The case for supporting mobile users with secure remote access

Your employees are mobile and your remote support strategy needs to be too - but manage the security risks of remote access tools. A study of IT support strategies across UK, Germany and France.

INTRODUCTION

Ovum view

Employees are increasingly mobile, whether IT wants them to be or not. Even when they are not officially allowed to use certain devices, bring your own device (BYOD) and employees' expectations that applications will be available to them on whatever screen they choose creates a highly complex new set of support and security challenges for IT.

Multiplatform device management and application management is helping IT solve the platform fragmentation and policy administration complexity of this challenge. However, an under-examined impact of the rise of enterprise mobility is how it is compounding the potential security vulnerability created by the use of remote access and support tools. Businesses are increasingly having to support remote and mobile workers and hence having to use remote access tools to support their devices. In addition, businesses are working with numerous vendors and third-party contractors that use remote access tools to access their companies' IT systems and devices, creating another source of security vulnerability associated with remote access tools. Finally, remote workers are increasingly self-selecting consumer-focused remote access tools to access corporate IT systems. What is concerning is that, while the data from this research shows that IT is aware of the security vulnerability posed by remote access tools, many IT departments across the markets surveyed (UK, Germany and France) do not have a complete view of what tools their employees or third-party suppliers are using.

This problem is only set to get worse. IT cannot put the mobility genie back in the bottle, and has to embrace this consumerised employee behavior or risk disconnecting from the business. Best practice involves supporting and enabling workers, as far as reasonably possible, to keep end-users productive no matter what device they choose to use or from which location they work. Hence the need for remote access and support is only going to increase. What is vital is that businesses

understand the security risks of some remote access tools, and use solutions that minimize these vulnerabilities. This paper will use data from a survey of 300 IT decision-makers in the UK, France and Germany to demonstrate that:

- Mobility is now ingrained into flexible working.
- Employees are doing more than just bringing their own devices to work, and IT needs to be aware of this behavior.
- New devices and applications provide new opportunities for business - but can also be a security risk.
- Companies are aware of the risk of the use of remote access tools, but many do not have a view on what tools their employees are using. This obviously precludes effective security management.
- A further challenge is the use of remote access tools by third-party partners and suppliers.

MOBILITY IS INGRAINED INTO FLEXIBLE WORKING

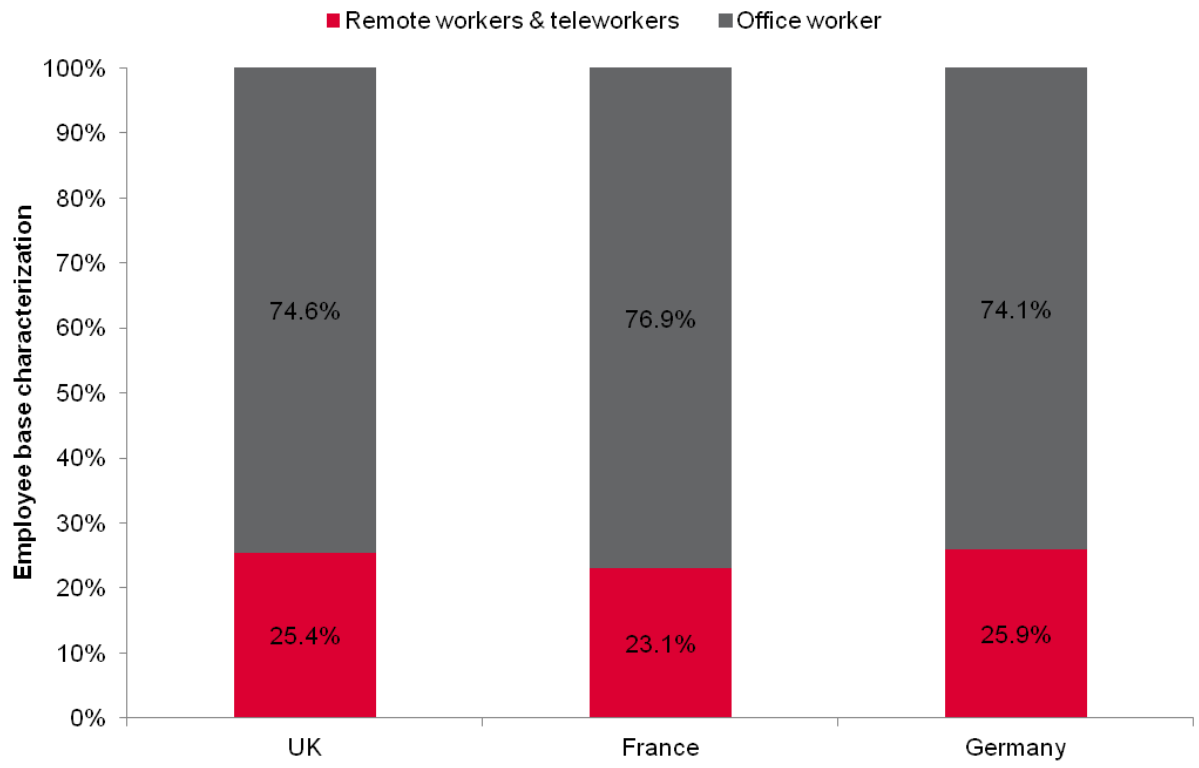
Flexible working is a common practice, and commonly supported by IT

High speed wireless broadband networks, the growth of smartphone, tablet and laptop computing and the development of cloud web services is making flexible, remote working increasingly commonplace. Having to be behind a corporate firewall to access an enterprise application is an anathema for users raised on Web 2.0 services such as Google, Salesforce.com or DropBox.

The businesses surveyed in this research across the UK, Germany and France, classified nearly a quarter (24.8%) of their workforce as remote workers or teleworkers (Figure 1.) with a high level of consistency across these national markets. Extrapolating out, this means that there are 25.3 million full time employees across these three markets that are not office based in 2013, and hence require remote support when they have a technology issue. It's also safe to assume that many of the workers classified as office-based occasionally work from home or the road, and hence require remote support during those times. By default IT focuses on supporting office-based workers. This after all is the baseline requirement of an IT department. However, remote and teleworkers are not always supported: 68% of enterprises taking part in this survey stated that support was provided for remote and teleworkers, leaving a significant proportion that do not provide it. What is encouraging is that businesses are demonstrating that they are adapting to new and more flexible working practices. Across Germany, UK and France there is a trend to increasing support for remote and teleworkers over the next 18 months.

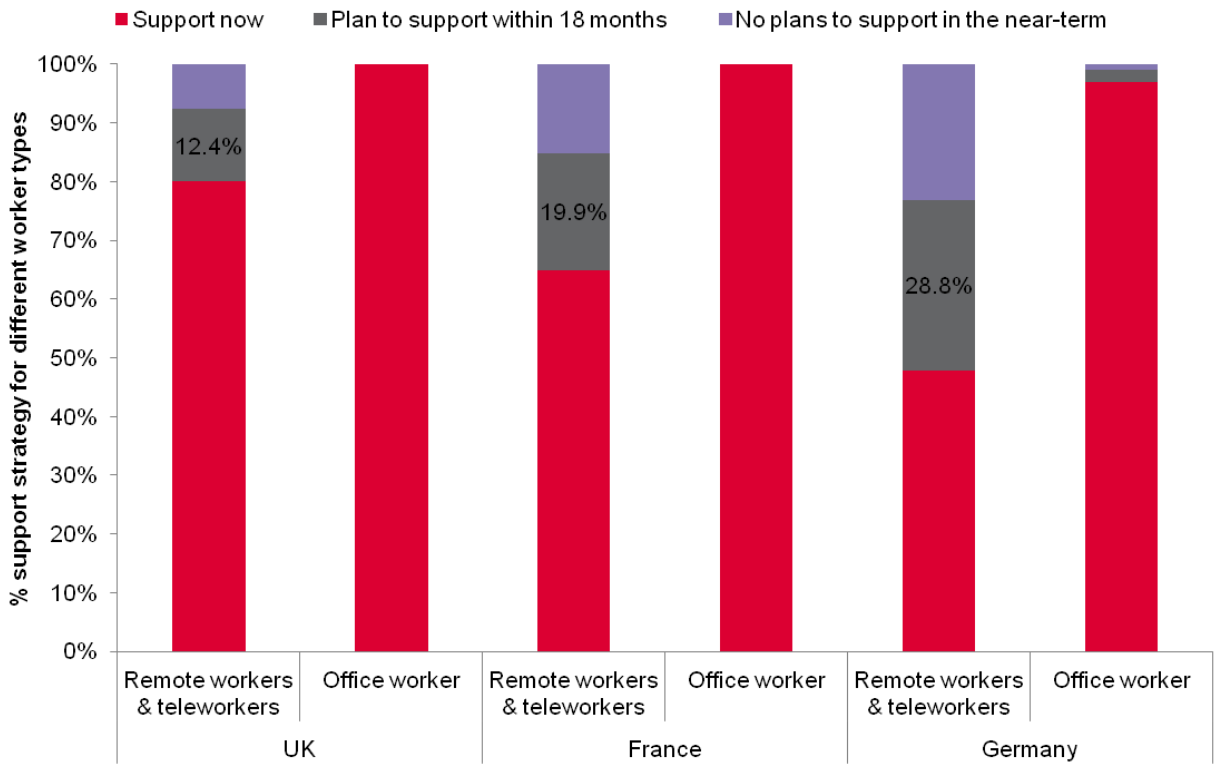
Germany is a highly regulated employment market where employee data privacy legislation imposes extensive constraints on IT’s ability to securely manage and monitor employee devices. As a result, respondents from Germany demonstrated the lowest level of remote and teleworker support today. However, even in this complex market, we see a high rate of growth when it comes to the forecast for providing support over the next 18 months at 28.8%.

Figure 1: % of companies' employees that are office-based versus remote and/or teleworkers in 2013



Source: Ovum

Figure 2: What level of IT support is there for remote and teleworker vs. office workers?



Source: Ovum

EMPLOYEES ARE BRINGING THEIR OWN DEVICES - AND MORE

Businesses are moving to support employee owned devices…

The underlying driver for both the IT consumerisation effect and the shift to flexible, mobile working is the growth in personal ownership of smartphones and tablets. According to Ovum's multimarket employee BYOD survey almost 70% of all full time employees who own a personal smartphone or tablet are using these devices to access corporate data.

However, it is critical to note that this usage is not an absolute substitute for PC usage. Employees are not rejecting the laptop or desktop as a device to be used for work. Instead the PC is just one of many screens that employees want to be able to use to do their job in a faster, more responsive, more agile manner, and increasingly the user does not want to distinguish between whether a device is personally owned or corporately provided. They just want to use the most convenient screen for the task at hand. While corporate agility is hard to measure, Ovum's research with both SME, mid-market and multi-national businesses indicates that the agility that comes with embracing and exploiting this behavior can create real competitive advantage.

In the research done for this paper, we see that IT organizations are indeed moving to support this activity but are not all there yet, as show in Figure 3. If they don't already support smartphones and

tablets, the majority are aiming to do so within the next 18 months, with a really significant growth in the number of businesses that plan to support personally owned smartphones and tablets over this period: an increase of 42.5% and 36.7% respectively.

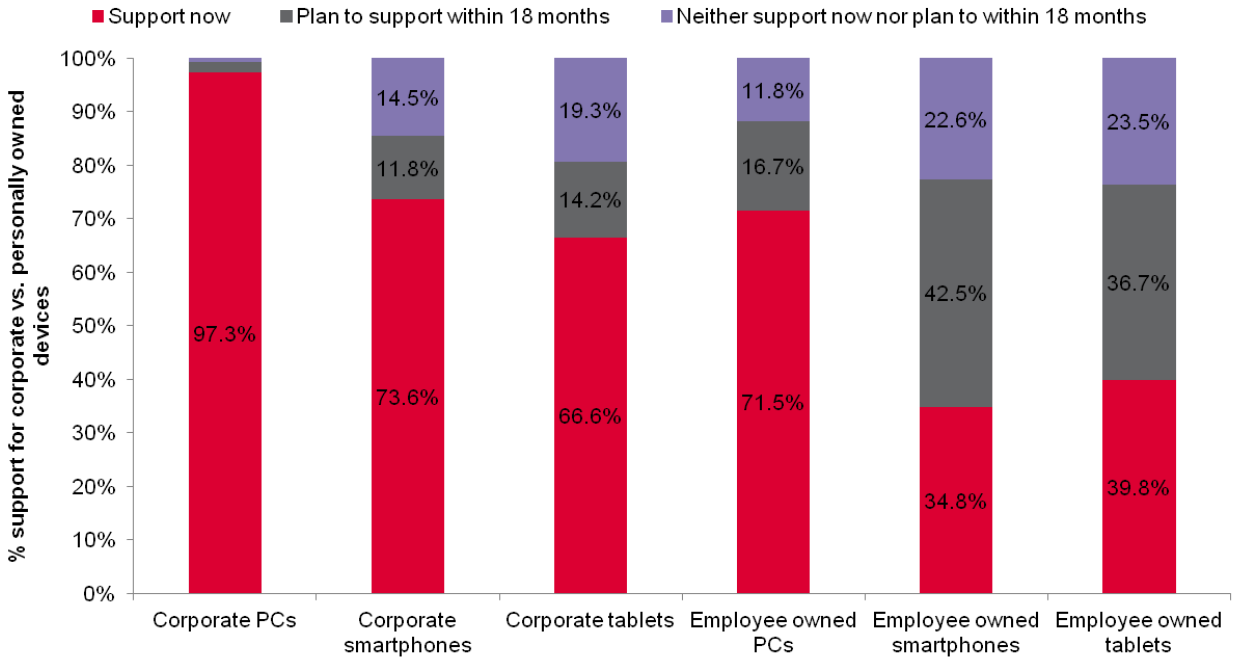
The message from the data is clear. IT is waking up to the reality of having to support multi-screening by their employees, whether these devices are personally owned or corporately provisioned.

But not necessarily with remote support tools

While IT support generally for these different types of devices is building, the picture for remote support of smartphones and tablets is not so strong. According to our research, few businesses currently use remote access tools to support smartphones and tablets, although the majority have plans to do so over the course of the next 18 months. However, a third of IT departments have no plans to implement remote support for smartphones in the near term.

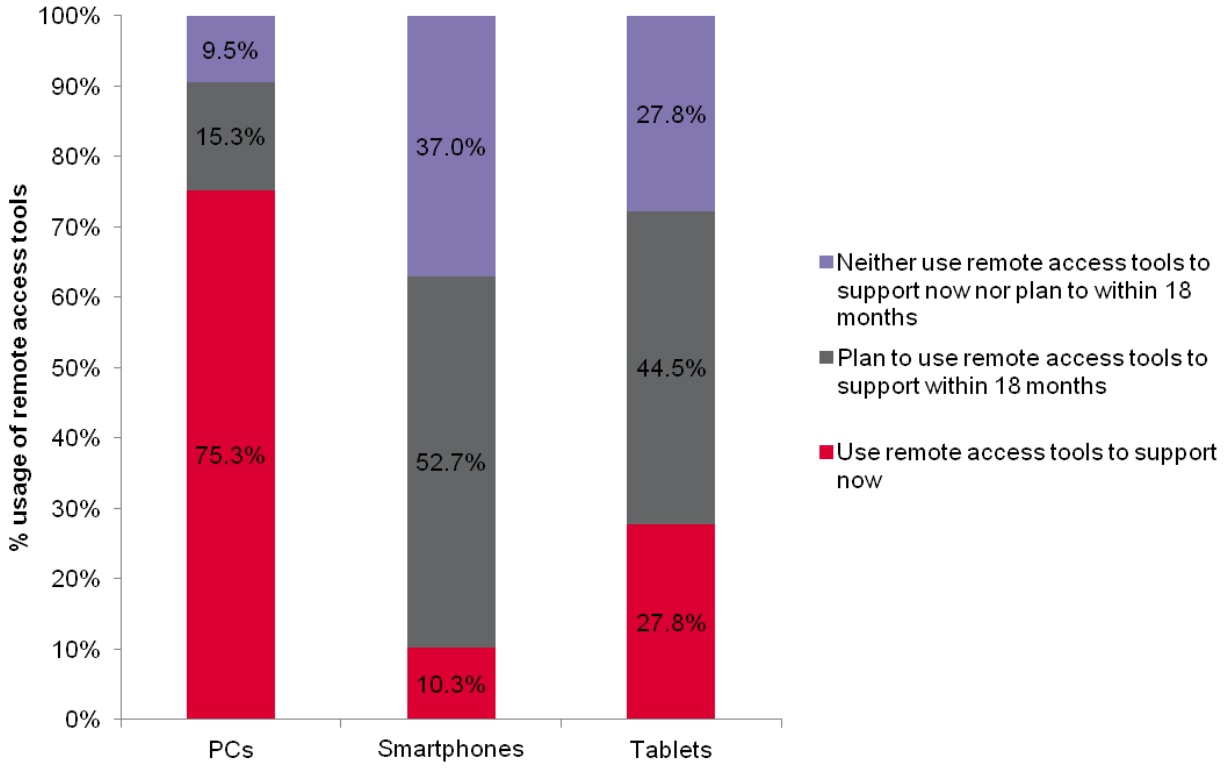
While iOS and some versions of Android limit remote screen-sharing and control, most mobile operating systems allow IT to use remote support tools to configure the device, co-browse with the end-user and view and control custom applications, if their remote support technology has these capabilities. So the current lack of remote support demonstrates a gap in support strategy when it comes to mobility. Businesses are being slow to fully support devices that are being used on a day to day basis already, and the impact will only be felt harder as more and more employees depend on smartphone or tablet devices.

Figure 3: IT support and planned support for corporate and employee owned devices



Source: Ovum

Figure 4: IT remote support for different types of devices



Source: Ovum

SUPPORTING THE MOBILE WORKER IS VITAL BUT AMPLIFIES THE SECURITY RISK OF REMOTE ACCESS

The new role of IT is to enable workers as far as possible

Enabling employees to work flexibly and remotely can open up a world of opportunities for businesses. It can transform existing processes and enable new markets, making workers more productive and efficient. And the proliferation of devices and applications that consumers can access means that it will only get harder and harder for IT to try and clamp down on employee access.

So, the role of the IT department is changing, moving from the position of gatekeeper to enabler and chaperone. CIOs need to find ways to enable employees to use the tools that they need to do their jobs as far as possible, at the same time as maintaining the security of corporate data.

Understanding the risks of remote access

While remote access tools can significantly improve IT support efficiency and effectiveness, they are also a major source of data breaches in the enterprise. Vulnerabilities in the tools themselves or misuse of access credentials create obvious vectors of attack. As mobile and remote working increases and businesses use more third-party vendors and services providers to manage aspects

of their systems, the need to understand, manage and address the risks posed by remote access tools becomes ever more important.

Data breaches that occur via remote access classically involve older point-to-point remote access tools. These basic tools require an open listening port to reside on the client computer in order to connect to it. Open listening services on Internet-connected computers are an easy target for hackers and a major source of compromise. Alternatively, many newer remote support tools are based on a SaaS framework, which eliminates the open listening port issue, but extends the circle of vulnerability to that SaaS vendor. By design, remote access tools act as a gateway into all other systems. If a company is unable to or simply uncomfortable putting all of their systems in the cloud, they should consider whether they want a remote access gateway accessible in the cloud.

79% of IT organizations surveyed in this study are using one of five major remote support tools today. Two of those tools are point-to-point solutions while the other three are all cloud-based. This means the majority of organizations are vulnerable to a data breach via remote access.

A key way to mitigate the risk of remote access is to use a solution that includes an appliance (physical or virtual) that resides in the corporate network. No matter how the remote support session is initiated, the connection is always outbound from the IT support individual and end user's devices to the appliance. This allows IT to support devices over the internet without using an open listening port or routing sensitive data and system access through a third-party.

The appliance-based approach effectively enables business to mitigate many of the risks associated with remote access, and can be a secure foundation for businesses to adapt to the growing need to support a remote and mobile workforce using a diversity of devices and platforms.

DO YOU KNOW WHAT REMOTE ACCESS TOOLS YOUR THIRD-PARTY SERVICE PROVIDERS AND EMPLOYEES ARE USING?

Vendor use of remote access tools creates additional risk

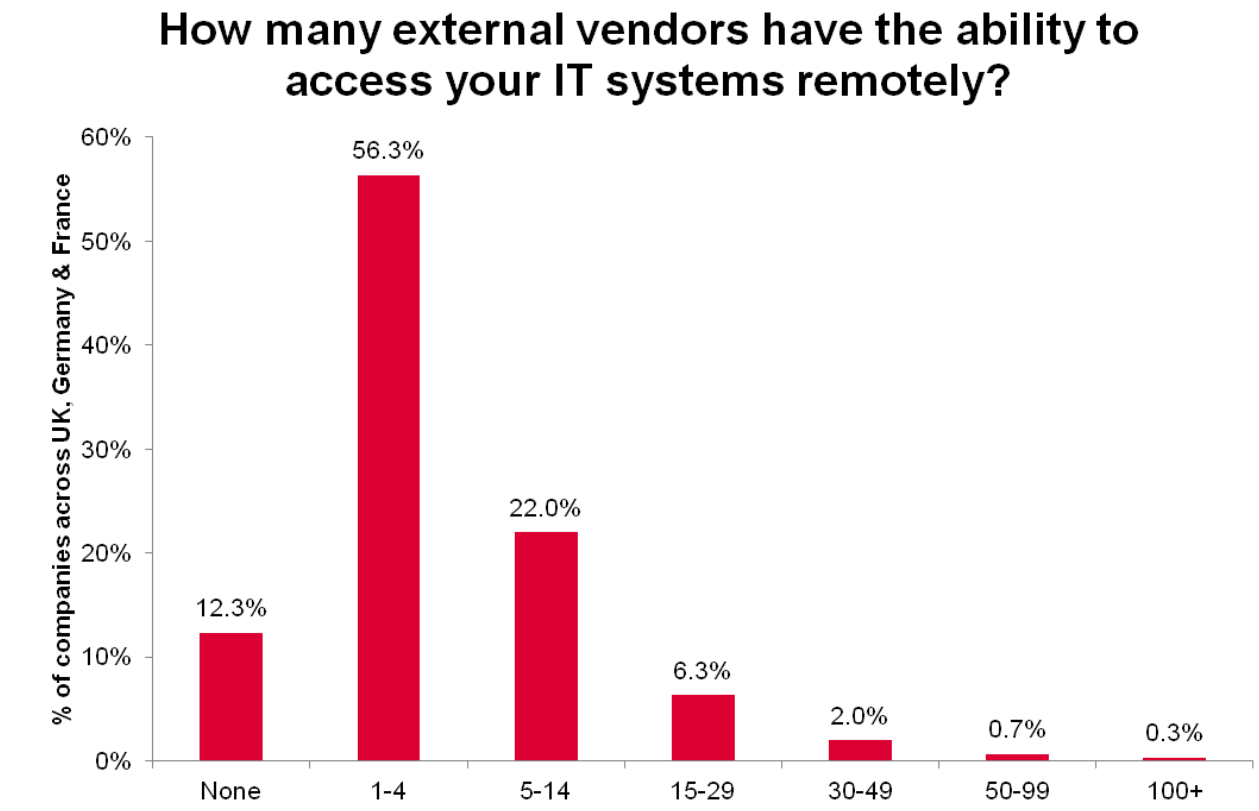
Unfortunately, the IT service desk is the not the only source of security vulnerability created through the use of the remote access tools. Third-party service providers and vendors also often use them to access, configure and support their clients' applications and systems. This can obviously improve the service they provide, but again the use of these remote access tools poses a potential security risk.

In the research for this paper, Ovum found that 88% of businesses surveyed across Germany, UK and France have at least one external vendor with ability to access their IT systems remotely, and 33.6% of these vendors are using remote access tools to support end users or manage other IT assets. If the tools they're using are point-to-point or SaaS, the same vulnerabilities described above are introduced into the companies' network. Plus, basic remote access tools often lack comprehensive audit trails, so businesses have little ability to track what their vendors are doing for compliance purposes. It is possible that remaining 66.4% of vendors are remotely accessing client systems through a general VPN that offers even broader access to the network and less

tracking and auditing capabilities. This effectively puts a companies' security and compliance management at the mercy of the vendor.

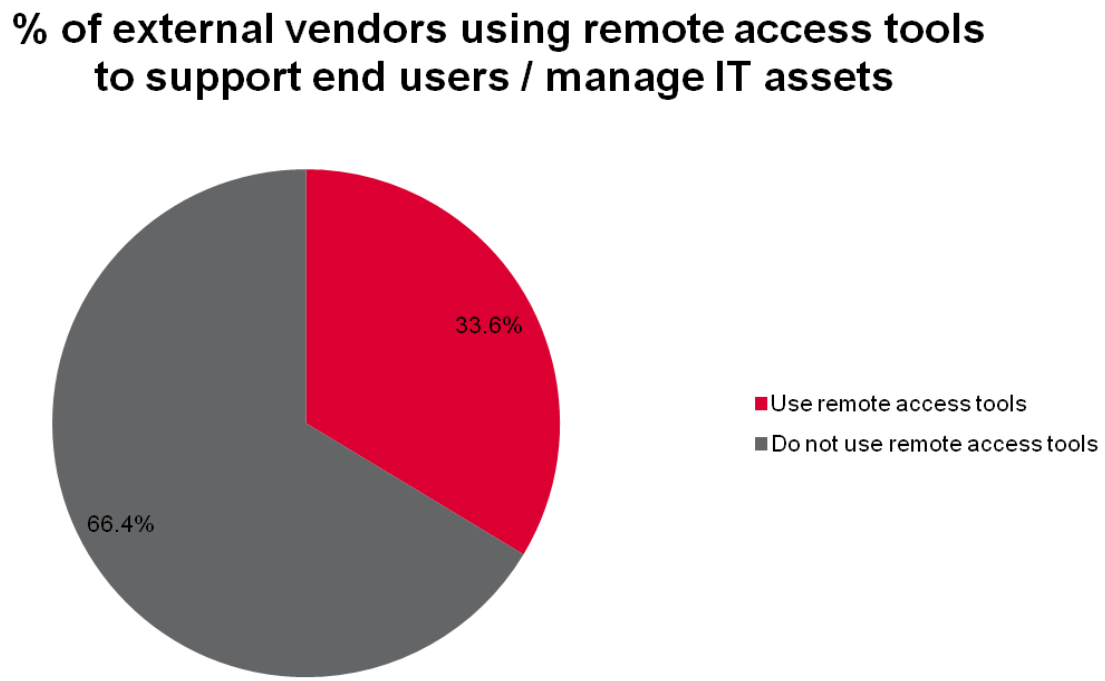
Remote access is key to delivering a good service, but IT should at the very least audit what tools are being used, and best practice should entail mandating only the usage of tools that are deemed secure.

Figure 5: 88% of businesses have one or more external vendors accessing their systems remotely



Source: Ovum

Figure 6: 34% of third party vendors are using remote access tools to manage their client company IT assets



Source: Ovum

The Bring Your Own App effect: employees are also finding their own remote access tools

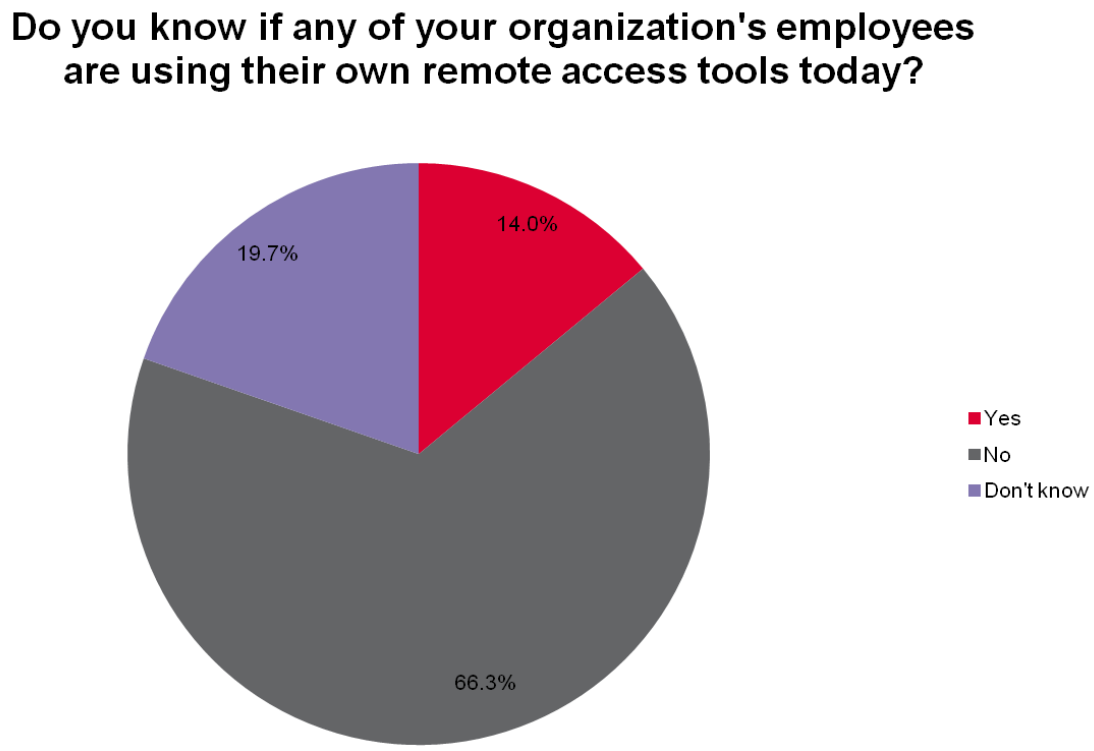
Employees are not just bringing their own devices to work, they are also finding their own applications to get the job done. Ovum has seen that this BYOA activity is widespread around third-party cloud productivity applications (e.g. file sync & share, VoIP, enterprise social networking) though our multimarket employee BYOD survey. For example, over 22% of employees are self-provisioning file sync and share tools such as DropBox or Google Docs to share corporate documents between their different screens or work groups. And 31% are using a self-provisioned VoIP application to communicate with their colleagues, predominantly Skype.

We also see it happening here in the context of remote access tools, with 14% of the IT decision makers surveyed indicating that they are aware that their employees are using remote access tools. 19.7% of the IT decision makers surveyed worryingly said that they did not know if employees were self-provisioning remote access tools or not. These employees are often using consumer-focused applications to remotely access files and systems on their laptop or desktop while working from a mobile device at home or on the road.

74% of those respondents who knew that their employees sourced their own remote access tools are either concerned about this behavior or unsure of whether it is a problem or not. This highlights

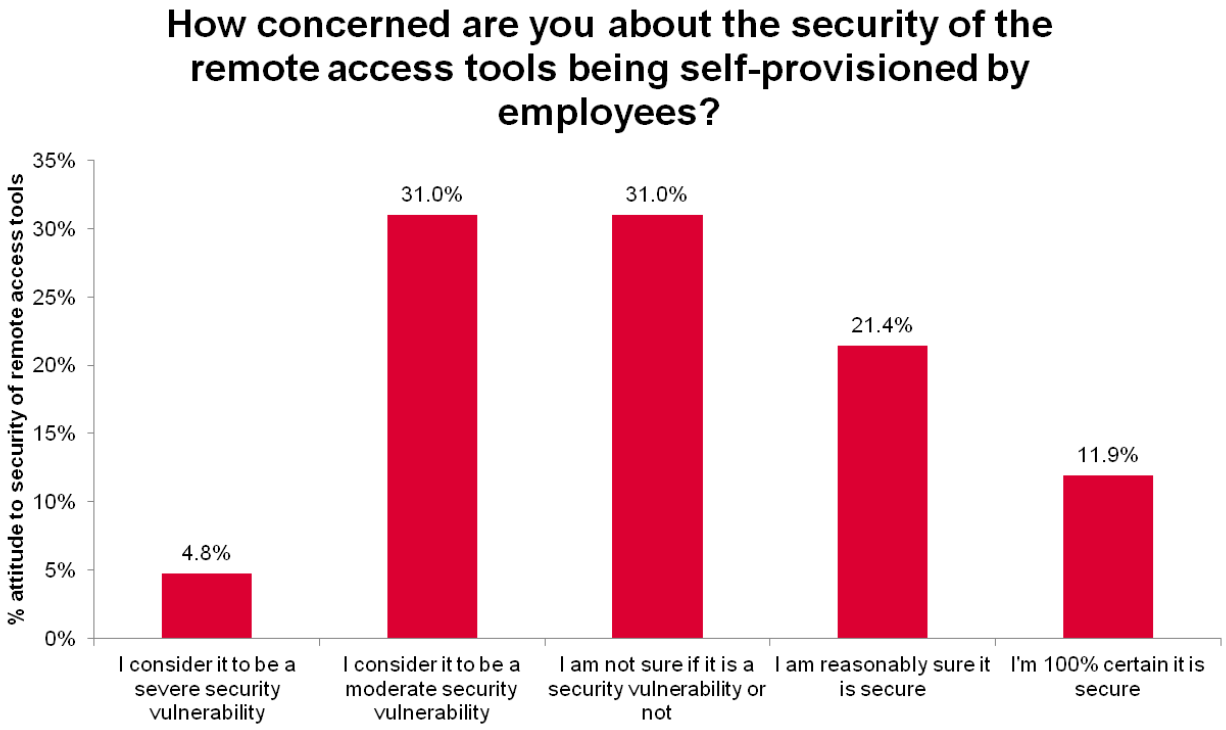
that IT departments are aware of the risks around BYOA and remote access, but are not doing much to deal with it.

Figure 7: A small percentage of employees are sourcing their own remote access tools - and IT doesn't always have a view of this behavior



Source: Ovum

Figure 8: IT is concerned about employee-provisioned remote access tools



Source: Ovum

This is symptomatic of the wider BYOA phenomenon. A significant proportion of increasingly technically educated and motivated employees will look to find whatever tools they can to get access to the information and services they need. IT needs to be proactive in their policies around and support of mobile devices to limit the use of employee self-provisioned remote access tools that may create security vulnerabilities.

SUMMARY

Work practices are becoming more flexible and agile. The use case for tying the employee to a desk or an office facility is waning. Nearly 25% of the full-time employed workforce of the UK, Germany and France are classified as remote or teleworkers, and businesses in all three geographic markets are signaling that they are planning to increase their level of support for remote or teleworker in the next 18 months.

Ingrained in these increasingly flexible working practices is mobility. BYOD is evolving into enterprise multi-screening, where employees demand a consistent enterprise application experience across tablet, smartphone or PC, irrespective of whatever network they are connected to or whether that device is corporately provisioned or personally owned. This is the reality of the challenge for IT in the increasingly mobilised enterprise, and a growing number of businesses are supporting personal and corporate smartphone and tablets. However, few are using remote tools to support smartphones and tablets today, suggesting that there is a disconnect in the support

strategy for the increasingly mobile workforce for many businesses. This is creating an inconsistent support experience for workers using multiple devices.

The essence of the new task for IT is to balance the delivery of a true multi-device employee experience without compromising security. However, some remote access tools themselves present security vulnerabilities. Many attacks on business come through point-to-point remote access solutions that open a listening port on a client device. SaaS remote access tools may eliminate the listening port vulnerability, but create a new circle of vulnerability around the SaaS provider itself. An appliance-based solution is a means to mitigate this risk, but the majority of organizations in this study are using point-to-point or SaaS solutions.

Remote access tools are vital to providing good service. But this also means that many business' IT vendors are also using these tools, creating a control and audit challenge. Businesses need to be aware that if a vendor is using a tool to access their systems they are putting their security and governance at the mercy of that vendor. This issue is further compounded by the increasing tendency of employees to self-select their own applications to get their job done and this may include remote access tools. This likewise amplifies the security vulnerability presented by the use of SaaS tools.

The onus is on IT to not only deliver great support to its increasingly mobile and remote workers, but to ensure that the tools being used to deliver this support limit the security vulnerabilities created by the mobile worker.

APPENDIX

Methodology

- Primary research with IT decision makers across UK, Germany and France (n = 100 for each geographic market)
- Ovum's on-going research in employee behavior trends in the enterprise including Ovum's BYOD multimarket employee behavior survey (n = 4,233)
- Ovum's on-going research with device management and application management vendors
- Ovum's on-going security research program
- Engagement with Ovum's research partner for this study, Bomgar

Author

Adrian Drury, Practice Leader, Consumer Impact Technology

adrian.drury@ovum.com

Richard Absalom, Senior Analyst, Enterprise Mobility & Consumerization

richard.absalom@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.