





Incident Response for Lawyers

Attack on your own systems:

BakerHostetler

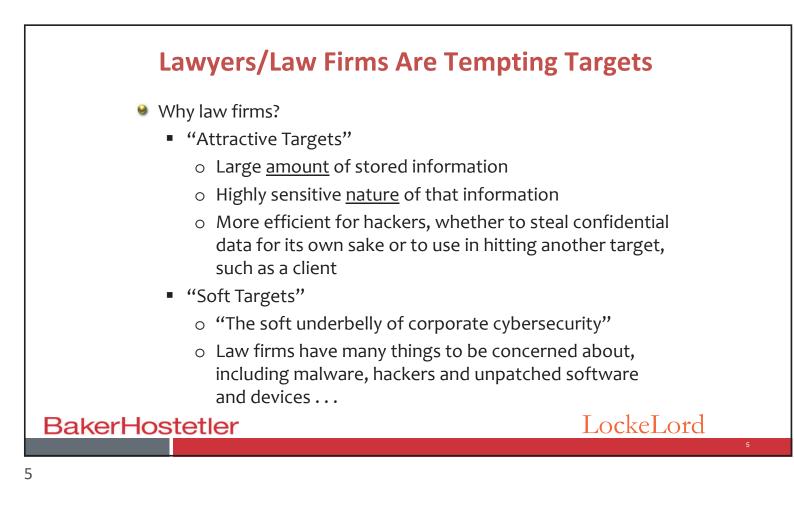
- Who do you call first?
 - Internal or External IT?
- Share exact details of what happened
- Develop containment plan
 - Is a vendor needed?
- Legal analysis if notification is required
 State & Federal laws? Model rules?
- Complete notifications



Attack on your client's systems:

- You may be their first call!
- Get a full explanation of what happened
- Who needs to be involved?
 Insurance? Vendors? Cybersecurity counsel?
- What value are you adding? — Contracting with vendors
 - Attorney-Client privilege
 - Develop containment plan
 - Is a vendor needed?
- Legal analysis if notification is required – Applicable state, federal or international laws?
- Assist with completing notifications
- Regulatory investigations
- Litigation





What types of information are at risk?

- "Confidential Information" in Attorney Files
- Trade Secrets
- Strategic Data
 - M&A targets and due diligence
 - Supply contracts, Pricing
 - Development Data/Reserve Estimates
- Personally identifiable Information of all kinds for employees, clients and third parties
- Payment Card / Bank Account Information





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: Data Security Incident Response and Attorney Obligations

Also available as part of the eCourse Data Security Incident Response and Attorney's Obligations

First appeared as part of the conference materials for the 46th Annual Ernest E. Smith Oil, Gas and Mineral Law Institute session "Data Security Incident Response and Attorneys' Obligations"