RFA

The Trusted Technology Partner

Locations
NEW YORK CITY
BOSTON
SAN FRANCISCO
PURCHASE
LONDON
LUXEMBOURG
SINGAPORE

7 Datacentres Globally:
NORTH AMERICA
UNITED KINGDOM
LUXEMBOURG

Sales@rfa.com
US +1 212 867 4600
UK +44 207 093 5010

Best Practices for Remote Work Cybersecurity

How can firms maintain cybersecurity when employees work remotely?

Telecommuting, which has become a new normal during the COVID Pandemic, can inadvertently lead to cybercrime. The CISA (Cybersecurity and Infrastructure Security Agency) recently issued an alert regarding vulnerabilities caused by remote access to organizations' computer systems. A proliferation of cloud-based apps makes it easier for bad actors to exploit holes in networks.

Regardless of whether you have one employee working on a mobile device while on a business trip or your entire team telecommuting from home offices, your firm's cybersecurity cannot be sacrificed for convenience. By clearly understanding your options to maintain cybersecurity in the new remote office environment, firms can safely navigate the cyber world and keep their firm; employees protected regardless of where or what device employees are using.

> **Your firm's cybersecurity cannot be sacrificed for convenience.**

Cyber Security and Telework

Maintaining your firm's cybersecurity while having employees in remote environments can be a challenge, but it can be mitigated with minimal risk if you plan for it and select the right options for your firm. Firms must assume that malicious actors will try to infiltrate networks, and you must prepare for the worst-case scenario.

How Do You Prepare for A Remote Workforce?

Business needs and structure vary, so there is no one-size-fits-all, but securing your network should be top of mind. Solutions should be matched to circumstances. Not all organizations can provide laptops to all employees. Some workers have been given laptops, but need more help securely managing access to data and networks. Regardless of hardware, there are ways that the network can be secured.

Connecting your Remote Workforce to the Office

There are four primary ways to secure a firm's network to allow remote access for employees.

The VPN Gateway: Virtual Private Network (VPN) gateways create secure access from an employee device to the VPN gateway and onward to your firm's internal network. In this way, your enterprise-level cybersecurity measures are extended to the VPN, which acts as a secure tunnel for each remote employees to go through.

Some VPN gateways can extend your firm's firewall rules to the employee computer regardless of where they are working through the use of a portable device. VPN gateways offer several great telework/remote features, but while communication is protected through the VPN gateway, the employee's computer may still be at risk of transmitting infected data if the computer itself has been compromised. A VPN gateway should only be used in conjunction with properly configured, company-owned hardware vs. BYOD (bring your own device) to maintain high-security standards and minimize the firm's internal network's risk.

Portals: In this method, telework employees access the firm's data and applications through browser-based webpages or a virtual desktop. All applications and data are stored on the portal's server and cannot be downloaded or saved on an employee's device without permission. This is an ideal method to maintain control over who is accessing your firm's data and its use. The inherent risk with portals depends on what permissions the employee has while accessing the portal. If the portal permits an employee to access other areas of the internet while connected, it could provide an unintended avenue for malicious actors to access your firm's network. It is prudent to restrict employees' access to other programs while the portal is in use. The greater access an employee has, the less secure the connection becomes.

Remote Computer Access Service: Remote computer access services empower an employee to remotely control a computer physically located in the corporate environment via an intermediate server or third-party software. When the two computers are connected, applications and data remain on your office computer, and your network's cybersecurity measures are enforced. Your remote device simply acts as a display for the work performed on the office machine. Due to the direct access, a remote desktop connection is considered high risk in cybersecurity terms. Proper configuration is critical. When setting up correctly, communication between the two computers is encrypted for data protection, but it is also encrypted from the organization's firewalls and threat detection. Regardless of how robust your cybersecurity measures are, if the employee's home computer, (BYOD) does not maintain the same protections as the office workstations, malicious data can penetrate your firm's network largely unnoticed during a remote desktop session.

Direct Application Access: Direct application access is probably the lowest risk to a firm's cybersecurity measures because it is best used only with low-risk applications. Using this method, employees can remote into a single application, usually located on the perimeter of your network, such as webmail. The employee doesn't have access to the entire network, permitting them to only work on select applications without exposing your firm's internal network to danger. Though there is much less danger posed by direct application access, it doesn't allow extensive work to be done. There is very little connection to data on your network, and little ability to take data to another application. It is best used when traveling or on a mobile device where complete access to the network is unnecessary.

Using company-owned and maintained hardware is the best option for your employees when working from home or on the go. Properly-maintained company laptops reduce the risk of unpatched or out-of-date software connecting to your network and often have more robust anti-virus/anti-malware protections than personal computers, (BYOD).

Begin planning for a new approach

Many organizations found themselves quickly moving to a remote work model, and security teams may not have had time to perform the basic endpoint hygiene and connectivity performance checks on corporate machines. Further complicating the matter are those employees who are working on personal devices when corporate machines were unavailable.

Firms should untimely ensure that corporate laptops have the minimum viable endpoint protection configurations for off-LAN activity. Security and risk teams should also be cautious with access to corporate applications that store mission-critical or personal information from any personally owned devices (BYOD).

Consider that many cybersecurity strategies are designed to merely protect a perimeter, simply checking the credentials of someone attempting to access and determine whether the actor is legitimate or malicious. But today, your firm's critical applications no longer have borders, meaning that security solutions have to protect more than just the perimeter, but the data also. Borderless Data Access Controls (BDAC) are one solution to consider. BDAC conducts strict identity verification, inspection and monitoring of every single user and every device trying to access your firm's private network — internal and external. It doesn't matter where the user or device is located. All face the same stringent scrutiny before gaining access to your sensitive data.

Under this zero trust model, trust isn't freely given. Everyone must pass a virtual "sniff test" every single time. BDAC asks "who, what, where, why, and how" for every given attempt to gain access to your firm's data and infrastructure, and relentlessly authenticaing it. A zero trust model provides the additional protection you need against both endpoint compromises (using phishing and/or malware) and attacks targeting your firm's borderless applications.

Locations

NEW YORK CITY
BOSTON
SAN FRANCISCO
PURCHASE

LONDON
LUXEMBOURG
SINGAPORE

7 Datacentres Globally:

NORTH AMERICA
UNITED KINGDOM
LUXEMBOURG

Sales@rfa.com
US +1 212 867 4600
UK +44 207 093 5010