Practical and Budget-Friendly Cybersecurity Tips for Lawyers

Mass LOMAP

May 5, 2021

Sharon Nelson, Esq. & John W. Simek

President and Vice President, Sensei Enterprises

snelson@senseient.com; jsimek@senseient.com

senseient.com 703.359.0700

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

The Sedona Conference Journal

Volume 21 2020

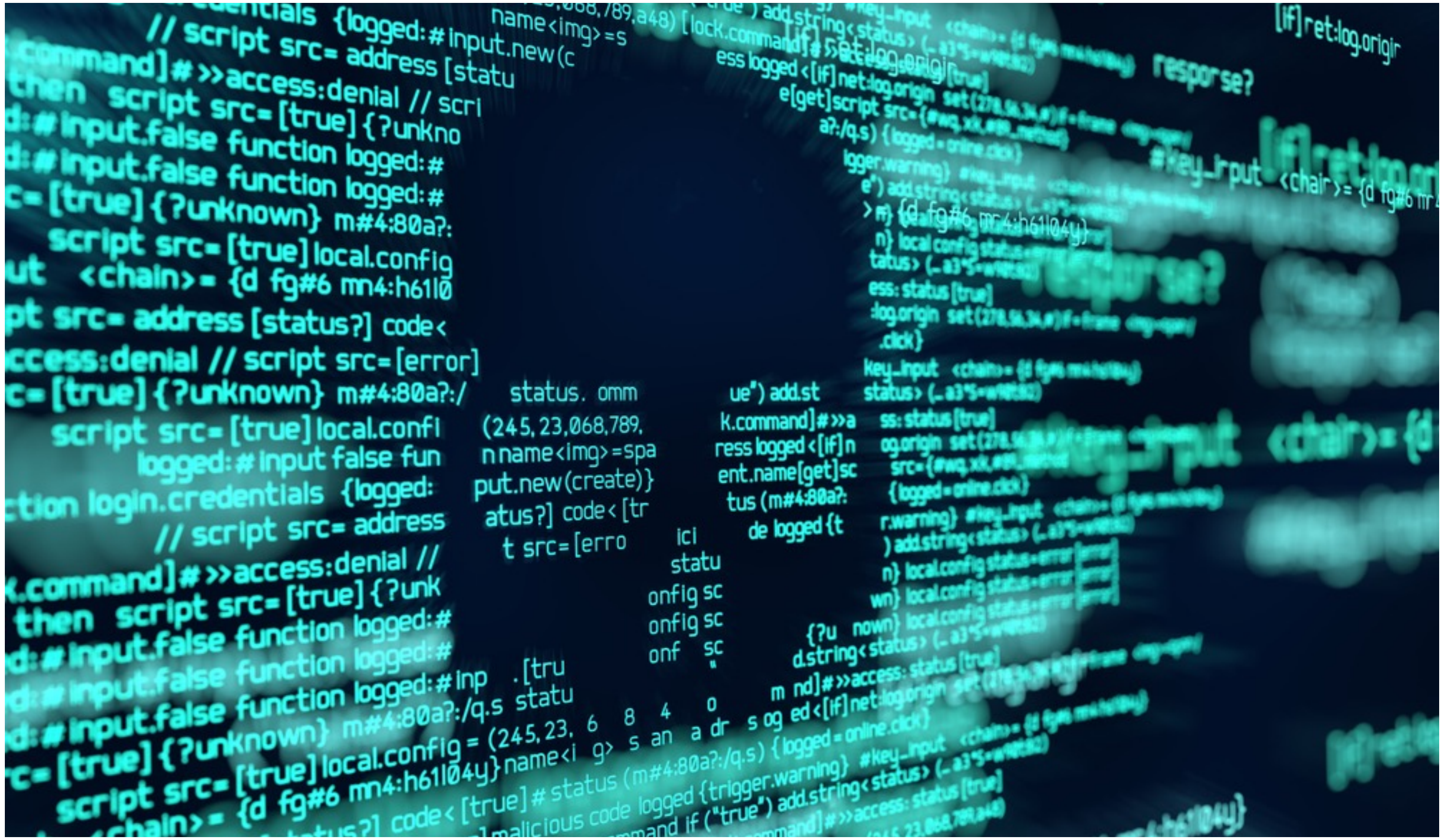
The Sedona Conference Commentary on Law Firm Data Security

The Sedona Conference

July 2020
Final Version

Recommended Citation:

The Sedona Conference, *Commentary on Law Firm Data Security*, 21 SEDONA CONF. J. 483 (forthcoming 2020), https://thesedonaconference.org/publication/Commentary_on_Law_Firm_Data_Security.



Beazley Group Report June 9, 2020

- 750% rise in ransomware in first six months of 2020
- Weaker security on home machines and networks
- Employees distracted and IT stretched thin - All threats predicted to accelerate

Ransomware

- Has become a scourge, especially in WFH environments
- Criminals often take your data, then encrypt it
- They demand two ransoms, one for the decrypt key and one to destroy your data – or they will sell/expose it

Business email compromise attacks (BEC)

- Spoofs a trusted individual (CEO/CFO)
- Convinces recipient to send financial info
- Purchase gift cards
- Change an employee’s direct deposit info
- Fraudulent wire transfers – e.g. change invoice data to redirect payments to a known vendor
- 75% increase in first 3 months of 2020
- Whopping 200% increase each week from April to May

Cybercriminals never miss an opportunity

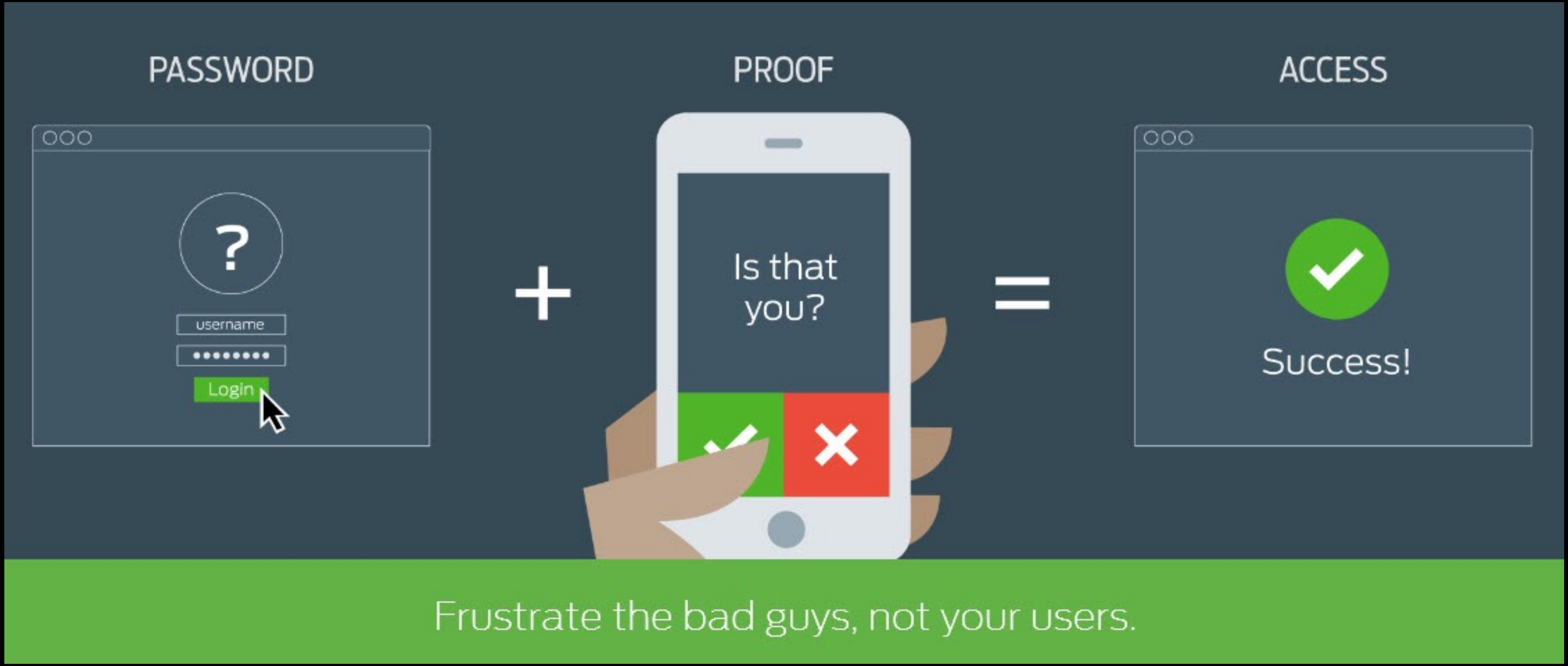
- They are fiercely attacking home networks – to get to the law firm network
- Extensive phishing campaigns, often using COVID-19 vaccine subjects to get people to click on a link or attachment

In a WFH environment employee training has never been more critical!

A Tug of War: Security vs. Convenience

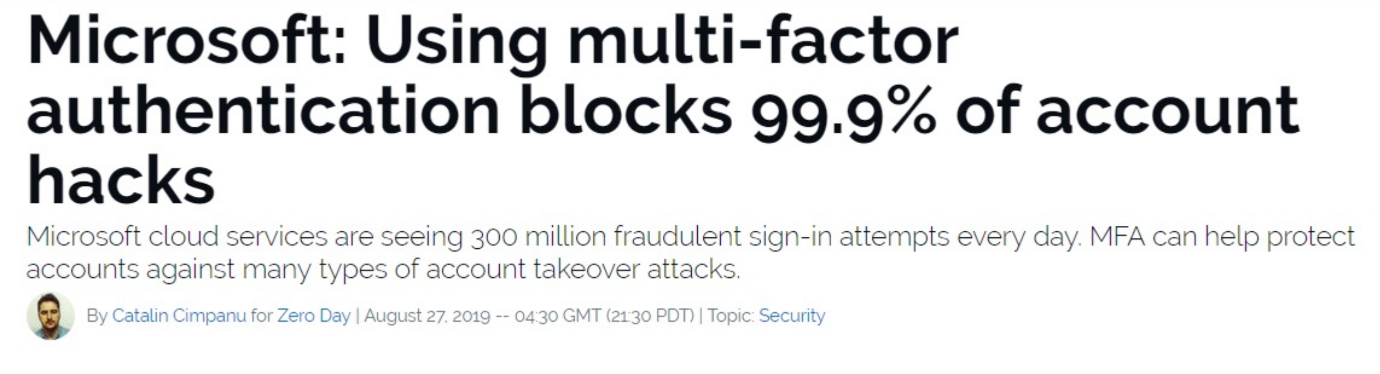
- Multifactor authentication
- The perfect example!

Multifactor Authentication



Frustrate the bad guys, not your users.

ZDNet



Microsoft: Using multi-factor authentication blocks 99.9% of account hacks

Microsoft cloud services are seeing 300 million fraudulent sign-in attempts every day. MFA can help protect accounts against many types of account takeover attacks.

By Catalin Cimpanu for Zero Day | August 27, 2019 -- 04:30 GMT (21:30 PDT) | Topic: Security

Duo Security

A tug of war: Security vs. Convenience

- Password creation
- Password management
- Password reuse
- Password sharing

Ethics
(the big five)

- Rule 1.1 Competence
- Rule 1.4 Communications
- Rule 1.6 Confidentiality
- Rule 5.1 Responsibilities of a Partner or Supervisory Lawyer
- Rule 5.3 Responsibilities Regarding Non-Lawyer Assistance

Competent and Reasonable Measures

01

Know it.

02

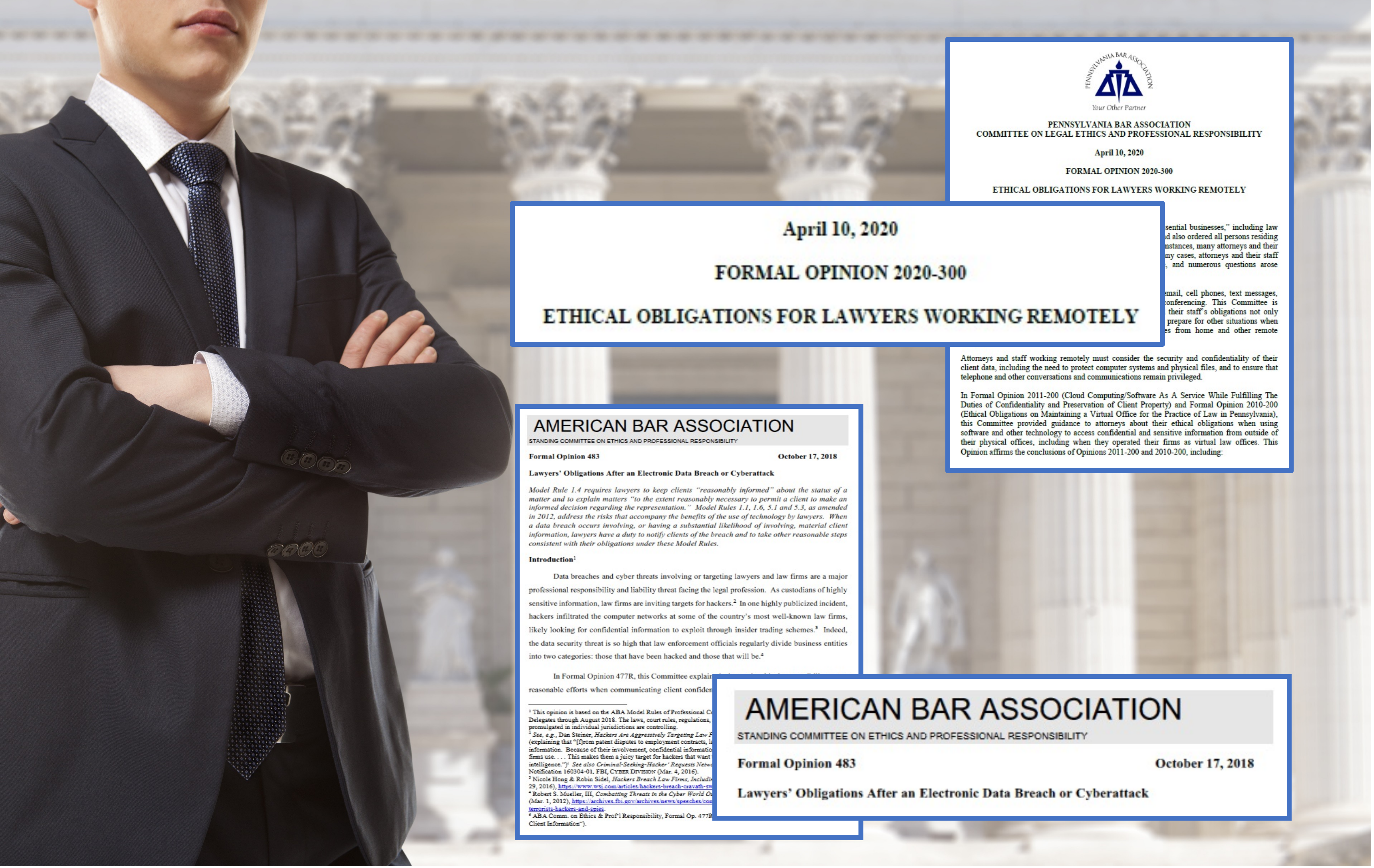
Learn it.

03

Get qualified help.

Qualified Consultant

Managed Service Provider (MSP)



Your Other Partner

PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

sential businesses," including law
d also ordered all persons residing
nstances, many attorneys and their
ny cases, attorneys and their staff
, and numerous questions arose

email, cell phones, text messages,
conferencing. This Committee is
their staff's obligations not only
prepare for other situations when
es from home and other remote

Attorneys and staff working remotely must consider the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.

In Formal Opinion 2011-200 (Cloud Computing/Software As A Service While Fulfilling The Duties of Confidentiality and Preservation of Client Property) and Formal Opinion 2010-200 (Ethical Obligations on Maintaining a Virtual Office for the Practice of Law in Pennsylvania), this Committee provided guidance to attorneys about their ethical obligations when using software and other technology to access confidential and sensitive information from outside of their physical offices, including when they operated their firms as virtual law offices. This Opinion affirms the conclusions of Opinions 2011-200 and 2010-200, including:

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients "reasonably informed" about the status of a matter and to explain matters "to the extent reasonably necessary to permit a client to make an informed decision regarding the representation." Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explain
reasonable efforts when communicating client confiden

[1] This opinion is based on the ABA Model Rules of Professional Co
Delegates through August 2018. The laws, court rules, regulations,
promulgated in individual jurisdictions are controlling.
[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law F*
(explaining that "[f]rom patent disputes to employment contracts, la
information. Because of their involvement, confidential informatio
firms use. . . . This makes them a juicy target for hackers that want
intelligence."); *See also Criminal-Seeking-Hacker' Requests Netwo*
Notification 160304-01, FBI, Cyber Division (Mar. 4, 2016).
[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Includin*
29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-sw
[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Ou*
(Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/com
terrorists-hackers-and-spies.
[5] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R
Client Information").

AMERICAN BAR ASSOCIATION
STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

ABA Formal Opinion 498: Virtual Practice

- https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf
- Standing Committee on Ethics and Professional Responsibility 3/10/21
- Competence, diligence and communication (Rules 1.1., 1.3 and 1.4)
- Confidentiality Rule 1.6 – are special precautions required?
- Apply all patches/security updates, use VPNs, have anti-malware software
- Assessment of security, complex passwords, encryption, backup
- Cloud computing –use reputable company, ensure access to client data
- Must have data breach policy

ABA Formal Opinion 498: Virtual Practice

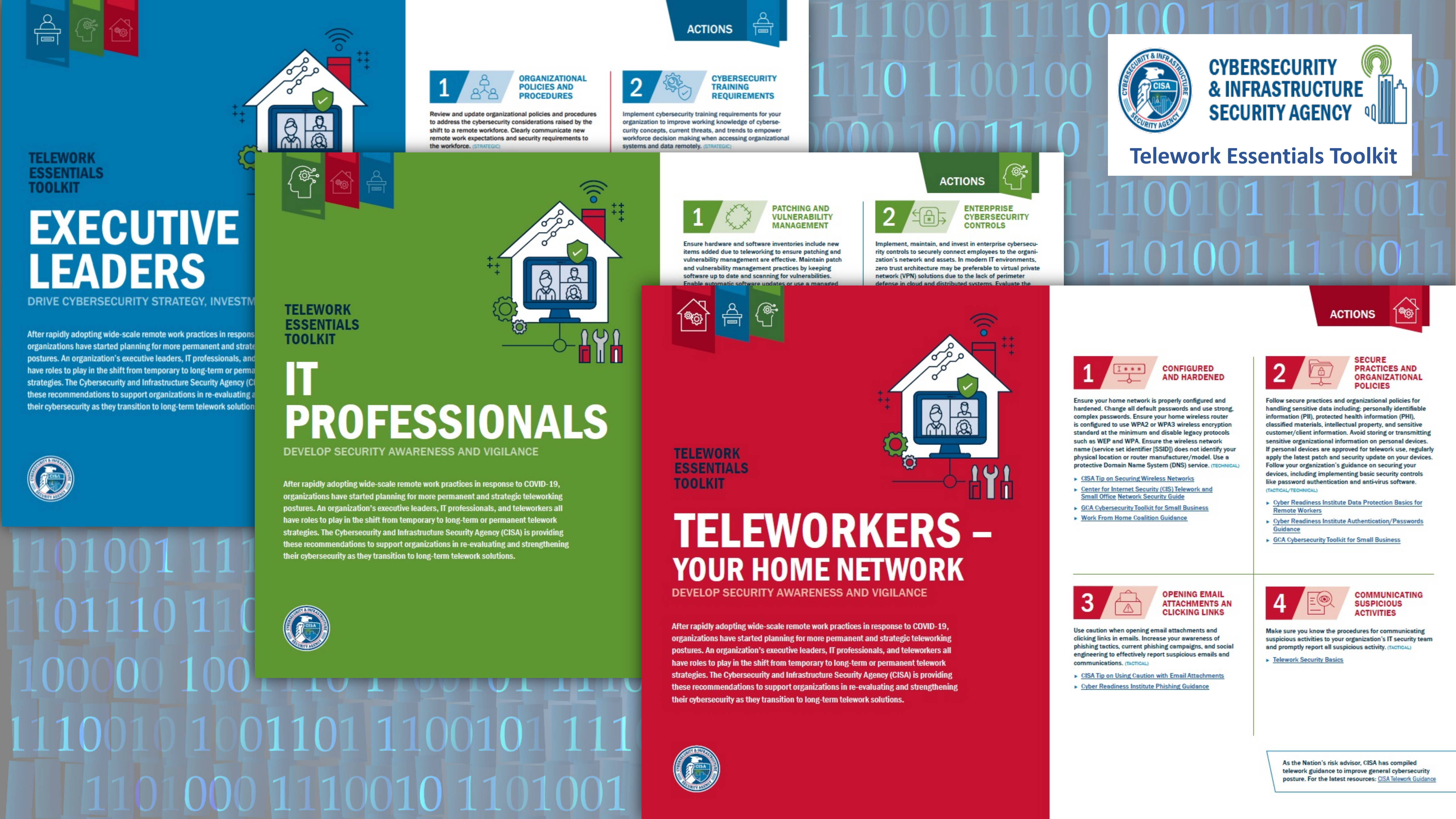
- BYOD policy needed, security training, ability to wipe devices if lost or stolen
- Video conferencing – must keep confidential at home or elsewhere, secure access to platform, inadvisable to record without client consent
- Disable IoT devices
- Secure way to exchange documents
- Designate mailing address
- “Available by appointment only” in “online instructions”
- Must be able to write/deposit checks, make electronic transfers, maintain full trust accounting records

Secure Configuration

- Strong password or passphrase
- Standard user account (not admin)
- Locking or wiping after *x* failed logon attempts
- Automatic logoff or shut down after *x* minutes of inactivity
- Current operating system, applications and plug-ins, with all current patches
- Security software with all updates
- Encryption

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Telework Essentials Toolkit



TELEWORK ESSENTIALS TOOLKIT

EXECUTIVE LEADERS

DRIVE CYBERSECURITY STRATEGY, INVESTM

After rapidly adopting wide-scale remote work practices in respons
organizations have started planning for more permanent and strate
postures. An organization's executive leaders, IT professionals, and
have roles to play in the shift from temporary to long-term or perma
strategies. The Cybersecurity and Infrastructure Security Agency (CI
these recommendations to support organizations in re-evaluating a
their cybersecurity as they transition to long-term telework solution

ACTIONS

1 ORGANIZATIONAL POLICIES AND PROCEDURES

Review and update organizational policies and procedures to address the cybersecurity considerations raised by the shift to a remote workforce. Clearly communicate new remote work expectations and security requirements to the workforce. (STRATEGIC)

2 CYBERSECURITY TRAINING REQUIREMENTS

Implement cybersecurity training requirements for your organization to improve working knowledge of cybersecurity concepts, current threats, and trends to empower workforce decision making when accessing organizational systems and data remotely. (STRATEGIC)

TELEWORK ESSENTIALS TOOLKIT

IT PROFESSIONALS

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 PATCHING AND VULNERABILITY MANAGEMENT

Ensure hardware and software inventories include new items added due to teleworking to ensure patching and vulnerability management are effective. Maintain patch and vulnerability management practices by keeping software up to date and scanning for vulnerabilities. Enable automatic software updates or use a managed

2 ENTERPRISE CYBERSECURITY CONTROLS

Implement, maintain, and invest in enterprise cybersecurity controls to securely connect employees to the organization's network and assets. In modern IT environments, zero trust architecture may be preferable to virtual private network (VPN) solutions due to the lack of perimeter defense in cloud and distributed systems. Evaluate the

TELEWORK ESSENTIALS TOOLKIT

TELEWORKERS – YOUR HOME NETWORK

DEVELOP SECURITY AWARENESS AND VIGILANCE

After rapidly adopting wide-scale remote work practices in response to COVID-19, organizations have started planning for more permanent and strategic teleworking postures. An organization's executive leaders, IT professionals, and teleworkers all have roles to play in the shift from temporary to long-term or permanent telework strategies. The Cybersecurity and Infrastructure Security Agency (CISA) is providing these recommendations to support organizations in re-evaluating and strengthening their cybersecurity as they transition to long-term telework solutions.

ACTIONS

1 CONFIGURED AND HARDENED

Ensure your home network is properly configured and hardened. Change all default passwords and use strong, complex passwords. Ensure your home wireless router is configured to use WPA2 or WPA3 wireless encryption standard at the minimum and disable legacy protocols such as WEP and WPA. Ensure the wireless network name (service set identifier [SSID]) does not identify your physical location or router manufacturer/model. Use a protective Domain Name System (DNS) service. (TECHNICAL)

- CISA Tip on Securing Wireless Networks
- Center for Internet Security (CIS) Telework and Small Office Network Security Guide
- GCA Cybersecurity Toolkit for Small Business
- Work From Home Coalition Guidance

2 SECURE PRACTICES AND ORGANIZATIONAL POLICIES

Follow secure practices and organizational policies for handling sensitive data including: personally identifiable information (PII), protected health information (PHI), classified materials, intellectual property, and sensitive customer/client information. Avoid storing or transmitting sensitive organizational information on personal devices. If personal devices are approved for telework use, regularly apply the latest patch and security update on your devices. Follow your organization's guidance on securing your devices, including implementing basic security controls like password authentication and anti-virus software. (TACTICAL/TECHNICAL)

- Cyber Readiness Institute Data Protection Basics for Remote Workers
- Cyber Readiness Institute Authentication/Passwords Guidance
- GCA Cybersecurity Toolkit for Small Business

3 OPENING EMAIL ATTACHMENTS AN CLICKING LINKS

Use caution when opening email attachments and clicking links in emails. Increase your awareness of phishing tactics, current phishing campaigns, and social engineering to effectively report suspicious emails and communications. (TACTICAL)

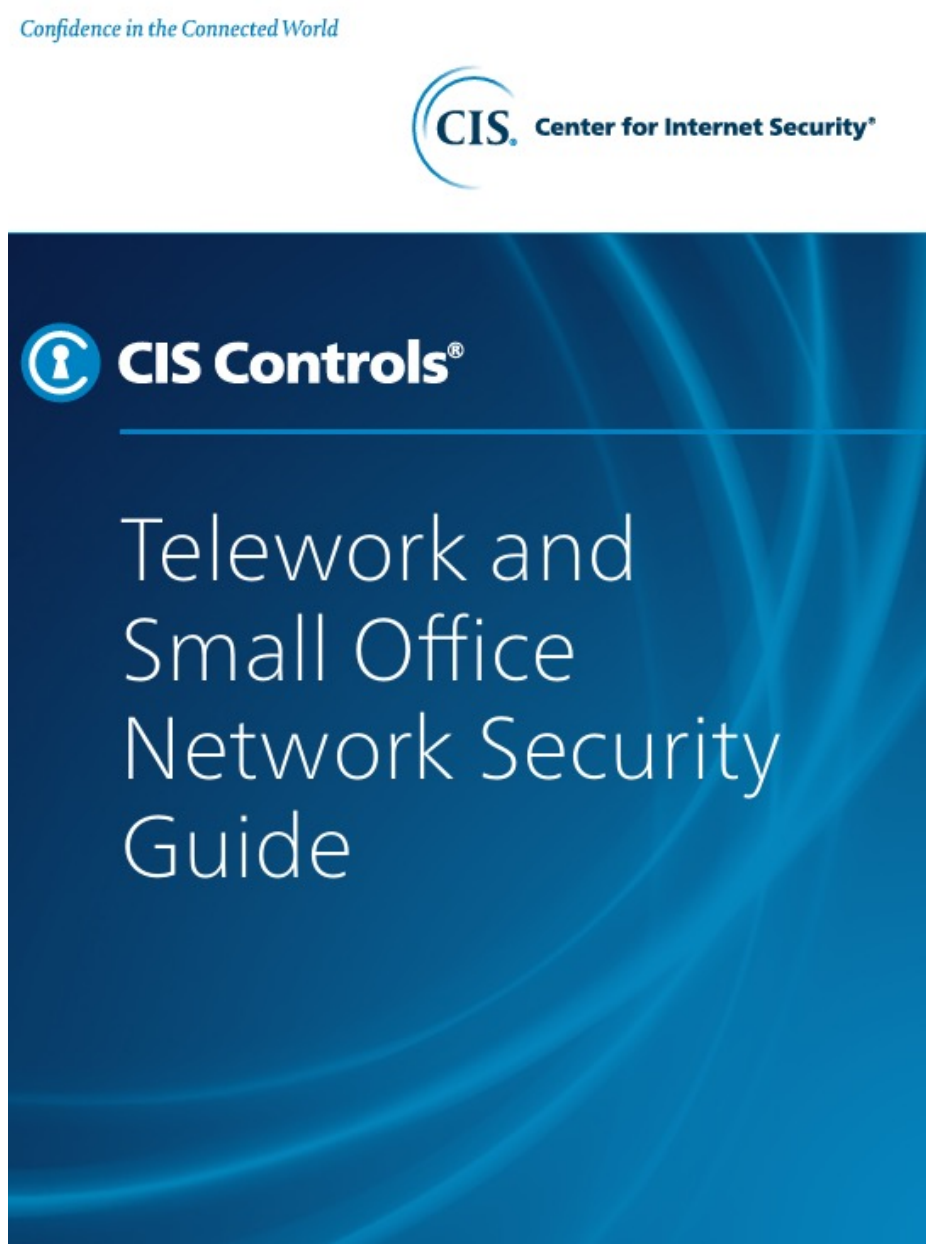
- CISA Tip on Using Caution with Email Attachments
- Cyber Readiness Institute Phishing Guidance

4 COMMUNICATING SUSPICIOUS ACTIVITIES

Make sure you know the procedures for communicating suspicious activities to your organization's IT security team and promptly report all suspicious activity. (TACTICAL)

- Telework Security Basics

As the Nation's risk advisor, CISA has compiled telework guidance to improve general cybersecurity posture. For the latest resources: CISA Telework Guidance

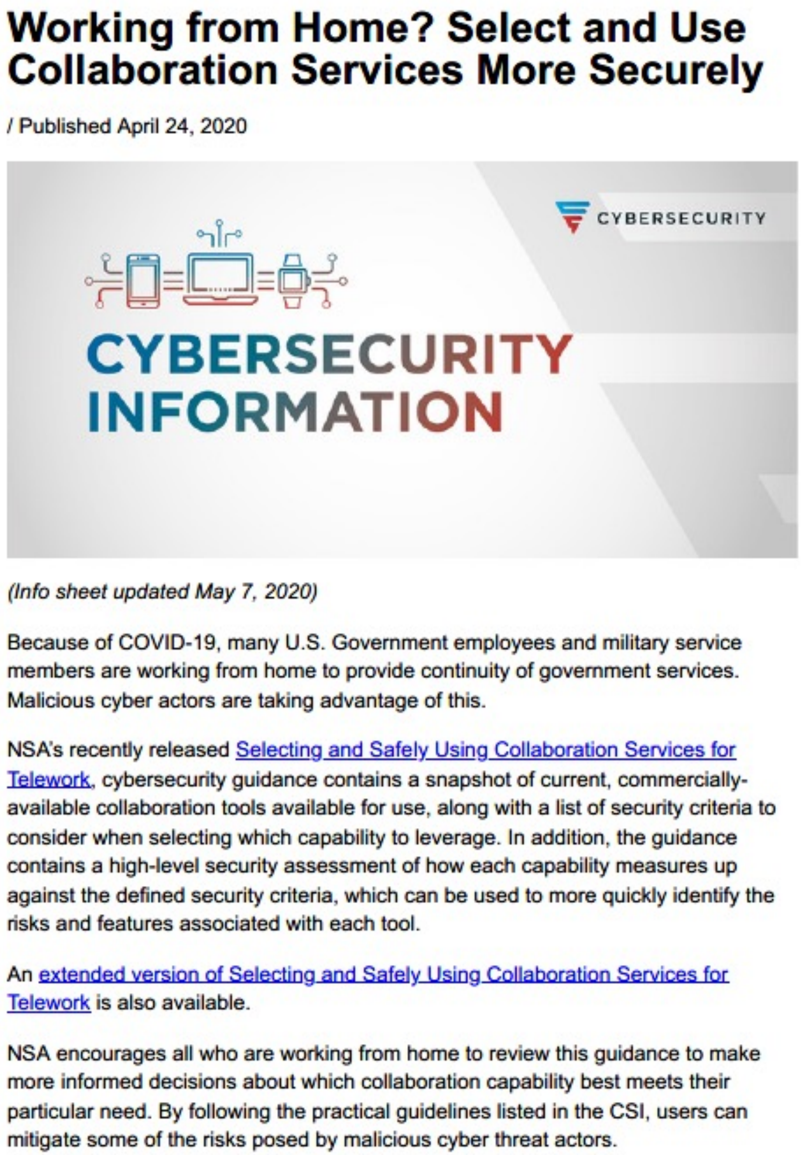


Confidence in the Connected World

CIS. Center for Internet Security®

CIS Controls®

Telework and Small Office Network Security Guide



Working from Home? Select and Use Collaboration Services More Securely

/ Published April 24, 2020

(Info sheet updated May 7, 2020)

Because of COVID-19, many U.S. Government employees and military service members are working from home to provide continuity of government services. Malicious cyber actors are taking advantage of this.

NSA's recently released Selecting and Safely Using Collaboration Services for Telework, cybersecurity guidance contains a snapshot of current, commercially-available collaboration tools available for use, along with a list of security criteria to consider when selecting which capability to leverage. In addition, the guidance contains a high-level security assessment of how each capability measures up against the defined security criteria, which can be used to more quickly identify the risks and features associated with each tool.

An extended version of Selecting and Safely Using Collaboration Services for Telework is also available.

NSA encourages all who are working from home to review this guidance to make more informed decisions about which collaboration capability best meets their particular need. By following the practical guidelines listed in the CSI, users can mitigate some of the risks posed by malicious cyber threat actors.

NSA May 7, 2020

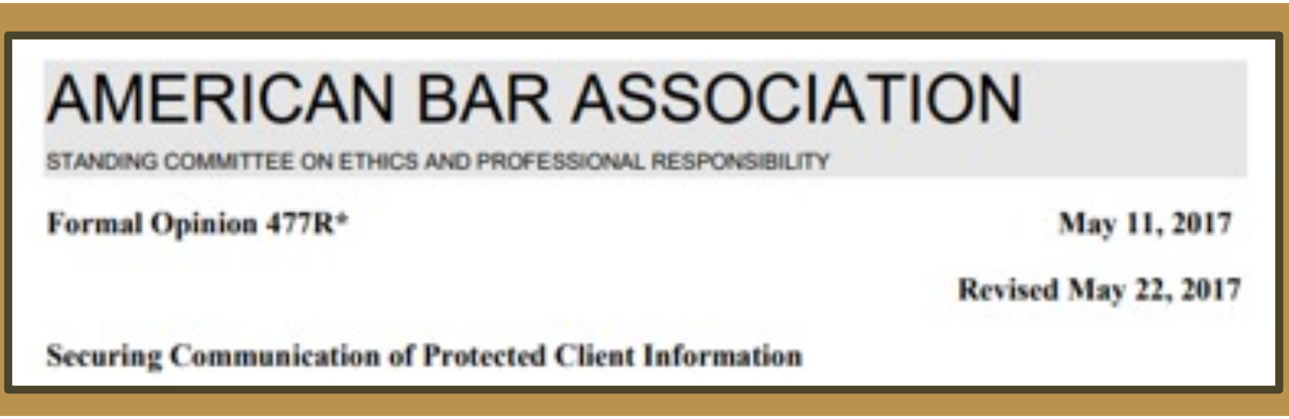
SANS Security Awareness Work-from-Home Deployment Kit

Everything you need to create a secure work-from-home environments during the COVID-19 pandemic and beyond.

https://www.sans.org/security-awareness-training/sans-security-awareness-work-home-deployment-kit

Work and Learn from Home Securely
With the coronavirus disrupting business as usual, organizations and school districts worldwide are implementing work-from-home policies. Not only does this pose new challenges for organizations that lack the processes and technologies required to secure a remote workforce, it puts an even greater burden on families who must quickly adapt to a new way of working and learning from home — and do so safely and securely.

Encryption



AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R*

May 11, 2017

Revised May 22, 2017

Securing Communication of Protected Client Information

- In transit
- At rest
- 2020 ABA Legal Tech Survey – 39% of lawyers use encryption when sending confidential data

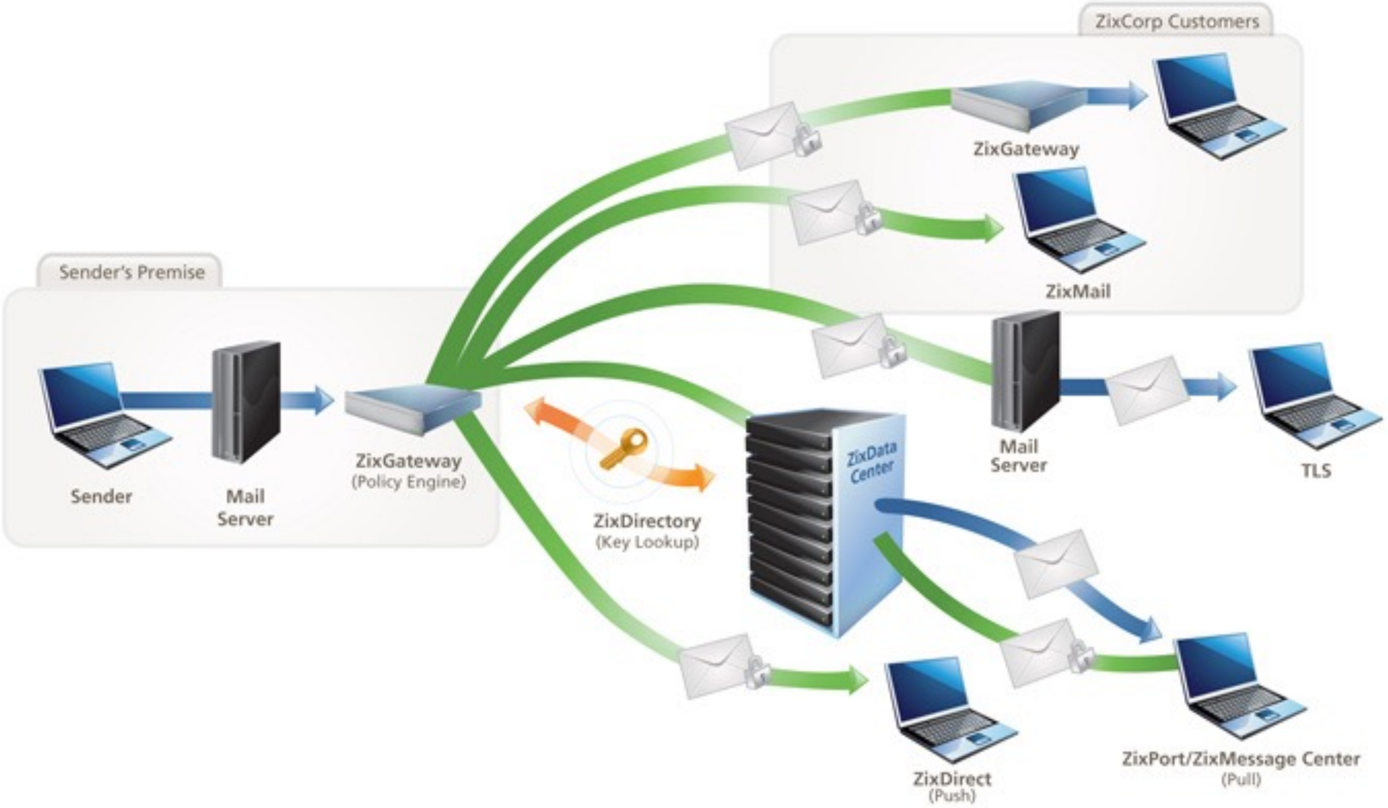
Disk Encryption

Operating System:

- Windows BitLocker
- Mac FileVault 2

Software:

- Symantec Encryption (PGP)
- Kaspersky Endpoint Security
- DriveCrypt PlusPack
- Sophos SafeGuard
- WinMagic



Encrypted email

- Proofpoint
- Mimecast
- Microsoft 365 - Azure Rights Management
- Sophos
- G Suite and Gmail Virtru
- Citrix Secure File Transfer
- HP SecureMail
- EdgeWave
- Trend Micro
- Symantec
- Through some case management portals

Smartphones and Tablets

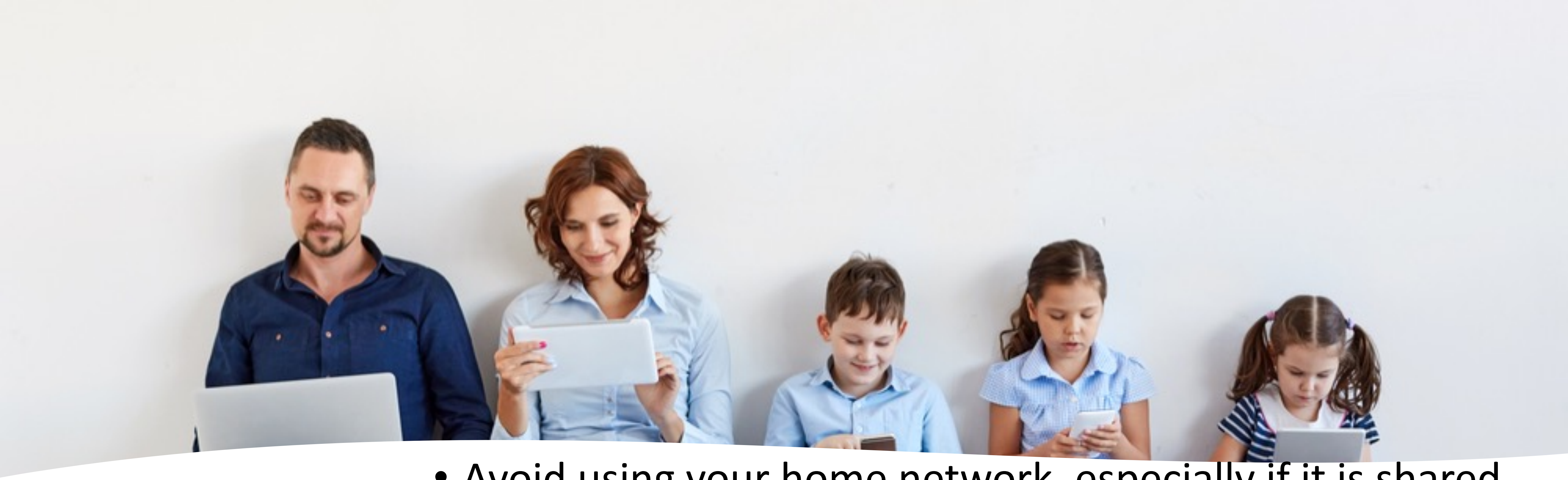
- Follow manufacturer’s instructions
- Use strong PIN or passcode
- Enable encryption
- Enable wipe after *X* failed log-on attempts
- Enable remote location and wiping
- Set auto timeout

Secure file sharing

- Encryption
- Password lock PDF, Zip, docx
- Version control
- Audit trail
- ShareFile

Use Business-Grade Tech

Microsoft



Network connectivity

- Avoid using your home network, especially if it is shared with family members
- You are competing for bandwidth
- If you DO use it:
  - Make sure it has WPA2 or WPA3 encryption and change the default login password and default Wi-Fi name/disable remote administration
  - Consider using a separate wireless network for work

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

Next generation Wi-Fi

Wi-Fi 6

WPA3

Mesh networks

Remote access software

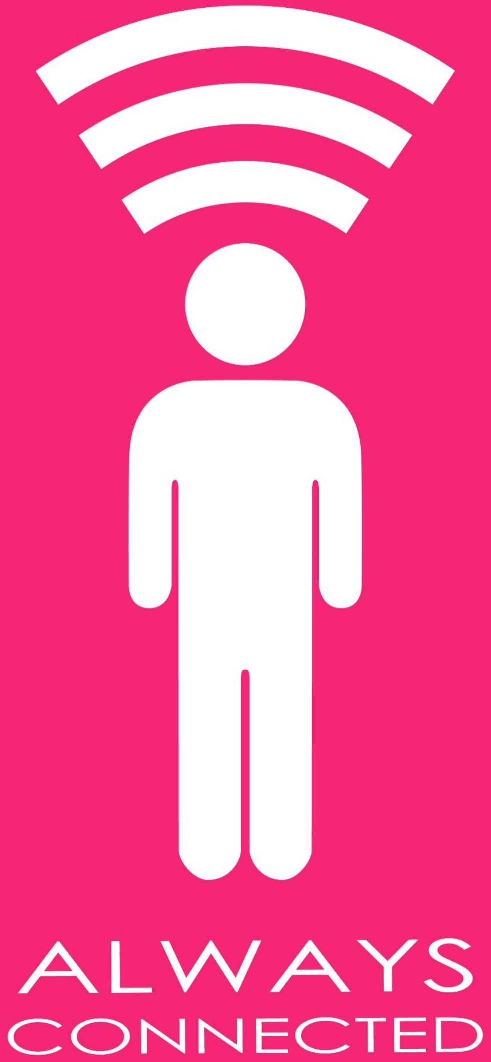
- Virtual Private Networks (VPNs)
- Many firms have VPNs but check the licensing and capacity for your implementation!
- Retrain employees on procedures for using the VPN, especially for those who don’t normally connect remotely

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

Connecting to your network from home

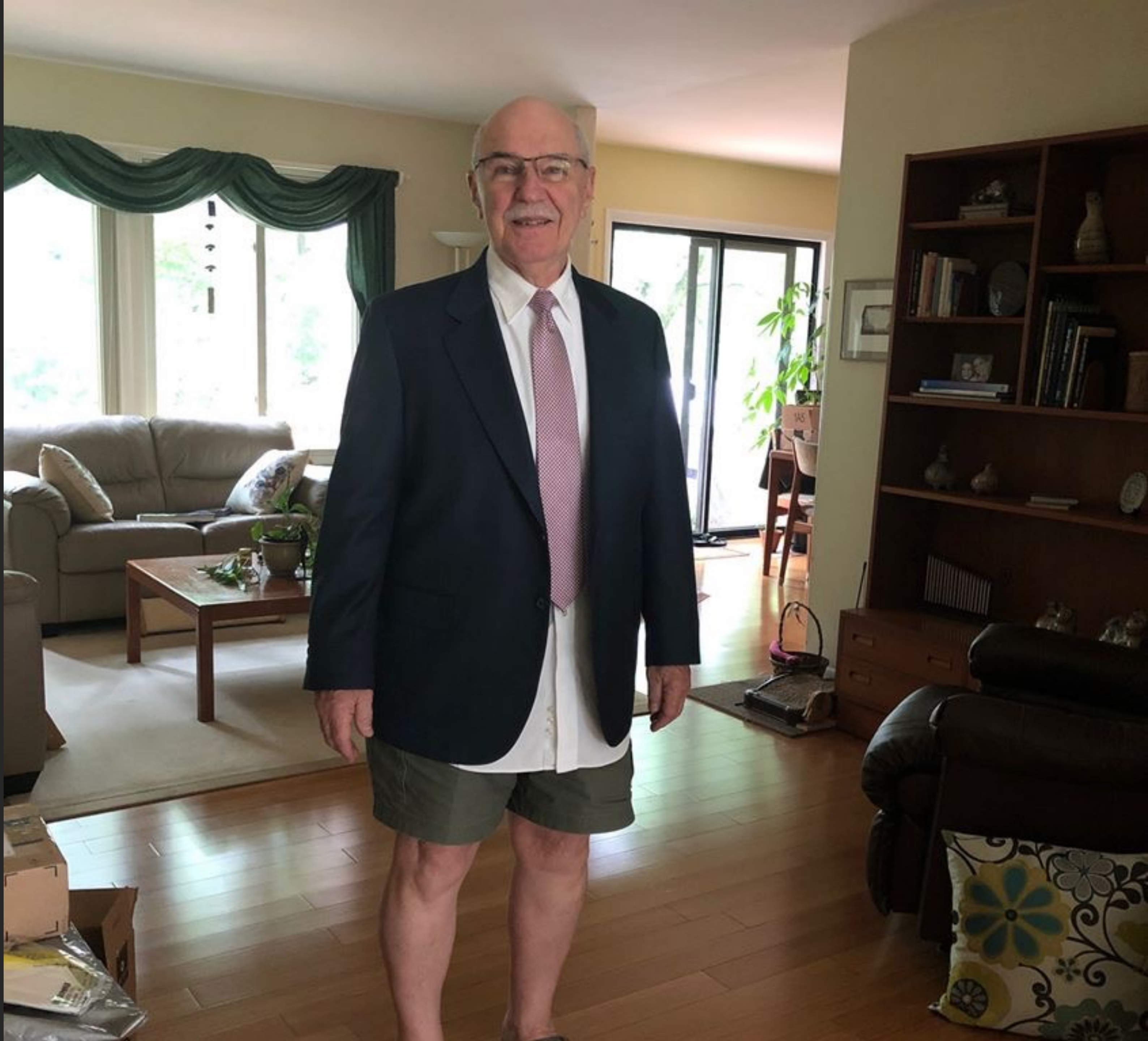
- Enable the Remote Desktop Protocol (RDP)?
- It’s disabled by default - it exposes your firm’s computers to the internet
- Larger firms with Terminal Services have controls in place to safely use RDP



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

Be professional!



Sharon D. Nelson
snelson@senseient.com

John W. Simek
jsimek@senseient.com