Cybersecurity staff are being transferred to IT support. That's adding to the risk of data breaches

zdnet.com/article/cybersecurity-staff-are-being-transferred-to-it-support-thats-adding-to-the-risk-of-data-breaches

Danny Palmer

The coronavirus pandemic has brought big changes to the cybersecurity industry, with the vast majority of security professionals now working from home – and almost half being reassigned to general IT support as organisations adapt to the challenges of remote working.

But it's a move that could be making organisations more vulnerable to hackers and cyberattacks.

A survey by International Information System Security Certification Consortium – also known as (ISC)² – examined how the global COVID-19 outbreak has affected the work of cybersecurity professionals since the shift towards remote working as a result of social distancing and lockdown measures to contain the coronavirus.

It's because of the sudden change in working that 47% of those surveyed say they've found themselves reassigned to general IT tasks as organisations adapt to the new reality.

In 90% of cases, the security team is working remotely full-time – the remaining 10% that are still going to an office are doing so either because their organisation is sensitive in nature and the work can't be done from home, or the company doesn't have the capability to allow full-

time remote work. In many cases, these people would prefer to stay home, but as some respondents put it, "duty calls".

In a significant number of cases, those duties involve dealing with a rise in the number of cyberattacks and other security incidents: overall 23% said the number of these had gone up since the transition to remote work and in some cases security teams are tracking double the number of incidents.

Worryingly, 30% of those security professionals who've been reassigned to IT say there's been a rise in security incidents against their organisation, compared to 17% who haven't changed roles but say they're dealing with more attacks. It could indicate that the organisations who are transferring security staff to IT are more at risk from hacking.

The rise in attacks comes as cyber criminals look to take advantage of coronavirus for their own gain by targeting remote workers, people who in many cases haven't worked from home before so are more vulnerable to falling victim to social engineering, phishing and other attacks – especially if coronavirus-related issues are used as a lure.

"COVID-19 hit us with all the necessary ingredients to fuel cybercrime: 100% work from home [WFH] before most organizations were really ready, chaos caused by technical issues plaguing workers not used to WFH, panic and desire to 'know more' and temptation to visit unverified websites in search of up-to-the-minute information," said one respondent.

And there are signs that security teams are struggling to find the resources they need to keep workers secure, with 15% saying that they don't have the tools required to keep remote employees safe, while another 34% say they have the tools for now, but fear it's only for the time being.

"Sharing this information helps our members and other professionals in the field understand the challenges their peers are facing, and hopefully realize they are not alone, even if many of them are feeling isolated as they adjust to working from home," said Wesley Simpson, COO of (ISC)².