

Cyber-Secure Attorneys: Ethical obligations, Ambiguities, & Practical Considerations

UT School of Law 2017 Land Use Conference

Thursday, April 6, 2017

Pete Haskel

Peter.Haskel@dallascityhall.com

214-670-3038

PRELIMINARY NOTES

1. Some of the Web sites that I cite in this presentation may require free registration, but most do not. I do not think any have a paywall, but no warranties.
2. Unless otherwise noted, all emphases within quoted excerpts are added.
3. Beware of root rot!

DISTINGUISH ETHICS OBLIGATIONS FROM OTHERS

Distinguish between ethics obligations relating to cybersecurity under Tex. Disc. R. Prof. Con. (the subject of this presentation) and other obligations to provide cybersecurity:

1. Contract: Special provisions in retainer agreements and sometimes in law office policies.
2. Tort: Due care required to avoid malpractice liability.
3. Regulatory: Depending on jurisdiction (e.g., if you are an associate for health care provider or represent financial advisers). See **Sedona Conference Data Privacy Primer Jan. 2017 Public Comment Version**, <https://thesedonaconference.org/download-pub/4983>; **Sedona Conference Commentary on Privacy and Info Security Nov. 2015**, <https://thesedonaconference.org/download-pub/4786> (both are free PDF downloads, registration required; both also discuss ABA Model Rules)
4. Other state ethics rules to extent that they may apply

CYBERSECURITY CHALLENGE

“IT security professionals used to warn that only two types of businesses exist: those that have been hacked, and those that will. Now, many are even more pessimistic and divide the world’s businesses into companies that know that they have been hacked, and those that don’t. . . .”

Untangling the Mystery of Cybersecurity Insurance,
<http://www.insidecounsel.com/2017/03/01/untangling-the-mystery-of-cybersecurity-insurance?ref=rss&slreturn=1488465652> (as of Mar. 2, 2017)

FUNCTIONAL ENVIRONMENTS

- Email
- Texting
- Mobile devices – including employee personal devices
- Web Sites & Social Media Sites
- Servers
- Cloud
- Files (embedded metadata, changes, annotations, drafts)
- Desk Top & Auxiliary Hard Drives, Disks, Thumb Drives, etc.
- Peripherals (printers, voice mail)
- PRINTOUTS!
- **CLIENTS', CO-COUNSELS' & EXPERTS' PLATFORMS**

CYBER SECURITY STAGES

- Sending
 - To clients, retained experts & co-counsel
 - To non-clients
 - Special situations requiring security precautions
 - insider trading prevention;
 - sealed pleadings;
 - conflicts walls within law firm or office
 - personally identifiable health information for health care provider
- Receiving – more limited control; malware protection & firewall
- Storing – multiple platforms; backups; ransomware defense; compartmentalizing access within law offices
- Investigating – risks of visiting unknown Web sites (Dark Web), anti-tracking
- Presenting – Limiting access (similar to sending)

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](http://utcle.org/elibrary)

Title search: Cyber-Secure Attorneys: Ethical Obligations, Ambiguities, and Practical Considerations

Also available as part of the eCourse

[2017 Land Use eConference](#)

First appeared as part of the conference materials for the
21st Annual Land Use Conference session

"Cyber-Secure Attorneys: Ethical Obligations, Ambiguities, and Practical Considerations"