The Legal Intersection of IT and Privacy

Why Legal And IT Should Be BFFs
Legal and IT: A Team
Legal and IT: The Dream Team

• Why does this matter?
• IT’s perspective
• Legal’s perspective
• Examples
Legal Requirements

• Statutes/Laws
  – HIPAA/HITECH
  – FERPA
  – GLBA
  – COPPA
  – GDPR
  – Foreign Regulations
  – State laws:
    • Data Security
    • 42 states + territories
    • ALL different

• Other
  – PCI Requirements
  – NIST critical infrastructure
  – Industry group “suggestions”
  – ACC Guidelines
  – NAIC Guidelines
Why do they all matter?

• Each is different
• Each imposes different responsibilities on IT and legal
  – Data protection
  – Data movement, storage, transmission
  – Contract contents

• Know your data.
Example:

- You are the CIO for a company that hosts an online platform for companies that allows their employees to log-on and review HR-related data. Business department comes to IT with a request from a current client to transfer data from hosted platform (in Texas) to in-house platform (in Germany).
  - To IT people in the room – any concerns with this?
Importance of Relationship

• Importance of terms and conditions in contracts:
  – Outline in writing (hopefully) the agreement between the parties
  – Disagreements, go to court
  – What if fundamental misunderstanding about what the terms actually mean?
Why Should You Care?

• Because what the attorneys agree to can have a direct impact on you.
  – Contracts that require you to adhere to certain data privacy and security standards
  – Contracts that change reporting requirements
  – Contracts that prohibit certain actions, such as transferring data without client’s permission
Cyber Security Risks

- One-third of U.S. population impacted by health breach
- 529 million records (and counting) breached in 2016
- > half a billion personal records stolen/lost between 2005 and 2015
  - That’s 2.5 x the U.S. population!!!
- In 2016, 1,140 incidents per organization per year
Some Examples

• Contractual Clause:
  – Vendor agrees to mitigate any security incident within 24 hours.
  – What are the problems here?
Another Example

• How about this clause:
  – Vendor shall have the right to change any security measures or programs at Vendor’s sole discretion.
  – To the IT folks in the room – any concerns with this clause?
Are we having fun yet?

• Another Clause:
  – Vendor shall notify Company immediately if a security incident occurs.

  – What are the problems with this clause?
System implications

- “Vendor shall encrypt all Client Data.”
  - Client Data is defined to include any and all data provided by client to Vendor, or that data collected, used, maintained, created, or stored by Vendor on behalf of Client.
The Legal/IT Discussion

- So how do you know when to get legal/IT involved?
  - Business decisions (Business relationships)
  - Involve legal at the beginning
  - Make sure Legal understands big picture IT processes and realities
  - Any time you contract with a vendor/service provider that touches systems/data
When should legal get IT involved?

• Early and often
• Know the data
  – Type
  – Location
• SOPs
• As soon as a breach is suspected
• When entering into new business relationships involving data
When it all goes wrong…

• All this only matters because of data breaches!
• Legal and IT will become well acquainted during a potential or actual breach.
• Better to meet and discuss ahead of time rather than making it up on the fly.
Summary

• Legal/IT teamwork matters because
  – Legal agreements impact IT responsibilities
  – IT practices should be reflected in legal’s actions

• Communication is Key!
  – If legal knows IT, and IT knows legal, business activities better reflect the needs and realities of a business.
Contact Information

Fredric E. Roth V
Thompson Coburn LLP
froth@thompsoncoburn.com    312-580-5060