SPECIAL CONSIDERATIONS FOR THE BUSINESS DATA BREACH

The University of Texas School of Law 31st Annual Technology Law Conference

May 24, 2018



Leslie C. Thorne haynesboone

Friday Afternoon, 4 P.M.





The Call





Potential Threats

- Contractors or service providers
- Employees/Former employees
- Competitors
- State-sponsored activity
- Hacktivists



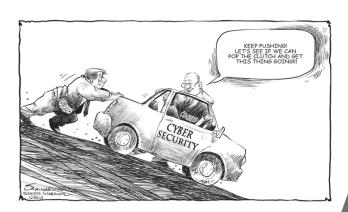
Minimizing Risks (Non-Technical)

- Stay apprised of threats (e.g., ISACs)
- Conduct a data inventory
- Develop appropriate policies and procedures
- Train employees on security issues
- Conduct tabletop exercises
- Manage vendor risks
 - > Due diligence
 - Contract provisions
 - Training and audit



Minimizing Risks (Technical)

- Patching and vulnerability management
- Penetration testing
- Detailed logging
- Firewalls
- Anti-Virus tools
- Encryption
- Behavior analytics









Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the <u>UT Law CLE eLibrary (utcle.org/elibrary)</u>

Title search: Special Considerations for the Business Data Breach

Also available as part of the eCourse 2018 Technology Law eConference

First appeared as part of the conference materials for the $31^{\rm st}$ Annual Technology Law Conference session "Special Considerations for the Business Data Breach"