NEWS RELEASE

MobileIron Research Reveals the Future of Work is Everywhere: More Than 80% of Global Workforce Does Not Want to Return to the Office Full-Time

10/6/2020

Securing mobile devices, apps, and users should be every CIO's top priority as employees work from anywhere in the new Everywhere Enterprise

MOUNTAIN VIEW, Calif.--(BUSINESS WIRE)-- **MobileIron**, (NASDAQ: MOBL), the mobile-centric security platform for the Everywhere Enterprise, today announced the results of a new study, which revealed that more than 80% of global employees do not want to return to the office full-time, despite one in three (30%) employees claiming that being isolated from their team was the biggest hindrance to productivity during lockdown.

This press release features multimedia. View the full release here: **https://www.businesswire.com/news/home/20201006005128/en/**

The traditional office environment has transformed to an 'Everywhere Enterprise,' in which employees, IT infrastructures and customers are everywhere – and mobile devices provide access to everything. Organizations must urgently secure users, devices, apps and services across the Everywhere Enterprise. (Photo: Business Wire)

The COVID-19 pandemic has clearly changed the way people work and accelerated the already growing remote work trend. This has also created new security challenges for IT departments, as employees are increasingly using their own personal devices to access corporate data and services. Adding to the challenges posed by the new "**Everywhere Enterprise**" – in which employees, IT infrastructures, and customers are everywhere – is the fact that employees are not prioritizing security. The study found that one-third of workers (33%) consider IT security to be a low priority.

The current distributed remote work environment has also triggered a new threat landscape, with malicious actors increasingly targeting mobile devices with phishing attacks. These attacks range from basic to sophisticated and are likely to succeed, with many employees unaware of how to identify and avoid a phishing attack. The study revealed that 43% of global employees are not sure what a phishing attack is.

“Mobile devices are everywhere and have access to practically everything, yet most employees have inadequate mobile security measures in place, enabling hackers to have a heyday,” said Brian Foster, SVP Product Management, MobileIron. “Hackers know that people are using their loosely secured mobile devices more than ever before to access corporate data, and increasingly targeting them with phishing attacks. Every company needs to implement a mobile-centric security strategy that prioritizes user experience and enables employees to maintain maximum productivity on any device, anywhere, without compromising personal privacy.”

The study found that four distinct employee personas have emerged in the Everywhere Enterprise as a result of lockdown, and mobile devices play a more critical role than ever before in ensuring productivity:

Hybrid Henry:

- Typically works in financial services, professional services or the public sector.
- Ideally splits time equally between working at home and going into the office for face-to-face meetings; although this employee likes working from home, being isolated from teammates is the biggest hindrance to productivity.
- Depends on a laptop and mobile device, along with secure access to email, CRM applications and video collaboration tools, to stay productive.
- Believes that IT security ensures productivity and enhances the usability of devices. At the same time, this employee is only somewhat aware of phishing attacks.

Mobile Molly:

- Works constantly on the go using a range of mobile devices, such as tablets and phones, and often relies on public WiFi networks for work.
- Relies on remote collaboration tools and cloud suites to get work done.
- Views unreliable technology as the biggest hindrance to productivity as this individual is always on-the-go and heavily relies on mobile devices.
- Views IT security as a hindrance to productivity as it slows down the ability to get tasks done; this employee also believes IT security compromises personal privacy.
- This is the most likely persona to click on a malicious link due to a heavy reliance on mobile devices.

Desktop Dora:

- Finds being away from teammates and working from home a hindrance to productivity and can't wait to get back to the office.
- Prefers to work on a desktop computer from a fixed location than on mobile devices.
- Relies heavily on productivity suites to communicate with colleagues in and out of the office.
- Views IT security as a low priority and leaves it to the IT department to deal with. This employee is also only somewhat aware of phishing attacks.

Frontline Fred:

- Works on the frontlines in industries like healthcare, logistics or retail.
- Works from fixed and specific locations, such as hospitals or retail shops; This employee can't work remotely.
- Relies on purpose-built devices and applications, such as medical or courier devices and applications, to work; this employee is not as dependent on personal mobile devices for productivity as other personas.
- Realizes that IT security is essential to enabling productivity; this employee can't afford to have any device or application down time, given the specialist nature of their work.

"With more employees leveraging mobile devices to stay productive and work from anywhere than ever before, organizations need adopt a zero trust security approach to ensure that only trusted devices, apps, and users can access enterprise resources," continued Foster. "Organizations also need to bolster their mobile threat defenses, as cybercriminals are increasingly targeting text and SMS messages, social media, productivity, and messaging apps that enable link sharing with phishing attacks. To prevent unauthorized access to corporate data, organizations need to provide seamless anti-phishing technical controls that go beyond corporate email, to keep users secure wherever they work, on all of the devices they use to access those resources."

The study polled 1,200 workers across the U.S., U.K., France, Germany, Netherlands, Australia, and New Zealand. To download a complimentary copy of the full persona report, please visit **here**.

About MobileIron

MobileIron is redefining enterprise security with the industry's first mobile-centric security platform for the Everywhere Enterprise. In the Everywhere Enterprise, corporate data flows freely across devices and servers in the cloud, empowering workers to be productive anywhere they need to work. To secure access and protect data across this perimeter-less enterprise, MobileIron leverages a zero trust approach, which assumes bad actors are already in the network and secure access is determined by a "never trust, always verify" model.

MobileIron's platform combines award-winning and industry-leading **unified endpoint management** (UEM) capabilities with **passwordless multi-factor authentication** (Zero Sign-On) and **mobile threat defense** (MTD) to validate the device, establish user context, verify the network, and detect and remediate threats to ensure that only authorized users, devices, apps, and services can access business resources in a “work from everywhere” world. Over 20,000 organizations, including the world’s largest financial institutions, intelligence agencies, and other highly regulated companies, have chosen MobileIron to enable a seamless and secure user experience in the Everywhere Enterprise.

View source version on businesswire.com: https://www.businesswire.com/news/home/20201006005128/en/

Media contact:

Jenny Pfleiderer

press@mobileiron.com

Analyst contact:

Becca Chambers

bchambers@mobileiron.com

Source: MobileIron