Cybersecurity Best Practices For Teleworkers

cyber security risk management

Summary: As the remote work trend intensifies, it brings to the forefront the importance of strong cybersecurity practices. We provide some insight.

The problem with remote work for your employees could be distraction related. After all, a whopping 23% of millennials still live with their parents, according to Zillow research. So, noise levels at home might not be conducive to such things. Bankers will need to think about the broader context for sure, no matter the path chosen on remote working arrangements.

To help you here, we remind our readers that we recently wrote about the growing trend of flexible work arrangements, which includes working remotely. As this trend intensifies, it brings to the forefront the importance of strong cybersecurity practices.

Community banks can be particularly at risk when it comes to remote work security risks, since they tend to have fewer resources. As such, if you are planning on having teleworkers (aka remote employees), it's important to establish a well-defined policy for them. This includes utilizing strong passwords that can't be re-used, since replicating passwords can leave multiple systems vulnerable to compromise. Two-factor authentication is also a must, since password credentials can be breached.

It's also advisable to encourage employees to log off at the end of the day and turn off network sharing and Wi-Fi and Bluetooth connectivity (or have your IT team force a shutdown through the system each night to effectively "lock" open doors). Banks should ensure that their software employs end-to-end encryption too.

An additional idea is to limit employees' access to sensitive data whether at work or remote. This is true for all employees, but can be especially important in the case of remote workers. Employees should only have access to data they need for their job. It's also advisable to restrict employees from downloading unapproved software onto any corporate equipment.

Banks also need to ensure that any devices used by remote employees have up-to-date firewall, anti-malware, and anti-virus software. These devices should be fully encrypted for protection in the event it is lost or stolen too. Additionally, banks should make sure they have the capability to remotely wipe corporate devices if and as needed.

Another must is for remote workers to log in securely via VPN, for example. Employees who log in via unsecured Wi-Fi are a danger to the bank's intellectual property. This can be especially nettlesome since many mobile devices have Wi-Fi auto connect features.

Banks can't afford to take for granted that remote workers are following all the rules. Rather, monitor remote workers using any number of tracking apps. Be mindful that some states may require employee consent for these purposes too.

For cost-savings and convenience, there's been growing demand to allow remote employees to use personal devices for work purposes, but banks need to understand the risks such as the potential for crosscontamination. One cyber regulator some time ago said they saw "bring your own device" more as "bring your own danger" when it comes to banks, so be extra diligent.

When it comes to security for remote workers, there's no simple solution, so expect to refine as you go and have layers of protection. It's critical for banks that offer this option to be sure intellectual property remains secure as well.

ON DEMAND HELP FOR COMMUNITY BANKERS

Community bankers face many difficult challenges every year, but you are not alone. Our experts stand ready to help you address a variety of issues. Go here to view options and opportunities.