Surge in security concerns due to remote working during COVID-19 crisis

blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/

Fleming Shi

May 6, 2020May 5, 2020

As people settle into the new way of working with many organizations working from home, it comes as no surprise that attention now turns to being productive as well as secure. In a recent survey, Barracuda found that almost half (46%) of global businesses have encountered at least one cybersecurity scare since shifting to a remote working model during the COVID-19 lockdown. What's more, an astounding 49 percent say they expect to see a data breach or cybersecurity incident in the next month due to remote working.

The global survey, which was commissioned by Barracuda and conducted by independent research agency Censuswide, includes answers from over 1,000 business decision makers in the UK, U.S., France, and Germany. More than half of respondents (51%) said they have already seen an increase in email phishing attacks since shifting to a remote working model.

51%
of organizations have already seen an increase in email phishing attacks since shifting to a remote working model
Barracuda
Your journey, secured.

Key findings include:

- 51% of respondents have already seen an increase in email phishing attacks since shifting to a remote working model
- 51% of respondents said their workforce is not proficient or properly trained in the cyber risks associated with remote working
- 46% are not confident their web applications are secure
- 50% have allowed employees to use personal email address and personal devices to conduct company work
- 40% of respondents have cut their cybersecurity budgets as a cost saving measure to help tackle the COVID-19 crisis

Pitfalls of a rushed transition

The survey results make it clear that the increase in cybersecurity concerns, and quantity of email phishing attacks aimed at businesses, is a result of the urgency of the COVID-19 crisis, which forced many companies to instantly implement a remote working system to protect the health and safety of employees. Inevitably, the switch to a complete remote working model in such a short space of time brought with it a myriad of security challenges, particularly with many employees using personal devices to exchange and share data.

In fact, Barracuda's research found that 51 percent of business decision makers agreed that their workforce is not proficient or properly trained in the cyber risks associated with long-term remote working. Additionally, 46 percent claimed they are not confident that their web applications are completely secure, and 50 percent have allowed employees to use personal email addresses and personal devices to conduct company work.

51% of business decision makers agreed that their workforce is not properly trained in the cyber risks associated with long-term remote working #RemoteWork Click To Tweet
Additional findings include:

- 46% of respondents have already had at least one cybersecurity scare since shifting to a remote working model
- 49% fully expect to see a data breach or cybersecurity incident in the next month due to remote working
- 50% would consider making workforce reductions if it meant company data protection and security could be properly funded
- 55% say they would not have implemented remote working within the next 5 years, had it not been for the COVID-19 crisis
- 56% plan to continue widespread remote working even after the crisis is over
- 53% report that the COVID-19 crisis had made them accelerate plans for moving all their data to 100% cloud-based model

56%
of organizations plan to continue widespread remote working even after the COVID-19 crisis is over
Barracuda.
Your journey, secured.

Risks of neglecting cybersecurity

Most worryingly, however, two in five businesses (40%) have admitted to cutting their cybersecurity budget as a cost-saving measure to help tackle the COVID-19 crisis.

This is certainly the wrong move. Since the COVID-19 pandemic swept the globe, opportunistic hackers are on the lookout to target vulnerable organizations, which may have weak security infrastructure in place during this difficult time. When cybersecurity is deprioritized or neglected by businesses, hackers can target untrained, susceptible remote workers with increasingly sophisticated and incredibly realistic email phishing attacks.

As many businesses enter their third month of remote working, it's time they refocus efforts on tackling this growing cyber threat. At this crucial time, one successful data breach could be the final straw for many businesses, which are already facing an uphill battle against COVID-19. And, in the current threat landscape, it's no longer a matter of 'if' a company's security will be tested by cyber criminals, it's a matter of 'when.'

Barracuda survey: 55% of respondents said they would not have implemented #RemoteWorking within the next five years had it not been for #COVID19Click To Tweet

Accelerated transitions

The COVID-19 pandemic significantly accelerated the transition to remote working, a trend that was gaining slowly gaining momentum but wasn't expected to be widespread anytime soon. According to the Barracuda survey, 55 percent of respondents said they would not have implemented remote working within the next five years had it not been for the current crisis. For many organizations, the change is likely to be a lasting one now that they've make the transition, though. More than half (56%) of respondents said they plan to continue widespread remote working after the crisis is over.

Another transition that has sped up in response to the current situation is the shift to the cloud. A full 53 percent report that the COVID-19 crisis had made them accelerate plans for moving all their data to 100-percent cloud-based model, a change that will have a long-term impact on how organizations operate.

Enable remote work while securing your data during the COVID-19 pandemic