CYBERSECURITY ALERT:

TIPS FOR WORKING SECURELY WHILE WORKING REMOTELY

ISSUED BY THE
TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE
OF THE
NEW YORK STATE BAR ASSOCIATION

March 12, 2020

Opinions expressed are those of the Committee preparing this Cybersecurity Alert and do not represent those of the New York State Bar Association unless and until the report has been adopted by the Association's House of Delegates or Executive Committee.

TECHNOLOGY AND THE LEGAL PROFESSION COMMITTEE

CO-CHAIRS

Mark A. Berman
Ganfer Shore Leeds & Zauderer LLP

Gail L. Gottehrer
Law Office of Gail Gottehrer LLC

COMMITTEE MEMBERS

Seth Agata
Mark A. Berman
Alison Arden Besunder
Shoshanah V. Bewlay
John D. Cook
Hon. Fern A. Fisher
Parth N. Chowlera
Tracee E. Davis
Sarah E. Gold
Gail L. Gottehrer
Maura R. Grossman
Ronald J. Hedges
Shawndra Jones
James B. Kobak, Jr.
Glenn Lau-Kee
Ronald C. Minkoff
David P. Miranda
Mauricio F. Paez
Marian C. Rice
Kevin F. Ryan
Prof. Roy D. Simon
Sanford Strenger
Ronald P. Younkins

AUTHORS OF THIS ALERT

Mark A. Berman
Patrick J. Burke
Todd D. Daubert
Gail L. Gottehrer
Ronald J. Hedges
Debbie Reynolds
Aishwarya Minochia

INTRODUCTION FROM THE CO-CHAIRS

As a result of the COVID-19 outbreak, numerous attorneys find themselves in uncharted professional territory, with their work lives and daily routines unexpectedly disrupted. Many attorneys who have worked in offices throughout their careers, with the benefit of administrative support, now find themselves forced to work from home, and not as comfortable as they would like to be with the technology they need to use in order to carry on their practices and comply with their ethical obligations remotely. Further complicating matters, in addition to the ever present cybersecurity risks attorneys face daily, we have seen an increase in malware and phishing schemes related to COVID-19.

Given our focus on providing practical, understandable, and timely cybersecurity resources to NYSBA members, the Committee on Technology and the Legal Profession has put together this Alert. It is designed to provide attorneys with a checklist of tips to help them work securely while working remotely. Like the *Key Takeaways* report we issued in February, the Alert is concise and easy to read. The Committee thanks Patrick J. Burke, Todd D. Daubert, Ronald J. Hedges, Debbie Reynolds, and Aishwarya Minochia, all members of its Cybersecurity Subcommittee, for their help in preparing this Alert.

CHECKLIST

With the spread of Coronavirus/COVID-19, it's important for law firms to quickly address their planning for having attorneys and staff serve their clients' needs from home. Here is a practical checklist of what firms need to consider to make that work, and to avoid cybersecurity risks inherent in remote lawyering:

- **If your firm doesn't already have a remotely-accessed digital workspace, get one.** (These are sometimes called VPNs, for Virtual Private Networks.)
    - Get one licensed, installed and tested by your IT personnel
    - It should enable access to email, documents and billing applications
    - It should have multi-factor authentication, meaning that even if the wrong person gains control over an attorney or staff member's personal device, they cannot access the firm's digital workspace unless they also possess that second device
    - Make sure your attorneys and staff know how to use it
    - Provide written instructions and hold tutoring sessions

- **If you already have a remotely-accessed digital workspace/VPN, make sure every attorney and staff member knows how to use it to access needed information.**

- **Consider providing attorneys with the ability to conduct telephone and video conferences from home.**
    - You may need to obtain or expand licenses for secure and reliable conference call and video conferencing services
        - Some attorneys may be tempted to use free services, which may not be secure, or services keep recordings of conversations and meetings by default, leaving those recordings out of the firm's control and protection. You should not do so.

- **Prepare attorneys and staff for work-from-home.**
    - Make sure attorneys and staff know how to access their work voicemail (and know their passcode)
    - Share personal telephone numbers among colleagues as a communications back-up
    - Verify that attorneys and staff members have access to a laptop, iPad or other devices so that they can use to work effectively from out of the office
        - Encourage them to check that their devices have all recommended system updates and patches installed
        - Advise them that these devices should require passwords (or facial recognition) for use
        - Warn about the risks of sharing the device with family members

- Attorneys and staff members need to know how to use the firm's remotely-access digital workspace. Double check with any who have not been accessing it regularly
    - Verify they all have the digital workspace properly installed on their out-of-office device
    - Verify that everyone has the accompanying multi-factor authentication app linked to the digital workspace properly installed on a smartphone or a second device
- Educate attorneys and staff on the dangers of linking to the firm's systems using insecure publicly-available WiFi, or using a home WiFi connection that lacks strong password protection
- Start moving copies of important paper copies of work materials from the office to home
    - Having client confidential information printed on paper in unsecure locations (including home) can be a security risk if stolen, lost or misplaced, so advise attorneys and staff not to do so unless it is unavoidable, where the benefits outweigh the risk
    - This paper should be securely shredded after use (not simply disposed of at home or in a public place), or brought back to the office

- **Prepare for the cybersecurity risks of remote working.**
    - Understand that all of the firm's efforts to prevent malware from entering the IT system have not been applied to attorney and staff personal devices
        - Personal devices may already be infected with malware, particularly if used by children or other family members who click unsafe links sent by hackers
        - Personal devices likely do not have the perimeter controls and virus detectors installed on firm systems, and often lack required patches to security flaws in their operating system and applications
    - Employees should not store confidential client digital documents, communications and other digital information outside of the firm's secured environment
        - Digital workspaces/VPNs generally only enable storage within the digital workspace/VPN
        - Beware of attorneys and staff who send copies of emails and documents through their personal email accounts
            - Set a policy forbidding saving of client confidential emails and documents directly on personal devices (they should be stored only on the firm's system, using the remotely-accessed digital workspace/VPN)

        - Warn against using personal devices that are not secure
            - Personal devices should be protected with strong passwords and, if possible, segregated with separate passwords for separate access for significant others or other family members
            - If possible, these devices should be encrypted when not in use (and consider advising that these devices should not be taken out of the home to prevent loss, particularly if not encrypted)
            - If client confidential data is saved to the devices' hard drives, it should be deleted as soon as practicable
            - Instruct attorneys and staff not to store or transfer confidential data using unapproved personal cloud service accounts
        - Consider requiring all attorneys and staff to change their passwords frequently during the course of the remote-working period
            - This reduces the scope of the threat if their personal device gets hacked (or already is)
        - Provide attorneys and staff with refresher training on avoiding cybersecurity risks, including phishing attacks (often effectuated by tricking email recipients to click links that release malware)
            - Consider sending attorneys and staff fake phishing emails, to test which of them clicks the links and require follow-up training

- **IT security should go on high alert.** Whether you have internal IT or outsource, they should be:
    - Watching closely for anomalies in activity on your system, evidence of hacking during this time of vulnerability
    - Keeping better logs of network activities, to enable better information about threats
    - Keeping a particular eye on remote access
    - Considering "stress-testing" your security protocols, perhaps randomly, to determine where vulnerabilities lie and plug them before bad guys can get into your firm's network

Lastly, consider the challenges of practicing law amid the Coronavirus/COVID-19 outbreak as a good time to review (or create) your firm's written Business Continuity Plan, and consider whether your firm has appropriate cybersecurity insurance, including for social engineering (and an appropriate amount of coverage).

As someone once wisely said:

> *"You never want a serious crisis to go to waste. And what I mean by that is an opportunity to do things that you thought you could not do before."*

For a comprehensive, yet readable, summary of practical cybersecurity considerations for law firms, take a look at ***Key Takeaways from the Cybersecurity Thought Leadership Conference of the Technology and the Legal Profession Committee of the New York State Bar Association (February 3, 2020)*** *by clicking this link:* https://nysba.org/app/uploads/2020/02/FINAL-NYSBA-Cyber-Key-Takeaways-13120.pdf