Regular instruction, maintenance necessary for business cybersecurity

By Kathryn D. Terry

Kathryn D. Terry

There is a lot of legal traffic and inquiry regarding increased incidents of cyber intrusion attempts and questions about vulnerabilities. Here are three quick-and-important tips to consider:

1. **Review:** We recommend you review your protocols and procedures, and *take the time to remind your employees* about phishing scams, as well as other common red flags like slow computer response and crashes/lock ups.
2. **Implement:** Also, be sure to implement multi-factor authentication at log in. Most insurance companies, financial institutions and business vendors are

requiring it already; all will be requiring it soon enough.

3. **Confirm:** Finally, never send a wire transfer without confirming the instructions over the telephone with all interested parties. We are seeing a lot of intercepted/false wire transactions right now.

The White House's bulletin on this subject is here for your convenience, as are your colleagues at Phillips Murrah. We can help you with responding to a cyber security incident, including emergency mitigation, insurance, notification issues required by various states and the federal government, mitigation and improving your own processes.

The emphasis of Kathryn D. Terry's litigation practice is in the areas of insurance coverage, labor and employment law and civil rights defense. She also represents corporations in complex litigation matters.

The Phillips Murrah Cybersecurity and Data Privacy team stands ready to assist you with your cyber and privacy responsibilities and challenges.

For more information on this alert and its impact on your business, please call 405.552.2452 or email Kathryn D. Terry.

*Follow our coverage on **FACEBOOK***