Working Remotely and Securely During COVID-19

IT Advice for 5 Key Areas

LEAPFROG®

Working Remotely and Securely During COVID-19

It's imperative to keep everyone on your team connected and productive while they're working from home. While managing a completely distributed workforce can be challenging, it's doable. Even on the fly.

In this paper, we'll look at the five key areas of working remotely and securely:

1. **Collaborating and communicating remotely**
2. **Ensuring employees can access what they need**
3. **Working around IT hardware supply-chain shortages**
4. **Securing the network for remote access**
5. **Protecting against ransomware and other scams**

In addition to covering overall objectives and do's and don'ts, we offer advice on how to fine-tune your processes for each key area. With each key area under control, you can focus on what you do best — running your business.

Collaborating and communicating remotely

Stay connected, productive, and protected.

Why this is a Key Area during COVID-19:
Your team needs to be able to work together to stay productive — your business and the economy depend on it. The collaboration and communication tools you choose and how you use them set the stage.

Shoot to recreate the feel of being in your office environment. Platforms should be secure (critical when discussing business), deliver high-performance, and, ideally, integrate with your back office platform so email, files, voice, etc. all work together. Your tools should meet your business requirements rather than the other way around. You'll likely run into problems later if you try to change your business requirements to fit a particular platform.

Fine-tuning once you've transitioned to remote working:
By now, your organization has likely settled into a remote-working routine (see below for do's and don'ts about the basics). Now is the time to evaluate how you're doing so far and to start looking at related short-, medium- and long-term strategies. You can ask:

- What has been working successfully and are there any outstanding obstacles or issues we need to address? Ex: IM archives, video-conferencing security, real-time document collaboration, call quality issues, slow platforms or internet during peak times.
- How does our team feel about our current processes?
- Do we plan to continue using these processes in the future or would it be wise to invest in improvements to be ready for a second (or third) pandemic wave?
- How could what we've learned about our teleworking experience translate into better strategies and budget decisions moving forward?

Managing the basics during COVID-19:
For a real-life example, see below.

Do's	Don'ts
Choose a secure Instant Message (IM) platform. It's best to establish a unified IM policy upfront and choose a platform that shows user availability because schedules are fluid.	**Don't use the chat platform you like best for personal use.** Employees need to be accountable for the business information they share.
Use a full-featured, secure meeting platform. It should accommodate the number of participants normally present in your meetings and allow access to the materials they need.	**Don't assume people are working regular hours.** They may have children at home or have to work at night to accommodate other responsibilities during the crisis.
Make sure the platforms are flexible. They should allow your team to work with customers as well as with each other and allow you to add or remove seats as needed.	**Don't forget to configure your availability settings.** It's important to let people know when you are and aren't working.
Get headsets for everyone. It's best to keep business communications private from other people who may be in the room. Headsets block out distractions, too.	**Don't get frustrated if attendees pause their end of communication during a session.** Working at home sometimes involves having to deal with unexpected family responsibilities.
Have a workable phone system option if your organization uses landlines. Use call forwarding in a pinch.	**Don't save meeting transcripts or recordings on your home computer.** Instead, save them to the company's network or cloud.

An example of how to manage this key area
A health services provider needed much of its workforce to use their own devices while working at home. Many employees had devices they could use but did not have the required Virtual Private Network (VPN) software client installed — without it, they would not be able to communicate and collaborate securely. By creating a standardized VPN configuration and a how-to document and video to go along with it, Leapfrog had the 300+ employees who needed VPN access up and running within a few days.

Additional information from our blog and partners

- Want to Conference Call or Collaborate In a Hurry? Try Teams or Hangouts
- How To Stay Connected Online Even If The Power Goes Out
- Cisco: Connected and Secure: Webex in Today's World
- Smarsh: How to Supervise Your Suddenly Remote Broker-Dealers and Investment Advisers (Webinar Recap)

Ensuring employees can access what they need

Stay connected, productive, and protected.

Why this is a Key Area during COVID-19:
When working from home, your employees should be able to access what they need to do their work just as they do when working at the office — or at least as close to that as possible. The more teleworking feels normal, the better.

Most organizations have a plan for remote access but typically it doesn't include your entire IT environment. And chances are it was not set up to accommodate everyone working remotely at the same time. To avoid bottlenecks and calls to IT for help, have a plan that spells out remote access protocols. To handle heavy remote access traffic, have (at a minimum) one or more VPN clients that can accommodate all of your users simultaneously. And to protect your company, have a web gateway to authenticate employees at login.

Fine-tuning once you've transitioned to remote working:
As your workforce began working from home, you may have had to work out some kinks with remote access (see below for do's and don'ts about the basics). Now is the time to evaluate how you're doing so far and to start looking at related short-, medium- and long-term strategies. You can ask:

- How closely do our remote-working processes mirror what we can accomplish while we're in the office? Ex: Permissions, easy (yet secure) access to the network resources, login efficiency, VPN bandwidth, end-user support.
- Is our team satisfied with their ability to get work done?
- Are we adequately protecting access to sensitive documents and data?
- Can we continue to meet our business needs if we operate in this capacity for the next few weeks (or months) and if we need to do this all over again in the future?

Managing the basics during COVID-19:
For a real-life example, see below.

Do's	Don'ts
Have at least two secure remote access methods. You need a backup method because ost IT environments were not designed for all employees to work remotely at the same time.	**Don't provide employees with too much network access.** Be even more deliberate about granting permissions during a crisis because of increased cyber threats.
Establish a temporary access protocol for teleworking. Decide in advance how to manage information access for employees who will only need it for a short time.	**Don't let employees use personal platforms for business.** While it can be easier to copy files into an app like Dropbox to work on them, this puts company information at risk.
Make sure administrators can remotely access workplace systems that are typically closed. You also need to be able to remotely control (or at least monitor) systems such as security cameras, lighting, and environmental controls.	**Don't get frustrated if things aren't working seamlessly at first.** It may take some time for your IT team to work out the teleworking kinks. Report any problems then give IT some time to work through them.
Consider augmenting on-premises files with auditable cloud-based file systems. Employees need to be able to edit work files and managers need to have an audit trail for versions.	**Don't stay logged into the VPN when you're not working.** Since VPNs can handle a certain number of concurrent sessions, not logging out could slow internet speed for others.
Consider VDI instead of buying new laptops to provide teleworking employee access to files. Shared terminal servers are another option to give employees the access they need.	**Don't leave work files open when you're not working on them.** Family members wouldn't purposefully delete work product but mistakes happen.

An example of how to manage this key area
A financial services company had just transitioned to centralized Virtual Desktop Infrastructure (VDI) to improve security and efficiencies. When COVID-19 hit, the company was able to scale up overnight, enabling everyone to work from home using their personal computers if needed. To manage access to personal printers and scanners, Leapfrog updated the VDI configuration then rolled it out to all employees. By having VDI in place, the company was able to pull off the mass transition to teleworking efficiently and securely.

Additional information from our blog and partners

- MFA During COVID-19: Eight Ways To Be More Secure
- Can't Find New Computers? Consider VDI During Supply Chain Disruption
- Varonis: COVID-19 Threat Update #1 (video about phishing, VPNs and monitoring)
- SecureWorks: Maintaining Cybersecurity in the Face of COVID-19-driven Organizational Change

Working around IT hardware supply-chain shortages

Stay connected, productive, and protected.

Why this is a Key Area during COVID-19:
Your employees need to have the right teleworking equipment to be productive. Computers and accessories are in high demand and the supply chain from Asia has been disrupted. New IT equipment is hard to find right now.

Until the supply chain returns to normal, work around the shortages in ways that don't break the bank or make your organization vulnerable to cyberattacks. Since whatever you buy you'll still own after the crisis, temporary options are often your best bet. If you're short on computers, Virtual Desktop Interface (VDI) allows employees to securely access your network from their home computers (Microsoft is offering three months of VDI free during the COVID-19 crisis). If you're short on less expensive equipment, use whatever you can find for the time being.

Fine-tuning once you've transitioned to remote working:
Now that you've figured out which tools your team will use when working from home (see the do's and don'ts below), it's time to think about your company's hardware from a longer-term perspective. You can ask:

- Are the current hardware workarounds we're using meeting our needs or would it be worth it to try to source additional devices to honor extended work at home orders? Ex: Laptops, monitors, keyboards, headsets, scanners, printers.
- Have there been any recent changes to the supply chain or the viability of our current hardware suppliers?
- Should we consider going the BYOD route with computers and peripherals in addition to smartphones?
- Should we consider adjusting our hybrid-cloud strategy or supplier and vendor options moving forward?

Managing the basics during COVID-19:
For a real-life example, see below.

Do's	Don'ts
Make sure any new computers you acquire meet your company's business standards. Deviating from your standard brand is fine if the alternative meets the same requirements.	**Don't invest in computers that won't meet your needs later.** Your employees probably have home computers comparable to the ones you can currently find at stores like Best Buy or Walmart. Use secure VDI during the crisis instead.
Be flexible and creative. Accessories that are relatively simple and low cost — headsets, keyboards, mice, monitors, port replicators — use whatever you can find.	**Don't bother buying Chromebooks or Netbooks.** They're watered-down computers that probably won't be able to run your VPN client or single sign-on solution.
Check your used inventory for accessories to send home with employees. You can also shop eBay, Rakuten, TigerDirect, and others if you come up short.	**Don't invest in used computers.** They may get you through the crisis but the time it takes for IT to configure them is usually not worth the cost. Again, VDI is a better option.
Get headsets for everyone. It's best to keep business communications private from other people who may be in the room. Headsets block out distractions, too.	**Don't make your employees fend for themselves.** Their solutions could be problematic for your IT department and organization.
Use cloud capacity for now and make purchases when they become available. The supply chain is starting to bounce back already.	

An example of how to manage this key area
Social distancing wasn't possible for the hundreds of employees working at a service company's call center. Working from home wasn't an option either because all of the employees didn't have reliable computers and internet connections at home. By setting up workstations inside the 31 company stores that had connectivity to the main office, they were able to disperse employees safely— but they still faced a supply-chain shortage for the appropriate headsets. Leapfrog worked with the customer to think out of the box and determined that gaming headsets would deliver the functionality and quality they needed and were available to source immediately.

Additional information from our blog and partners

- Can't Find New Computers? Consider VDI During Supply Chain Disruption
- Should You Replace IT Hardware or Just Get Rid of It?
- Cisco: Navigating supply chain disruptions for agile retail (for the retail and hospitality industries)

Securing the network for remote access

Stay connected, productive, and protected.

Why this is a Key Area during COVID-19:
Remote access is the number one attack vector for hackers use to gain access to your computers and networks. Hackers will exploit any vulnerability they can find to steal data, steal personal information, inject malicious code, or alter or delete files — the outcome can be catastrophic.

Make sure your company is secure during this crisis by securing remote access to your network. With everyone working from home, it's imperative to confirm the identity of each user by implementing Multifactor Authentication (MFA). Just because employees are accessing your network from home doesn't mean your company should accept risk it otherwise wouldn't. Don't skimp on adding other protections as well and be clear with employees about what is and isn't acceptable regarding company data.

Fine-tuning once you've transitioned to remote working:
With your first (and maybe second) round of remote-access security issues behind you, it's time to take a deeper look at risk and compensating controls. Stay the course with the do's and don'ts listed below, and also think about protecting your network from both a more granular and integrated perspective. You can ask:

- Are the remote-access security practices we're currently using sufficient to protect our organization while employees are working from home? Ex: Wireless encryption protocol, vulnerability management, MFA, digital asset protection, backups.
- Have we considered potential increases from insider risk and other threats? (Note: Risk in 2020 was greater before COVID-19 hit.)
- Have we updated our runbooks to reflect any changes we've made to secure remote access and documented any gaps we found?
- Do we want to consider how to get the same or similar visibility over our IT environment now that it extends into our employees' homes while teleworking?

Managing the basics during COVID-19:
For a real-life example, see below.

Do's	Don'ts
Use Multifactor authentication (MFA) for <u>everything</u>.	**Don't allow employees to use consumer remote access apps.** Apps like GoToMyPC or LogMeIn on work or home computers are not monitored and can be used to bypass security protocols.
Implement a remote access single sign-on solution. When employees sign on at the office, they do so from a trusted domain — not so when working from home. You need a solution specifically for remote access.	**Don't give employee home computers unfettered access to your network.** Limit what employees can do from unmanaged computers and restrict file sharing and copying.
Provide a secure way for employees to change expired passwords. Passwords time out for security purposes.	**Don't relax password requirements even temporarily.** Now is the time to tighten requirements instead.
Implement a remote access single sign-on solution. When employees sign on at the office, they do so from a trusted domain — not so when working from home. You need a solution specifically for remote access.	**Don't permit sending company files via email.** This bypasses security controls and can put your company at risk.
Require your IT security team to review access logs more often. They need to check every IP address, which can take time when everyone is working from home. It's better to review a shorter log more frequently to not miss anomalies.	**Don't try to convert employees' home computers into company computers.** Making home computers part of your network will allow data downloads. Permitting console access instead is much more secure.
Invest in endpoint protection software for your employees' home computers. Buy antivirus protection that's up to your company's standards for your employees' computers. It's worth the investment. Most IT companies are offering deals right now.	**Don't forget to talk about security with your employees.** Let them know it's in everyone's best interest to keep the company network secure and protected.

An example of how to manage this key area
A real estate company provides laptops to most of its hundreds of employees so they can occasionally work remotely when working in the field. However, cybersecurity protections for zero-day threats and other web-based malware were designed to protect the laptops while working in the office — that's where work requiring the most stringent security took place. With COVID-19, the company needed to unify security and access while everyone transitioned to working at home. Leapfrog worked quickly to implement a new endpoint management system that extends the cybersecurity protection remotely during this crisis and any that follow.

Protecting against ransomware and other scams

Stay connected, productive, and protected.

Why this is a Key Area during COVID-19:
Your organization is far more vulnerable to ransomware during this crisis — scammers are out in full force. Reports put phishing attack increases at 350% and 667%, and Google recently reported having detected 18 million COVID-19 malware and phishing Gmail messages per day. Often the email content seems compelling and urgent to get your attention.

All employees should be on the highest alert. Ransomware can be hidden in compromised websites, USB drives, and unsecured wireless networks and routers in addition to phishing emails. When most everyone is working at the office, it's easier for employees to follow best practices and for your IT department to notice anomalies. But with everyone working from home, normal routines are disrupted, stress is high, and spotting unusual activity or anomalies is harder. Everyone needs to be extra careful and eagle-eyed.

Fine-tuning once you've transitioned to remote working:
By now you have likely covered the basics of securing your network from bad actors while teleworking (see below for do's and don'ts) — now it's time to refine your strategy and catch up with compliance issues if needed. Look for any security gaps and assess how what you're currently doing positions you to manage new threats. You can ask:

- What's working and not working with our ability to secure our team's personal devices and verify everyone is following security protocols? Ex: Patching, managing configurations, backing up company data, using battery backups (UPS), keeping up with security awareness training.
- Are we continually reminding our team to look out for phishing and other scams and share anything suspicious with IT?
- Are we complying with the regulatory requirements that apply to us and, if not, what's our plan to get up to speed?
- What improvements can we make now and in the short- and long-term to fortify our newly distributed network?

Managing the basics during COVID-19:
For a real-life example, see below.

Do's	Don'ts
Warn employees about the massive increase in phishing. They need to know the company (and themselves) are at increased risk for ransomware. Remind them not to open emails from unknown sources, click links or open attachments.	**Don't relax your vigilance on backups.** Even if your IT team is busy, they should not put backups on the back burner. The ability to quickly restore quickly from backups is critical if you get attacked.
Double-down on your security awareness training. Have your employees bone up on their training and do internal phishing tests to see who's vulnerable. If you're not currently enrolled in security awareness training, look at KnowBe4, PhishLabs, Cofence, and Proofpoint.	**Don't fall for coronavirus-related scams regardless of how official or harmless they seem.** It's easier to fall for a ransomware ploy when you're worried or curious. Scams include everything from stimulus check payments to coronavirus cures.
Invest in a next-gen email protection platform. Spam filters aren't enough anymore. You need a platform that uses baselines and machine learning.	**Don't trust unknown individuals or companies pitching services.** Stick to companies with whom you already have a relationship or have a reputation you can verify.
Be aware of social engineering scams unrelated to email. Be extra skeptical of anyone reaching out about personal or financial information — these are red flags. Research any solutions you're shopping for on your own.	**Don't send wire transfers without personal verification.** Thwart man-in-the-middle attacks by calling to get routing and account information by voice, then ask the recipient to check the account to make sure the money arrived.
Make sure your backups are air-gapped. Disconnect backups from your network — ransomware can encrypt backups.	**Don't try to do too many things at once.** Mistakes are easy to make when multitasking. Take the time to be vigilant.
Tell employees what to do if they believe they've been hacked, ransomed or targeted for fraud. Share the relevant portions of your security playbook (or Incident Response Plan, IRP) with all employees.	**Don't keep concerns to yourself — even little ones.** If something doesn't seem right, let your IT department know right away. This is the IT version of "See something, say something."

An example of how to manage this key area
A fundraising consultancy had moved a lot of IT services to the cloud and was in the process of completely integrating its IT environment. When COVID-19 struck and everyone had to work from home, it changed the way employees were accustomed to working — theirs is a collaborative, in-person culture. To stick as closely as possible to the way employees preferred to work while also protecting sensitive financial data, the consultancy needed to quickly add secure remote access for more than 80 employees. Leapfrog set up and integrated a collaboration platform and a cloud file system that can only be accessed through invitation-only, token-based Multifactor Authentication (MFA). Ransomware is not a threat because stolen credentials alone won't grant access to the unified system.

Manage all five key areas to stay on top of business

With the five key areas under control and operating smoothly, you'll get work done, protect your network, and gain insights into improvements you can make moving forward. Be sure to:

1. **Continually look at what's working and what's not**
2. **Survey your team periodically to get front-line input**
3. **Consider the things you'd do differently if there's a second (or third) wave**

While challenging, the adjustments your organization is making to the way it operates can pay off for months and years to come.

Leapfrog Services is a managed IT service provider that's been helping organizations meet their goals since 1998. As our clients' IT partner, we design and operate outsourced solutions that adhere to the highest standards and deliver consistent, secure levels of service. Being of service is at the heart of what we do — we've been heavily involved with the nonprofit community since our inception. Leapfrog has contributed millions of dollars in technology services and our team members serve on nonprofit boards and committees, advise, and volunteer. We believe organizations do best when they leverage IT expertise and capacity from a partner that's committed to integrity, service, and people. Learn more at leapfrogservices.com.

You can reach us at 404-870-2122 or leapfrogservices.com.

LeapFROG®