The Cybersecurity Risks of Remote Work

cyber security employees

Summary: Hybrid work arrangements are here to stay. Given this reality, CFIs should be aware of the cybersecurity risks created when people work from home and how to protect against them.

In 1975, billionaire Howard Hughes anchored his ship, the Glomar Explorer, in the Pacific Ocean, claiming that he was mining manganese nodules — mineral masses found along the ocean floor that are an important component of steel. In reality, Hughes' ship was a cover for Project Azorian, a CIA mission to retrieve a Soviet submarine that sank in 1968. Artifacts from Project Azorian are on display in the CIA's museum, but don't expect to visit them anytime soon: the museum is housed within the CIA's Langley, Virginia headquarters and therefore closed to the public for security reasons.

Unfortunately for financial institutions, keeping sensitive information safe is no longer as simple as keeping physical documents under lock and key. With hybrid and remote work arrangements a seemingly permanent part of the employment landscape, community financial institutions (CFIs) need to be aware of the cybersecurity risks that are created when people work from home, particularly when they connect through the cloud.

Remote Security Challenges

The benefit of hybrid work arrangements is that employees can work from anywhere and are no longer tied to an office. But working remotely means disconnecting from an organization's security and leaving IT departments with what is often little clarity regarding the security measures that employees have in place outside the office. It has not gone unnoticed by hackers that many remote employees use third-party applications to connect to the cloud, or work from personal devices they set up themselves that may have outdated operating systems or lack proper encryption. Even if an individual's computer is well secured, data can still be exposed through secondary devices such as cameras and printers, which people often overlook.

According to professional services association Praxity, the FBI's Internet Crime Complaint Center, there was a 300% increase in the number of cybercrimes reported at the onset of the COVID-19 pandemic. VMware, a cloud services provider, found that 76% of global cybersecurity professionals attribute that uptick to people working remotely.

Fortifying Your Security

Ensuring adequate security for hybrid workers requires broadening your organization's strategy and identifying any wireless connections that may not be well protected. One of the most important things CFIs can do on the security front is to clearly communicate with employees and set clear cybersecurity policies and best practices for remote workers. Employees need to understand the risks that can be created by something as simple as sending information through a personal email account or a device with a weak password, or utilizing an unsecured Wi-Fi connection. IT support should also be easily accessible for remote employees, and they should take the time to review the individual security of each hybrid or remote worker, walk them through security measures they should be taking, and why.

The following are a few things IT specialists should be aware of when reviewing whether your organization's security is adequately configured for hybrid work.

- **Encryption.** Require and provide software and tools for employees to encrypt online communications and Wi-Fi connections.
- **Secure devices.** Consider requiring that employees use only company-supplied laptops and devices for work that are equipped with biometric security measures.
- **Up-to-date software & antivirus.** Ensure that operating systems have been updated with the latest patches and make it clear to employees the importance of not ignoring upgrade notifications. You'll also want to verify that updated antivirus protection and data loss software is active on each employee's computer.
- **Password protection.** Set strong password requirements and make sure employees know what makes a strong password. Also, require that employees update passwords at regular set intervals.
- **Authentication methods.** Improve the security of virtual private networks (VPNs) by adding multi-factor authentication so that employees will be notified and have to confirm their identity whenever anyone tries to access data. Though financial institutions have long utilized VPN to secure remote connections for employees, hackers have become increasingly sophisticated in their efforts to hack such security measures by exploiting compromised credentials available on the dark web. The extra security of MFA adds another gate to keep out unauthorized individuals.
- **Consistent monitoring.** Continuously monitor your organization's security landscape and look for any weaknesses that hackers could take advantage of.

In a hybrid work environment, failing to educate employees about less-than-obvious security risks can translate to major security issues for CFIs. With hackers targeting the weaknesses created by hybrid work arrangements, establishing clear and thorough remote security measures is critical for CFIs.

PCBB PODCAST: EXTRAORDINARY SALES RESULTS

PCBB's podcast — Banking Out Loud — has a new episode! Listen for insights on successful selling, including three tips for success and three mistakes to avoid, with guest speaker Archie Kelley, Managing Principal of SalesPhysics.

ECONOMY & RATES

Rates As Of: 11/21/2022 05:40AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.34	0.12	4.28
6M	4.61	0.04	4.42
1Y	4.71	0.09	4.33
2Y	4.50	0.02	3.77
5Y	3.99	-0.24	2.73
10Y	3.81	-0.25	2.29
30Y	3.90	-0.27	1.99

FF Market	FF Disc	IORB
3.83	4.00	3.90

SOFR	Prime	OBFR
3.80	7.00	3.82