COVID-19: WORKING REMOTELY – WHAT ATTORNEYS NEED TO KNOW TO AVOID CYBER THREATS AND PRIVACY RISKS

I. Introduction (Mike Kassak)

II. Cyber Risks Presented as a Result of Working Remotely

1. Proposed Questions to Vanessa:

   1. As a general rule, could you provide an overview of the general ways in which cyber criminals are able to take advantage of people and gain access to networks.

   2. What unique risks are posed by people working from home as a result of the coronavirus crisis?
      - People are more anxious
      - Unique Covid-19 schemes
      - People working remotely, not following normal protocols
      - Devices used without normal security
      - Possible ransomware
      - IT Support stretched too thin dealing with other issues

III. Tactics For Mitigating Cyber Risks Presented From Increased Remote Use

A. Preparations For Additional Remote Workers

   1. Proposed Question to Josh:

      What preparations can law firms take even now to prepare for and adjust to an increased remote workforce?

   2. Proposed Question to Ryan:

      What are some of the adjustments you have seen from a small to solo-practitioner viewpoint?

   3. Proposed Question to Tony Dolce:

      Tony, it is my understanding that Chubb has always had a number of remote workers but obviously that number will increase dramatically as a result of the coronavirus. What additional changes or preparations has Chubb made to prepare itself for the increased number of remote workers?

B. Best Practices
1. **Same General Question to Josh, Ryan and Tony:**

There are several “Best Practices” law firms can employ to mitigate against a successful cyberattack or cyber incident caused by having a remote workforce. Let’s break that down into some specific areas:

1. Encryption, use of home devices and email accounts, and the use of the home network are paramount issues. What should lawyers and law firms be looking for?

2. Phishing and ransomware attacks. What steps should attorneys take to mitigate against those risks?

3. The use of VPNs vs. Wi-Fi – what should lawyers know?

4. Increased use of Zoom? What are some drawbacks or dangers?

IV. **Other Issues**

A. **Ethical Issues**

1. **Proposed Question to Josh:**

   What are some of the ethical issues implicated as a result of a cyber-attack?

   - What does ABA Formal Opinion 477R say and how to lawyers comply with the Model Rules upon which it is based?

   - What does ABA Opinion 483 say and how to lawyers comply with the Model Rules upon which it is based?

**NOTE:** Ryan, please feel free to add to this section as you see fit.

B. **Client Guidelines**

1. **Proposed Question to Tony:**

   Many clients, including Chubb, have certain requirements regarding cyber threats and privacy. How are these requirements affected, if at all, by the increased remote activity?
2. (Josh) (Ryan) What are the typical client requirements have, and what should firms do to ensure compliance with them in these challenging times?

C. Laws

Data security and privacy laws still apply, notwithstanding the unprecedented times we are in. What are some of those laws and what should law firms remember? (Josh)
Suggested Readings

NOTE TO READERS: The electronic version of this document contains hyperlinks to publicly-accessible (and trusted) copies of resources cited below. To retrieve a resource, hover the cursor over and click on the citation that you want. (You must be connected to the Internet for the click navigation function to work)

I. A Sampling Of Cybersecurity Laws And Rules Important To Attorneys

A. “State Data Security Breach Notification Laws” (a/k/a “Mintz Matrix”), available at Mintz.com (current through September 1, 2019)

B. American Bar Association, Standing Committee On Ethics and Professional Responsibility, Formal Opinion 483,” Lawyers’ Obligations After an Electronic Data Breach or Cyberattack” (October 17, 2018)

II. Working From Home Cautions From 2020 COVID-19 Pandemic

A. Cautionary Tales


2. “Multiple Phishing Attacks Discovered Using The Coronavirus Theme,” Spider Labs Blog (Trustwave.com) (February 13, 2020)

3. “Hackers Find New Target As Americans Work From Home During Outbreak.” TheHill.com (March 14, 2020)

4. “Update :Coronavirus-Themed Domains 50% More Likely To Be Malicious Than Other Domains,” Check Point blog (March 5, 2020)

B. Helpful Checklists For Working Safely From Home During Pandemic

2. “Addressing Cybersecurity Risks During the COVID-19 Pandemic,” New Jersey Cybersecurity And Communications Integration Cell (March 12, 2020)


III. Useful, More Detailed Government Resources

A. FBI. Internet Crime Complaint Center website) (a/k/a/ IC3) (essential for response to business email frauds)


C. Federal Trade Commission:

   1. Cybersecurity For Small Business (online handbook)
