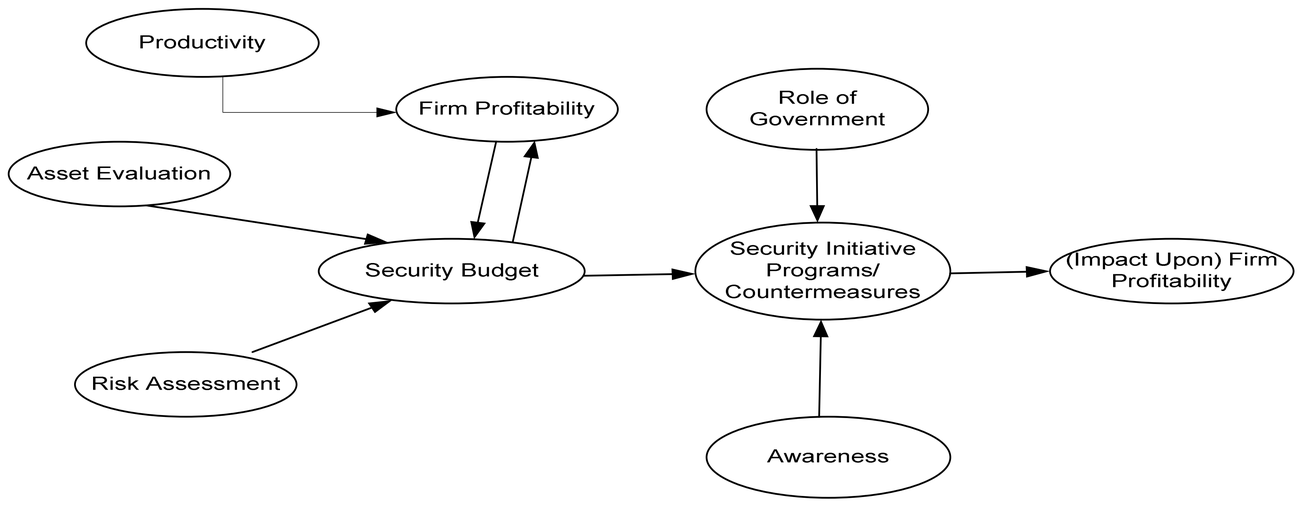
EVALUATING THE ORGANIZATIONAL PROCESS OF SECURING INFORMATION ASSETS FROM THE THREAT OF CYBERATTACKS OR CYBERTERRORIST EVENTS: AN EXPLORATORY STUDY

Objectives

This study is designed to investigate the managerial process of securing organizational information assets. This investigation proposes the following research goals:

- to extend the knowledge of security practitioners' understanding of cyberterrorism, their perceptions regarding the impact of cyberattacks or cyberterrorism and their perceptions regarding safeguards implemented within organizations
- to extend the knowledge regarding nature of relationships (e.g. assessment, impact and safeguards) between constructs within the structural model
- to identify key ideas encompassed in each of the operationalized constructs,(as a result of the exploratory factor analysis)

Informal Organizational Process



*Arrows representing the direction of influence

Proposed Cyberterrorism Definition

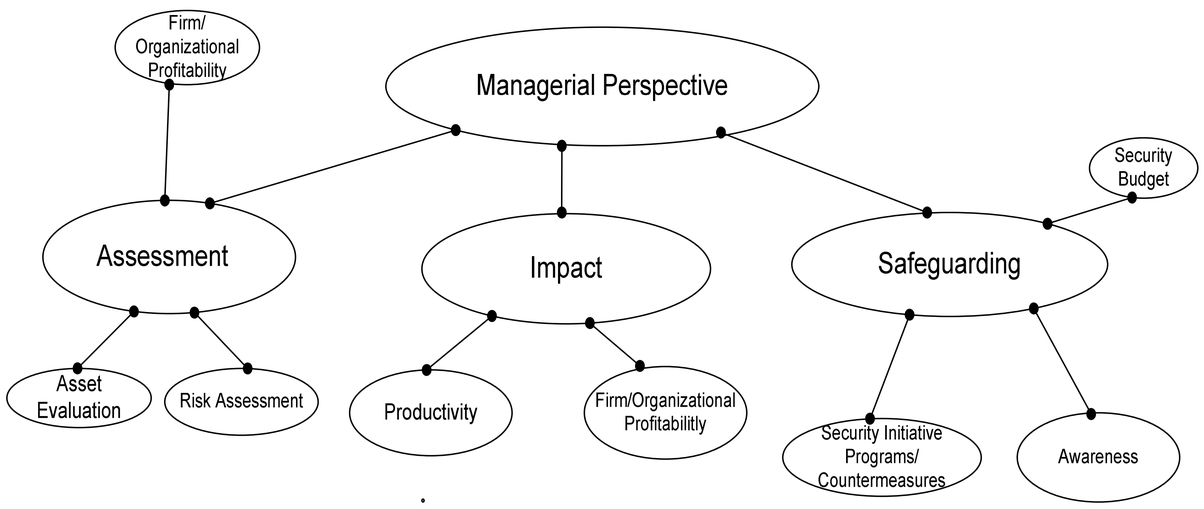
Despite the myriad of definitions that seem to be proliferating, there seems to be *two common themes* that each of the definitions possess. In order to qualify as an act of cyberterrorism, the following two criteria must be met: a *political motivation* and a *destructive result*.

Cyberterrorism Definition from a Managerial Perspective

Malicious cyberspace activity that results in mistrust in the security of an organization's (i.e. business, government, economy, military, etc.) networks or hinders the ability to provide advertised services with high quality, speed of transactions, privacy-confidentiality of personal information, security and integrity of transactions, can be categorized as cyberterrorism.

Conceptual Framework

Construct Development



Contributions of the Study

*Since I/T practitioners were surveyed (138 out of 198 == 69.7% response rate), the results of this investigation are indicative of what information security practitioners deem important.

* This investigation seeks to establish constructs relating to the organizational activities of assessment, impact and safeguards involved in securing information assets.

* A definition of cyberterrorism from a managerial perspective is proposed.

* A managerial process-oriented approach to securing organizational Information assets from the threat of cyberattacks and cyberterrorist event is proposed.

Conclusions

*Each of the constructs were identified, defined and operationalized.

*The constructs were validated through exploratory factor analysis (EFA).

*The components generated from the EFA have high factor loadings (from 0.5 and greater.)

*No constructs merged, which suggests that the constructs were perceived distinctly as intended.

*The Cronbach alphas for most of the constructs were above 0.7, except for two constructs, which suggests that the constructs have a high degree of internal consistency , even for exploratory studies.

*Investigation –first step in the development of a model for studying issues confronted by organizations when securing their critical information assets, and operationalizing this model in the form of developing constructs and a a survey instrument. Initial results seem promising.