Working from home causes surge in security breaches, staff 'oblivious' to best practices

zdnet.com/article/working-from-home-trend-causes-surge-in-cybersecurity-costs-security-breaches

By Charlie Osborne for Zero Day | August 20, 2020 -- 10:00 GMT (03:00 PDT) | Topic: Working from home: The future of business is remote

Hybrid survival: Tips on how to manage our gradual return to the office

The COVID-19 pandemic shows little sign of slowing down, and for many businesses, employees are still working remotely and from home offices.

While some companies are gearing towards reopening their standard office spaces in the coming months -- and have all the challenges associated with how to do so safely to face -- they may also be facing repercussions of the rapid shift to remote working models in the cybersecurity space.

In the clamor to ensure employees could do their jobs from home, the enterprise needed to make sure members of staff had the right equipment as well as network and resource access.

However, according to Malwarebytes, the rushed response to COVID-19 in the business arena has created massive gaps in cybersecurity -- and security incidents have increased as a result.

On Thursday, the cybersecurity firm released a report (.PDF), "Enduring from Home: COVID-19's Impact on Business Security," examining the impact of the novel coronavirus in the security world.

Company telemetry and a survey conducted with 200 IT and cybersecurity professionals suggest that since the start of the pandemic, remote workers have caused a security breach in 20% of organizations.

As a result, 24% of survey respondents added that their organizations had to pay unexpected costs to address cybersecurity breaches or malware infections after shelter-in-place orders were imposed.

In total, 18% of those surveyed said cybersecurity was not a priority, and 5% went further -- admitting their staff were "oblivious" to best security practices.

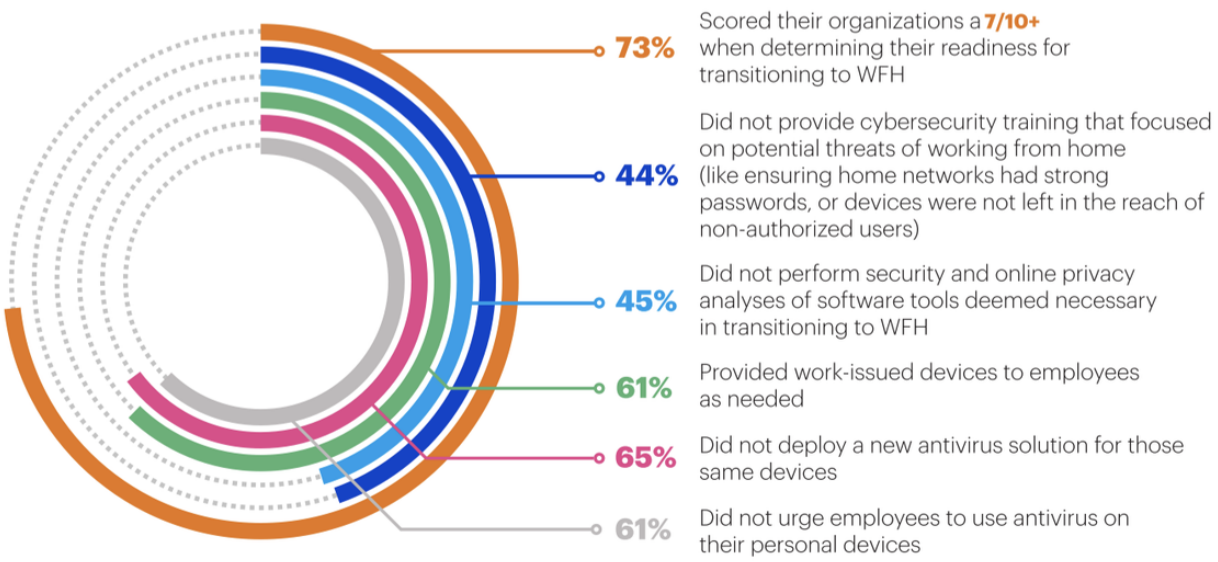
According to the cybersecurity firm, business email compromise, the quick shift to cloud services -- which may include improperly-configured buckets or access controls -- and improperly secured corporate Virtual Private Networks (VPNs) are all contributing to the emerging issue.

In addition, phishing email rates relating to COVID-19 have surged, with thousands of separate campaigns and fraudulent domains connected to the pandemic coming under the scrutiny of multiple security firms.

The UK National Health Service (NHS)'s key workers, for example, were hit with roughly 40,000 spam and phishing attempts between March and the first half of July, at the height of the pandemic in the country.

Malwarebytes cited NetWiredRC and AveMaria, remote desktop access-capable malware families, as common payloads for COVID-19-related phishing schemes.

Roughly 75% of survey respondents were positive about the transition to remote working, but 45% said that no additional security checks or audits were performed to check the security posture of these necessary changes. In addition, while 61% of organizations did provide their staff with remote working devices, 65% did not consider the deployment of any new security tools together with the equipment.



"Threat actors are adapting quickly as the landscape shifts to find new ways to capitalize on the remote workforce," said Adam Kujawa, director at Malwarebytes Labs. "We saw a substantial increase in the use of cloud and collaboration tools, paired with concerns about the security of these tools. This tells us that we need to closely evaluate cybersecurity in relation to these tools, as well as the vulnerabilities of working in dispersed environments, in order to mitigate threats more effectively."
