Cybersecurity Checklist
Self-Assessment Tool

General prevention and preparedness	✓
Conducts a cybersecurity audit of the entire organization at least annually	
IT and/or legal department audits legal service providers	
Has a data incident response team	
A member of the legal department is on the company's data breach response team	
Has a data incident response plan	
Incident response plan was updated in past 12 months	
Has cybersecurity insurance	
Has mandatory training on cybersecurity for all employees	
Collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks	
New vendor contracts contain termination right in case of security issue	
Has rights to audit sub vendors	
Requires 3rd parties to notify of cybersecurity risk	
Participates in Operation Security (OPSEC)	
Retains a forensic company to assist should a breach occur	
Has data map (data categorized & identified types)	
Tracks mandatory training requirement and attendance for all employees	
Tests employees' knowledge of mandatory training	
Conducts mock security event	
Conducts tabletop exercises	

Policies	✓
Password policy	
Social media policy	
Document retention policy	
Website privacy policy	
Employee manual acceptance policy	
Internet and access management	
BYOD policy	
Encryption policy	

Staffing	✓
Chief Information Officer (CIO)	
Corporate Counsel re: data privacy, compliance & strategy	
Chief Information Security Officer (CISO)	
Chief Risk Officer (CRO)	
Chief Privacy Officer (CPO)	
Chief Security Officer (CSO)	

Confidence	✓
You have high confidence 3rd party vendors protect you from cybersecurity risks	