Think through what limitations on VPN usage may exist. This will help ensure it can support the number of employees needing to connect.

2. Use MFA (Multi-Factor Authentication) on the VPN and any remote connections. This adds an extra layer of security by requiring additional information to access the VPN. Implement this sort of security layer anywhere you can.

3. Keep all VPNs and network infrastructure devices up to date on patches. The Department of Homeland Security CISA website has some guidance on VPN security. This includes advice on how to keep VPNs updated and which cyber threats to look out for. (https://www.us-cert.gov/ncas/alerts/aa20-073a)

ADDRESS WIFI RISKS

At-home networks are typically not as secure as corporate networks. While working at home your employees probably have several devices connected to the same WIFI as well. This can cause security risks when opened to personal devices, home appliances and more. Company-provided hotspot connections may be an option for some organizations. You should also consider the speed of your employees’ home internet connections. They may not have the bandwidth to support their entire family now working from home, or children using devices to stream video on the same WIFI. This isn’t necessarily a security concern, but it may have an impact on employee productivity.

PREPARE FOR UPDATES

While your employees are away from the office, they may need to connect back to the company network in order to get certain updates. That can include OS, anti-virus and vulnerability scanning.

SET A SECURITY POLICY

Before sending your staff home, make sure you have a security policy in place for remote work. Employees may not be aware of the security measures they should follow, or how to safely conduct business from home. For many, this is the first time their jobs have been done remotely. Creating written-out guidelines helps educate your staff, while keeping your company safe. This way everyone will be on the same page and will hopefully lessen any confusion.

NIST (National Institute of Standards and Technology) has guidance on what to include in a policy/standard for any organization choosing to use telecommunication. There are also cybersecurity threats listed for everyone working remotely to be aware of. You can find their recommendations under the NIST publications, titled “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.” (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf)

ESTABLISH A SECURE CONNECTION

While your employees are working remotely, you should provide secure connectivity to corporate resources. Organizations that have never allowed for remote work will need to make resources available that were only accessible internally before now. There are a few ways you can help ensure the security of your network, while staying connected.

1. Utilize a VPN (Virtual Private Network). A VPN will help establish a secure connection between the office and employees who are working from home.

2. Think through what limitations on VPN usage may exist. This will help ensure it can support the number of employees needing to connect.

3. Use MFA (Multi-Factor Authentication) on the VPN and any remote connections. This adds an extra layer of security by requiring additional information to access the VPN. Implement this sort of security layer anywhere you can.

4. Keep all VPNs and network infrastructure devices up to date on patches. The Department of Homeland Security CISA website has some guidance on VPN security. This includes advice on how to keep VPNs updated and which cyber threats to look out for. (https://www.us-cert.gov/ncas/alerts/aa20-073a)

By Megan Howard, Pratum Director of Security Services

Patterson Law Firm, L.L.P.
Mediations and Arbitrations

Patrick V. Waldron
Workers’ Compensation and Civil Litigation
Member of American Academy of ADR Attorneys, AV Rated with 25 years of civil litigation and workers’ compensation experience
pwaldron@pattersonfirm.com

Gregory A. Witke
Civil Litigation including Personal Injury, Construction and Professional Negligence
Member of International Academy of Dispute Resolution, AV rated with over 30 years of litigation experience
gwitke@pattersonfirm.com

www.pattersonfirm.com 505 Fifth Avenue, Suite 729 Des Moines, IA 50309 515-283-2147

The Iowa Lawyer
April 2020
Depending on your process for updates, you may need to let your staff know a certain time of day this can be done so they can be sure their devices are on and ready for the necessary maintenance.

**Educate Your Employees**

Cybercriminals know how to take advantage of hot topics. There have already been scams targeting people looking for more information on COVID-19. During times of fear, people are more susceptible to these sorts of scams. Employees can also feel more relaxed in their home, which could mean they’re more comfortable opening suspicious emails.

Remind your staff to stay vigilant. Educate them on the importance of checking sources before clicking on links and never sending money to anyone without verifying the recipient. That may mean an extra phone call, instead of walking down the hall.

If you’re working from home, you may not consider the dangers of leaving your computer unlocked. If you have children, pets, spouses or roommates wandering around, they may unknowingly click on something that causes issues. Having a cat or toddler accidentally delete important files while you walk away from an unprotected device could be bad news. Instead, just follow the same practices you should be doing at the office by locking your computer any time you need to step away.

While it may be tempting to use your favorite computer or tablet when working from home or other remote locations, it’s not the best security practice. If you work for an organization with a diligent IT staff, they will be continually updating software and security measures on your company devices and networks. The same cannot always be said about your personal devices. You may not follow the same strict protocols as professional technical staff would. You also may not be able to afford the same level of technical controls that your company can. By connecting a personal device to private information, you are potentially putting your company at risk.

**Ensure Your Incident Response Plan is Ready**

Your Incident Response Plan is always a crucial part of your business. Now is the perfect time to make sure it is up to date and you know how to enact it remotely. If a cyber incident occurs, do you have the ability to investigate and mitigate the threat from outside the office? Start working on the answers to these questions as soon as possible, if you haven’t already.

Having a security plan in place, educating your staff and being prepared for possible threats will make this time of uncertainty more secure and manageable for your business. If you have questions about any of these recommendations, Pratum is an Iowa-based cybersecurity firm ready to help improve your security posture. You can find more information on our services at www.pratum.com.

---

**You can trust over 35 years of experience protecting lawyers.**

*Put your trust* in the carrier created by lawyers, run by lawyers, exclusively serving lawyers.

- Works exclusively with lawyers professional liability insurance
- Specializes in solo to mid-size firms
- Returned over $60 million in profits to policyholders since 1988
- Offers an array of services to mitigate risks

Protecting Your Practice is Our Policy.

Get a fast quote today!

[www.mlmins.com](http://www.mlmins.com)

or contact Clayton Jones

402-699-1985 or cjones@mlmins.com