

University of Texas CLE  
41<sup>st</sup> Annual Page Keeton Civil Litigation  
Conference  
November 3, 2016

## CYBERSECURITY ITEMS THAT EVERY LAWYER SHOULD KNOW – BUT ESPECIALLY LITIGATORS



Elizabeth [Rogers](mailto:Rogers@gtlaw.com) | [rogersel@gtlaw.com](mailto:rogersel@gtlaw.com) | 512-320-7256  
Shawn Tuma | [Shawn.Tuma@solidcounsel.com](mailto:Shawn.Tuma@solidcounsel.com) | (214) 472-2135



## THE CYBERSECURITY RISKS



## Cybersecurity needs for companies (and firms).

- Strong cybersecurity basics.
  - Policies and procedures focused on cybersecurity.
    - Social engineering.
    - Password and security questions
  - Training of all employees.
  - Phish all employees (esp. executives).
  - Signature based antivirus and malware detection.
  - Multi-factor authentication.
  - Backups segmented from the network.
  - Incident response plan.
- Encryption for sensitive and air-gap for hypersensitive data.
- Adequate logging and retention.
- Third-party security and supply chain risk management.\*
- Intrusion detection and intrusion prevention systems.\*





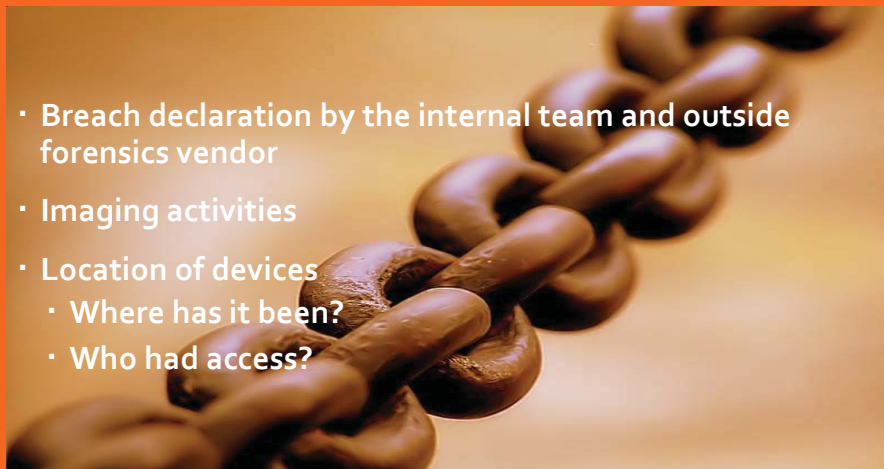
## ***Breach!*** Immediate Priorities

- **Leadership!**
- Assess the situation
- Be a counselor
- Instill confidence
- Bring peace
- Facilitate rational thought & rational behavior



## WHY THE CHAIN OF CUSTODY IS IMPORTANT

- Breach declaration by the internal team and outside forensics vendor
- Imaging activities
- Location of devices
  - Where has it been?
  - Who had access?



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: Cybersecurity Items that Every Lawyer Should Know – but Especially Litigators

Also available as part of the eCourse

[Answer Bar: Technology for Litigators](#)

First appeared as part of the conference materials for the  
41<sup>st</sup> Annual Page Keeton Civil Litigation Conference session  
"Data Security"