5 WAYS USERS CIRCUMVENT SECURITY MEASURES AND HOW TO PREVENT IT

Workers usually choose convenience over security, especially if you force them to jump through too many hoops. But there are steps you can take to shift the balance back in security's favor.

Cybersecurity experts support and encourage locking down sensitive data to keep it out of the wrong hands. On the other hand, they say, companies can go overboard with restrictions making it hard if not nearly impossible for workers to do their jobs efficiently. So, they find workarounds. It's a scenario that slows productivity and, ironically, puts the data itself in jeopardy.

Organizations don't need to overhaul their operations to achieve a better balance of security measures and usability, experts say. They can instead start by addressing several common areas where workers tend to sacrifice security for productivity. Here are some areas to examine.

Complex password requirements - Passwords are a security staple, yet organizations that create overly complex password policies such as long passwords, excessive special characters, and aggressive change policies often entice workers write down or, even worse, store them in a computer file to remember them. Security professionals recommend organizations be smarter with their password policies and limit the complex requirements to more reasonable levels.

Sharing passwords - Although it's not smart from a security standpoint, workers do so because they need to share access to their files with co-workers. To counteract such actions, organizations need to more accurately identify which users need access to which files and then create policies on how to security-enable that shared access.

Sign-in overload - Multiple log-in and authentication requirements to are a drag on productivity. These drags push workers to circumvent log-in requirements by transferring the data they need out of secure applications and putting it in an easy-to-access spot. Identity and single sign-on applications, tokens, and biometrics are effective solutions where quick and easy access is needed.

Data held hostage - The need to protect sensitive data has become paramount for most organizations. Added layers of protection often slow productivity and push workers to unsafe practices like copying files, or snapping photos of information needed. Organizations are creating problems for themselves if they treat all data with the same sensitivity. Instead, spend more upfront work on data classification to protect sensitive information while removing barriers to information that most workers use for their jobs

Cumbersome workflow - Workers sharing, scanning, emailing, and printing documents in the normal course of their duties are either not aware of the potential security risks, or they are but move forward anyway because they must to get their job done. Companies need to invest in the technologies and system designs that make it easy for workers to follow the rules and, more importantly, automate as much of that as possible.

We have to look at the human process flow, so security is not obtrusive, and we have to look at these process flows and insert security appropriately and based on the risk, so there's not one size fits all.