45% of UK Companies Postponed Cybersecurity Initiatives for a Month or More to Focus on Remote Work Setup

Submitted by: Positive Marketing
Thursday, 18 June 2020

Sectigo “2020 Work-from-Home IT Impact Study” data reveals impact of pandemic on business productivity, performance, and security

18 June, 2020—MANCHESTER—March 2020 saw the beginning of worldwide lockdown measures that forced the majority of businesses worldwide to work remotely in response to COVID-19. Organizations quickly pivoted their operations from office environments to work-from-home (WFH) models, significantly impacting productivity, performance, and security. These are among the findings of the “2020 Work-from-Home IT Impact Study,” commissioned by Sectigo (https://sectigo.com/) and conducted by independent research firm Wakefield Research, which polled 500 IT professionals at companies with at least 1,000 employees in the UK, U.S., Canada, Germany, France, and Ireland, to understand the impact of the worldwide crisis on large businesses.

Transforming to a fully remote work environment required quick updates to technology, processes, and procedures, resulting in repercussions to revenue and cybersecurity. Surprisingly, the survey revealed that despite the need to adapt to a rapidly changing work environment, IT professionals report that their organizations saw performance improvements. In fact, almost half of UK respondents (49%) report that employee productivity at their company has increased as a result of WFH measures.

“As C-Level executives continue to embrace the increased productivity of a distributed workforce, they need to consider new approaches to security that rely on automation and secure digital identities,” said Sectigo CEO Bill Holtz. “The reality is that the enterprise currently uses a mix of authentication tools that frequently includes outdated or weak methods. This research indicates that with many employees remaining at home for the foreseeable future or even permanently, refining how we grant and manage digital access is more important than ever.”

Postponed Revenue to Ensure Business Continuity

While increased productivity may be one positive outcome, it certainly isn’t an immediate reality for many, as survey responses indicate that enabling remote workers came at the expense of more than just effort and time. Nearly 40% of those surveyed overall—36% in the UK—said that their organizations had to delay revenue-generating initiatives for a month or more to prioritize the setup and success of remote work and ensure their businesses were fully operational with little-to-no downtime.

While investing in WFH infrastructure was critical for business continuity, project delays have a potential long-term impact across the enterprise. Many IT professionals indicate that establishing WFH infrastructure compromised other important work in their departments. Similar to the number of those reporting that IT projects were forced to freeze, 45% of UK respondents said that they had to postpone cybersecurity initiatives for one month or longer as they focused on remote work setup.

Despite Transitional Challenges, Productivity Increases and WFH Cultures Grow

IT professionals feel that they and their coworkers have stepped up their performance despite the challenges of transitioning to WFH. More than half (53%) of UK IT professionals feel employee productivity has increased since the start of widespread remote work, while only 12% feel it has decreased. This confidence in productivity is especially high among IT professionals in executive positions. The study found that across regions, C-Level IT pros (63%) are more likely than mid-level (40%) and non-management (41%) IT pros to feel that overall productivity has increased. Since productivity is directly linked to increased revenue, this perception bodes well as enterprises move beyond the lockdown and jumpstart projects that have been stalled.

Not surprisingly, with productivity sustaining or increasing, 65% of UK respondents think that the number of remote workers at their company will increase somewhat (49%) or increase significantly (16%), compared to the pre-COVID-19 level, indicating a lasting impact from the pandemic.

A Mix of Remote Access Solutions Leaves Companies at Risk

While Zoom-bombing might have made headlines, only 33% of UK respondents expressed concern about that risk, while many more UK IT professionals worry about traditional cybersecurity threats. Phishing or other malicious emails (47%) and insecure Wi-Fi (48%) pose a higher perceived risk to remote work environments, outweighing concerns around Zoom-bombing, as well as unknown personal computers and BYOD devices (27%).

When it comes to securing networks, applications, and other systems from unauthorized access, UK respondents use various measures, including several with known vulnerabilities. An unfortunate fact is that strong and proven authentication technologies, such as user identity certificates (58%) and biometrics (26%), frequently take a back seat to methods with widely known weaknesses, including traditional username and password (74%) and hardware-token multi-factor authentication (68%).

False Sense of Security?

Although security breaches doubled in 2019 and the broad use of traditional security measures have proven to be vulnerable, two-thirds of UK respondents believe that their companies are investing “the right amount” on cybersecurity right now. However, 95% of UK respondents are likely to undertake additional measures to improve security and business continuity in the next 12 months due to widespread remote work—with 52% indicating that they would increase security for data and applications, compared to the pre-COVID-19 level, once offices are reopened.

For more information, the Sectigo “2020 Work-from-Home IT Impact Study” is available for download here (https://sectigo.com/resource-library/2020-work-from-home-it-impact-study).

Survey Methodology

The 2020 Work-from-Home IT Impact Study was conducted by Wakefield Research (www.wakefieldresearch.com) between May 15th and May 26th, 2020, among 500 IT professionals at companies across industries with at least 1,000 employees in the U.S., Canada, Germany, France, Ireland, and UK. The margin of error for the results is +/- 4.4 percentage points.

About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com (http://www.sectigo.com) and follow @SectigoHQ.

# # #

UK Media Contacts:

Ines Mitsou
Positive
+44 (0)770 388 4664
imitsou@positivemarketing.com

Max Bailey
Positive
+44 (0)793 331 8525
mbailey@positivemarketing.com