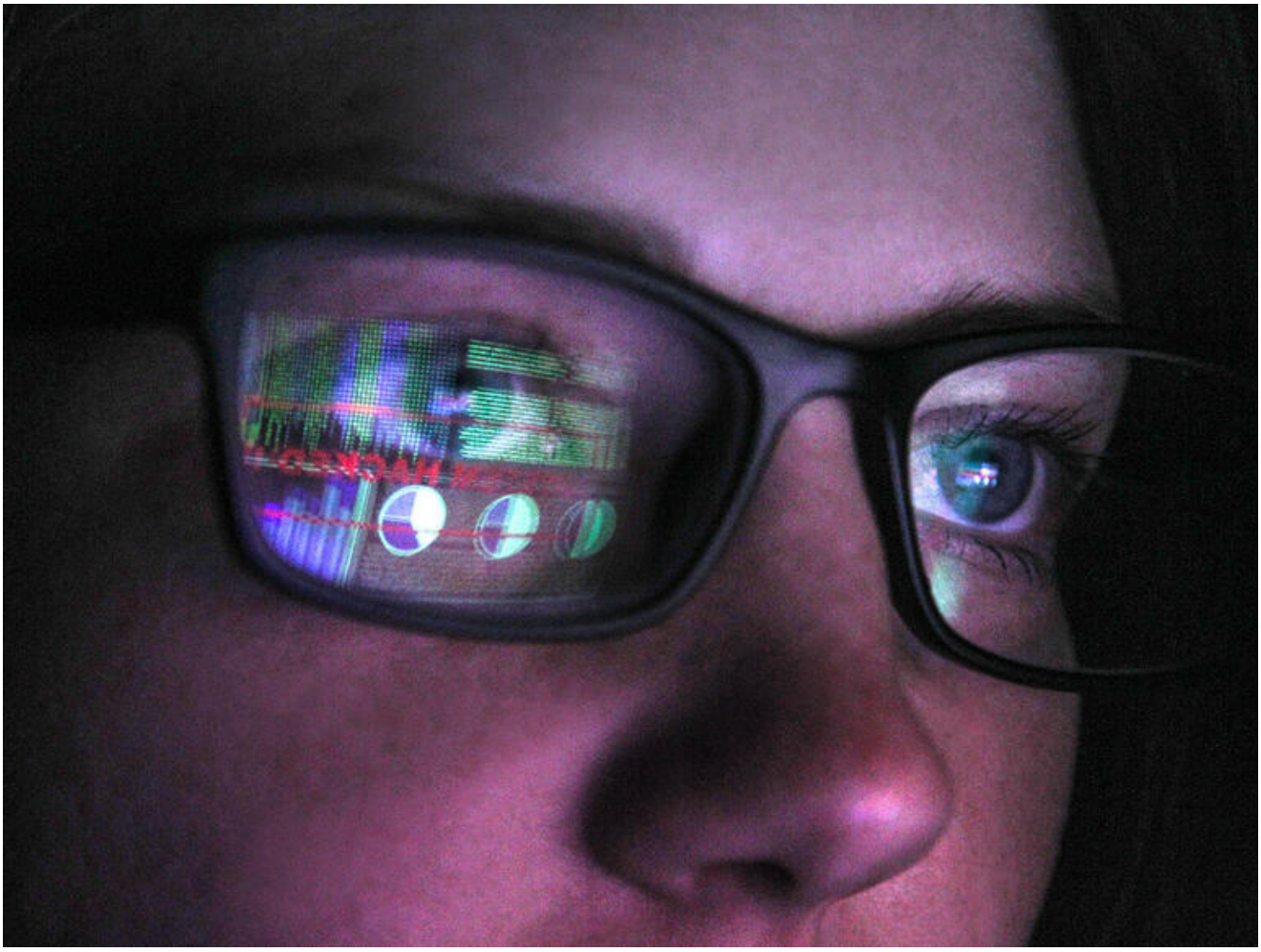
WFH is a cybersecurity "ticking time bomb," according to a new report

techrepublic.com/article/wfh-is-a-cybersecurity-ticking-time-bomb-according-to-a-new-report

R. Dallon Adams

IT teams are experiencing employee pushback due to remote work policies and many feel like cybersecurity is a "thankless task" and that they're the "bad guys" for implementing these rules.



GettyImages/Petri Oeschger

At the onset of COVID-19, companies around the globe shifted to remote work on short notice. The revamped operations transformed the traditional workday and cybersecurity efforts for companies virtually overnight, leading to new challenges for remote workers and IT teams. On Thursday, HP released an HP Wolf Security report titled "Rebellions & Rejection." The findings detail employee pushback due to company cybersecurity policies and operational drawbacks for IT teams overseeing these networks.

"The fact that workers are actively circumventing security should be a worry for any CISO– this is how breaches can be born," said Ian Pratt, global head of security for personal systems at HP, in a press release. "If security is too cumbersome and weighs people down, then people will find a way around it. Instead, security should fit as much as possible into existing working patterns and flows, with technology that is unobtrusive, secure-by-design and user-intuitive."

Remote work: A cybersecurity "ticking time bomb"

During the initial shift to remote operations, ensuring business continuity took precedent for many companies. At the same time, these new operations also presented security risks with remote workers logging on from home on a mixed bag of personal and company devices.

According to the HP report, 76% of respondent IT teams said "security took a back seat to continuity during the pandemic," 91% felt "pressure to compromise security for business continuity" and 83% believe remote work has "become a 'ticking time bomb' for a network breach."

The switch to remote work has also led companies to adopt new policies regarding telecommuting with these rules ranging from home office requirements to internet speeds and security standards. According to the HP report, virtually all respondent IT teams (91%) said they "updated security policies to account for WFH" and 78% "restricted access to websites and applications."

"CISOs are dealing with increasing volume, velocity and severity of attacks. Their teams are having to work around the clock to keep the business safe, while facilitating mass digital transformation with reduced visibility," said Joanna Burkey, CISO at HP, in a press release. "Cybersecurity teams should no longer be burdened with the weight of securing the business solely on their shoulders, cybersecurity is an end-to-end discipline in which everyone needs to engage."

Employee burnout: IT teams feeling dejected

The findings also identify "frustration" among office workers who feel these IT security restrictions impede their day-to-day workflows. For example, about half of respondent office workers said "security measures result in a lot of wasted time," 37% thought "security policies and technologies are too restrictive," according to the report.

Interestingly, the age of remote workers may impact their sentiments regarding company security policies. According to the report, 48% of workers between the ages of 18 and 24 believe "security policies are a hindrance" and 54% were "more worried about deadlines than exposing the business to a data breach" and 39% were unsure of their company's data cybersecurity policy.

In the IT space, playing the role of network security police amid a remote work experiment at scale comes with lots of red tape and no shortage of drawbacks. According to the report, 80% of respondent IT teams said they "experienced pushback from workers who do not like controls being put on them at home with surprising frequency" and 69% said "they're made to feel like the 'bad guys' for imposing restrictions on employees" and 80% felt IT cybersecurity has "become a 'thankless task.'"

"To create a more collaborative security culture, we must engage and educate employees on the growing cybersecurity risks, while IT teams need to better understand how security impacts workflows and productivity," Burkey said. "From here, security needs to be re-evaluated based on the needs of both the business and the hybrid worker."

Remote network security threats

Over the last year, cybersecurity attacks have surged with the switch to remote work. A portion of the report highlights IT perceptions regarding the threat level of various cyberattack methods as employees "increasingly" telecommute on networks with potential security issues. Ransomware topped the list (84%) followed by laptop- and PC-focused firmware attacks (83%), unpatched devices with exploited vulnerabilities (83%) and data leakage (82%), in order.

"Man-in-the-middle attacks" and account/device takeovers (81%), IoT threats (79%), targeted attacks (77%) and printer-focused firmware attacks (76%) round out the top eight perceived threats.