2017 Mobile Security Report

iPass

CONTENTS

Two of the most significant trends in the enterprise today are increasing workforce mobilization and a shocking rise in cybersecurity threats, due to the expansion of mobile attack surfaces.

As mobile devices have become more widely embraced by the enterprise, they have become the primary device for many employees due to their convenience and functionality. Even organizations that don't provide mobile devices to their employees can expect their workers to use their own mobile devices for business tasks – with little or no oversight from IT.

As a result of their growing popularity, mobile devices have become a great target for cybercriminals, a vector to steal valuable corporate data or simply to gain access to the corporate network where bigger targets lie in wait.

Public Wi-Fi hotspots have long been one of the most popular means of attack, and they continue to present a significant challenge for employers who simply want to ensure that their increasingly mobile workers remain connected and productive and, most importantly, secure.

Surveying 500 CIOs and senior IT decision makers from the U.S., U.K., Germany and France, the iPass Mobile Security Report 2017 overviews how organizations are dealing with the trade-off between enforcing security policies and enabling a mobile workforce. The report's findings include the following:

- Organizations consider C-level employees, including the CEO, to be at the greatest risk of being hacked.
- Coffee shops are regarded as the most dangerous public Wi-Fi venue.
- Organizations are increasingly concerned about growing mobile security risks, and man-in-the-middle attacks are deemed the greatest threat.
- U.K. organizations demonstrate the least concern for mobile security threats and public Wi-Fi risks by far.
- U.S. organizations consistently rank among the highest for concerns about mobile security, yet their actions rarely follow suit, as they continue to allow the use of public Wi-Fi hotspots and encourage the use of MiFi devices.

Mobile security is a growing concern for businesses in 2017

With a significant increase in mobile-related data breaches over the course of 2016, it's no surprise to hear that CIOs and senior IT decision makers remain concerned about mobile security threats. Indeed, organizations appear to be increasingly worried about mobile security in 2017. Almost half (47 percent) of respondents said that they were 'very' concerned about mobile security threats, up from 36 percent in 2016. In total, 93 percent of organizations said that they were 'very' or 'somewhat' concerned by the mobile security challenges associated with a growing mobile workforce.

U.S. organizations were the most likely to be worried, with 98 percent of organizations citing that they were 'very' or 'somewhat' concerned. Europe is slightly less concerned; yet a still sizable 89 percent of respondents worried about increasing mobile threats.

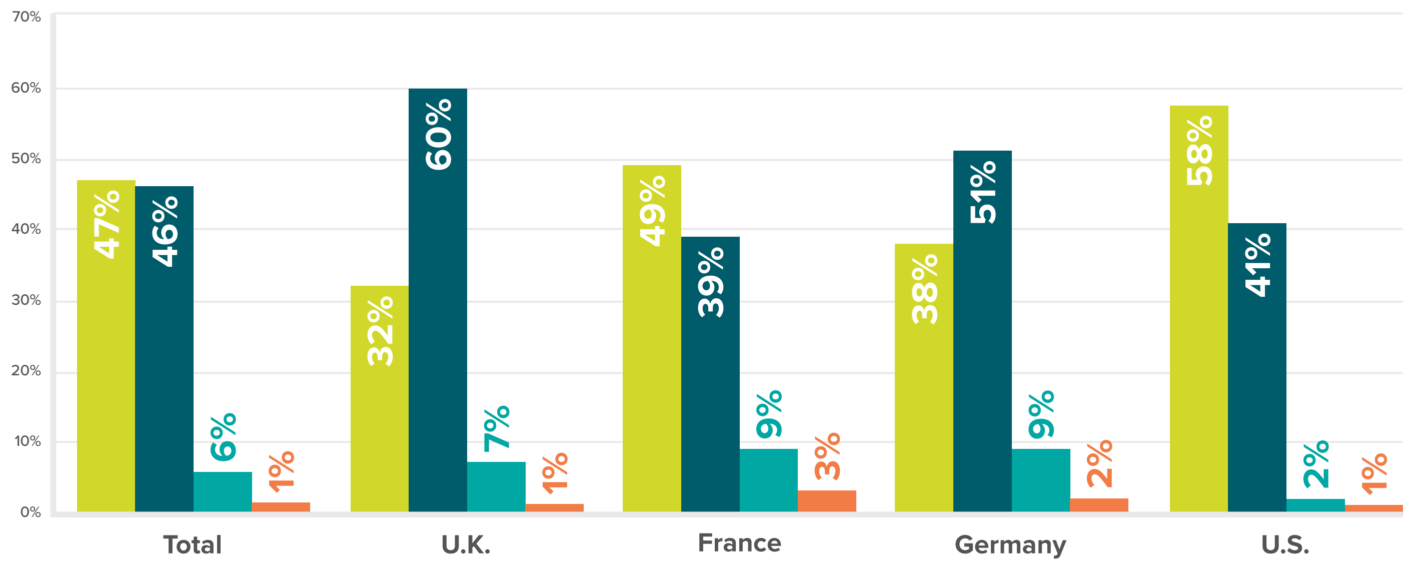
However, the starkest point of comparison is between the U.S. and U.K. Only 32 percent of U.K. respondents said that they were 'very' concerned about growing mobile security threats, compared to 58 percent of U.S. respondents.

FIG 1:

Source: Vanson Bourne

With a growing mobile workforce, are you concerned this presents an increasing number of mobile security challenges, as staff look to access corporate data/systems from a number of different locations using a multitude of devices and connection methods (e.g. free Wi-Fi hotspots)?

- A Very concerned
- B Somewhat concerned
- C Not very concerned
- D Not at all concerned



Beware of the coffee shop

Internet connectivity is essential for many business tasks, from checking email to video conferencing. Wi-Fi is incredibly popular with mobile workers. However, the security risks of using public Wi-Fi hotspots are well known, connecting to them without appropriate security will result in comprising both personal information as well as critical corporate data.

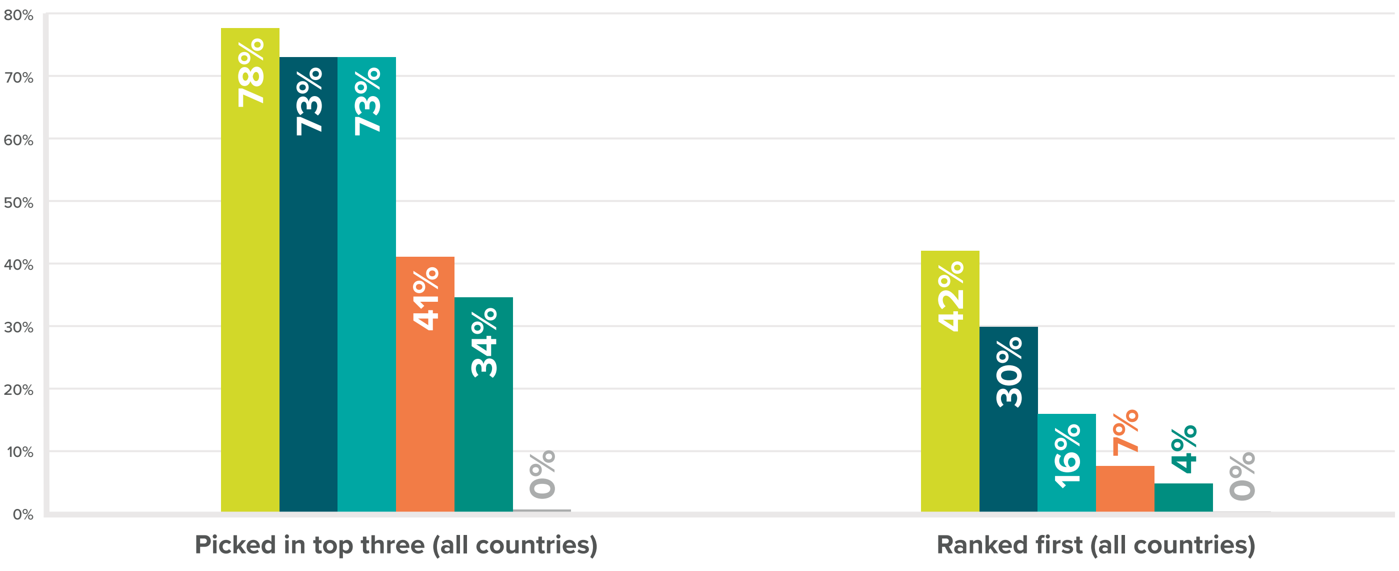
Wherever there is an unsecured public Wi-Fi network, there is the threat of attack. However, coffee shops are seen as the most dangerous public Wi-Fi venue of all. Perhaps, this is due to their popularity and convenience, as 78 percent of respondents chose coffee shops as one of their top three most popular locations. In total, 42 percent of respondents ranked coffee shops as the number one location. Airports came in second. And exhibition centers are considered the least concerning venues.

FIG 2:

Source: Vanson Bourne

Regardless of whether you or your employees use them, please rank your concern about public Wi-Fi security at the following venues:

A Cafés/coffee shops
B Airports
C Hotels
D Exhibition centres
E In-flight
F Other (please specify)



Man-in-the-middle attacks pose greatest threat

Cybercriminals will always follow the money. Just as they cashed in on the e-commerce boom, they were also remarkably quick to realize the ROI of targeting mobile professionals. The attacks themselves are becoming increasingly varied and sophisticated. Our research shows that man-in-the-middle attacks are considered to be the greatest mobile security concern of using public Wi-Fi hotpots (69 percent). This is when a hacker secretly attacks the data flowing to and from the internet to the mobile device.

However, man-in-the-middle attacks are not the only mobile security threat mobile workers face. More than half of respondents also said they were worried about unpatched operating systems, hotspot spoofing and a lack of encryption.

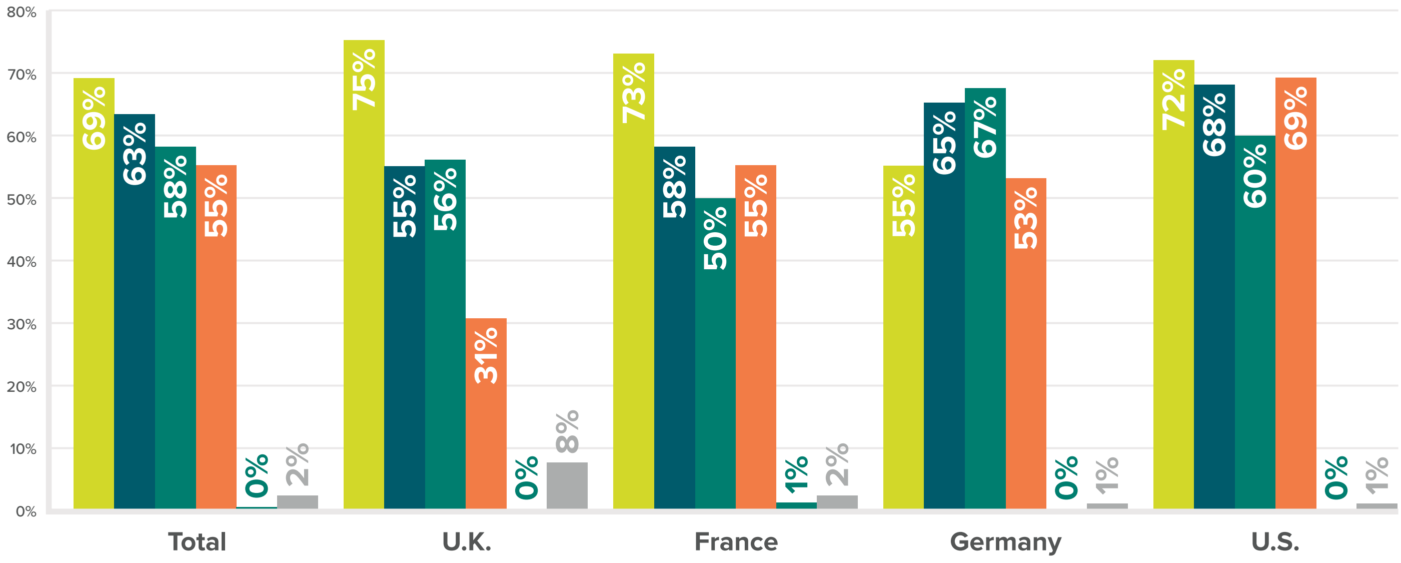
That being said, not everyone perceives a mobile security threat when accessing public Wi-Fi. In the survey, nearly one in ten U.K. respondents said that they have no security concerns at all regarding using public Wi-Fi. Contrast that with the U.S. and Germany, where only one percent of respondents answered in this way.

FIG 3:

Source: Vanson Bourne

What mobile security threats concern you when employees are using public Wi-Fi hotspots?

- A Man-in-the-middle attacks (where attackers secretly intercept communication between two parties without their knowledge)
- B Lack of encryption
- C Hotspot spoofing
- D Employees using insecure/unpatched mobile operating systems and applications
- E Other (please specify)
- F No mobile security threats concern me when using public Wi-Fi hotspots



CEOs are the greatest threat to the enterprise

In the event of a data breach, ultimately the buck stops with the CEO. It is therefore common to see C-level employees such as the CEO or CIO pay for high-profile data breaches with their jobs. However, ensuring cybersecurity is not only a C-suite responsibility; it appears businesses also consider their C-level employees as the primary targets of mobile security attacks.

In total, 40 percent of respondents said that C-level employees, including the CEO, are at the highest risk of being hacked outside of the office. Contributing factors could include the fact that senior employees have privileged access to highly sensitive and/or valuable corporate data and systems. They also travel regularly for business and tend to be more active across multiple mobile devices.

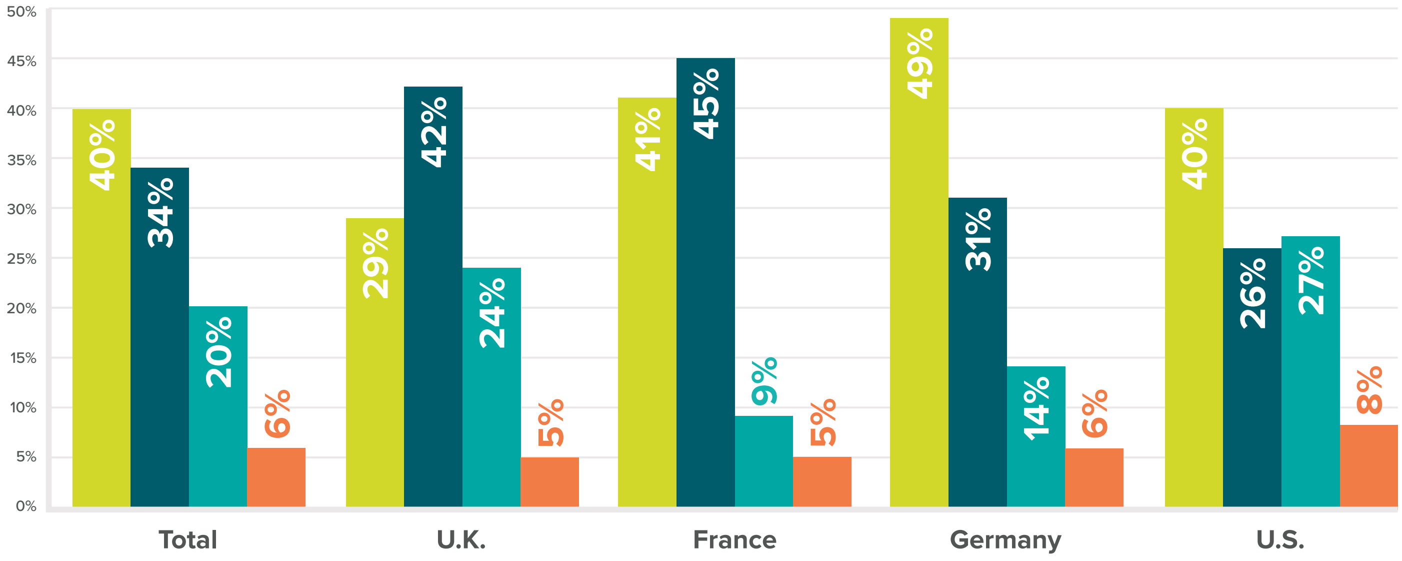
Regarding regional trends, Germans are the most worried about their C-level executives, with nearly half of respondents (49 percent) highlighting them as the great risk.

FIG 4:

Source: Vanson Bourne

In your experience, which role is typically most at risk of being hacked when working outside of the office?

- Ⓐ The CEO and other C-level executives
- Ⓑ Senior management
- Ⓒ Mid-level employees
- Ⓓ Interns/junior staff



Businesses opt to ban public Wi-Fi

Having already established that organizations are increasingly concerned about mobile security threats, their plan for how to mitigate them should come as no surprise, i.e. banning the use of public Wi-Fi hotspots. Indeed, 68 percent of organizations currently ban the use Wi-Fi hotspots. Almost a third (31 percent) of businesses ban their use at all times (up from 22 percent in 2016), with an additional 37 percent banning their use sometimes. Furthermore, 14 percent of organizations plan to introduce a ban on public Wi-Fi hotspots in the future. This is down from 20 percent in 2016 which might suggest that many organizations have introduced a ban in the last 12 months.

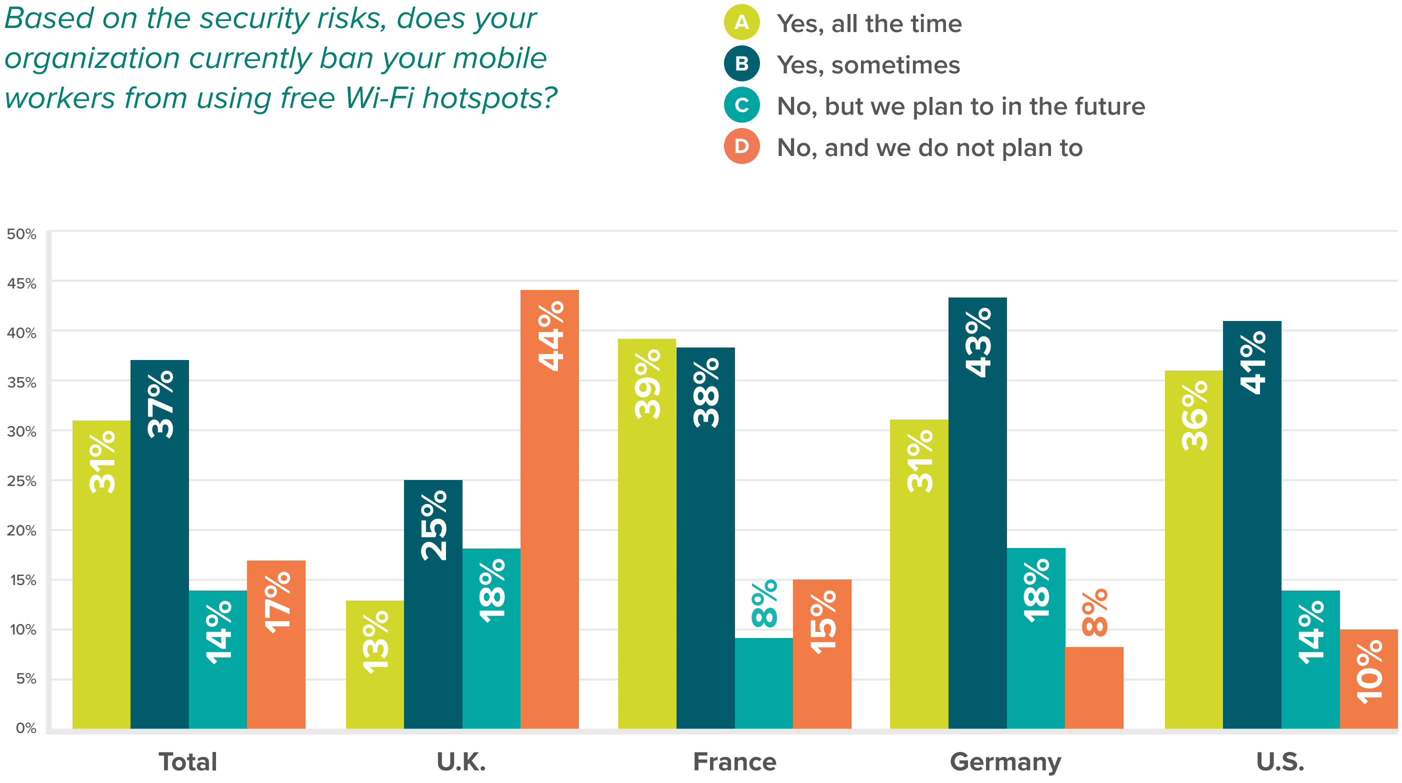
The U.K. is the most trusting of public Wi-Fi, with nearly two thirds of businesses (62 percent) not currently banning hotspot use and an additional 44 percent saying that they never plan to. In stark contrast, this figure is only 10 percent in the U.S. and 8 percent in Germany.

However, while the banning of public Wi-Fi hotpots may sound like a logical security decision, it may end up being detrimental to business goals. Modern organizations know that, security risks aside, they need to ensure that their employees remain connected and productive at all times. With the majority of electronic devices shipped worldwide being Wi-Fi only, blocking connectivity to Wi-Fi hotspots at coffee shops, hotels, airports and in flight could result in a drastic reduction in productivity. Instead, businesses should be looking to solutions like Virtual Private Networks to ensure security, regardless of the connectivity option users make.

FIG 5:

Source: Vanson Bourne

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



MiFi lives on despite security concerns

Despite the ubiquity of smartphone devices, most of which can become a public Wi-Fi hotspot, 75 percent of enterprises still allow or encourage the use of dedicated MiFi devices. Twenty-four percent of organizations surveyed supply or actively encourage their use, more than the percentage of organizations, which have banned their use due to security reasons (18 percent). In France, 29 percent of organizations ban the use of MiFi, which is much higher than the U.K. (11 percent) and the U.S. (15 percent), showing that the security concerns of MiFi devices are far more keenly felt there.

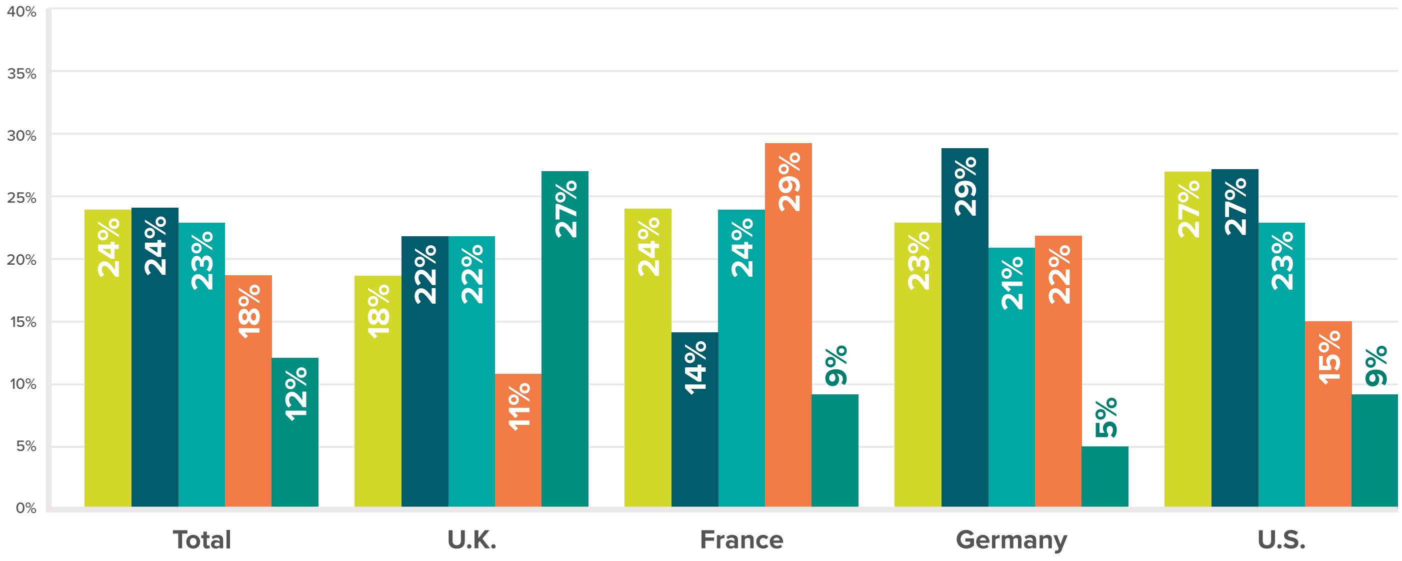
The flip side of this is that U.K. organizations are the most likely to encourage the use of other connectivity options (27 percent), suggesting that MiFi devices are not particularly popular in the U.K., whether for security reasons, like in France, or otherwise.

FIG 6:

Source: Vanson Bourne

Do you allow your employees to use MiFi devices (devices that are capable of becoming a personal hotspot or router)?

- A Yes, we supply MiFi devices and/or actively encourage their use
- B Yes, we allow employees to use their own MiFi devices anywhere
- C Yes, we allow employees to use their own MiFi devices, but only outside the enterprise
- D No, we have banned them due to security concerns
- E No, we encourage other connectivity options instead



Conclusion

The enterprise is more aware of the mobile security threat than ever, in terms of the highest risk locations, job roles and security threats. However, it is still struggling to find the right balance between productivity and security. Many enterprises are still resorting to banning the use of Wi-Fi hotspots entirely, despite the productivity boost they can provide when used correctly and securely.

The simple fact is that employees want to stay connected and productive, both inside and outside of the office. For convenience and guaranteed service, mobile workers will always seek out Wi-Fi connectivity, regardless of the security risks involved and may even do so if their employer has banned the use of public Wi-Fi hotpots. We are living in a mobile-first, Wi-Fi-first world, and businesses must ensure that their mobile workers are equipped with the services that allow them to get online and work securely at all times.

*The research was carried out during March 2017 and was conducted by independent research company Vanson Bourne.

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 60 million hotspots in more than 120 countries, 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 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