Securing hybrid and remote workforces now and in the future

Businesses are embracing the transition to a permanent remote workforce, but with it comes heightened cyber security risk. Here's what to do to keep your business safe.

Key takeaways

- Remote and hybrid workforces are likely a permanent fixture, so it's important to create and maintain secure digital infrastructures.
- Having remote staff expands an organization's threat surface, with an increasing number of threats able to gain entry.
- Multiple layers of security controls, processes and employee education are necessary to maintain digital resiliency and business continuity in a permanent hybrid or remote work structure.

Two years after our sudden and necessary shift to remote work, people are returning to the office. But with 91% of employees wanting to maintain some form of flexible work — whether that's keeping a full-time remote schedule or a hybrid of remote and in-office hours — it's clear that the hybrid workplace is here to stay.[1] In fact, some estimate that by 2026, 40.7 million Americans will be working remotely — a 108% increase over pre-pandemic levels.[2]

Although a work-from-anywhere model has benefits for both employers and employees, traditional layers of cyber security do not provide enough protection. The digital infrastructure necessary to support remote workers is inherently more vulnerable to threats than on-premises security. Each remote worker who connects to the corporate network represents a new point of access and a new potential security risk that didn't exist previously.

The combination of an expanded threat surface with remote (and possibly careless) gatekeepers has been far too enticing for opportunistic cyber criminals. The FBI reported a 69% increase in internet crime complaints in 2020,[3] and ransomware payments reached an estimated $692 million that same year — a dramatic 455% increase over the previous year.[4]

[1] Gallup, "Remote Work Persisting and Trending Permanent," October 2021.
[2] Upwork, "Future Workforce Report 2021," September 2021.
[3] FBI, "2020 Internet Crime Report," March 2021.
[4] Chainalysis, "2022 Crypto Crime Report," February 2022.

Because businesses initially had little choice in 2020 but to rapidly transition to a mostly digital framework, their focus then was on efficiency and functionality over security. Today, as companies shift to remote and hybrid work as a permanent fixture, security models must evolve to minimize risk and tamp down the level of cyber crime aimed at organizations.

Traditional security is no longer enough

Traditional layers of protection, such as firewalls and on-premises network security, don't offer enough defense for a permanent remote or hybrid work environment. Threats that didn't penetrate the hard-wired corporate perimeter or expose organizations to mission-critical risk in the past become more dangerous with a dispersed workforce.

For instance, in the pre-pandemic landscape, a distributed denial-of-service (DDoS) attack could shut down some elements of a business by taking a website or service offline, but it mostly affected external-facing digital operations. With a remote workforce, a DDoS attack could cripple an entire organization by taking down the virtual private network (VPN) that remote workers rely on to access corporate resources.

"Some estimate that by 2026, 40.7 million Americans will be working remotely — a 108% increase over pre-pandemic levels."

Additionally, cyber security risk increases exponentially when workers leave the corporate perimeter, with networks jeopardized by an increase of unsafe activity from remote employees themselves. Without personal oversight, remote workers are more likely to practice poor cyber security hygiene. In fact, one in three employees believe they can get away with riskier security behaviors while working remotely, and 56% of IT leaders believe employees have picked up bad security habits working from home.[5]

Common security missteps

Connecting with unsecured networks

Using unsecured home or public Wi-Fi to connect to the company network leaves it vulnerable to malware and other cyber threats. Poor (or absent) security controls on these networks allow cyber criminals to gain easy admission.

Examples: *Public Wi-Fi, home networks*

Using personal devices for work

Personal devices often lack the security software and configurations that IT teams load onto corporate devices. When users connect their potentially compromised personal devices to corporate networks, they weaken the security perimeter. Meanwhile, sensitive personal data, email and other files and functions can be easily accessed by co-workers.

Examples: *Desktop PCs, laptops, personal cell phones*

Integrating Internet of Things (IoT) devices

The proliferation of smart home devices introduced new threat vectors when employees started working from home. IoT devices often have limited default security settings. When connected to the same network used by remote employees, they can create unsecured entry points to a corporate network if users don't practice good password hygiene or ensure that all software and patches are up to date.

Examples*: Home assistants, smart locks and appliances, wearable tech*

[5] Tessian, "Back to Work: Security Behaviors Report," June 2021.

Employing Shadow IT

As employees rapidly adapted to working remotely, many sought workarounds to increase productivity, such as cloud-based collaboration tools. This so-called "shadow IT" — i.e., the use of technology solutions that haven't been vetted by the IT department — can pose significant security risk. Any shadow IT downloaded to corporate devices without IT knowledge introduces risk not only of hefty fines for noncompliance and unauthorized use, but also of destabilizing organizations' digital infrastructures.

Examples: *Productivity software, cloud storage, messaging apps*

Exposing data

Employees may leave corporate or personal devices unattended in their apartments or homes, with proprietary data out in the open for roommates, guests or family members to see. Risk of data theft or extortion increases when remote workers leave their computers without closing laptop lids or changing settings to "sleep."

Examples: *Financial data, customers' personal information, vendor names*

New security best practices

To better support safe remote and hybrid work, organizations need to strengthen and expand their security perimeter, tools, protocols and training by incorporating the remote environment into their risk modeling. Most importantly, businesses need to ensure that they build both resiliency and scalability into their security and support systems.

In order to do so with some degree of permanence, organizations should incorporate the following considerations into their security posture:

Update security processes

Processes that were developed for physical workplaces did not consider the elements needed for a resilient digital infrastructure. Be sure your security processes — such as incident response, monitoring and reporting — are updated to support remote work.

- **Update incident response plans** with contingencies for remote or hybrid employees, including alternate secure modes of communication for staff or business partners and protocols for maintaining productivity during a security event.
- **Revise identity verification and access management processes** to consider stronger authentication controls and more stringent access policies, which better support a remote digital infrastructure.

Resiliency check: *If a cyber incident were to take place, does every employee know what to do? Run security drills, penetration tests and tabletop exercises to test company policy against specific scenarios. Then examine cyber security plans holistically for gaps in protection and opportunities to layer defenses.*

Establish internal communications protocols

How do employees communicate in this new environment? When all employees were on premises, it was easy to walk to someone's desk and informally discuss concerns or validate processes. Now a digital network provides the communications channels to support these conversations.

- **Provide key tools,** such as vetted communications software and employee education on safe, informal digital interactions.
- **Issue shared processes** and institutional knowledge to new and partner employees.

Resiliency check: *If the tools above or corporate network becomes compromised, how would you communicate with your employees? Have you planned on alternative ways to keep your company's workforce informed and engaged during a cyber incident that compromises those channels?*

Establish external communications protocols

When thinking about how to communicate sensitive information with clients, vendors, investors or shareholders outside the organization, which key security principles need to be in place?

- **Expand external communications policies** to include remote channels, such as data sharing and file transfer, financial transactions, mergers and acquisitions and shared confidential customer information.
- **Route best practices for safe external communication** to all relevant parties, including comprehensive guidance on each channel, audience and approved device, as well as boundaries for what's acceptable to share.

Resiliency check: *Understand when and how to communicate securely with external parties in the day-to-day, as well as in the event of a cyber incident. Communication during these incidents is critical in maintaining relationships with the key groups above, requiring timely disclosure based on risk tolerance thresholds.*

Upgrade security education

In the past, most security training programs focused on elements within the control of the teams supporting technology and security, and employees traditionally received a single annual review of that information. Organizations now need to significantly transform employee education to include hybrid environments and move to continuous awareness/education models that remind workers of the security risks and controls in place to keep them and the company safe.

- **Increase security awareness** by updating employee education to include best work-from-home practices and cyber security hygiene. Provide remote workers with specific policies, including software patching schedules, approved devices and communication channels, and data protection procedures. Keep employees aware of changes to the policies and ensure all content is easy to understand and follow.
  - For optimal engagement, consider increasing training frequency but decreasing the length of the module — and delivering in a multi-sensory medium, such as a short virtual demonstration, online quiz or infographic.
- **Enable patching policies:** Enforce and communicate key patching policies for end point compliance to remote and on-premises employees. This encompasses all corporate software and devices from mobile (phones and tablets) to fixed (desktops and servers).

- **Distribute data policies:** Ensure data owners have defined the security level assigned to all data and communicated with employees who have access to said data. IT/IS can then coordinate the policies and requirements for handling that data, as well as determine and implement the tools necessary to secure data at rest, in motion or in use.
- **Define accepted device usage:** Controlling the types of devices a bring-your-own-device (BYOD) program will support is critical in limiting a known set of risks introduced by said devices. Compatibility and security are strengthened by strong and enforced guidelines while time spent troubleshooting is reduced, allowing for IT and IS teams to focus on higher-level, strategic initiatives.

Resiliency check: *Don't forget to include partners who interact with company resources in security training programs. Expanding educational requirements to key partners is important because they share a responsibility in protecting the digital ecosystem on which the business and its partners rely.*

Provide tools to protect remote endpoints

Before remote work became prominent, companies often offered little security oversight of the devices issued to the scarce number of employees who worked outside their walls. Today, because remote workers make up a much higher percentage of an organization's staff, they should all be issued secure corporate devices and tools that help them avoid some of the pitfalls of working from home.

- **Issue endpoints,** such as laptop computers, phones, tablets and servers to remote employees. Require both configuration and tooling that provide layered security, which can reduce risks to companies by securing localized data and protecting communications between the device and corporate resources.
- **Determine if limiting or blocking personal activity** on corporate devices is right for your firm. Allowing personal activity could introduce risks to your network.
- **Provide discounted or free security tools,** such as antivirus and malware detection software, to encourage security maintenance for personal devices.

Resiliency check: *Combine endpoint security with backend tools, such as VPN with multifactor authentication (MFA) and strong logging and monitoring. A VPN helps remote employees create a secure connection to the corporate network, and MFA layers additional security to protect that connection. Using secured company devices, updating those devices when software or hardware needs patching and connecting to the corporate network through a secure VPN greatly reduces risks introduced by personal devices, shadow IT and home networks.*

With more than 90% of employees planning to work from home at least one day per week,[6] organizations must prepare for a future of permanent hybrid and remote work. By considering remote work in risk modeling, implementing new policies, and issuing employees the proper tools and guidelines, businesses will elevate the security of not only their own organization but their employees' personal digital landscapes as well. This will only serve to strengthen the overall security of your company and the cyber health of your employees. ■

[6] Apollo Technical, "Statistics on remote workers that will surprise you," January 2022.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:
Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.

BANK OF AMERICA