UC Berkeley Boalt Hall/School of Information
Chief Security Officer Study
Summary

Aaron Burstein, Deirdre Mulligan, and David Thaw

Our primary research objective is to understand how the legal system influences large organizations' decisions about cybersecurity investment. The set of laws that potentially affect investment is vast, including data security breach notification laws; laws requiring corporations to maintain internal controls over information; sector-specific information privacy laws; and laws prohibiting the misappropriation of trade secrets and other forms of intellectual property, computer abuse, and invasions of individual privacy.

An organization's responses to these laws depends both upon the formal provisions of the laws and upon the organization's own culture and economic interests. This connection between specific legal obligations and other forces within an organization is generally absent from current models of cybersecurity decisionmaking. We hope to contribute an understanding of this connection through this research.

We propose to conduct a series of 10-15 qualitative interviews of chief security officers (CSOs) from public corporations headquartered in the United States. We will select CSOs from corporations that represent the major sectors of the U.S economy, with an emphasis on firms that own or operate key elements of the national information infrastructure. CSOs (or their functional equivalents) both are involved at the management level and have the requisite technical expertise to represent the cybersecurity issues facing their organizations across our broad research perspective. These interviews will be 90-120 minutes in length, and will use an open-ended, qualitative approach.

Technical research into problems of cybersecurity have generated a set of approaches to produce more secure information systems, although general agreement as to their priority is lacking. We will structure our interviews around these overarching principles of cybersecurity in order to determine the extent to which they are aligned with legal and regulatory incentives.

Our interviews will yield data with two primary uses. First, the data will provide direct insight as described above that may be used to consider improvements in legal regulation, economic incentivization, and industry involvement activities to achieve cybersecurity goals. Second, our analysis of the data will provide a framework that can be used to interpret existing quantitative data and inform future quantitative analysis to derive more detailed and in-depth knowledge for improving cybersecurity among the nation's digital infrastructure.