to collect and analyse data based on new behaviours. This assists with making better and more informed decision-making for the future. It also decreases the burden on IT staff, freeing them up to focus more on the overall security strategy and posture of the organization.

Skills shortages will worsen

The current skills shortage situation paints a concerning picture for organizations – and the challenge is set to increase.

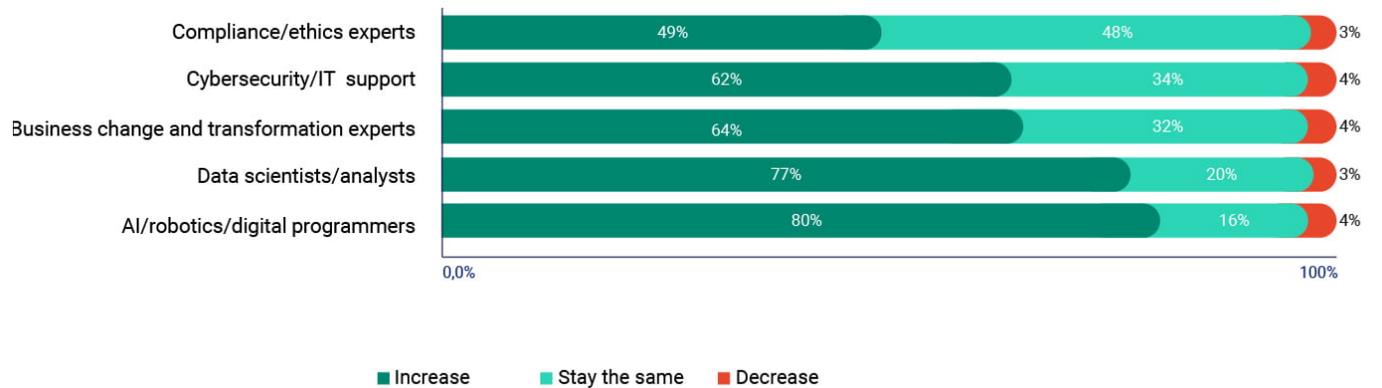


Fig 4: How will advancing digital transformation (incl. robotics) impact your resource skill needs in the next two years?

Source: 2020 Global Customer Experience Benchmarking Report, NTT Ltd.

Three steps to rescue, recover and redevelop



1. Rescue

In the immediate aftermath of a major event, nearly all organizations are in react and rescue mode. That is, the enactment of continuity plans to place the business into survival mode. Focus on the most important things, freeze everything else not related to the survival of the business. Defensive strategies are required to retain and maintain your two most important assets, your employees and your customers.



2. Recover

On the recovery side, now is the time to fix the things that, during the immediate aftermath of the crisis, had merely 'band aids' applied – ensuring a repeat attack or event does not take place. For example, employees may have had to use their own devices to access the corporate network from home. As remote working continues to progress, the scaling of corporate approved devices will take place and security policies updated in line with the new way of working. However, new learnings can be derived when analysing data collected during a massive shift in behaviour, such as entire workforces operating from their homes. Data collection needs to be done in a systematic way that's searchable; which is where platform-delivered services become vital in the recovery process. If you're going to reach the suggested third step of 'redevelop', it's crucial you have a knowledge store, a repository of information you can farm, helping to inform how you approach redevelopment.



3. Redevelop

Having been through a major event and adapted the organization considerably, there now sits a wealth of platform-enabled data to enable and drive new efficiencies. For example, changing the business model from the front end of the go-to-market to the back end of the supply chains. Consider the remote working example during the outbreak of COVID-19 and the considerable changes and impact this had. Being forced into changing models and then having the ability to understand its impact through the collection of data will have huge implications for the way in which business operates.

While some organizations are in better positions to recover and restore their operations than others; for all, there's a simple three step process to ensure that while you focus on the here and now, you can keep future ambitions in sight too.

A photograph of two people standing on a long wooden pier extending into a calm lake. The sky is a mix of purple, pink, and blue, suggesting a sunset or sunrise. The water is still, reflecting the sky. The pier is covered with fallen brown leaves. The overall mood is serene and contemplative.

Theme 2

Transformation reimagined

Sorry, you must sign up in the [online version](#) to view this content.



Theme 3

Expertise and service provision

Sorry, you must sign up in the [online version](#) to view this content.



Conclusion

Building a better business

Sorry, you must sign up in the [online version](#) to view this content.

Thank you for reading

2020 Global Managed Services Report