Working Remotely and Securely: What Lawyers Need to Know

Louisiana State Bar Association
April 15, 2020

Presenters: Sharon D. Nelson, Esq. and John W. Simek
President and Vice President, Sensei Enterprises, Inc.
jsimek@senseient.com; snelson@senseient.com
https://senseient.com; 703-359-0700

Coronavirus: Tech Issues for Lawyers Working at Home

by Sharon D. Nelson, Esq., John W. Simek and Michael C. Maschke

The world is trying to deal with the coronavirus pandemic in a variety of ways. Controlling the spread of the deadly virus is at the top of the list. Travel is being restricted, and some countries have even closed their borders. The United States has been slow to react, but recent events have accelerated action by the federal government, states and major corporations. Social distancing and maintaining clean hygiene practices are the normal mode of operation now. More and more businesses are asking their employees to stay at home where possible. Some are being commanded by civil authorities to have their employees work from home.

What does that mean for the practice of law? How will you meet with clients? Many firms have or will adopt a telework environment and allow their employees to work from home. Making the working remotely decision will have different consequences depending on your current capabilities and whether a plan is already in place. While we can't cover all the possibilities and capabilities of every law firm, we'll attempt to attack some of the common considerations.

Equipment

Let's start with a very basic item…the computer. Hopefully, everyone is already using a laptop as their main office machine. If not, expect some popular models of laptops to be in short supply. Worst case, you may have to find a Best Buy, Target, Walmart, etc. and see if you can purchase a consumer-grade machine. If you planned properly, laptop users are already configured for remote access. Perhaps now would be a good time to modify your infrastructure plans and budget for laptops and docking stations for those folks that need a mobility option.

Some firms are telling all employees to work from home. Believe it or not, people are picking up their work computers, monitors, keyboards and all other peripherals on their desk and taking them home. We can't imagine the headaches the IT support people will have instructing a user to connect all the cords and devices up properly, not to mention configuring the desktop to connect to the home network. Our suggestion is to avoid taking desktops home and just deal with laptops and home machines. It will save a lot of headaches, wasted time and support costs. Speaking of home machines…they bring a whole new set of problems and liability which we'll address later.

If your employees are working from home (or other remote location) for an extended period of time, we recommend having an external monitor, full-size keyboard (wireless preferred) and mouse available. You will be much more productive with a full-sized keyboard and a larger screen. Another consideration is printing. Understand that you may need to help your employees configure their home printer (if they have one) to work with the firm's computer. If they don't need to print, so much the better. That should pretty much do it for the hardware requirements.

Workspace

If possible, designate a separate area as your work environment. The space should be away from the kitchen, living room, family room, or other active family areas. If you don't have a desk available, you can always use a table for your work surface. As mentioned earlier, use an external monitor and full-sized keyboard to create a more comfortable, productive work environment. Consider positioning your work area, so you have a view out of a window if possible. The view will help when you have those periods of mental blocks. Working in a windowless area will make you feel like you're in prison, which isn't a good thing. Of course, maybe it was like that in the office!

Network Connectivity

Many of us have a home wireless network that can be used for our work-at-home environment. We recommend avoiding using your home wireless, especially if other family members are also working from home. Besides the security issues, connecting to the home wireless means you are competing for bandwidth with all the other connected devices. Now would be a good time to make sure your home wireless is protected with WPA2 encryption.

We suggest that you connect your computer directly to an Ethernet connection. You can purchase a long Ethernet patch cord if you are not too far away from your internet router. Ideally, you would have a hard-wired Ethernet connection in your house (we do) for your home office. As an alternative, purchase a powerline Ethernet adapter. The adapter provides Ethernet connectivity utilizing the electrical wiring in your house. You plug one adapter in an electrical outlet near your router and a second adapter where you set up your computer. The TP-Link AV1000 Powerline Ethernet Adapter is an excellent choice and is around $55 on Amazon.

Depending on your situation, you may need to get re-educated in how to use the hot spot capability of your smartphone. While the connection speed may be a little slower, it's a more secure network than connecting to free Wi-Fi at a Starbucks, McDonald's, etc. Our long-standing recommendation has been to avoid any free Wi-Fi and use your hot spot, even if using a VPN. For the record, you shouldn't be working at a public facility during these times anyway. The health risk is just too great, even if your locality/state permit it

Remote Access Software

There are a lot of choices for provisioning remote access. Many firms will already have a VPN (Virtual Private Network) available. Make sure you check the licensing and capacity for your VPN implementation. If your entire firm is working remotely using a VPN, there may not be enough capacity at your office to handle the load. Check with your IT personnel to see if there are any limitations with using a VPN. It's probably a good idea to refresh the procedure for using the VPN with those that will be connecting remotely, especially if they don't regularly access the firm's network with the VPN.

While we're talking about VPNs, not all VPNs are created equal. As organizations increase the use of VPNs for working at home, more vulnerabilities are being discovered. The bad guys are

shifting focus to target VPNs since they know so many more users will be remote during the pandemic. In addition, make sure the latest Windows security updates and patches are installed. It goes without saying that you should be using MFA (multi-factor authentication) for your VPN and any other remote access solutions. Have your IT support personnel review AA20-073A: Enterprise VPN Security (https://www.us-cert.gov/ncas/alerts/aa20-073a) from CISA for technical details about using and securing VPNs as a result of the COVID-19 pandemic.

Without getting too much in the weeds, there is a concept with VPNs called split tunneling. Basically, you configure the VPN to route desired traffic through a specific encrypted tunnel. As an example, one tunnel would be configured to send work traffic to your office, and a second tunnel would be for all other internet traffic. This helps reduce the bandwidth requirements at your office as only traffic destined for the firm's network would be coming in. Normally, you would not be implementing split tunneling for a variety of reasons, but now may be the time to change the configuration to allow more capacity since there will be a lot more work-at-home employees.

Some firms will want to enable the Remote Desktop Protocol to connect to their office computers. Words of caution – there is a reason the Remote Desktop Protocol is disabled by default on Windows computers. Generally, it's not recommended to expose your firm's computer(s) to the internet using Remote Desktop Protocol. Larger firms with Terminal Services have controls in place to safely use the Remote Desktop Protocol.

Another alternative is to use a remote-control solution such as LogMeIn. Many of our clients already have LogMeIn licenses available as part of the desktop monitoring solution that we deploy. If you use a remote-control solution, you will have to leave your office computer turned on at all times.

Larger firms may already have a remote access solution such as Citrix or Microsoft Terminal Services. As previously stated, make sure you have sufficient licenses and bandwidth for all the intended connections, and you have configured MFA for both Citrix and Microsoft terminal server.

Using Home Computers

We understand that not everyone is using laptops as their primary work computer and law firms don't want to spend the money to purchase laptops for remote employees. Many firms want their employees to use their home computers to work remotely. Understand that there are a LOT of issues and concerns when you decide to allow a home computer to connect to the firm network even if you are using a VPN.

The obvious concern is security. The firm doesn't own or control the home machine. You really don't know what security software may be installed or if the computer is fully patched with the latest updates. The reality is that many solo and small firm lawyers will be using home computers to connect to the office.

One of the first considerations is to determine what you will do about the security software on the home machines. Will you allow employees to use their personal security software and enforce it through policy? We would suggest a better approach is to extend your law firm's licensing to the home machines. In other words, make the home machines part of the centrally managed endpoint security system that already exists for the office. Such an approach may not be economically feasible, depending on your size and licensing terms. If you are using an MSP (managed service provider) for your IT needs, you should be able to add licenses on a monthly basis instead of paying an annual fee for each seat, which could get pretty expensive.

Do the employees have the necessary software on their home computers? At this point, you are probably rethinking the options for using cloud services. If you subscribe to Office 365, users could use Office in the cloud or possibly install Office on their home computer. If you use a VPN to connect, does the employee already have the appropriate software installed and configured? Bottom line…you will need to assess what capabilities will be required for your work-at-home employees and address any gaps that may exist.

Another challenge with home machines is the mixing of business and pleasure. Make sure you understand any applicable data protection laws (e.g. GDPR). Using a home computer puts you at risk for exposing client confidential data. It would be a nightmare if you inadvertently shared confidential data using your personal social media account. If you do use your home computer for work, try to limit (or ban) family members, especially children, from using the machine. Family members may be duped into downloading malware that compromises your computer and may transfer to your firm's network.

Telephone and Mail

Don't forget to address how you will handle telephone calls, especially those inbound from current or potential clients. If you have traditional phone lines, don't forget to forward the firm's number(s) to a number that you will be using to answer calls prior to closing the office. If you are not going to forward the number, have a message for callers to advise what number to call and how best to reach you.

The situation is so much better if you have VoIP phones. You should be able to just take your VoIP phone home, connect it to your home network, and it will ring just like it was sitting on your desk. As an alternative, you may have a soft phone available, where you install software on your computer to emulate your desk phone. You would then use your computer sound and microphone (or headset) to answer and make calls.

Don't forget about mail deliveries. Will the post office deliver mail if your office is closed? You may have to have the mail held at the post office or have the mail delivered to an alternate address. Once you've decided where the mail will end up, someone needs to handle it. The mail should be scanned (converted to electronic form) and sent to the appropriate person. Obviously, you'll need a scanner. You may be able to use your copier as a scanner if you don't have a separate scanner. An alternative is to use a scanning app for your smartphone.

Video Conferencing

Instead of face-to-face meetings, many law firms are utilizing some sort of video conferencing capability. There are a lot of choices out there to connect with people visually. As a result of the coronavirus situation, many companies are allowing temporary free usage. As an example, Microsoft is offering free usage of Teams for up to six months. Office 365 subscribers already have Teams included, but we're sure not all your clients are using Office 365.

Zoom is a very popular video conferencing solution. There is a free version that can host up to 100 participants. The company has lifted the 40-minute time restriction for the free version. The Pro version is an affordable $15/month. Of course, many larger firms already have enterprise accounts for services such as GoToMeeting or Webex, to name a couple.

To state the obvious, you will need some sort of camera to participate in a video conference call. Most modern-day laptops are equipped with a webcam for video calls. You could even use your iPad or smartphone with some of the video conferencing apps. Another consideration is sound. The built-in microphones for laptops or phones don't sound particularly good if you are on the receiving end. Consider using a headset (with microphone) or earbuds. You'll be able to hear better, and so will all the other participants.

Don't forget where you physically sit during the video conference. If your back is to an open window, the brightness may make you difficult to see. Objects behind you may be distracting too. Think about what the person on the other end is seeing. Be cognizant of those around you too. Family members may be able to hear you discussing confidential information even if you are wearing a headset.

Finally, remember the recommendation to connect your computer to a wired Ethernet port? Utilizing Ethernet will significantly improve the stability of your connection during your video conferencing call. The last thing you want is choppy video or garbled audio when you are working with a client or other counsel.

Cloud to the Rescue

Is it too late to move to the cloud? Not in our opinion. Putting your client's confidential information in the cloud brings different considerations for security. How does the cloud provider protect your data from unauthorized access? Will you need to encrypt the data before you use the cloud service? There are so many great tools available to enhance your law practice.

Cloud-based practice management is a good place to start. We've already mentioned Office 365 for your productivity software. There are options for document management and document assembly in the cloud too. Backups are critical for surviving a ransomware attack. We've always recommended having a local backup and additional encrypted versions stored in the cloud too.

If you are not currently in the cloud; it's probably not a good time to take your critical business functions and move them to the cloud during the current pandemic. However, we're sure you can see the value of using cloud services for any future disaster that may come along.

Opportunity Knocks

The cybercriminals never miss an opportunity to profit from a disaster. The coronavirus pandemic is no different. The goal is to target people searching for information about the virus and infect them with malware. Thousands of domain names have suddenly been registered to host malicious websites. The bad guys know that a lot of people are now working from home and have initiated campaigns targeting those remote users. Be particularly vigilant concerning requests to reset your password even if the email looks like it is valid.

Final Tip

If you are not currently participating in a work-at-home environment, you should be planning for it in the future. If you have a laptop as your primary work machine, bring it home every day. That way, you'll be ready to respond quickly should the situation change overnight. It would also be prudent to have any needed data readily accessible. Perhaps now would be a good time to have secure cloud storage so you could access the data from anywhere.

Hopefully, your firm has some sort of policy for the changing of passwords. It is no longer necessary to change passwords as frequently as we have done in the past, but they should be changed periodically for the time being. There is no reason these days to change your password at intervals of less than 90 days. No matter what your password expiration policy is, if you are closing your firm, you should change your password prior to leaving the office and starting your work-at-home experience. Changing the password will reset the timer so that it hopefully won't expire while you are not physically connected to the firm's network.

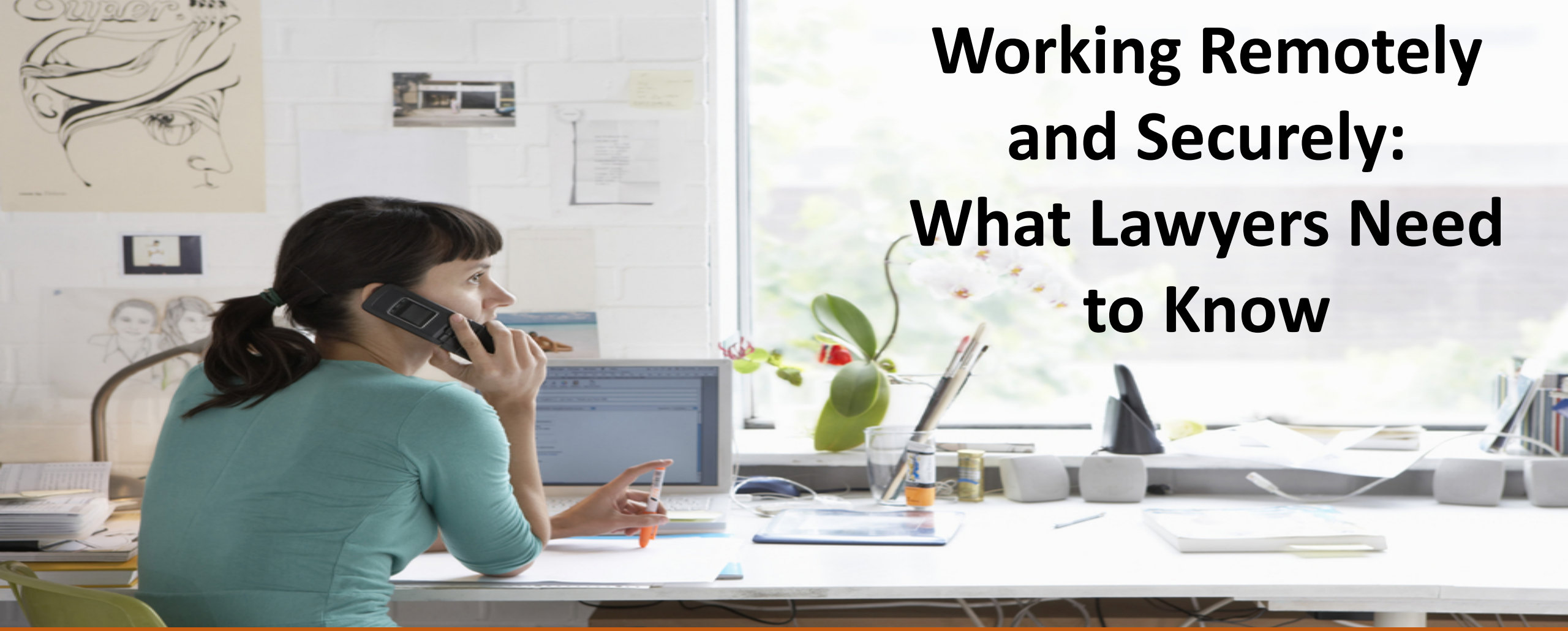
Final Thoughts

As we mentioned at the beginning, it would be impossible to address every situation a law firm may encounter during the coronavirus pandemic. Hopefully, some of our suggestions and recommendations will assist in your practice and allow you to serve your clients well in these difficult times. Be safe out there.

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.*

Michael C. Maschke *is the CEO of Sensei Enterprises, Inc. He is an EnCase Certified Examiner, a Certified Computer Examiner (CCE #744) a Certified Ethical Hacker and an AccessData Certified Examiner. He is also a Certified Information Systems Security Professional.*
mmaschke@senseient.com.

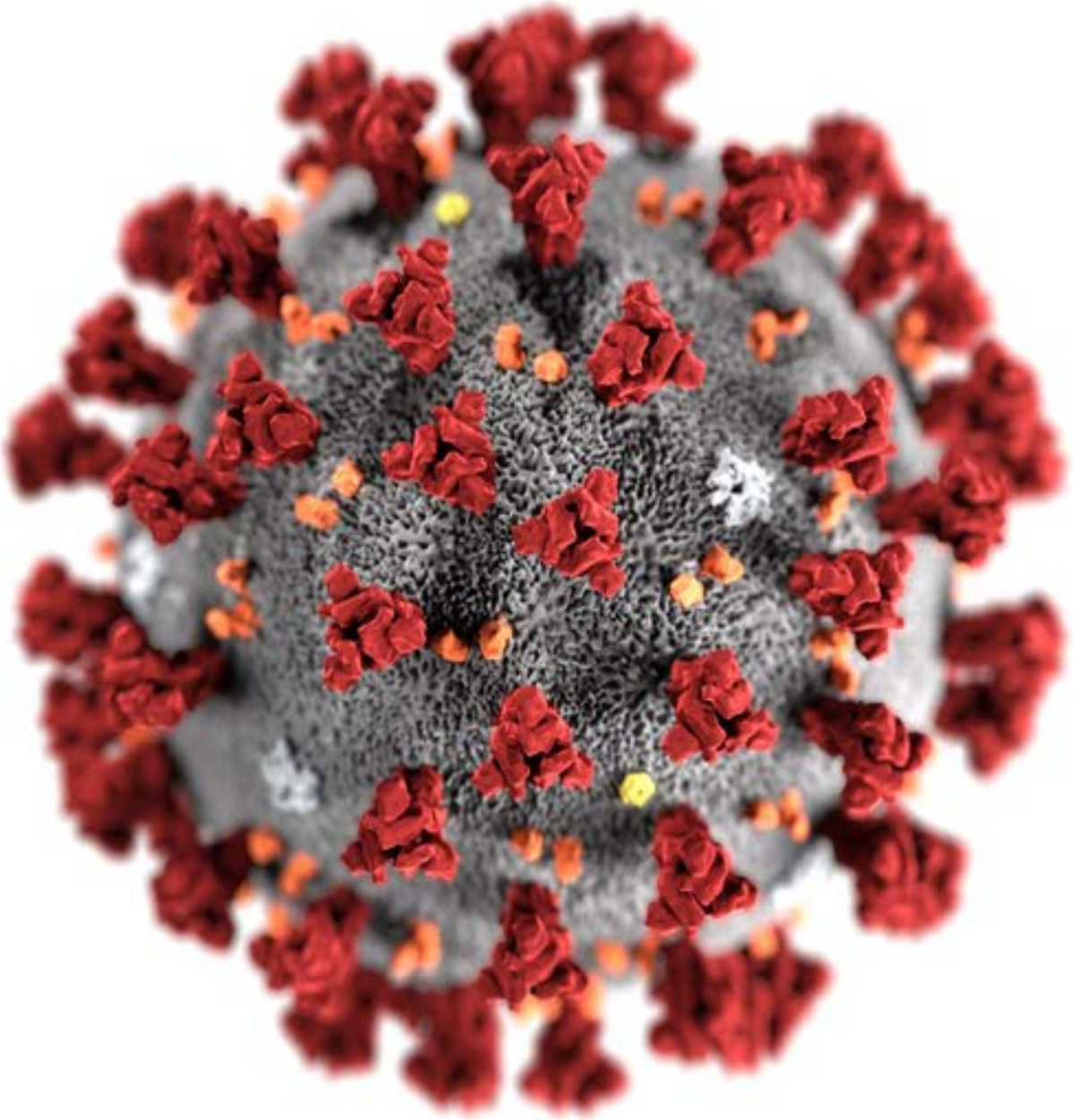


Working Remotely and Securely: What Lawyers Need to Know

Sharon Nelson, Esq. & John W. Simek
President and Vice President, Sensei Enterprises, Inc.
snelson@senseient.com; jsimek@senseient.com
senseient.com 703.359.0700

COVID-19

- Has fundamentally changed the practice of law
- Shelter in place and lockdowns
- Travel restrictions
- Social distancing
- Maximum precautions
- How long will this go on?



The rush to enable working at home

Most law firms had no plan for teleworking

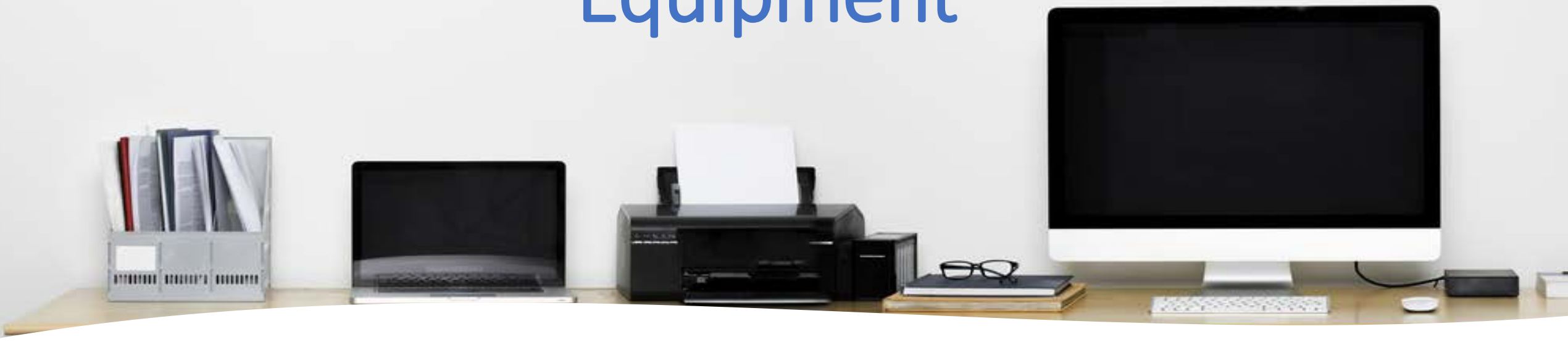
No contingency plan for governments closing law firm offices

Many ad hoc plans did not consider cybersecurity or ethics

Ethics
(the big three)

- Rule 1.1 Competence
- Rule 1.4 Communications
- Rule 1.6 Confidentiality

Equipment



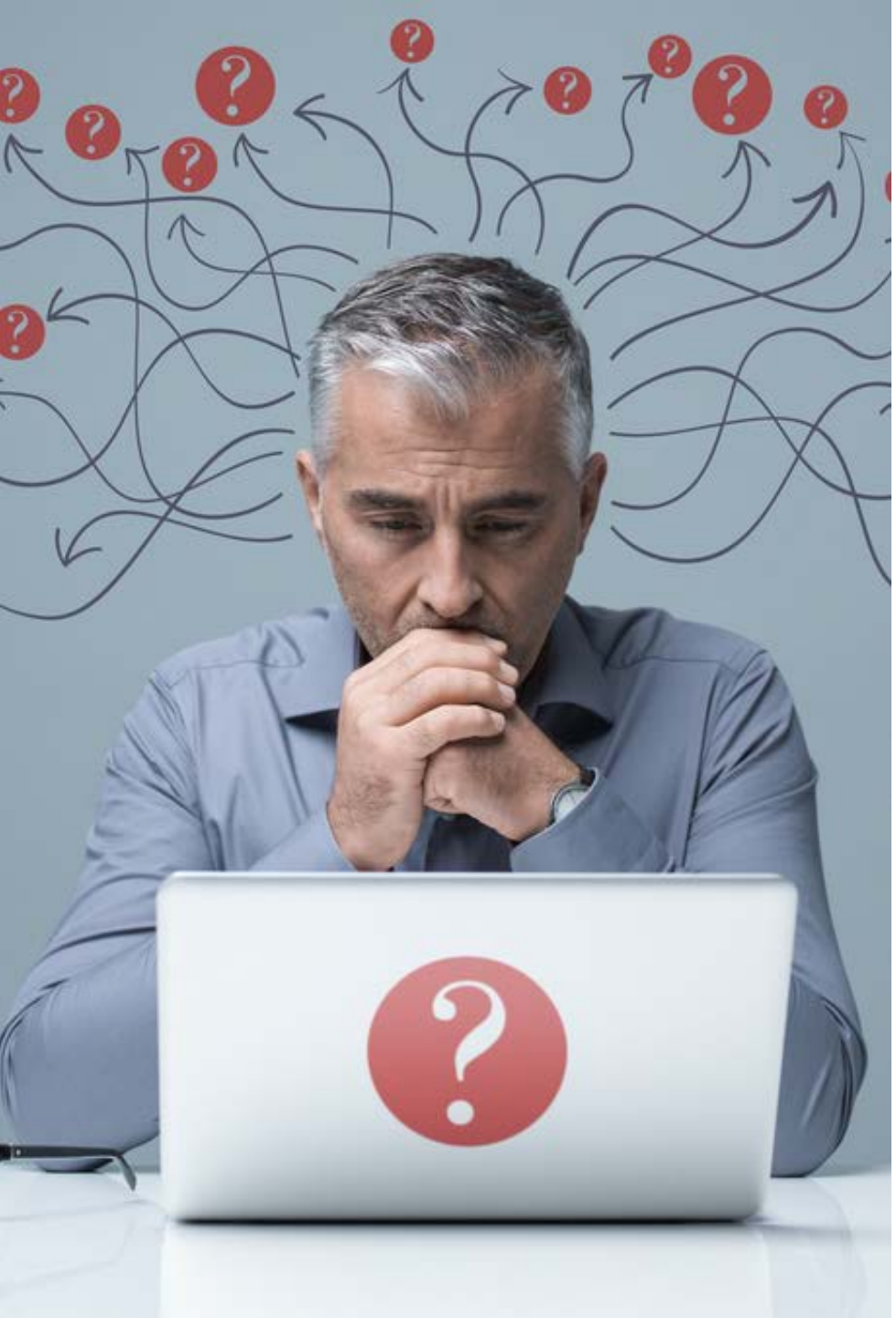
Best bet is to issue everyone a laptop as primary work device

Take home every night – no use of that laptop by family members

At home, have a full-sized keyboard (wireless preferred), external monitor and mouse

Home printer?

Scanner needed?



Home computers

- No good reason to use them for business
- Firms don’t know whether they are fully patched/what security software is installed
- So why are in they in use?
- Budget reasons
- IT/cybersecurity management headaches

Home computers

- Have a policy for the use of home computers
- Best practice? Extend security software licensing to home machines
- Make home machines part of the centrally managed endpoint security system

Home computers

- Be mindful of licensing requirements if you use a managed service provider
- If you use a VPN, does the employee have the software installed and configured?

Home computers

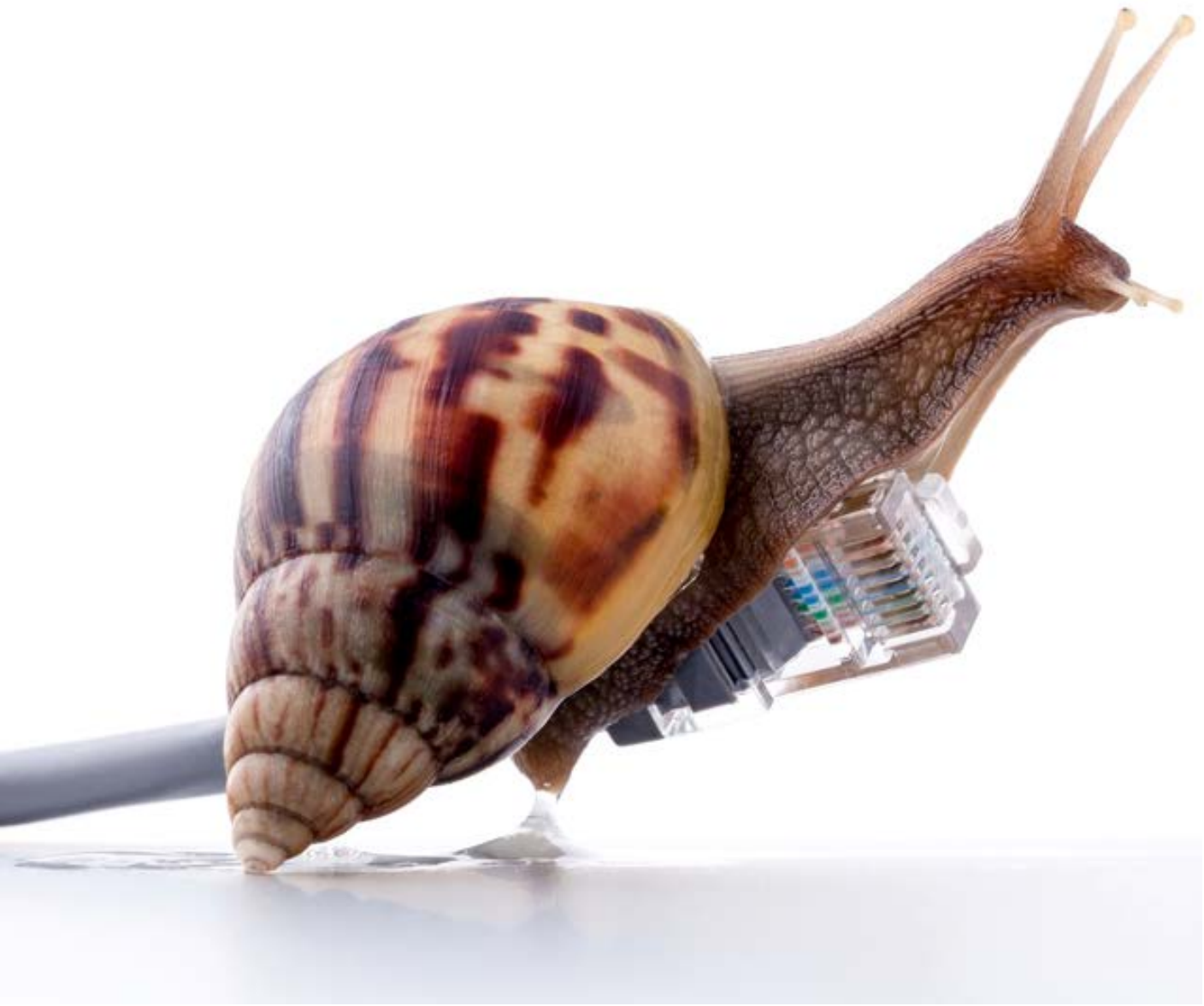
- Are you an Office 365 firm? Use Office in the cloud
- Do you use other software in the cloud?
- If your software is on-premises, you may want to rethink moving to the cloud

Home computers

- Best practice: Ban family members from using the machine used to connect to the firm
- Be careful with your own use of the machine

Network connectivity

- Avoid using your home network, especially if it is shared with family members
- You are competing for bandwidth
- If you DO it use, make sure it has WPA2 encryption and change the default login password and default Wi-Fi name



Network connectivity

- Suggest you connect your computer directly to an Ethernet connection
- Purchase a long Ethernet patch cord if you're not too far from your router
- OR – purchase a powerline Ethernet adapter (provides connectivity using the electrical wiring in your home)
- TP-Link AV1000 Powerline Ethernet Adapter: Around $55 – a good choice

Network connectivity

- Use the hot spot on your smartphone
- Speed may be a little slower but it is secure
- Avoid free Wi-Fi everywhere! Yes, even if you have a VPN

Remote access software

- Virtual Private Networks (VPNs)
- Many firms have VPNs but check the licensing and capacity for your implementation!
- Retrain employees on procedures for using the VPN, especially for those who don’t normally connect remotely

VPN Alert!

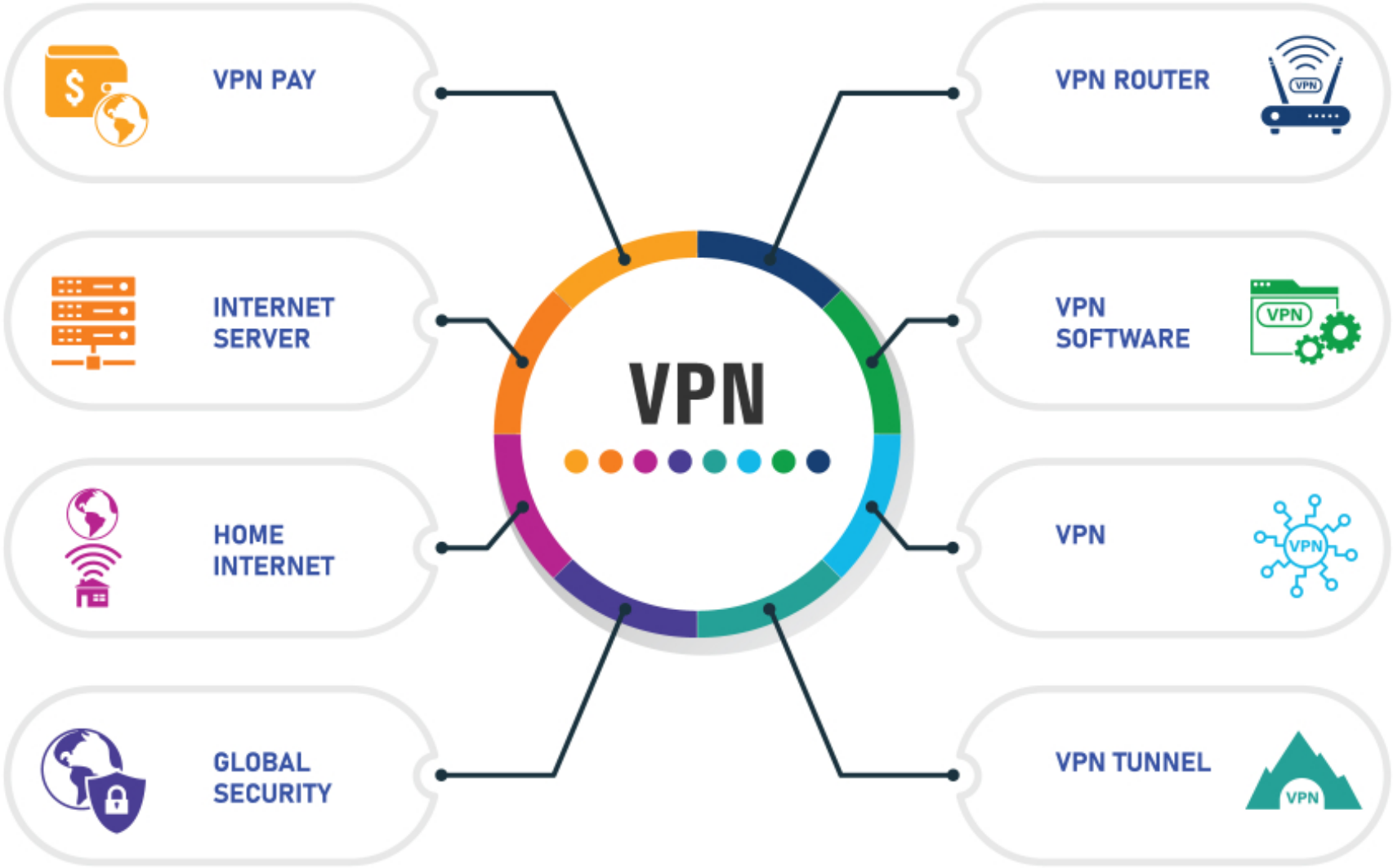
- Bad guys are targeting them, especially with working from home – and there are vulnerabilities
- Make sure latest Windows/macOS security updates and patches are installed
- MUST use MFA (multifactor authentication) with your VPN and other remote access solutions

VPN Alert

- Have your IT support personnel review the Cybersecurity and Infrastructure Security Agency (CISA) recommendations on enterprise VPN Security https://www.us-cert.gov/ncas/alerts/aa20-073a - published in March 2020 in response to working at home due to the coronavirus threat

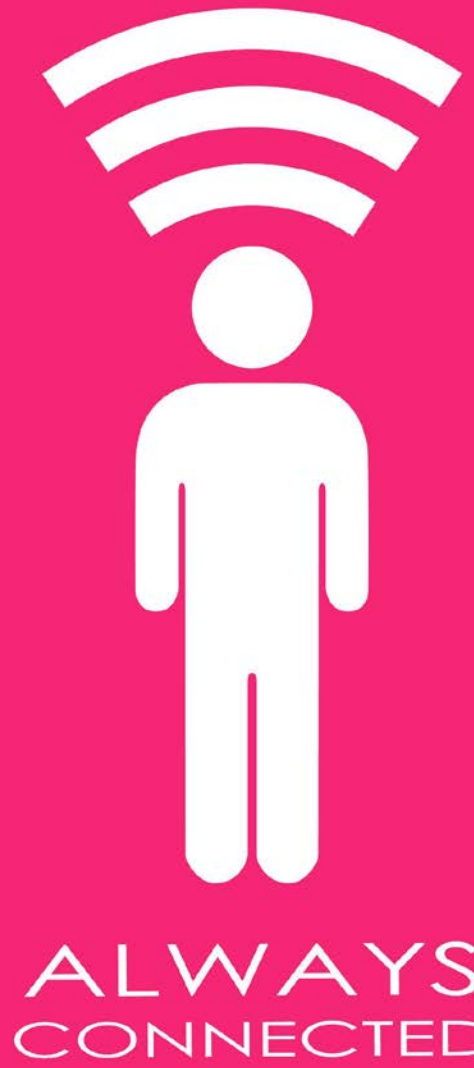
VPN Split Tunneling

- “In the weeds” warning!
- What is it?
- Why would you want to implement now?



Connecting to your network from home

- Enable the Remote Desktop Protocol (RDP)?
- It’s disabled by default - it exposes your firm’s computers to the internet
- Larger firms with Terminal Services have controls in place to safely use RDP



Other remote control solutions

- LogMeIn – common in smaller firms
- May be part of your desktop monitoring system (if you have one)
- Larger firms – often use Citrix or Microsoft Terminal Services
- Make sure you have both sufficient licenses and bandwidth
- Make sure you have MFA configured for both Citrix and your Microsoft terminal server

Telephones

- Traditional phone lines? Forward the firm's number to a number you can answer before closing the office
- Otherwise, leave a message on how best to reach you
- VoIP Phones? Take the phone home and connect it to your home network.
- Soft phones? Install software on your computer to emulate your desk phone – use computer sound and headset to answer/make calls

Mail deliveries

- Can someone go once a day to deal with mail?
- If building is closed, have mail held at post office? Maybe not a great idea right now
- Deliver to an alternate address (may take 7-10 days for postal service)

Mail deliveries

- The person who gets the mail may need a scanner or phone scanning app to distribute mail to recipients
- How will checks be handled? Using a phone app may be best for remote deposits
- Arrange for packages to go to an alternate address (FedEx and UPS should be operating)

Video conferencing

- Communications more effective if they can see your face
- Many offer temporary free conferencing
- Microsoft Teams – up to six months
- Zoom – has a free version, but many may need the features of the Pro version (we did!) Only $15 per month
- Larger firms usually have enterprise accounts with GoToMeeting or WebEx – or one of the others

Video conferencing

- Laptops have cameras for video conferencing, but you can also use iPad or smartphone with some video conferencing apps
- Built-in microphones for computers and phones are not optimal
- Use a headset with a microphone or ear buds with microphones

Video conferencing

- Using Ethernet will improve stability of your connection
- Make sure there’s not too much light behind you
- Make sure family members cannot overhear

Cloud to the rescue?

- Even now, the cloud may a good place to be – encryption considerations
- Time to make the move now? Experts disagree
- Office 365 is a great place to be
- Case management in the cloud is desirable

Cloud to the rescue?

- Backups in the cloud are critical
- Document management and document assembly
- Do your due diligence before signing up for cloud services

Cybercriminals never miss an opportunity

- They are fiercely attacking home networks
- Extensive phishing campaigns, often using coronavirus-related subjects to get people to click on a link or attachment

Cybercriminals never miss an opportunity

- Emails asking them to reset password, emails pretending to be from the Center for Disease control – it's the Wild West out there
- Objective isn't the home machine – it's the law firm network

IT assistance for home

- Most can be assisted remotely
- Utilize Google/YouTube
- There are lots of instructional videos online
- Onsite IT visits may be required

Workspace at home

- Privacy considerations
- Light considerations
- IoT devices around?
- Windows elevate mood

Looking at the future

The future ain’t what it used to be – Yogi Berra

If you need Sensei's IT, cybersecurity or digital forensics services,
please email us at sensei@senseient.com or leave a message at 703.359.0700.