Protect Your IT Environment: Best Practices for Remote Work Security in 2024

LeapFrog®

Protect Your IT Environment: Best Practices for Remote Work Security in 2024

Still popular since becoming vital during the COVID years, remote work offers benefits for both employers and employees. More and more in today's business workplace, the majority of data and business systems are cloud-based. This presents a much more complicated risk management situation for your business. Combine that with remote staff, the risk to your IT environment increases — breaches, malware, ransomware, device and network access, social engineering, the temptation to use workarounds, and other threats — are more likely when people work away from the office. Fortifying your organization's IT infrastructure involves two parts: setting up a network built for "zero trust" and employees complying with the rules, regulations, and guidelines set in place.

23% of U.S. employees work remotely while 41% work a hybrid model

Fortify your Infrastructure

Whether you have a fully remote staff, a hybrid staff, or a handful of employees needing to occasionally access their work files and emails remotely, you should build your IT infrastructure to securely support this convenience.

Your IT department should build out using these three pillars:

Operations

- Implement a zero-trust or conditional access solution that is integrated into all major business. Sy Configure all devices with the latest software and security controls with automatic patches
- Review access logs more often and check every IP address to check for anomalies
- If feasible, issue company devices to maintain more control over security measures

Solutions

- Leverage zero-trust or conditional-access rules to limit access to authorized users and authorized devices
- Shore up remote access security practices, including implementing multifactor authentication across the board (and ideally a remote access single sign-on solution) and reviewing wireless encryption protocol, vulnerability management, digital asset protection, and backups
- Explore virtual desktop environments and implement cloud computing
- Use tools and platforms built for a distributed workforce when moving resources to the cloud

Policies

- Update your runbooks to reflect any changes you've made to secure remote access and document any gaps you find
- Publish your company's audit policy that defines what IT will be looking at to balance security and privacy
- Frequently conduct employee training sessions on cybersecurity and recognizing current phishing scams
- Create and enforce company compliance by implementing the latest best in cybersecurity practices, including an Incident Response Plan

Ensure Employees Stay in Compliance

Working remotely can be seen as a privilege due to its flexibility and convenience, and employees need to understand the importance of adhering to the rules, regulations, and standards you set as a company. Your staff is your most important firewall and when everyone knows what's required, they can comply. To do this, they need to be given clear expectations. Your employees need to understand your policies inside-out so they can follow them. Your goal is to protect your company while making it easy for employees to comply. These steps can guide you:

1. Update your Compliance Policy for remote work

- Make sure your policy is clearly written (and not bone-dry), board-reviewed, and available online for easy access and quick reference
- Include your approved systems, apps, and any external media (like flash drives and hard drives)
- Consider endpoint protection software for your employees' personal computers
- Stress the importance of secure Wi-Fi and encourage employees to use secure, private Wi-Fi networks and avoid public Wi-Fi for work-related tasks
- Define the types of information that must always stay on the company network and the process for sending approved sensitive information
- Write specific requirements for multi-factor authentication, password, and encryption, including your processes for communications, data storage, wireless routers, and router traffic
- Incorporate a Media Sanitization Policy that covers the disposal of sensitive information, including hard copies, if needed
- Other policies to consider integrating or updating:
    - Security Awareness Training Agreement
    - Confidentiality Agreement
    - Bring Your Own Device (BYOD) Agreement
    - Sanction Policy
    - Incident Response Plan

2. Consider bringing in a reputable training company

- Hands-on training and continuous testing translate theory into real-life action — this applies to employees at all levels, including leadership
- Choose a company that makes learning interesting and engaging — subpar or boring training modules don't encourage learning or compliance
- Determine your required time frames for completion and make completion mandatory
- Ask for feedback about the training and change training companies if your employees are dissatisfied

3. Shore up your oversight team

- Enable your compliance officer to be supported by a compliance committee
- Require monitoring and auditing (including spot-checking) of all staff and regular internal reporting
- Review and update your investigation plan and require follow-through on corrective actions and discipline
- Establish a hotline for confidential and anonymous reporting of compliance issues

4. Continue to talk about compliance a lot

- Emphasize that your employees are your company's first line of defense, that you rely on them to keep your business operating successfully, and that it's important for everyone to work as a team
- Send a strong signal at every reasonable opportunity that compliance is a priority
- Include compliance messaging in your internal communications
- Remind your entire team to be vigilant in looking out for scams and sharing anything suspicious with IT
- Inform all staff — new and veteran — about the policy updates you're making and why
- Be clear about your training requirements and what you expect on a continual basis
- Lead by example by talking about compliance improvements you've made to your own workflow
- Congratulate your team on its successes — recognition from the top has a positive impact

As remote work continues to transform, so must your cybersecurity strategies. By building a fortified IT infrastructure, ensuring employee compliance, and applying these best practices, you can drastically reduce risks and safeguard your IT environment against threats and cyberattacks.

Remember cybersecurity is an ever-evolving process – staying vigilant and proactive is key in defending against threats.

If you need support in securing and monitoring your IT environment, Leapfrog delivers outsourced services that fit easily into your company's mid-market business model. With over 25 years of MSP, MSSP, and cyber risk management experience, you can expect Leapfrog to allow your remote employees to work seamlessly and securely within your company environment.

Leapfrog offers outsourced managed IT and cybersecurity services that fit easily into your business model. With over 25 years of MSP, MSSP, and CyberRisk Management experience, we help a broad array of companies simplify their IT operations while improving their security and resiliency. Our services are scalable, aligned, and built on a proven methodology, and our culture (we call it "Frogma") is built on Integrity, Service, and People so you get personalized, best-in-class support.

96%
say they will continue to partner with Leapfrog for the next 12 months

97%
say Leapfrog is more effective than their in-house IT staff

96%
are happy with our after-hours support

97%
have confidence in Leapfrog security

If you're ready to take your IT and cybersecurity services to the next level, Leapfrog is ready to help. Please call 866-260-9478 or contact us at sales@leapfrogservices.com.

@leapfrogservices | 404.870.2122 | www.LeapfrogServices.com | 1190 W. Druid Hills Dr. Ste. 200, Atl, GA 30329