REDESIGNING EDO CASTLE: A SOCIOTECHNICAL SYSTEMS APPROACH TO SECURITY FOR MNES IN AN AGE OF ASYMMETRIC THREATS

ABSTRACT

Complex organizations, particularly organizations as high profile and complex as multinational enterprises (MNEs) develop internal and external logics (strategies, cultures, structures, processes, asset disposition, and people processes) based upon external environmental factors as well as internal organizational factors. The last twenty years have been characterized by increased turbulence, uncertainty and risk for these MNEs (DeCieri and Dowling, 2012). Existing defensive designs have been superseded by new forms of global threats. This conceptual review paper is an effort to synthesize approaches, models and ideas from the divergent fields of corporate security practitioners, international human resource management (IHRM) researchers and global strategists. The ultimate goal is to present a unified, systematic framework to better understand the critical dimensions and issues related to balancing the openness inherent in global business practices with the protection of assets and the far flung elements in a MNE’s value chain (Burke and Cooper, 2008).

The first section of the paper, entitled “Context”, reviews the environmental dynamics that have prompted MNEs to retrofit major elements of their business processes while still continuing ongoing business operations. A four part “risk management model” from security literature (identify risk, assess risk, management and evaluate results) is presented with the goal of so organizing activities and practices so as to reduce overall systems risk.
An historical approach to security management as a profession – from its origins in a military model, to the development of a law enforcement model, to the more recent adoption of a business model – is outlined. Roles, structures and responsibilities for security activities and risk reduction are presented. Particular emphasis is placed on the role of the HR unit in security activities at MNEs and the advantages and disadvantages of outsourcing selected elements of security practices as opposed to maintaining the function in house.

The second section of the paper, entitled “Components”, presents a model of security activities in a MNE based upon sociotechnical theory (Miner, 1982, Chapter 4), a longstanding school of organizational theory emphasizing the interaction between people and technologies as synergistic control components. Security domains for “Data”, “People” and “Things” (Fine and Wiley, 1971; Fine, Holt and Hutchinson, 1974) are outlined as the core of a model designed to present a series of issues MNEs address. These issues, in their totality, describe a security philosophy, strategy processes, structures and practices. A series of these critical security dimensions are presented by way of an example of the components in a security portfolio: concentrated versus dispersed assets, reinforced, versus redundant assets, extensive versus minimal security zones, and bimodal (secure versus not secure) versus graduated levels of security for data, people and things assets.

The third section of the paper, entitled “Constellation”, presents a series of combinations of component practices. Applying contingency theory (Lawrence and Lorsch, 1969) MNEs operating in the personal service sector of the economy, or with mass production technologies are predicted to emphasize “people” centered security
practices, with data and things as secondary security activities. Alternately, firms operating in the knowledge sector of the economy or applying continuous process technologies are predicted to emphasize “data” centered security responses with people and things as support security activities. Distribution or logistics based firms are predicted to emphasize “things” centered security responses with data and people as secondary security activities.

Firm history, critical historical events, organizational culture and institutional state of origin are presented as internal factors that may determine the manner in which data, people and things are configured to provide for risk assessment and minimization.

The final section of the paper, “Conclusions” presents a review of potential weaknesses in this model and sets out a research agenda based upon the elements and patterns described in the “Components” and “Constellations” sections of the paper. The goal is to validate and operationalize this vocabulary of security processes and practices for further investigation. Such a set of issues, practices and strategies can act as the basis for a series of descriptive questionnaire items applied to determine activities and practices available to MNE strategists and work toward a set of commonly accepted best practices. We are aware of the need for secrecy in MNE security practices so as to avoid countermeasures, so this empirical process will be problematic. Given the wide ranging nature of security practices for MNEs, encompassing the expatriate literature (“people”) cross cultural and comparative research (institutional and critical issues) as well as strategic MNE concerns, the area of security and risk assessment is likely to be of a significant and ongoing nature (Czinkota et al. 2010).
REFERENCES


