AHERN INSURANCE BROKERAGE

AHERN Update

As provided by Hinshaw & Culbertson, LLP— leaders in risk management.

AXA XL is the #1 global commercial property & casualty insurer, with gross written premium of $19 Billion in 2018. AXA XL's core operating insurance and reinsurance companies have one or more of the following financial strength ratings: A.M. Best A+, S&P AA-.

SAN DIEGO COUNTY BAR ASSOCIATION

AHERN Insurance Brokerage, San Diego County Bar Association's Premier Member Benefit Provider since 2004, is pleased to offer SDCBA members an exclusive Professional Liability Program with AXA XL. **SDCBA members can save up to 20%.**

Call (800) 282-9786 to speak with an AHERN Professional or visit us online at aherninsurance.com/associations/sdcba.

COVID-19 Scams Are Contagious

Risk Management Question

What precautions can lawyers, staff, and law firms take to avoid pandemic cyber scams?

The Issue

As more attorneys and even law firm staff take up social distancing and working from home, the related cyber risks increase. Hackers have well-rehearsed playbooks that seek to exploit distributed workforces using remote connections. As a result, lawyers and staff should be more vigilant and take more precautions than when working from the office. Among other things, hackers are circulating phony but legitimate looking:

- COVID-19 outbreak maps.
- Emails purportedly from IT teams to employees with the subject line: "ALL STAFF CORONAVIRUS AWARENESS" describing a seminar at which the company will discuss what it's doing in response to COVID-19, which includes a link to register for the seminar.
- Emails purporting to be from vendors about COVID-19 tools and strategies that include links to PDF and Word Documents that invite the recipient to click and open the attachment.
- SMShing messages closely resembling the employer's phone number, indicating that the recipient needs to "click here" to find out about modified firm operations.

These harmless and legitimate looking emails and attachments are loaded with malware which deploy remote access tools (RAT), keystroke logging malware, desktop image capturing malware and ransomware. Hackers are looking to potentially gain control of lawyers' and staffs' remote access into the firm or to encrypt computers and anything else the malware can reach.

Risk Management Solutions

So what can lawyers do to protect themselves and their firm?

1. Always think before you click.

2. Never click on an email or text message from anyone who you don't know.

3. If you receive an attachment in an email or text message you were not expecting, even if it's from someone you know, call the person at a known telephone number (not the number listed in the message) to confirm the message is legitimate.

4. If you click on something that you should have avoided and a box opens that asks for your password or to supply some information or to click on a link to enable a later version of software – Stop, Close Out and Immediately Call Your IT Department to have a scan run on your device.

5. Remember the ongoing risk of public Wi-Fi. If you can connect to Wi-Fi without a password, then the network is insecure. Do not use unsecure Wi-Fi for connecting to a your work server and don't use it to do any personal banking or sending any type of confidential or personal information.

6. Avoid working in public spaces where third parties can view screens or printed documents.

More than ever it's important to follow the classic Hill Street Blues' watch commander's advice: Let's be careful out there.