2018 Mobile Security Report

iPass

CONTENTS

Mobile working is increasingly becoming the norm for many enterprises, with industry analyst Strategy Analytics predicting that there will be 1.75 billion mobile workers by 2020. At the same time, mobile security threats are on the rise: according to the McAfee Mobile Threat Report Q1 2018, 16 million users were hit with mobile malware in the third quarter of 2017.

The use of free public Wi-Fi continues to pose the biggest mobile security threat for enterprises. Yet with connectivity being vital to productivity, today's 'Wi-Fi first' mobile worker often turns to free public Wi-Fi as their first port of call. With millions of Wi-Fi hotspots globally, all with varying security credentials, how can enterprises ensure the connections that their mobile workers use are secure? At a time when data protection is paramount, enterprises need to strike a balance between keeping their data and systems secure, while not hampering the productivity of their mobile workforce.

Surveying 500 CIOs and senior IT decision makers from the U.S., U.K., Germany and France, the iPass Mobile Security Report 2018 examines how organizations view today's mobile security threats and employees' use of free public Wi-Fi.

The report's findings include the following:

- The majority of CIOs suspect their mobile workers have been hacked or caused a mobile security issue in the last 12 months
- CIOs have seen the most Wi-Fi related security incidents happen at cafés, airports and hotels
- CIOs believe mobile security risks have increased due to the rise of BYOD
- Banning employee use of free Wi-Fi hotspots is still the preferred security measure for most organizations
- Employee VPN usage is on the rise, but the majority of CIOs are still not confident their mobile workers are using them all the time

Businesses suspect their mobile workers are being hacked

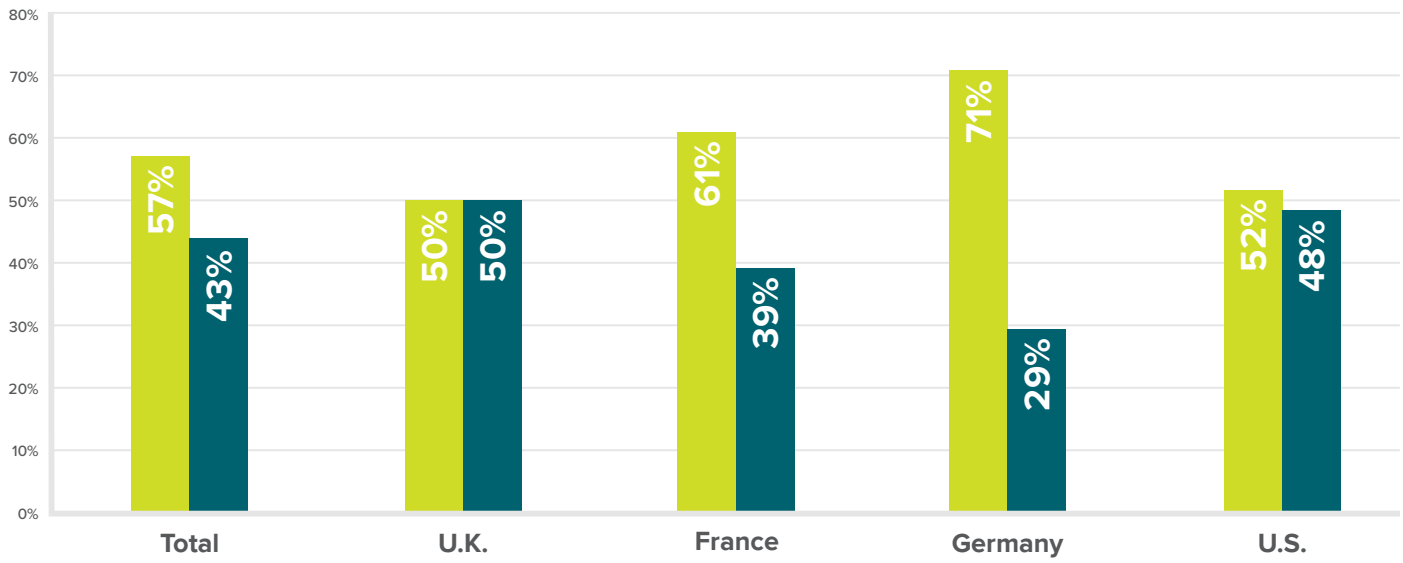
Today's professional rarely stays in one fixed location; they could be at an airport departure lounge or hotel one day and working at a café between meetings the next. Wherever they are, mobile workers can likely find free or on-demand Wi-Fi to access the corporate systems and data they need in order to do their job.

For all the benefits this brings, it has also significantly increased business risk. Indeed, more than half (57%) of respondents said they suspect that one or more of their mobile workers has been hacked, or caused a mobile security issue, in the last 12 months. Respondents in Germany (71%) were particularly concerned that they had been exposed to mobile security issues in the last 12 months.

FIG 1:

Source: Vanson Bourne

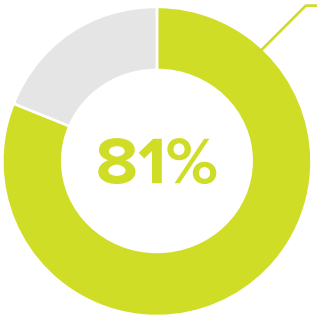
Do you suspect that one or more of your mobile workers has been hacked or caused a mobile security issue in the last 12 months?



Cafés, airports and hotels: a hotspot for Wi-Fi related security incidents

Overall, 81% of respondents said they had seen Wi-Fi related security incidents in the last 12 months, with cafés, airports and hotels being cited as the most vulnerable locations. This is perhaps not surprising, as all these locations see a high turnover of visitors each year and the level of security at each hotspot varies.

Of those respondents that had seen a Wi-Fi related security issue in the last 12 months, nearly two-thirds (62%) had seen them occur in cafés and coffee shops. The problem is particularly acute in the U.K., where 81% had seen cafés and coffee shops contribute to Wi-Fi related security issues. There were also significant geographic differences when it came to Wi-Fi related security issues at airports: more than two thirds (68%) of U.S. respondents said they had seen incidents at airports, in contrast to only 39% in the U.K.

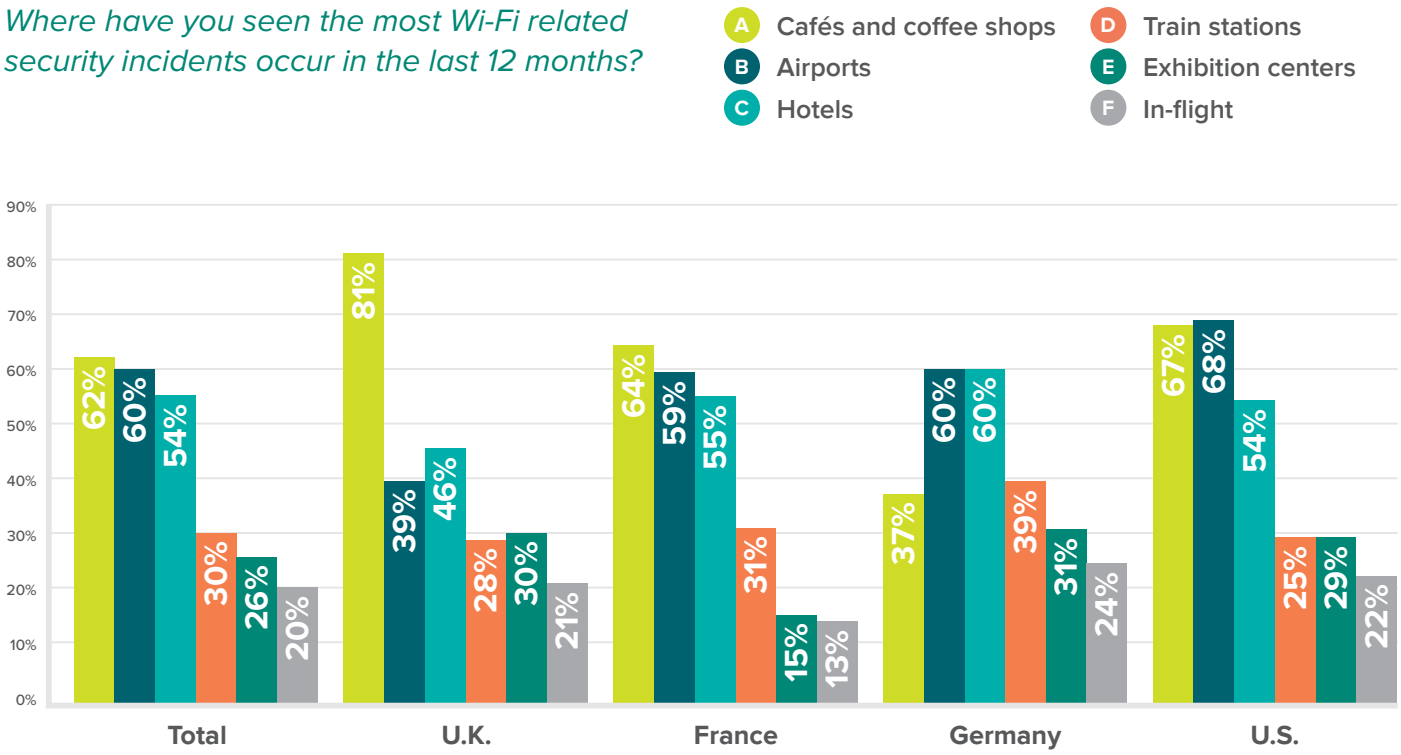


Percent of organizations that have seen Wi-Fi related security issues in the last 12 months.

FIG 2:

Source: Vanson Bourne

Where have you seen the most Wi-Fi related security incidents occur in the last 12 months?



BYOD: Bring Your Own Danger?

The concept of bring your own device (BYOD) is now commonplace: despite the large number of people working remotely, Gartner says fewer than a quarter (23%) have been supplied with a mobile device by their employer. This leaves enterprises open to security risks, as they do not have control over the security settings or capabilities of devices that are being used.

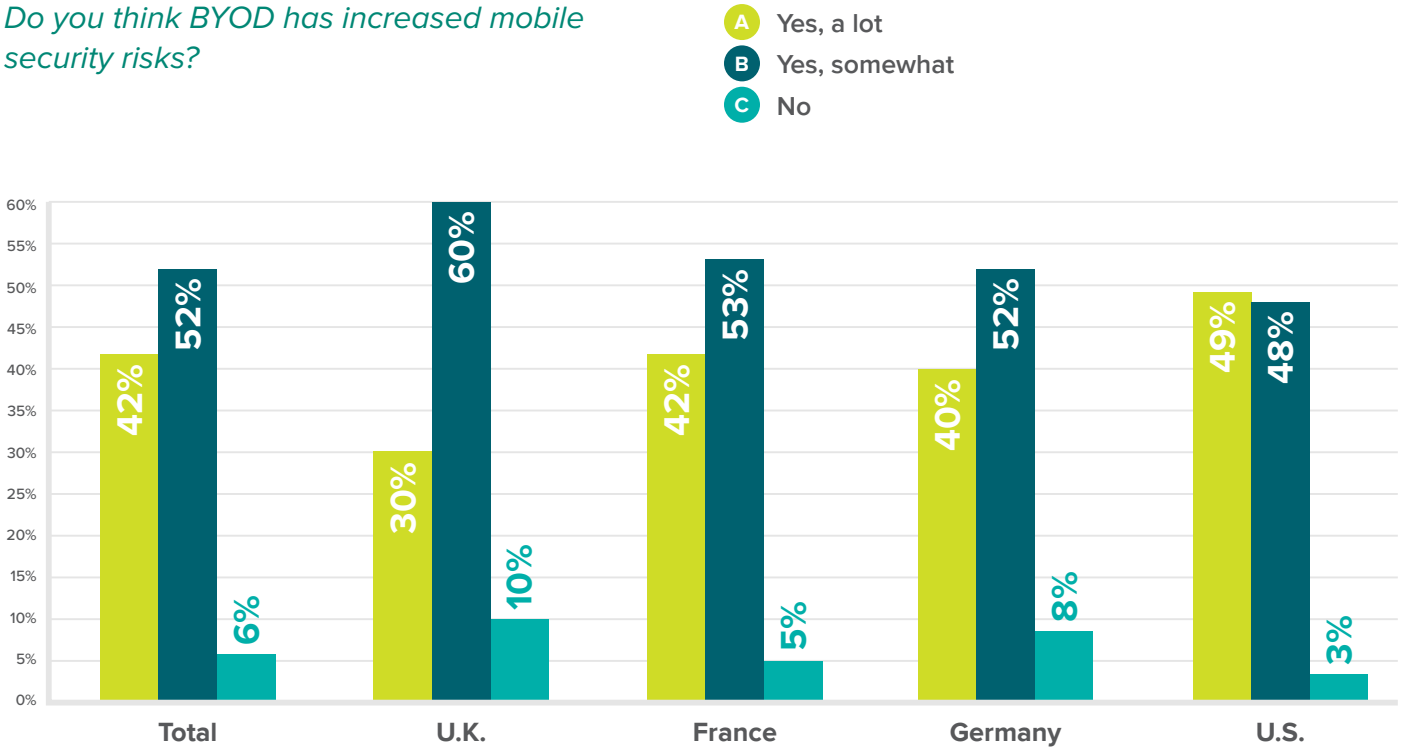
Enterprises are in a Catch-22 situation when it comes BYOD. Many enterprises realize it can improve not only employee productivity, but also wider job satisfaction. However, there is a trade-off with potential security risks.

Survey respondents recognize that the risk has been increased by BYOD, with 94% reporting that they think BYOD has increased mobile security risks.

FIG 3:

Source: Vanson Bourne

Do you think BYOD has increased mobile security risks?



Mobile security challenges remain a huge concern

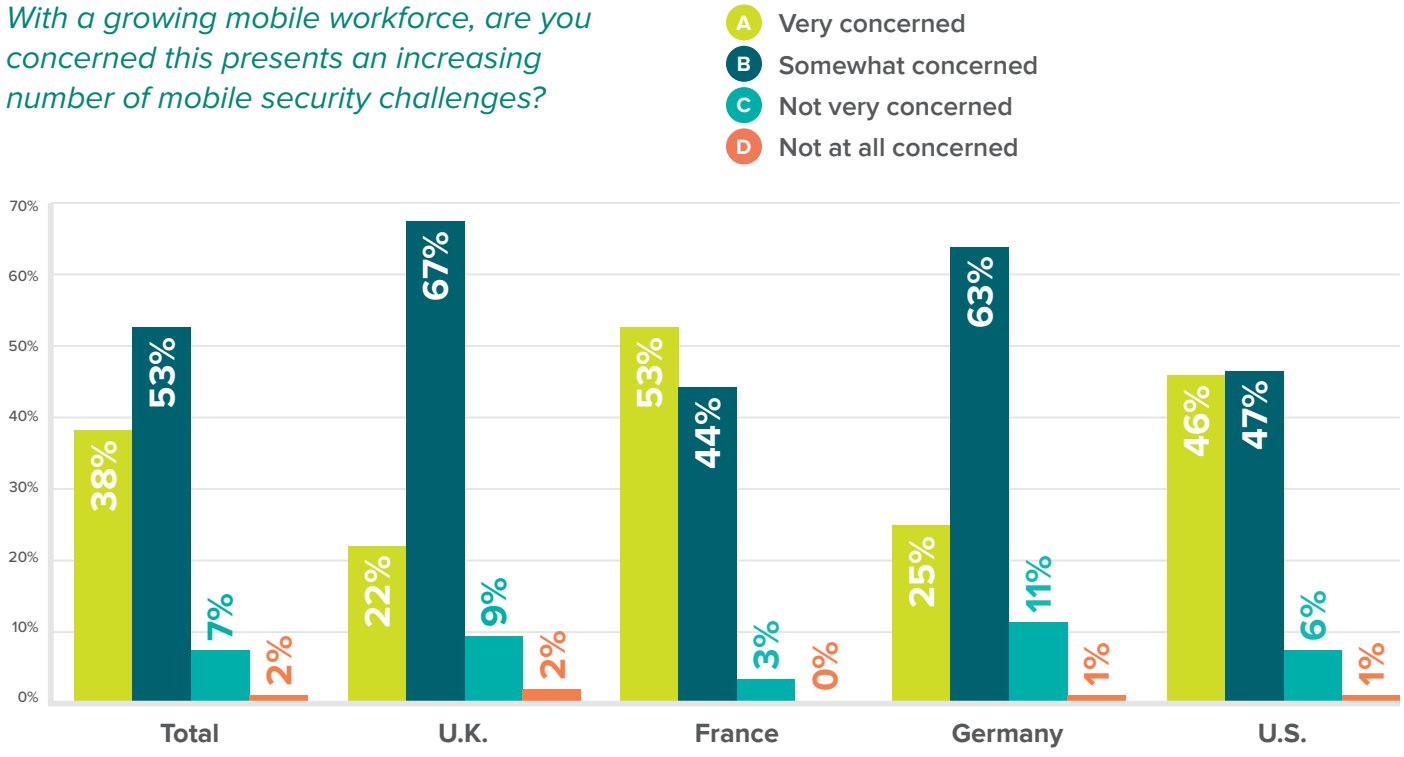
Based on the earlier statistics, it's not surprising that enterprises remain concerned about the security risk posed by the growing number of mobile workers. Overall, 92% of organizations said they were very concerned or somewhat concerned their growing mobile workforce presents an increasing number of mobile security challenges.

There's a perfect storm brewing: a rapidly growing mobile workforce, the explosion of free public Wi-Fi coupled with ever more sophisticated hackers.

FIG 4:

Source: Vanson Bourne

With a growing mobile workforce, are you concerned this presents an increasing number of mobile security challenges?



Banning public Wi-Fi

When organizations take action to stop mobile security threats in their tracks, they're likely to take a direct approach—stopping the problem at the source by placing a blanket ban on the use of free Wi-Fi hotspots.

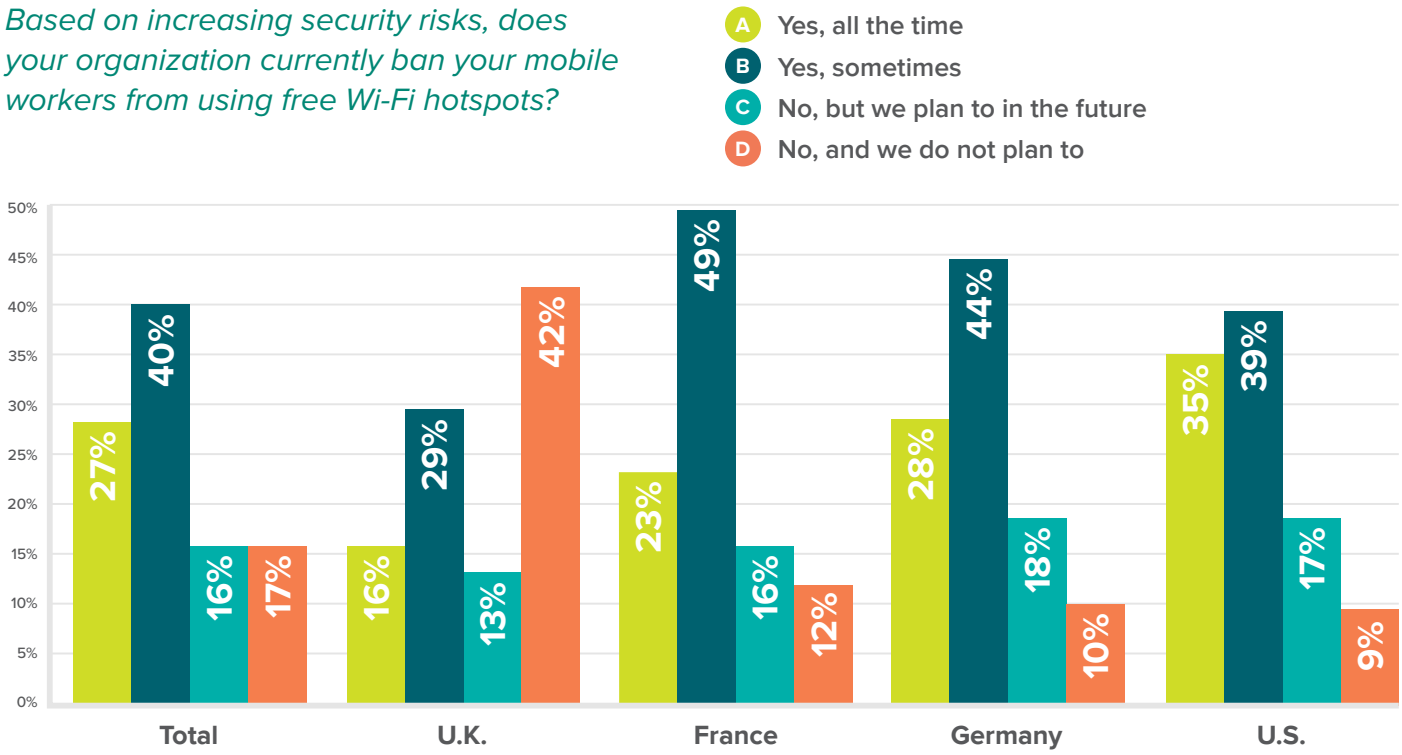
Bans have been introduced by 67% of respondents, with 27% banning the use of free Wi-Fi hotspots at all times and 40% banning their use sometimes. A further 16% plan to introduce a ban on public Wi-Fi hotspots in the future. U.K. enterprises seem to be taking the most liberal approach, with 42% of organizations stating they have no plans to ban employees from using free Wi-Fi hotspots.

An outright ban might sound like the best course of action to take, but is likely to have a negative impact on the wider business, making it more difficult for remote workers to remain connected and productive at all times. As most electronic devices only have a Wi-Fi connection, banning mobile workers from accessing free-Wi-Fi connections at coffee shops, hotels and airports is akin to cutting off your nose to spite your face. So how can organizations achieve the best of both worlds when it comes to security and productivity?

FIG 5:

Source: Vanson Bourne

Based on increasing security risks, does your organization currently ban your mobile workers from using free Wi-Fi hotspots?



Mobile VPN: A missed opportunity?

Virtual Private Networks (VPNs) can be a great way to secure remote connections to data and central systems, providing an alternative to a blanket ban on free Wi-Fi hotspots with an extra layer of security, which has to be deployed by the end user each time they wish to connect.

VPN usage is increasing: in 2016, just 26% of enterprises were fully confident mobile workers were using a VPN every time they went online, but that figure has jumped to 46% in 2018. That does however leave more than half (54%) of respondents reporting that they still aren't fully confident that their mobile workers use a VPN every time they go online. This figure leaps in the U.K. and France, where 62% and 59% of respondents, respectively, said they weren't fully confident that their mobile workers are using a VPN when they go online.

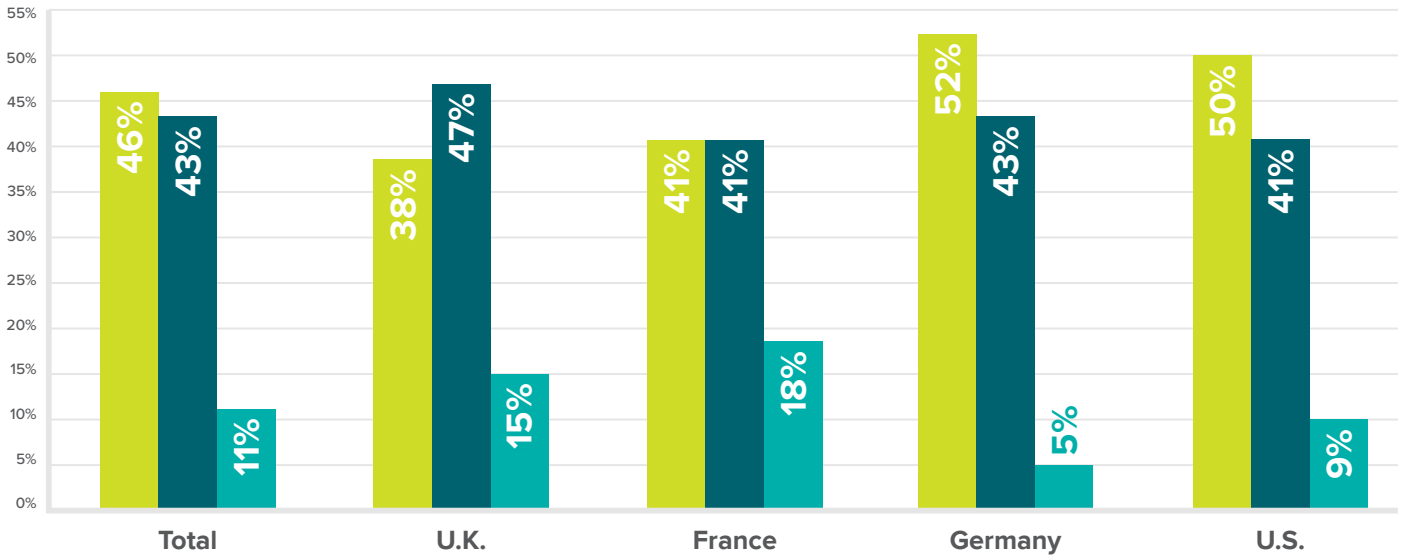
There are several barriers preventing mobile workers from connecting to VPNs, including the fact that mobile workers might not want personal data to run over the corporate network and that connecting to VPNs can take extra time. The challenge lies in building employee knowledge of the importance of using VPNs every time they go online, and how to connect to one in a quick manner.

FIG 6:

Source: Vanson Bourne

How confident are you that your organization's mobile workers use a VPN every time they go online?

- A I am 100% confident that our mobile workers use a VPN every time they go online
- B I am somewhat confident our mobile workers use a VPN every time they go online
- C I am not confident our mobile workers use a VPN every time they go online



Conclusion

Enterprises are increasingly aware of the fact that the huge growth in mobile working presents new security issues to worry about. IT teams are no longer fully in control, as connectivity and access to corporate systems now extends beyond the four walls of the office.

The huge, global growth in free Wi-Fi hotspots continues apace, so organizations outright banning employees from using them is a somewhat short-sighted approach. The fact is, mobile workers will always seek out connectivity, irrespective of the security risks involved, if it enables them to get work done. In today's connected and increasingly 'Wi-Fi' first world, enterprises need a modern mobile working strategy that empowers employees, as opposed to stopping them in their tracks.

Rather than imposing a blanket ban on the use of free public Wi-Fi, they should make all employees aware of the benefits of using VPNs to connect securely, and make the process of connecting to one as simple as possible. This way they can maintain security while also keeping employees productive, no matter where they are located.

About iPass

iPass (NASDAQ: IPAS) is a leading provider of global mobile connectivity, offering simple, secure, always-on Wi-Fi access on any mobile device. Built on a software-as-a-service (SaaS) platform, the iPass cloud-based service keeps its customers connected by providing unlimited Wi-Fi connectivity on unlimited devices. iPass is the world's largest Wi-Fi network, with more than 64 million hotspots around the globe, at airports, hotels, train stations, convention centers, outdoor venues, inflight, and more. Using patented technology, the iPass SmartConnect™ platform takes the guesswork out of Wi-Fi, automatically connecting customers to the best hotspot for their needs. Customers simply download the iPass SmartConnect app to experience unlimited, everywhere, and invisible Wi-Fi.

iPass Corporate Headquarters
3800 Bridge Parkway
Redwood Shores, CA 94065

phone: +1 650-232-4100
fax: +1 650-232-4111

www.ipass.com