Institutional constraints on security historically focused on traditional criminal enforcement and a slow but steady increase in civil remedies through the twentieth century. Professional security protection could satisfy reasonable assurance criteria by managing legal and regulatory risks based on commonly-held understandings of burglary, theft, conversion and widely-understood but related institutional constraints in the protection of physical property. This focus retained effectiveness so long as physical security over tangible property appeared successful, even extending to the maintenance of control over mainframe computers and their peripherals. However, the proliferation of networked computers has made access and storage ubiquitous, vastly increasing the vulnerability of confidential data, private information and critical national security infrastructure. Security and privacy regulation compliance responsibility now falls much more harshly on both organizations and most of their individual personnel. These complex new duties constrain organizations in the data management industry as well as suppliers and users of data and all participants in the information supply chain, including consultants, software suppliers, applications service providers, maintenance, outsourcing and communications providers.Other factors exacerbate these liability risk management difficulties. Advances in network computer storage and use, the broadening perception of heightened value of information and the pervasive availability of rich data warehousing increase the vulnerability of data management. Risks of information theft and integrity losses as well as the explosion of privacy rights and national security concerns now require pervasive and fuller understanding of liability risk management principles/techniques among all managers and subordinates in the data management industry and in government. Information suppliers, handlers, owners and network service providers are increasingly exposed to civil litigation, regulatory oversight/compliance and criminal prosecution for various information-related wrongs. For example, confidentiality is compulsory for corporate trade secrets, privacy is required for personally identifiable information about individuals and secrecy is mandatory over matters of national security; all of which create complex legal duties that are fundamentally driving the design of information handling processes. This course surveys legal and regulatory constraints on information security and privacy practices.

452

Legal and Regulatory Environment of Privacy and Security