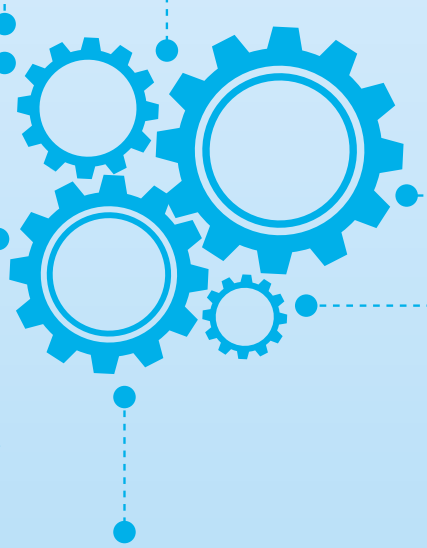
THE EMEA

2021

TOMORROW'S DIGITAL WORKPLACE

European Mobile & Remote Working Survey

CONTENT



ABOUT THIS SURVEY

The mobile revolution is changing the way we work and live, never more so than in the current climate, and is impacting almost every aspect of our daily lives. But keeping up with the rapid evolution of mobile technology is a challenge for organisations across the world, of all sizes and in all sectors.

To delve deeper into the trends, insights, and attitudes towards these modern ways of working, the EMEA Group conducted a survey of 329 European organisations from the group's regions of Switzerland, Germany, France, UK, Ireland, Belgium, and the Netherlands.

We were particularly interested in gaining insights into how Covid-19 has changed the world of work in these countries. Respondents ranged from company leaders and key decision-makers to engineers and sales professionals, providing a rounded view of how this fundamental shift is affecting all aspects of businesses.

COUNTRIES INVOLVED

France, Netherlands, Ireland, UK, Germany, Belgium, Luxembourg, Switzerland

RESEARCH PERIOD

Mid-December 2020 – February 2021

TOTAL RESPONDENTS

329

WELCOME TO THE FUTURE

OF THE DIGITAL WORKPLACE

The benefits of flexible, mobile and remote working on employee engagement are well-established but adoption has not always been a top priority for organisations. This changed dramatically during 2020 as the Covid-19 pandemic was a catalyst for change, making the ability to work from home an absolute necessity rather than a fringe benefit.

It is no surprise, therefore, that our survey shows a step change in remote working capability. The percentage of organisations with a majority of the workforce capable of remote working has risen from 50% before Covid-19 to 88% during Covid-19. However, this significant increase in adopting and implementing home working solutions at short notice and on a large scale has created challenges.

Tactical solutions that rely on applying technology designed for the office in a home environment often lack flexibility, scalability and longevity. Our survey shows that organisations can, and must, do more to unleash the full potential of the digital workplace by rethinking the strategy, technology and support that underpin it.

What are the major challenges European organisations have faced? How have they addressed these challenges? What steps do they still need to take? These are just some of the questions we asked as part of our European Mobile & Remote Working Survey 2021, the key insights from which are outlined in this report. The Enterprise Mobility Expert Alliance (EMEA) is the largest community of digital workplace experts in Europe. Our vision is to help organisations succeed in creating a workplace that combines the best possible employee experience with the manageability, security and efficiency demanded by IT and security teams.

This report is intended to help organisations at every level of digital workplace maturity, in any sector. Whether you are starting out on your digital workplace strategy or you are looking to refine existing plans, we hope you find insights and inspiration to turn your digital workplace vision into a strategic asset and a real competitive advantage. Our report reveals that those organisations who had already invested in a digital workplace strategy, with strong foundations in mobile technology, were best placed to meet the needs of a distributed workforce in a secure and manageable way, providing employee choice, flexibility and ease of use without sacrificing security or manageability.

We are encouraged that many organisations have put in place at least some of the foundations to support a digital workplace strategy. However, this report clearly highlights that there is still much untapped potential and that more can and should be done with technology to maximise the benefits of the digital workplace for organisations of all sizes and in all sectors.

THE ENTERPRISE MOBILITY EXPERT ALLIANCE

ADJUNGO, FRANCE
Cédric Girardclos
and Sébastien Gabriel,
Managing Partners

BLAUD, NETHERLANDS
Thierry Lammers,
CEO

CWSI, IRELAND & UK
Ronan Murphy,
CEO

EBF, GERMANY
Markus Adolph and
Marco Föllmer,
Managing Partners

MOBCO, BELGIUM & LUXEMBOURG
Ulrik van Schepdael,
CEO

NOMASIS, SWITZERLAND
Philipp Klomp,
CEO

SURVEY METHODOLOGY

This study was conducted by an independent market research agency, hopp Marktforschung, on behalf of the Enterprise Mobility Expert Alliance (EMEA). Online survey data was collected between December 2020 and February 2021. The data sample comprised 329 individual responses from a range of business decision-makers, IT operators and senior leaders from European organisations across a range of industry sectors. A full breakdown of the survey respondents' demographics is included at the end of this report.

EXECUTIVE SUMMARY

UNLEASH THE FULL POTENTIAL OF A TRULY DIGITAL WORKPLACE

Building a modern workplace that provides an outstanding employee experience can result in higher productivity and employee retention rates, creating strategic advantage and competitive differentiation. However, implementing technology solutions that meet the changing demands of employees, address the growing and evolving security risks and can be supported in a streamlined way is challenging. Heterogeneous device landscapes, many integrated technology solutions and rapid innovation cycles create high levels of complexity.

On a positive note, our survey shows there is much unrealised potential. Below, we highlight four major findings from our research to help you win the mindshare, funding and resources required to build a business case for your future digital workplace.

01 FOCUS ON EMPLOYEE EXPERIENCE, NOT ENDPOINT MANAGEMENT

OPTIMISE YOUR MOST VALUABLE ASSET BY INVESTING IN EMPLOYEE EXPERIENCE

Of those respondents who have implemented, or plan to implement, a remote working strategy, employee-related objectives were the key drivers. Employee experience and productivity were both rated in the top three factors driving a remote working strategy by 81% of respondents, well ahead of the next most important factor (security, 38%).

The business case for this is straightforward; providing a better employee experience leads to more engaged, productive and loyal employees. 89% of respondents said that their productivity was the same (43%) or better (46%) when working remotely compared to working in the office.

Technology can play a key role in enhancing employee experience, but our survey suggests that businesses can and should do more in this area. For example, fewer than half of respondents (42%) follow the best-practice approach of tailoring employee device choice to the demands and context of their role. Additionally, user-friendly security measures such as conditional access, which can speed up employee authentication, are still not widely deployed (40%).

Issues with user experience were also cited as a common challenge to adopting remote working by 44% of respondents, second only to broadband connectivity issues (48%).

Organisations should make employee experience a major strategic priority. Initiatives such as the regular tracking of board-level Key Performance Indicators (KPIs) on employee experience and the creation of a cross-functional Chief Employee Experience Officer (CEEO) role could be catalysts for a mindset shift from simply managing endpoints to truly enhancing employee experience.

02 A MODERN WORKPLACE NEEDS MODERN SECURITY

CONFIDENCE IS HIGH BUT THERE IS A FALSE SENSE OF SECURITY

Our survey shows that confidence in data security is high, with almost three-quarters of respondents either very or fairly confident in their ability to secure corporate data on remote or mobile devices. However, a closer look at the data suggests this confidence may be misplaced and that, against a backdrop of growing and evolving cybersecurity threats, organisations need to review the adequacy of their security measures for remote and hybrid working.

Only half of respondents have any kind of Data Loss Prevention (DLP) technology in place, fewer than half (42%) restrict access to third-party app stores; a common source of malware, and only 37% have a mobile threat solution in place, suggesting that security teams are applying less stringent controls on mobile devices than laptop or desktop devices. Additionally, one-third of respondents have not delivered any kind of mobile security awareness training to employees.

On an optimistic note, our survey clearly identifies security as a key future priority, with 45% of respondents ranking it as their number one remote working priority in the coming year and 88% ranking it in their top three priorities for the coming year.

Security has traditionally been viewed as a barrier to providing a good user experience, but modern security does not require a trade-off with ease of use. Organisations should adopt Zero Trust security principles wherever possible – never trust, always verify – and consider modern security tools such as data classification and control, privilege management and risk-based conditional access.

These tools, implemented correctly alongside clear security policies and regular security training, can enhance the employee experience and provide a robust security posture to support future hybrid and remote working models.

03 EXISTING TECHNOLOGY HAS SIGNIFICANT UNTAPPED POTENTIAL

SIMPLE ADOPTION MEASURES CAN TURBOCHARGE RETURN ON INVESTMENT

Our survey found that the existing technology solutions in place to support remote and mobile working are not used to their full potential. Almost three-quarters (72%) of respondents have a Unified Endpoint Management (UEM) platform in place but many organisations are not using this to manage devices other than mobiles and tablets. Only 57% use their UEM platform to manage Windows laptops and even fewer use it to manage MacBooks, desktops and other device types.

Furthermore, respondents are failing to take advantage of the more advanced features of today's UEM platforms. Almost half (43%) are not using features that can streamline the deployment and retiring of devices and over one-third are not using fleet management or advanced security features. As a result, opportunities to enhance the employee experience are missed and additional workload is placed on already stretched IT service desks.

IT leaders should evaluate their existing technology stack against their organisation's strategy and objectives. Our survey clearly shows that quick-win opportunities exist to deploy more features on existing solutions, demonstrating rapid return on investment through operational cost savings.

In the medium to longer-term, organisations should adopt an integrated Unified Endpoint Management strategy, enabling configuration of management profiles, device compliance policies, application policies and data protection policies for multiple device types and operating systems through a single console.

04 EXTERNAL EXPERTISE CAN FAST-TRACK DIGITAL WORKPLACE SUCCESS

LACK OF INTERNAL SKILLS AND RESOURCES SHOULD NOT BE A BARRIER TO PROGRESS

Our survey shows that digital workplace technology is predominantly managed by internal IT teams with only one-third organisations surveyed using external providers. This finding goes some way to explaining why many of the more advanced features of digital workplace technologies are not more widely deployed.

The pace at which UEM solutions, devices and operating systems are evolving and the rapid shift to supporting a remote working model during Covid-19, are creating difficult demands on IT teams. Lack of time (55%), lack of skills (45%) and a need to focus internal employees on more strategic projects (48%) were the top three reasons cited by organisations for using external expertise.

Organisations should objectively evaluate their capability to deploy, support and optimise modern workplace technologies and react quickly to changing conditions. External providers may bring additional costs but the benefits in terms of operational efficiencies, reduced risk, greater flexibility and enhanced employee experience can make a compelling business case.

An experienced external provider can free up internal resources to focus on their core functions, help to avoid false starts and significantly speed up project delivery, enabling the benefits of digital workplace projects to be realised more quickly. They can also offer greater flexibility to scale resources to cope with unexpected surges in demand.

01 REMOTE & HYBRID WORKING ARE THE NEW REALITY

The rapid adoption of remote working practices during the Covid-19 pandemic, and the positive results in terms of productivity, have proven to organisations that a remote or hybrid digital workplace is the most likely model of future work. This seems like a win-win situation. Employees are increasingly demanding work-from-home options as they enjoy the benefits of less commuting time, lower travel costs and increased flexibility. Organisations are enticed by the advantages of more satisfied employees and lower real estate costs.

However, this brave new world of work must be underpinned by the right technology, and our survey found that current solutions need to be adapted to provide the necessary levels of resilience, security and manageability to support the future digital workplace.

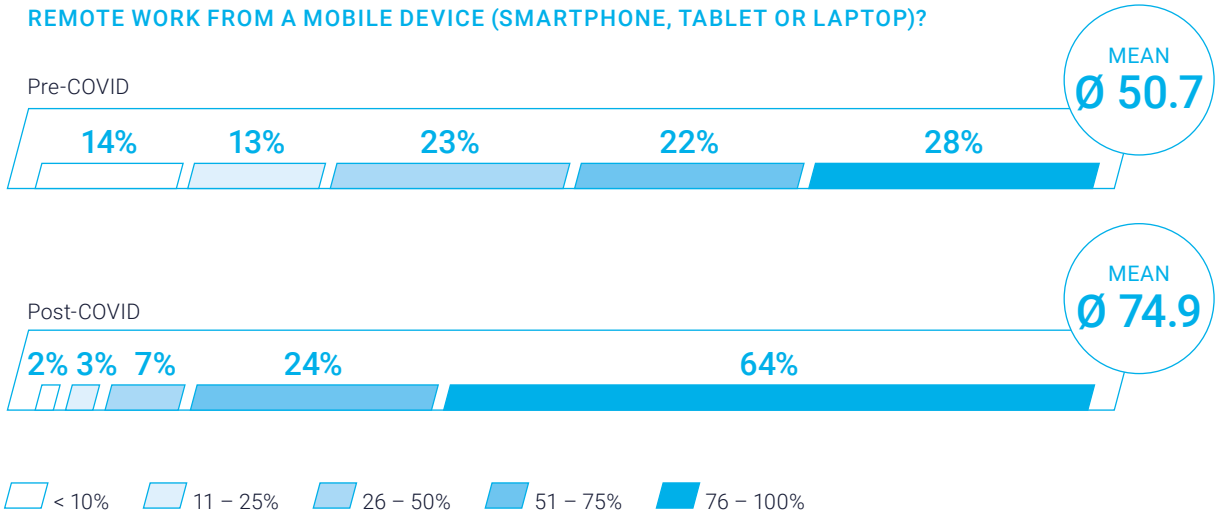
THE DIGITAL WORKPLACE IS NOW A STRATEGIC PRIORITY

Unsurprisingly, our survey shows that there has been a sharp upward trend in the adoption of remote working, driven by Covid-19. Pre-pandemic, on average, only half of organisations surveyed were able to work remotely. This increased to 75% post-pandemic.

Furthermore, the proportion of organisations surveyed who enabled more than three-quarters of their employees to work remotely increased from just 28% pre-pandemic, to 64% post-pandemic.

Amount of workforce capable of remote working – Pre- and Post-Covid

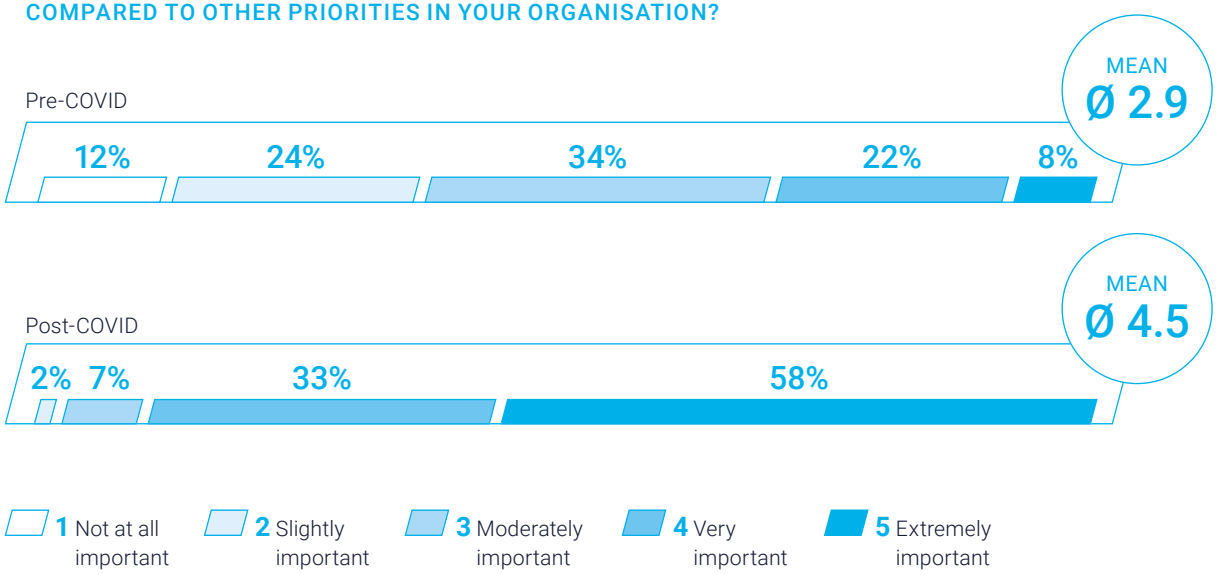
WHAT PERCENTAGE OF YOUR ORGANISATION'S WORKFORCE WAS/IS CAPABLE OF REMOTE WORK FROM A MOBILE DEVICE (SMARTPHONE, TABLET OR LAPTOP)?



BASIS: ALL RESPONDENTS

Comparison of remote working importance – Pre- and Post-Covid

HOW IMPORTANT WAS/IS THE ADOPTION OF REMOTE WORKING TECHNOLOGIES COMPARED TO OTHER PRIORITIES IN YOUR ORGANISATION?



BASIS: ALL RESPONDENTS

This has pushed remote working and the digital workplace firmly up the strategic agenda. Prior to Covid-19, only 30% of respondents rated the adoption of remote work technologies as very or extremely important. Post-Covid-19, this has risen to 91%.

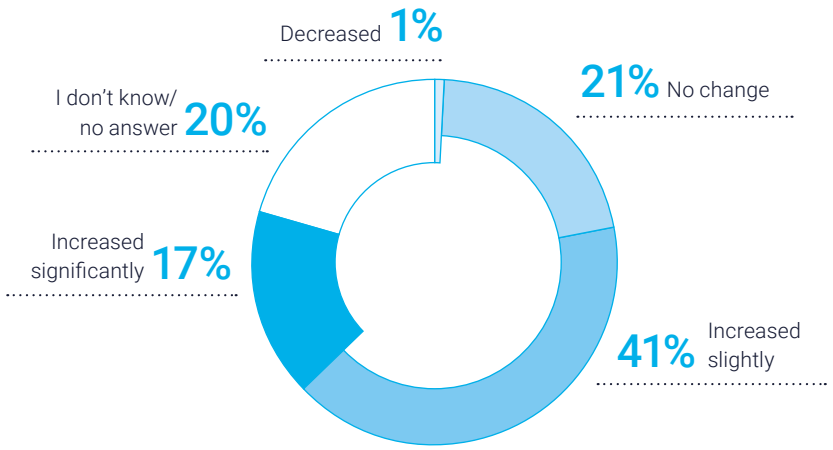
HAVING A DIGITAL WORKPLACE STRATEGY PAYS DIVIDENDS

Adapting to a remote working model has required some increased investment in technology for the majority of organisations. 58% of respondents reported either a slight or significant increase in technology spend.

However, those respondents who already had a digital strategy in place were much less likely to have seen an increase in spend (51%) than those with no digital strategy in place (72%). This suggests that those with a clear strategy were better prepared to cope with the changes required to support a rapid adoption of remote working.

Remote Work Spending since COVID

HOW HAS YOUR ORGANISATION'S SPEND ON ENABLING AND ENHANCING REMOTE WORKING CAPABILITIES CHANGED SINCE COVID 19?



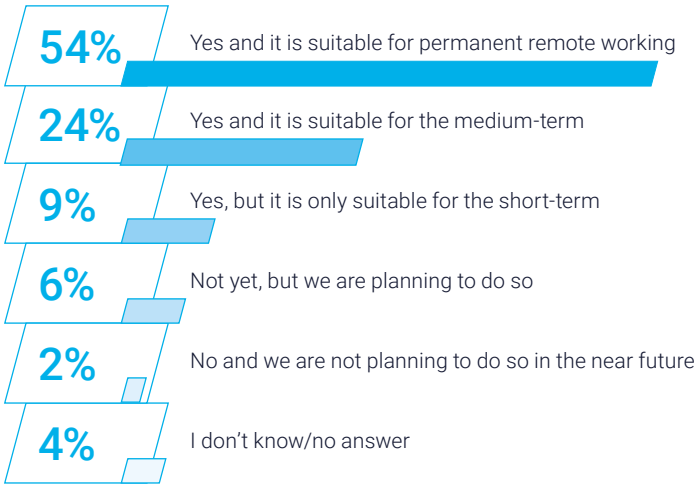
BASIS: ALL RESPONDENTS

DIGITAL WORKPLACE TECHNOLOGY NEEDS TO CATCH UP

Remote working adoption has increased significantly and quickly but almost half of respondents (46%) indicated that their current solution is not suitable for long-term or permanent remote or hybrid working. It is clear that further investment will be required in this area in the next 12 months.

Remote working adoption suitability

HAS YOUR ORGANISATION ADOPTED REMOTE WORKING OR HOME WORKING AS PART OF YOUR DIGITAL WORKPLACE STRATEGY?



BASIS: ALL RESPONDENTS

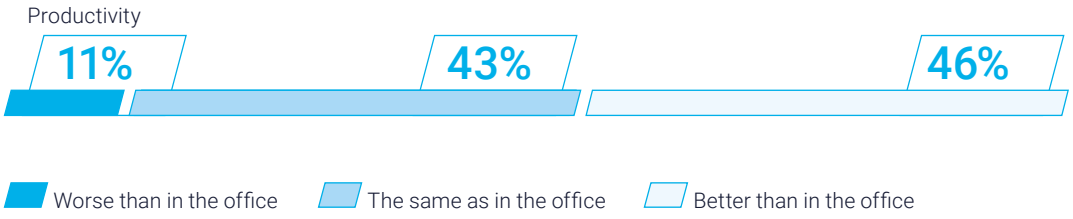
THE REMOTE WORKING GENIE IS OUT OF THE BOTTLE

The overwhelming experience of our respondents during Covid-19 is that a decentralised workplace is not only possible, but in many cases more productive than the traditional office-based model. A staggering 89% of respondents say their productivity when working remotely is either higher than, or the same as, when working in the office. Almost half of all respondents (46%) claim to be more productive.

While a small minority of respondents (11%) experienced a drop in productivity, it is clear that organisations can no longer cite broad productivity concerns as a barrier to making flexible working options available to their employees.

Comparison of remote working to office working

HOW WOULD YOU RATE THE FOLLOWING ELEMENTS OF WORKING REMOTELY COMPARED TO WORKING WITHIN THE OFFICE?



BASIS: ALL RESPONDENTS

OUR RECOMMENDATIONS

Our survey shows that a majority of organisations have enabled most of their workforce to work from home. The technology solutions that facilitated this were, in many cases, deployed in short order with limited time for planning. We recommend organisations should invest now to future-proof their digital workplace technology and provide a satisfactory employee experience by:

ORGANISATIONS SHOULD

- Identifying user personas to understand where and how employees in different roles will want or need to work in the future
- Optimising the technology stack for each identified persona type
- Investing in upgrading or replacing technologies that are not suitable for the medium-to-long-term
- Considering work-from-anywhere capability, rather than just work-from-home capability, to support future hybrid work models

The workplace – no matter where it is located – must offer a consistent positive experience to be able to provide high levels of employee satisfaction, motivation and productivity.

02 THERE IS A FALSE SENSE OF SECURITY

A decentralised workforce and remote working practices create an attractive target for cyber criminals. The use of personal devices, a lack of privacy and the use of new, unfamiliar technology all provide fertile ground for those looking to profit from cybercrime. The volume and sophistication of cyber threats continues to grow, exacerbated by human errors, typically caused by lack of awareness or training.

In the face of these risks to valuable or sensitive data, organisations seem confident in their security posture. However, our survey shows that this confidence is not supported by the facts, with a surprisingly high number of respondents failing to take advantage of modern security tools and practices.

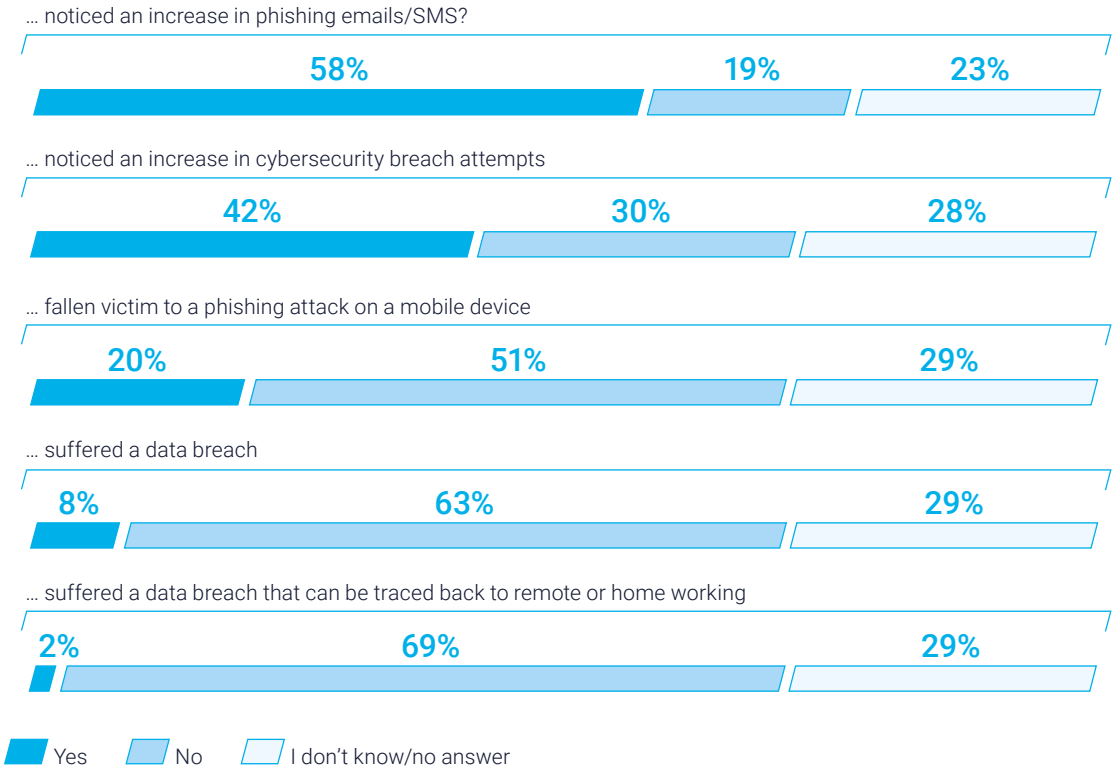
PHISHING ATTACKS, HUMAN ERROR AND RANSOMWARE ARE THE BIGGEST SECURITY CONCERNS

Almost 60% of organisations surveyed have seen an increase in phishing emails or SMS messages in the last 12 months, and one in five organisations has fallen victim to a phishing attack. These numbers may be even higher, as between 23% and 29% of businesses could not or would not say whether they had seen instances of threats increasing. If an attack remains undetected, sensitive data is at an even greater risk because countermeasures are taken far too late, or not taken at all.

Phishing (71%), human error (56%) and ransomware (47%) are seen as the top three IT security threats by businesses in the next 12 months. These concerns are linked. For example, phishing attacks are becoming more sophisticated and more difficult for employees to detect. This is particularly prevalent on mobile devices where the user is working on a smaller screen, may be distracted or multi-tasking, and where URL links and email addresses cannot be verified as easily as on larger format laptops or desktops.

Data security problems in the last twelve months

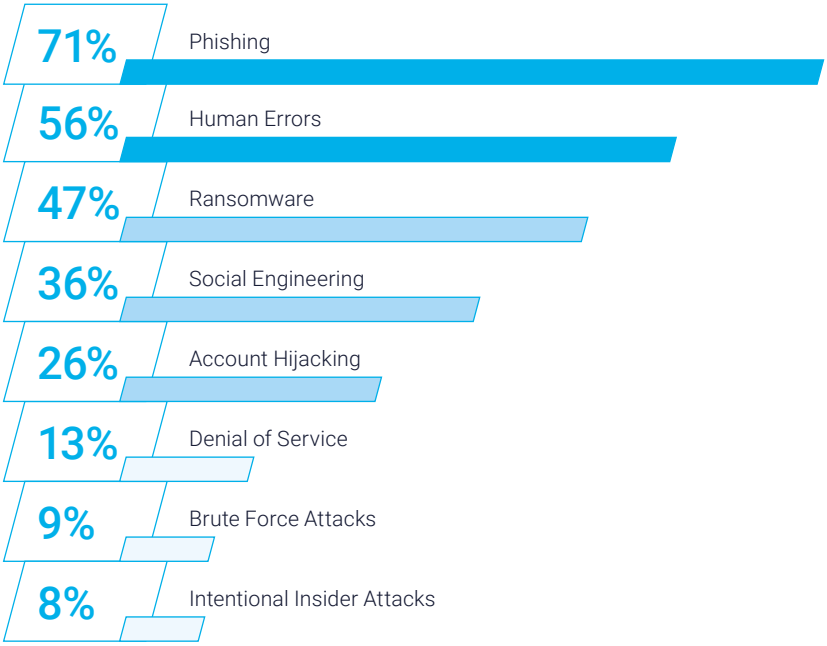
IN THE LAST 12 MONTHS, HAS YOUR ORGANISATION…



BASIS: ALL RESPONDENTS

Security threats in the next 12 months

WHAT DO YOU BELIEVE ARE THE TOP 3 IT SECURITY THREATS FOR YOUR ORGANISATION OVER THE NEXT 12 MONTHS?



BASIS: ALL RESPONDENTS; MULTIPLE ANSWERS POSSIBLE

MANY ORGANISATIONS LACK BASIC, IMPORTANT SECURITY MEASURES

Against a backdrop of growing and evolving cybersecurity threats, it is clear that organisations need to review the adequacy of their security measures for remote and hybrid working and do more to protect their data and assist their employees in thwarting potential cyber attacks. However, our survey shows that many organisations lack important security measures.

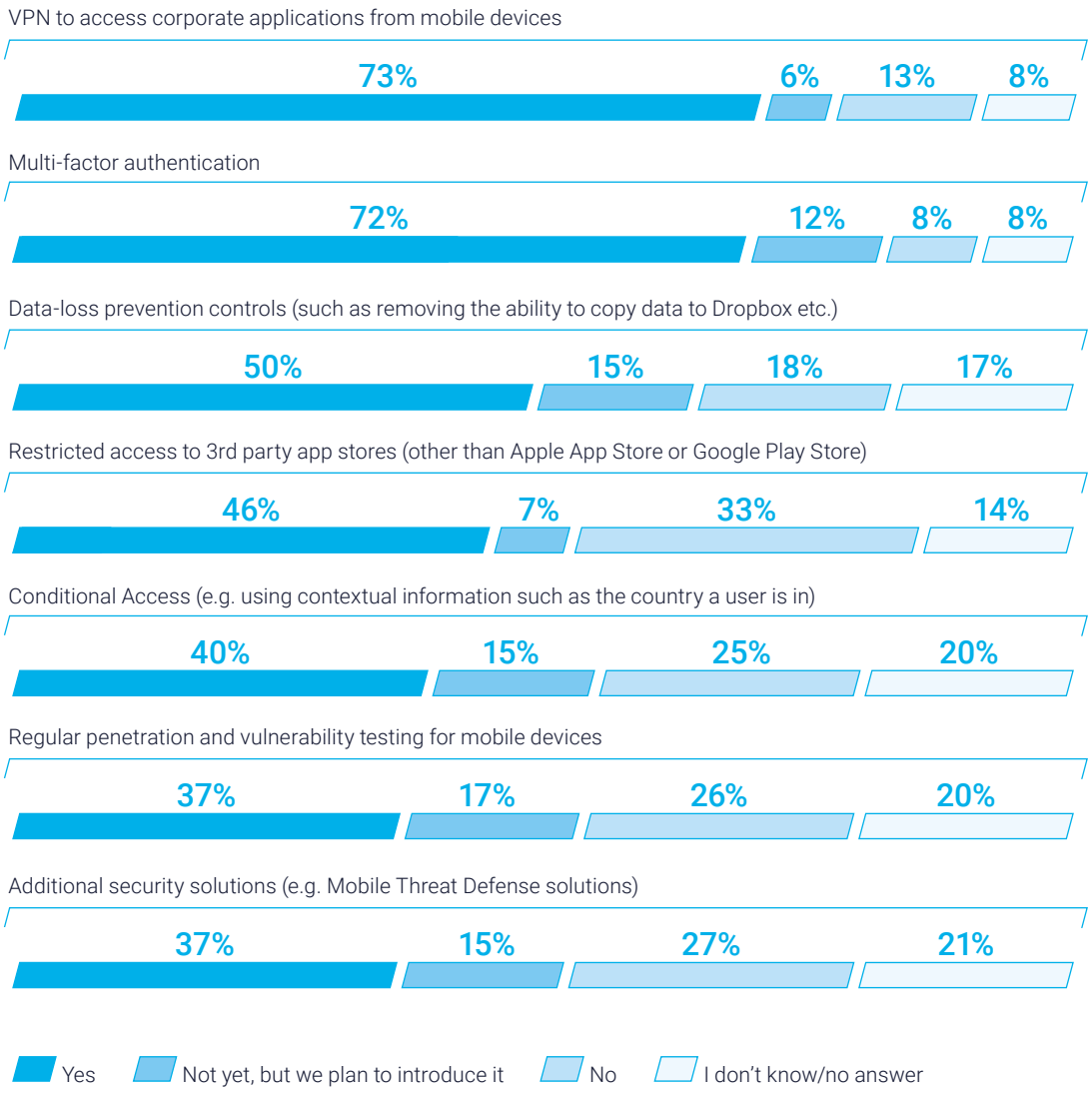
- Just over one-third (37%) of organisations have a mobile threat defence solution in place, despite phishing being considered the most serious threat over the coming year. Only the same percentage of respondents perform regular penetration and vulnerability testing for mobile devices
- More than half of respondents (58%) allow the use of third-party app stores (other than the Apple Store or Google Play Store), a common way for malicious applications to be downloaded onto devices
- One in two organisations do not have Data Loss Prevention (DLP) controls in place to prevent corporate data from being copied from emails or applications into personal file-sharing services such as Dropbox or Google Drive
- The situation is better, but still far from adequate, when it comes to basic security

measures such as the use of Virtual Private Networks (VPNs) or Multi-Factor Authentication which are still not used by one in five respondents.

Of those organisations which have, or plan to introduce, a Unified Endpoint Management (UEM) solution, just over one-third (35%) do not use the solution's advanced mobile security and data protection features, which represents a missed opportunity to improve security.

Security measures for devices

IN TERMS OF SECURITY MEASURES FOR DEVICES USED FOR REMOTE WORKING WHICH OF THE FOLLOWING ARE IN PLACE IN YOUR ORGANISATION:



BASIS: ALL RESPONDENTS

TOO LITTLE IS BEING DONE FOR EMPLOYEE AWARENESS

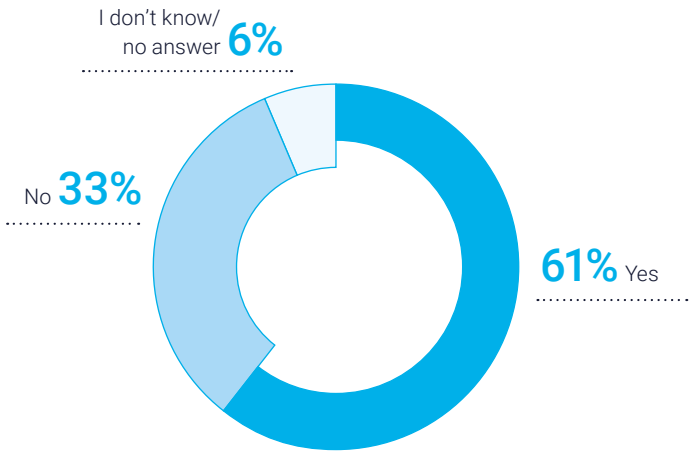
Human error was identified as the second-biggest anticipated cyber threat in the coming 12 months, and employee awareness is an important factor in averting potential security threats, particularly in relation to phishing and social engineering. Yet, worryingly, one-third (33%) of organisations have not provided any kind of mobile security awareness training to employees.

CONFIDENCE IN SECURITY IS MISPLACED

Our survey showed that respondents' confidence in their data security is high, with almost three-quarters (73%) either very confident, or fairly confident, in their ability to secure corporate data on remote or mobile devices. However, our survey suggests this confidence may be misplaced.

Security awareness training

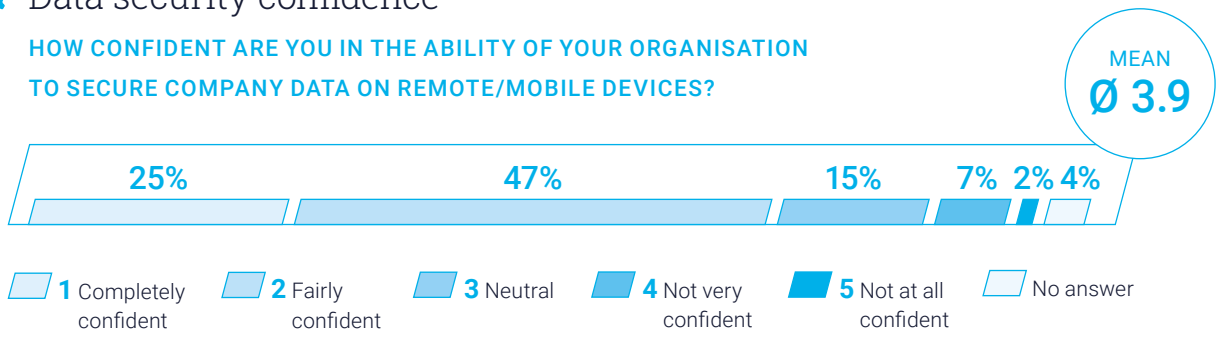
HAS MOBILE SECURITY AWARENESS TRAINING BEEN DELIVERED IN YOUR ORGANISATION?



BASIS: ALL RESPONDENTS

Data security confidence

HOW CONFIDENT ARE YOU IN THE ABILITY OF YOUR ORGANISATION TO SECURE COMPANY DATA ON REMOTE/MOBILE DEVICES?



BASIS: ALL RESPONDENTS

OUR RECOMMENDATIONS

Our survey shows that there are still different security standards, and security technologies, for different device types, with security teams typically applying less stringent controls on mobile devices than either laptop or desktop devices. Cyberattacks – especially phishing attacks – are steadily increasing and becoming more professional. The rapid implementation of widespread remote working practices due to Covid-19 has opened up new vulnerabilities. Companies are not doing enough to protect their data in terms of both the application of security technology and raising employee awareness on security issues.

ORGANISATIONS SHOULD

- Adopt Zero Trust security principles wherever possible, supported by clear policies on who, when, how and with which device corporate data and applications can be accessed
- Introduce clear separation between business data and private data, with sufficient security standards for business data and privacy policies for private data
- Use an integrated tool (ideally a UEM platform) to centrally manage and secure all endpoints and ensure that devices are configured to comply with security policies, that secure apps and software updates are deployed, and that corporate data can be wiped from devices when necessary
- Use Virtual Private Networks (VPNs) to ensure that data exchanged between employee devices and the organisation's network is encrypted and secure
- Adopt security technologies that detect and identify risks before they cause damage. For example, technology to detect phishing attacks or malicious apps, or to protect digital identities, could significantly reduce the risk posed by careless employee behaviour
- Educate employees through regular, mandatory information security awareness training and exercises such as simulated phishing attacks to inform them on best practice and help them to identify and report potential security incidents.

Security does not need to be a barrier to positive user experience. In fact, modern security can enhance the employee experience, providing a robust security posture to support future hybrid and remote working models.

03 EMPLOYEE EXPERIENCE IS PARAMOUNT

It is critical that your digital workplace is secure, but to be effective, it must also be user-friendly. If processes such as authenticating into accounts, accessing data and applications, or commissioning new devices are too complex, employee satisfaction and productivity drops and IT workload increases.

The business case for providing a great employee experience is straightforward; it leads to more engaged, productive and loyal employees. Technology can play a key role in enhancing employee experience and is generally viewed positively, but our survey suggests that businesses can and should do even more in this area.

EMPLOYEE EXPERIENCE AND PRODUCTIVITY ARE DRIVING STRATEGY

For the organisations surveyed who have implemented, or plan to implement, a remote working strategy, employee-related objectives were the key drivers. Both employee experience and employee productivity were rated as one of the top three factors driving a remote working strategy by 81% of respondents, well ahead of the next most important factor (cybersecurity, 38%).

However, when it comes to future investment, the focus is on improving security, with almost double the number of respondents ranking this as their number one spending area vs either employee experience or productivity.

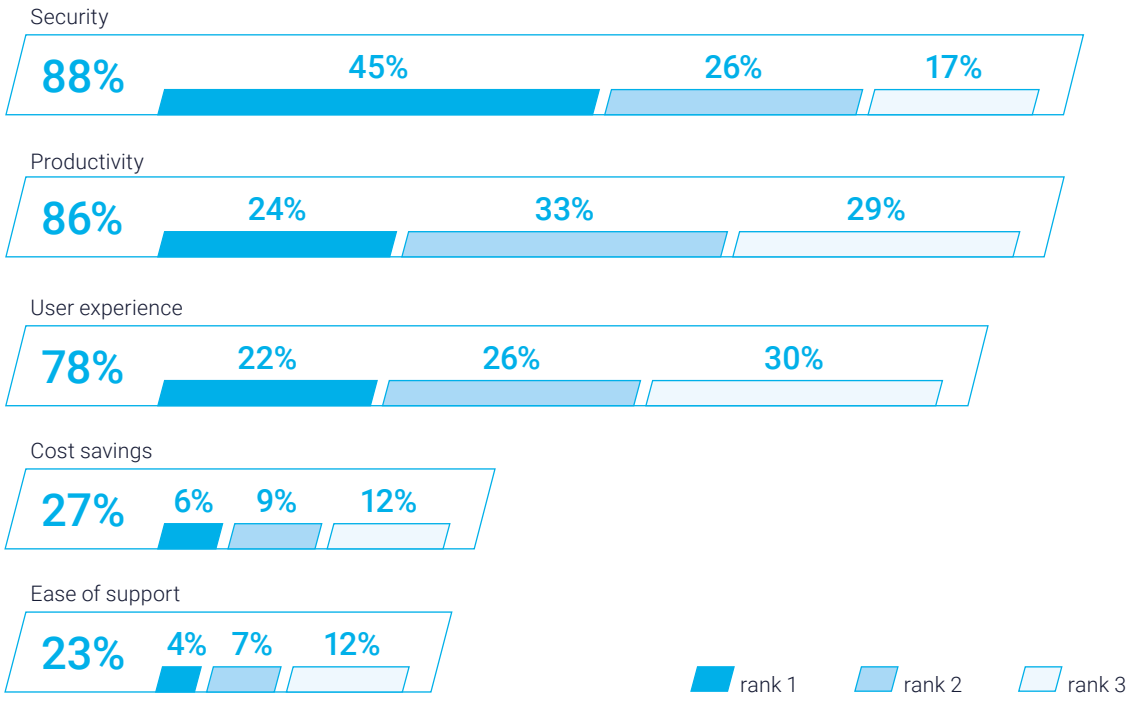
Driving factors for working strategy

CHOOSE THE THREE MOST IMPORTANT FACTORS DRIVING YOUR ORGANISATION'S DIGITAL WORKPLACE/REMOTE WORKING STRATEGY.

BASIS: IF REMOTE WORKING STRATEGY IMPLEMENTED OR PLANNED; MULTIPLE ANSWERS POSSIBLE

Ranking of future priorities for remote working

PLEASE RANK THE FOLLOWING FACTORS IN ORDER OF IMPORTANCE WHEN IT COMES TO YOUR DIGITAL WORKPLACE/REMOTE WORKING STRATEGY OVER THE NEXT 12 MONTHS – STARTING WITH THE MOST IMPORTANT ONE?



BASIS: ALL RESPONDENTS

LEVELS OF SATISFACTION WITH REMOTE WORKING TECHNOLOGY ARE GENERALLY HIGH

The vast majority of respondents (between 76% and 89%) are either satisfied or very satisfied with the Possibility of remote working.

THE REMOTE WORKING EXPERIENCE IS NOT HOMOGENEOUS

Our survey shows that not everyone has the same user experience while working remotely and some elements of the remote working environment are difficult for the organisation to control. For example, almost half of respondents (48%) experienced connectivity and broadband problems, while a similar percentage (44%) reported user experience issues. These issues can lead to lost productivity and frustration with remote working.

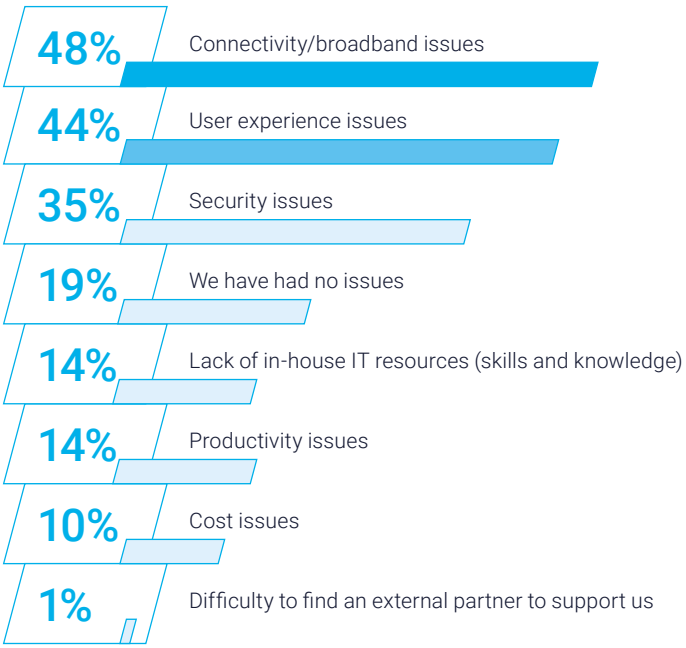
TECHNOLOGY THAT ENHANCES EMPLOYEE EXPERIENCE IS UNDER-UTILISED

Almost half (43%) of organisations that have implemented a Unified Endpoint Management system, or are planning to do so, do not use its device lifecycle management features. These enable devices for new employees to be accessed and configured in a few simple clicks, saving the employee time and reducing the workload for the IT team. With distributed teams working in different locations, this is increasingly important.

Furthermore, almost half of organisations (40%) have not adopted conditional access policies. These can provide simpler authentication for employees by taking into account additional contextual security information (such as the device being used or the location the employee is in). When combined with Single Sign-On this technology, is a good example of how security and usability can be achieved at the same time.

Challenges to adopting remote working

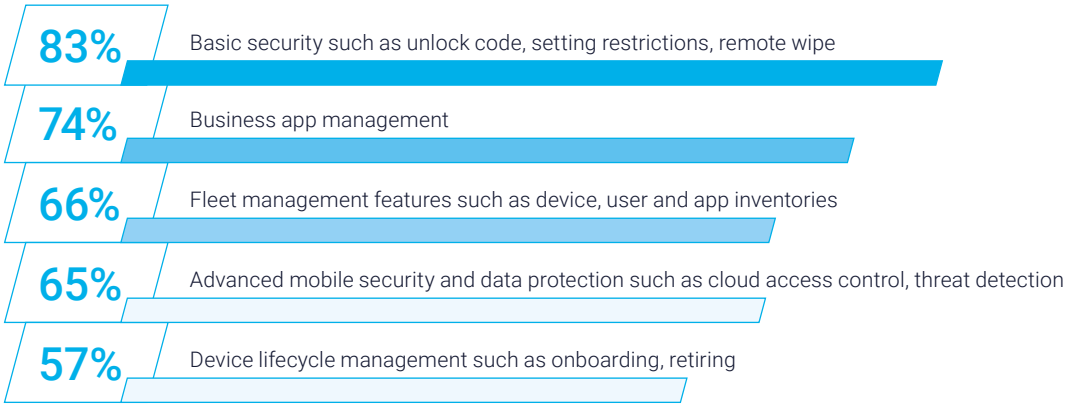
WHAT HAVE BEEN THE THREE BIGGEST CHALLENGES YOU HAVE FACED WHEN ADOPTING REMOTE WORKING OR HOME WORKING AS PART OF YOUR DIGITAL WORKPLACE STRATEGY?



BASIS: IF REMOTE WORKING ADOPTED; MULTIPLE ANSWERS POSSIBLE

UEM feature usage

WHICH OF THE FOLLOWING UEM FEATURES DOES/WILL YOUR ORGANISATION USE SELECT ALL THAT APPLY?



BASIS: IF USING OR PLANNING TO USE A UEM; MULTIPLE ANSWERS POSSIBLE

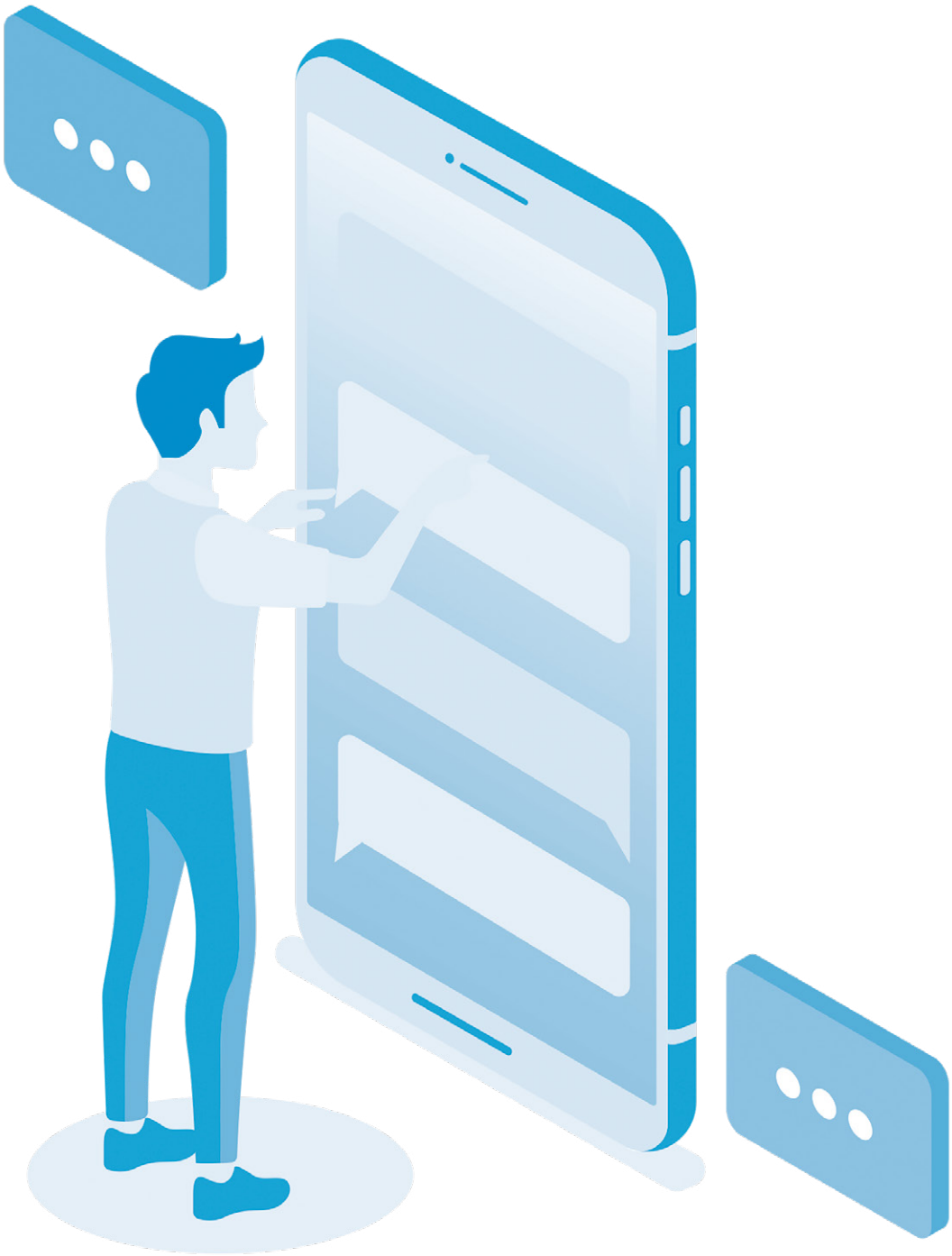
OUR RECOMMENDATIONS

Employee experience and productivity are clearly the key strategic drivers of digital workplace and remote working initiatives. However, organisations are not exploiting the full potential of existing technologies to further enhance the employee experience. While they are planning on investing in employee experience in the coming 12 months, the investment level is significantly behind that for security. As remote and hybrid working is likely to become a permanent part of many business models, the digital workplace must be high up the strategic agenda and receive more visibility and attention at board level.

WE RECOMMEND THAT ORGANISATIONS SHOULD:

- Introduce Key Performance Indicators (KPIs) for employee experience at board level, for example, an Employee Net Promoter Score
- Appoint a cross-functional C-level leader, perhaps a Chief Employee Experience Officer (CEEO) to take a holistic approach
- Invest in and implement employee experience-centred technologies such as conditional access for secure and user-friendly authentication, solutions that stabilise network connections or reduce bandwidth demands, and device enrolment programmes to simplify the rollout process of devices
- Adopt a persona-based approach to device choice, matching the demands and activities of an employee's role with the right technology

A truly digital workplace must strike a balance of being both secure and user-friendly.



04 EXISTING TECHNOLOGY CAN WORK HARDER

The ability to manage and secure employee devices, wherever they are, is fundamental to any IT strategy and never more so than in today's work-from-anywhere world.

The evolution of device management tools from Mobile Device Management (MDM) to Enterprise Mobility Management (EMM) and now to Unified Endpoint Management (UEM), has provided organisations with the capability to manage mobile devices, tablets, laptops, desktops, rugged devices and even wearables through one single platform.

Our survey showed that the majority of respondents have a UEM platform in place, but that many organisations are not using these tools to anywhere near their full capability. As a result, organisations are missing out on the associated security and management benefits and delivering sub-optimal return on investment.

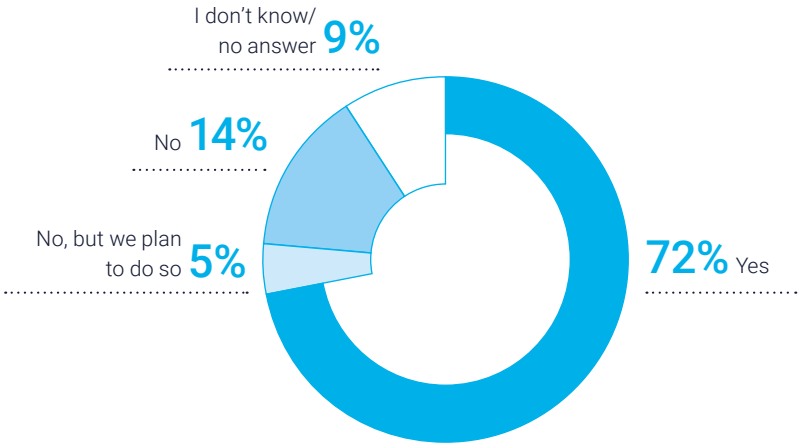
THERE IS A GULF IN UNIFIED ENDPOINT MANAGEMENT (UEM) ADOPTION

77% of organisations have adopted or plan to adopt UEM. However, there is a clear gulf between larger, more mature organisations (where adoption is at 85%) and smaller businesses (where fewer than half of organisations with less than 100 employees, and only two-thirds of organisations with between 100 and 1,000 employees, have adopted a UEM solution).

Organisations without UEM have significant "blind spots", no visibility of device compliance status and no capability to apply even basic security controls to devices. They are likely to face major challenges in enabling meaningful digital transformation and effective remote working.

UEM system usage

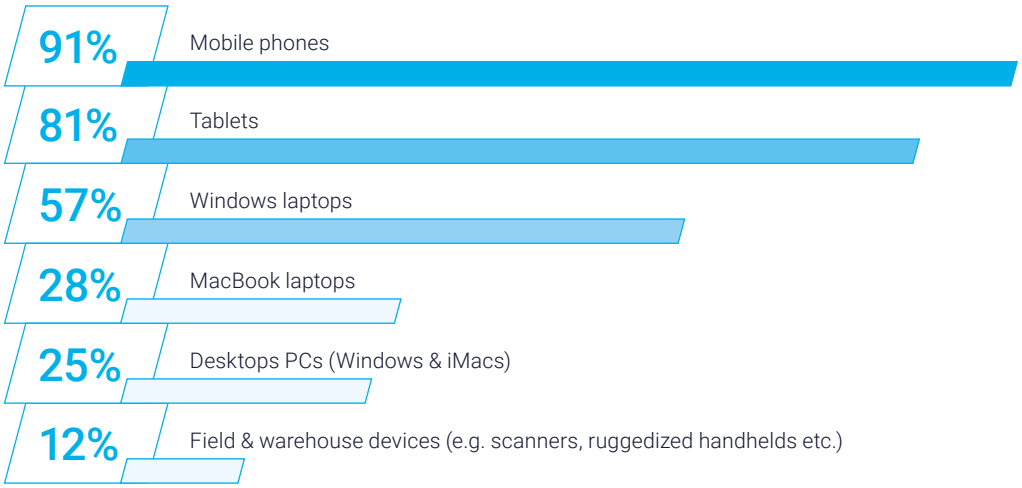
DOES YOUR ORGANISATION USE A UNIFIED ENDPOINT MANAGEMENT (UEM) SYSTEM SUCH AS MOBILEIRON, MICROSOFT INTUNE, VMWARE WORKSPACE ONE, JAMF?



BASIS: ALL RESPONDENTS

UEM application

WHICH DEVICES DOES/WILL YOUR ORGANISATION MANAGE USING YOUR UEM PLATFORM(S) SELECT ALL THAT APPLY?



BASIS: IF USING OR PLANNING TO USE A UEM; MULTIPLE ANSWERS POSSIBLE

ORGANISATIONS ARE NOT MAXIMISING RETURN ON UEM INVESTMENT

Of those organisations that have deployed a UEM platform, most limit its use to smartphones and tablet devices and are not taking advantage of using a single platform to manage a much wider range of devices – including laptops, desktops, rugged handhelds and even wearables – across a wide range of operating systems.

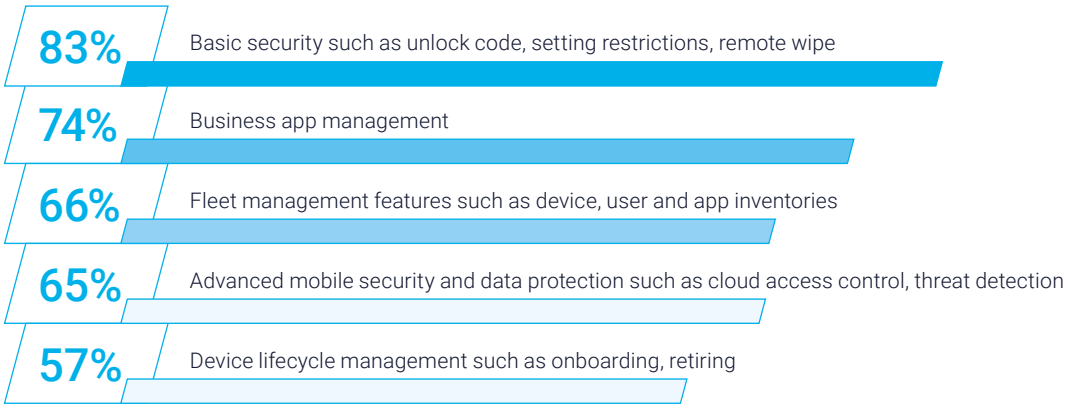
Only 57% currently use their UEM to manage Windows laptop devices, 28% to manage MacBooks, and only 25% use the system to manage desktop devices.

In addition, many advanced features available within UEM solutions remain unused. Only 65% of respondents with a UEM solution are using advanced security and data protection features such as cloud access control, encrypted containers, threat detection multi-factor authentication and conditional access, to help to ensure that company data is well-protected in the face of ever-growing security threats.

Only 57% of organisations are using device lifecycle management features such as on-boarding and retiring. Effective device lifecycle management can significantly streamline these activities, resulting in lower IT overheads, increased employee productivity and an enhanced user experience.

UEM feature usage

WHICH OF THE FOLLOWING UEM FEATURES DOES/WILL YOUR ORGANISATION USE SELECT ALL THAT APPLY?



BASIS: IF USING OR PLANNING TO USE A UEM; MULTIPLE ANSWERS POSSIBLE

BRING YOUR OWN DEVICE MODELS ARE NOT POPULAR

Corporate ownership models are still heavily preferred and personal enablement of corporate devices is now the norm (COPE). Just 36% of organisations have adopted a Bring Your Own Device (BYOD) model, where employees use their own device in the course of their work duties.

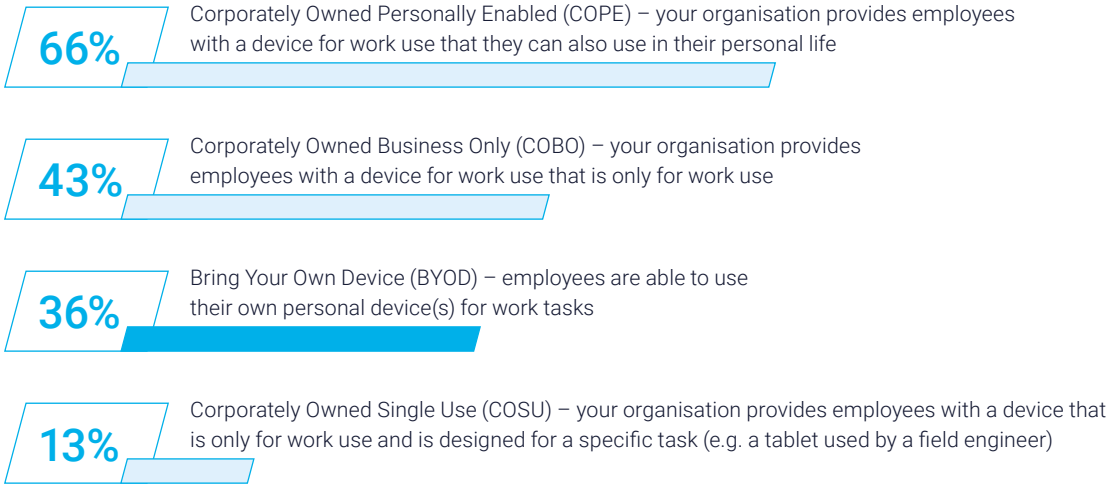
Benefits of a BYOD approach include attractive cost savings to businesses, due to the need for fewer purchased corporate devices, and an enhanced user experience, due to the familiarity of the device to the employee and the need to only carry one device.

However, these benefits appear to be more than offset by the perceived challenges posed by a BYOD strategy, including the security of corporate data, the privacy of employees and the ability of organisations to support a wide range of devices.

Most Unified Endpoint Management and mobile security solutions now enable the effective separation, management and security of corporate data and applications from personal data and applications without compromising employee privacy. However, these do not appear to be well understood or utilised.

Device ownership strategy

WHAT DEVICE OWNERSHIP MODELS DOES YOUR ORGANISATION USE FOR SMARTPHONES, TABLETS AND LAPTOPS?



BASIS: ALL RESPONDENTS; MULTIPLE ANSWERS POSSIBLE

DEVICE SELECTION SHOULD NOT BE ONE-SIZE-FITS-ALL

Fewer than half (42%) of organisations are using a needs-based or persona-based approach to corporate device selection, with almost one third of organisations adopting a "one-size-fits-all" strategy.

A single device strategy can seem attractive from a management and support perspective, and may be the right approach in a highly homogenous environment. However, in a typical mixed use-case environment, any benefit from streamlined device support will be more than outweighed by negative impacts including reduced productivity and a poor employee experience.

Additionally, device costs may actually be increased as a "highest common denominator" effect means that higher specification devices are provided to employees whose role may only require more basic capability.

OUR RECOMMENDATIONS

Our survey shows that true UEM integration is happening, but only slowly. Organisations are not using existing tools to their full capability although the need for the right technology to support hybrid working models has been pushed up the strategic agenda by Covid-19.

WE URGE ORGANISATIONS TO

- Adopt UEM technology if they have not already done so. Cloud-based, SaaS options offer consumption-based license models with full support and limited upfront costs, making UEM affordable for even smaller businesses
- Perform a "health check" of existing UEM technology to identify quick-win areas for immediate improvement, including opportunities to manage more device types or activate additional features
- Create a three-year UEM adoption strategy to benefit from simplified management and security of multiple device types through a single pane of glass. A supporting business case can be made using reduced operating and support costs, reduced security risk, savings on the replacement of point software solutions and enhanced employee experience
- Consider a Bring Your Own Device (BYOD) model. Modern UEM solutions and mobile operating systems offer viable options to secure and manage corporate data on personal devices and can lead to significantly reduced device costs in the right use cases
- Adopt a persona-based approach to identify the right device types for employees, taking into consideration role-based use cases, work location, connectivity requirements, longevity and lifecycle management
- Actively manage, or use a knowledgeable third-party provider to manage, your UEM platform to ensure continued alignment with business objectives and consistent return on investment

05 REMOTE AND HYBRID WORKING REQUIRES A CHANGE IN IT MINDSET

The sudden move to remote working resulting from Covid-19 required a rapid change of approach for employees but it also created significant workload and ongoing challenges for IT teams. Delivering a best-in-class digital workplace and an excellent employee experience requires strategic planning, in-depth know-how, sufficient resources, the right technologies, and investment.

In addition, constant adaptation and reaction to new developments and requirements are necessary. Companies must put in place the right foundations of skills and capability to be able to react quickly and be flexible enough to successfully shape the digital workplace today and in the future.

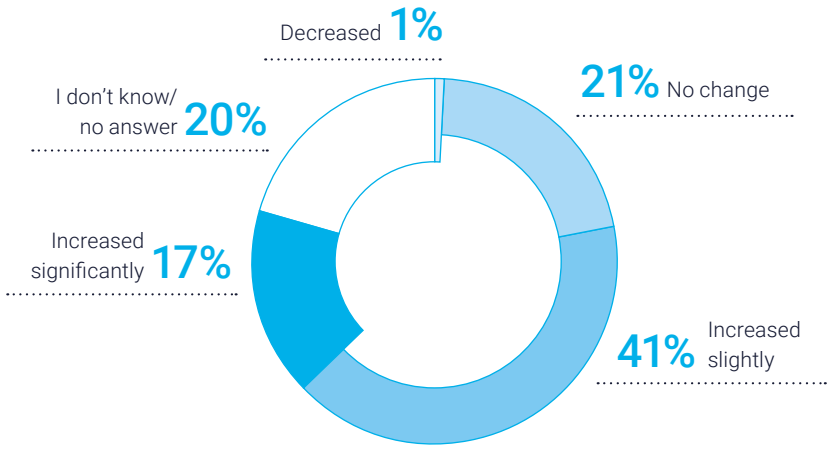
LACK OF CLEAR STRATEGY RESULTS IN MORE UNPLANNED IT INVESTMENT

Overall, 58% of the organisations surveyed needed to increase IT spending to create or improve remote working capabilities during the pandemic, with just under one-fifth (17%) needing to do so significantly.

More organisations without a digital working strategy required unplanned investment than those with a strategy already in place. Almost three-quarters (72%) of those without a strategy required additional unplanned investment, compared to just over half (51%) of those with a strategy in place.

Remote Work Spending since COVID

HOW HAS YOUR ORGANISATION'S SPEND ON ENABLING AND ENHANCING REMOTE WORKING CAPABILITIES CHANGED SINCE COVID 19?



BASIS: ALL RESPONDENTS

Support resources for remote working

WHO MANAGES SUPPORT FOR DIGITAL WORKPLACE AND REMOTE WORKING TOOLS WITHIN YOUR ORGANISATION SELECT ALL THAT APPLY?

BASIS: ALL RESPONDENTS; MULTIPLE ANSWERS POSSIBLE

ORGANISATIONS ARE TOO RELIANT ON INTERNAL SKILLS

The rapid shift to supporting a remote working model, the scale at which UEM solutions, devices and operating systems are evolving, and the wealth of features available all place strain on IT services. However, only one in three (34%) of the organisations surveyed use external providers to help manage digital workplace tools.

The internal skills gap is a key reason why organisations fail to optimise the technology stack for remote and hybrid working and goes some way to explaining why the more advanced features of digital workplace technologies are not more widely utilised.

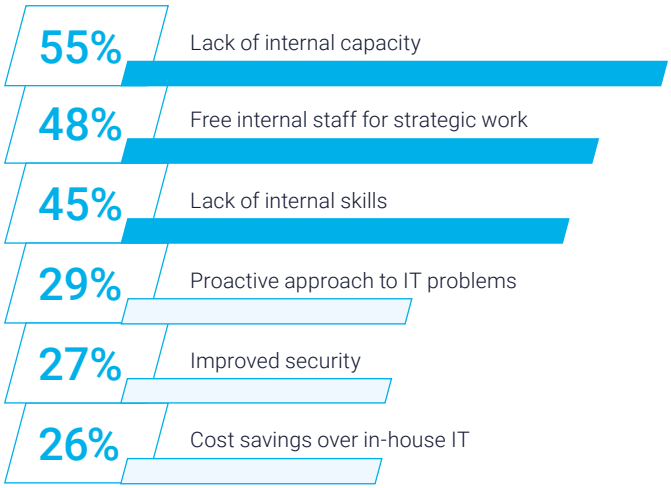
CAPABILITY AND CAPACITY ARE THE CATALYSTS FOR USING EXTERNAL PROVIDERS

55% of those respondents who do enlist the help of external IT service providers are doing so because they lack the internal capacity for handling remote working, 48% want to free their employees for strategic work, and 45% lack the necessary knowledge. 29% see it as a proactive approach to IT problems.

A lack of sufficient capacity can result in a “keep the lights on” mentality within overworked IT teams who think only tactically, look for shortcuts and can be slow to respond to changing conditions.

External provider justification

PLEASE LIST YOUR ORGANISATION'S TOP 3 REASONS FOR USING AN IT SERVICE PROVIDER.



BASIS: IF USE OF AN EXTERNAL PARTNER; MULTIPLE ANSWERS POSSIBLE

OUR RECOMMENDATIONS

Our survey highlights that almost half (46%) of respondents do not have a digital workplace that is suitable for the long-term. Now is the time for organisations to take stock.

SPECIFICALLY, WE RECOMMEND THAT ORGANISATIONS

- Develop a digital workplace technology roadmap to support the organisation's strategy, aided by business cases focusing on employee experience and operational efficiency.
- Objectively evaluate their internal capability and capacity to plan deploy, support and continually optimise modern workplace technologies for the future.
- Source and engage knowledgeable, certified and proven external partners to supplement in areas where capability gaps are identified. This enables organisations to replace fixed labour costs with variable external costs on a pay-per-use basis.
- Consider managed service options for digital workplace technologies, which can help reduce total cost to operate by removing the need for hiring, training and retention activities.

In an age of IT skills shortages, organisations should consider building longer-term relationships with external providers. The right partner can provide additional capacity, increase flexibility, reduce risk and enable rapid responses to unexpected changes in conditions and if this past year has taught us anything it is to expect the unexpected.

HOW THE EMEA CAN HELP

The Enterprise Mobility Expert Alliance (EMEA) is the largest group of mobility experts in Europe, with a clear focus on the management and security of the devices, operating systems, applications and connectivity that make up the mobile ecosystem.

Our members are specialists in modern, mobile technology including strategy, security, software development, solution design and build, managed deployments, support and managed services.

EMEA members share resources, market intelligence, best-practice and research and development, and have aligned our service offerings to enable pan-European 24/7 support with experts on call to support a range of leading modern management and security software solutions.

We believe that work is an activity, not a place, and our members are trusted by some of Europe's largest brands and government organisations to deliver digital workplace solutions that provide best-in-class employee experience without sacrificing security, compliance or privacy.

CONTACT

Find out more about how the EMEA can help you take the next step on your digital workplace journey at **HTTPS://EMEA.MOBI/**

Or contact your nearest member organisation directly.

ADJUNGO

contact@adjungo.fr
+33 805 69 04 32
adjungo.fr

BLAUD B.V.

hello@blaud.com
+31 88 030 9000
blaud.com

CWSI

info@cwsi.ie
+353 1 2932 500
cwsisecurity.com

EBF-EDV BERATUNG FÖLLMER GMBH

info@ebf.com
+49 221 47455 0
ebf.com

MOBCO

sales@mob.co
+32 2 6699 500
mob.co

NOMASIS AG

sales@nomasis.ch
+41 43 377 66 55
info@nomasis.ch

emea.mobi

adjungo
managed mobility services

BLAUD

CWSI

EBF

mobco
we mobilize your business

nomasis
secures your mobility