Cardozo School of Law
Spring 2020
Cybersecurity Law – Syllabus

Adam Cohen
adam@digitaldiscipline.org
(646) 369-0431

Date	Subject Matter	Notes
February 3	Fundamentals of Cybersecurity	• the "CIA triad" and the objectives of cybersecurity broadly (including concepts like "defense in depth" or "layered security") • the "domains" of information systems security according to the "Common Body of Knowledge." • data protection based on state, i.e., data-in-transit, data-at-rest, data-in-use. • components of modern enterprise information technology environments.
February 10	Sources of Cybersecurity Law and Legal Standards	• different kinds of laws directly and indirectly related to cybersecurity ("Cybersecurity Law") (e.g., data security, data retention/limitation, data privacy, biometrics). • various sources of authority for Cybersecurity Law (e.g., state, federal gov, industry regulators, foreign, etc.). • Comparing and contrasting sources of best practices and standards in relation to Cybersecurity Law (e.g., NIST, CSC, regulatory guidance, legal ethics opinions). • relationship between Cybersecurity Law and Data Privacy Law.
February 17	FTC as Cybersecurity Regulator	• FTC authority to regulate cybersecurity • scope of FTC cybersecurity authority • history of FTC cybersecurity enforcement • lessons learned from that history
February 24	State Cybersecurity Laws	• the landscape of non-uniform state Cybersecurity Law regarding data breach notification requirements. • state laws about data limitation and retention in relation to cybersecurity • state Cybersecurity Law regarding specific types of data (e.g., biometrics, IoT, social media). • state data privacy law in relation to cybersecurity
March 2	Financial Services and Healthcare	• statutes and regulatory agencies involved in Cybersecurity Law pertaining specifically to financial services and healthcare organizations. • key federal financial services regulations for cybersecurity. • content and implications of the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies. • HIPAA in relation to cybersecurity.
March 9	Data Breach Litigation	• standing in data breach litigation

		• common law causes of action in data breach litigation. • class certification issues in data breach litigation
March 16	Criminal Law, Anti-Hacking Laws and Active Defense	• roles of various law enforcement agencies and types of threat actors in relation to Cybersecurity Law. • criminal law sources for prosecutions against alleged cybercriminals and exploring illustrative notable cases • selected "anti-hacking" laws, such as the Computer Fraud and Abuse Act, provisions of the DMCA and more, in relation to cybersecurity. • "active defense" or "hackback" as an approach to cybersecurity.
March 23	Government, Government Surveillance and Government Contractors	• impact of the Edward Snowden and other disclosures of NSA cybersecurity materials. • Cybersecurity Law specifically covering government agencies and organizations doing business with certain types of such agencies. • historical case studies involving breaches of government cybersecurity • international treaties and agreements regarding cybersecurity, cybercrime and cyberwarfare.
March 30	Incident Response and Disclosure Issues	• detecting and distinguishing information security incidents and events. • legal issues involved in responding to such incidents, including but not limited to data breach notification requirements, evidence preservation and collection and protecting investigative materials from disclosure. • Developing incident response plans and playbooks.
April 6	Corporate Governance and Employment Issues	• Cybersecurity Law and publications by non-governmental associations and organizations regarding corporate governance of cybersecurity (e.g., SEC, NYDFS, trade, industry and professional associations).
April 20	Third Parties and Information Sharing	• Cybersecurity Law and publications by non-governmental associations and organizations regarding organizational relationships with third party service providers and vendors. • the concept of information sharing groups and reviewing the behavior and impact of such groups in practice.
April 27	Review for Exam	