

## Association for Information Systems AIS Electronic Library (AISeL)

---

AMCIS 2007 Proceedings

Americas Conference on Information Systems  
(AMCIS)

---

December 2007

# Information Security Economics: An Investigation of Demand-Driven Innovation and Market Value

Lara Khansa

*University of Wisconsin, Madison*

Follow this and additional works at: <http://aisel.aisnet.org/amcis2007>

---

### Recommended Citation

Khansa, Lara, "Information Security Economics: An Investigation of Demand-Driven Innovation and Market Value" (2007). *AMCIS 2007 Proceedings*. 395.

<http://aisel.aisnet.org/amcis2007/395>

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# INFORMATION SECURITY ECONOMICS: AN INVESTIGATION OF DEMAND-DRIVEN INNOVATION AND MARKET VALUE

Lara Khansa<sup>1</sup>, Doctoral Candidate in Information Systems  
Dissertation Advisor: **D. Liginlal**

Department of Operations and Information Management, School of Business  
University of Wisconsin, Madison

## Abstract

*The proposed research integrates theories of demand-driven innovation and market value creation to explain (i) the role of demand in driving innovation in information security and (ii) the role of innovation in projecting firm performance thus determining firm market value. Time series and event study analyses are applied to show that malicious attacks, primarily those that exploit software vulnerabilities, create more demand for security firms' products and services, in turn driving additional innovation and generating more demand. It is also shown that innovation by information security firms boosts investors' confidence. Additional findings, based on a trend analysis and pilot study, suggest that regulations and standards are a key driver of demand for information security products and services. We propose supplementing the latter study with interviews of decision makers at US firms to further understand the drivers of innovation in the information security area.*

**Keywords:** Information security, innovation, malicious attacks, stock market value, time series regression, event-study analysis, interviews.

## Motivation

Agile e-business and globalization have exposed the IT infrastructures of firms to new breeds of malicious attacks, launched with the goal of committing fraud and making illegal profits. This, in turn, has triggered complex and dynamic interactions among firms who invest in IT and information security products and firms who innovate to design those products. This dynamic environment and its impact on the market value of information security firms, as depicted in Figure 1, constitute the subject of the proposed research.

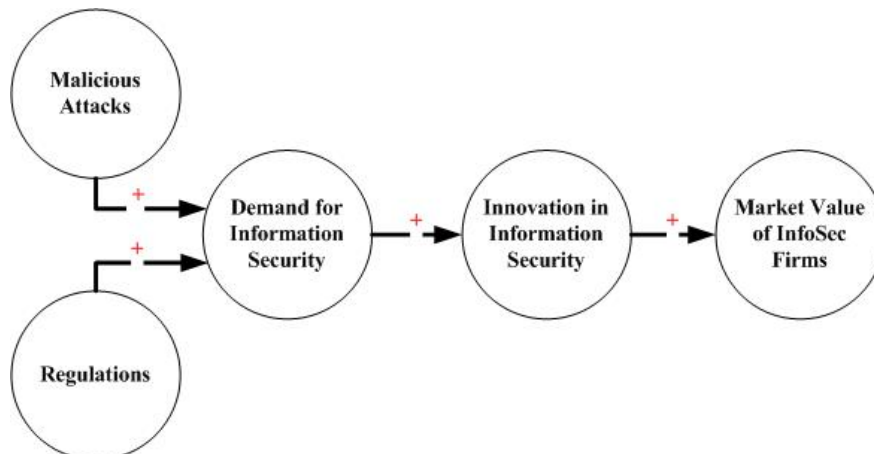


Figure 1. Demand-driven innovation and market value in a malicious environment

<sup>1</sup> Email: [lzkhansa@wisc.edu](mailto:lzkhansa@wisc.edu), Phone: 608-213-3436

## Literature Review Summary

This research builds upon contemporary literature which investigates the role of demand in steering innovation and that of innovation in projecting firm performance thus driving market value.

Several researchers have investigated the effect of demand in driving innovation. For example, Adner and Levinthal (2001) presented a demand-based view of technology evolution that is focused on the interaction between technology development and the demand environment, offering an alternative to supply-side explanations of the technology life cycle. Similarly, Casadesus-Masanell and Chemawat (2006) analyzed a dynamic mixed duopoly between Linux and Windows emphasizing the demand-side learning effects that generate dynamic scale economies. The role of regulations in driving innovation has also been well-researched. Wagner and Dittmar (2006), for example, emphasized that Sarbanes-Oxley (SOX) has made accounting procedures more efficient and has improved the quality of financial data, benefiting not only statutory compliance but also organizational and shareholder fundamentals.

The market value creation stream of research has received its fair share of scrutiny. In particular, Kim et al. (2006) discussed how innovation in information systems, specifically supply chain, can be viewed as firm resources that enhance channel capabilities and improve stock market performance. Hendricks and Singhal (2003), on the other hand, showed how product defects, particularly supply chain glitches, resulted in production and shipment delays and consequently destroyed the market value of the firm in question.

## Research Design

### Research Questions

This research is based on two central themes: (1) Studying how malicious attacks and regulations affect demand, in turn driving innovation and (2) How investors react to innovation by information security firms.

The first two research questions investigate the role of malicious attacks and regulations in bolstering demand.

1. *How significant is the relation between firms' investments in information security and the virulence of prior malicious attacks?*
2. *Has the announcement of information security regulations induced a significant increase in demand for information security products and services?*

The following formulation completes the investigation of the first theme by establishing the mutual link between demand and innovation.

3. *Does more demand for information security products and services induce more innovation on the part of information security firms? Does this additional innovation, in turn, entail more demand?*

The last two research questions address the second theme related to market value creation.

4. *Does the stock price of security firms increase with higher R&D spending, while controlling for prevailing market performance?*
5. *Does the public announcement of new virus strains result in increased investor confidence in the expected future performance of the stock price of information security firms?*

### Methodology

The research employs vector auto-regression methods and event study analyses to investigate the proposed hypotheses. The analyses are based on the collection and processing of revenues and R&D expenses of information security firms, historical market prices, and data about the virulence of malicious attacks. The variables used in the analyses are described next.

**Virulence:** Data pertaining to the damages caused by malicious attacks are not available directly from firms, as corporate decision makers are unwilling to fully disclose the dollar impact of malicious attacks on their IT infrastructures. Macro data about malicious attacks were gathered from three major anti-virus vendors, preprocessed into dollar damages, and cross validated against other publicly available sources. This produced sufficient credibility in the subjective assessments of the dataset.

**Demand:** The revenues of information security firms were used to quantify firms' investments in information security. The revenue index, as designed, is an accurate measure of information security investments because the revenues of information security firms are determined by the total amount of income from the sale of all their goods and services during a given

period. To construct this revenue index, we selected twenty-five vendors of information security products and services encompassing security-related technology sectors and representing a significant market share.

**Innovation:** R&D expenses of information security firms are used to quantify the extent of their innovation efforts.

All five time series were analyzed for autocorrelation, trend, and seasonality. Lag differencing was performed when necessary prior to conducting further analyses.

The above mentioned research methods are complemented by an exploratory study of a random sample of US firms and interviews with CSO of US firms to further explore the demand-side aspects of innovation.

## Analysis and Results

### Time Series Analysis

Hypotheses 1 and 2, which formulate research questions 1 and 4 respectively, are tested using time series regression analyses. Following are the hypotheses and their associated results.

#### Hypothesis 1

*Higher levels of past virulence entail higher levels of firms' information security investments*

$$\text{Revenue}(t) - \text{Revenue}(t-1) = a' + b'[\text{Virulenc}(t-i) - \text{Virulenc}(t-i-1)] + c'[\text{Revenue}(t-j) - \text{Revenue}(t-j-1)] + \varepsilon'_t$$

$$H_0 : \exists i: b' > 0 \text{ and } \exists j: c' > 0$$

Hypothesis 1 relates firms' investments in information security to the virulence caused by past malicious attacks. The conjecture is that high levels of malicious virulence entail higher firms' investments in information security because firms, at a macro level, seek additional immunity when past attacks have been particularly destructive.

*Result:* Firms significantly increase their investments in information security when faced with higher virulence of malicious attacks (Coefficient: 0.466; t-Stat: 1.892)

#### Hypothesis 2

*Higher levels of innovation in information security lead to an increase in the stock prices of information security firms*

$$\text{Price}(t) - \text{Price}(t-1) = a' + b' \text{Market\_Return} + c'[\text{Innovation}(t-j) - \text{Innovation}(t-j-1)] + \varepsilon'_t$$

$$H_0 : b' > 0 \text{ and } \exists j: c' > 0$$

Hypothesis 2 is consistent with our analysis of prior literature that has examined the impact of innovation on market valuation and has unanimously noted a positive relationship between R&D investment and market value.

*Result:* Demand-driven innovation creates market value (Coefficient: 1.545; t-Stat: 3.406).

#### Hypothesis 3

Hypothesis 3 states, as formulated in research question 3, that demand and innovation are mutually causal. Time series analysis helped validate this hypothesis and showed that the lag 0 cross-correlation between both time series is 0.516.

### Event-study Analysis

Hypothesis 4, which formulates the fifth research question about the effect of virus announcements on the market value of information security firms, was validated using event study analysis, which confirmed that the cumulative abnormal returns of information security firms are prevalently positive (76.67%) with a significantly positive weighted average (weighted average CAR=0.00642) at both the 95% and the 99% confidence levels.

## Additional Findings

Hypothesis 5, designed to validate the remaining research question about the role of regulations in driving innovation in information security, was tested using a pilot study and trend analysis with the following results.

### *Pilot Study*

To qualitatively study the impact of regulations on firms' demand for information security products, we conducted a pilot study by interviewing 69 decision makers of US firms (51% usable response rate). The majority of respondents (54%) indicated that top executive support for information security investments has been significantly increasing, driven by regulations and the compelling need to safeguard brand name and image and avoid litigations. Similarly, around 63% of respondents indicated that resource allocation for information security investment has significantly increased, while 29% recognized the increase has been moderate. The remaining 8% of respondents acknowledged management's resource allocation to information security has been static (6%) and even moderately decreasing (3%). Investment decisions in a majority of companies (more than 57%) were driven by technical requirements and integration issues clearly indicating that technological innovation is influenced by regulations.

### *Trend Analysis*

We mapped the timing of the various regulations identified to the demand curve to assess how demand has fared in relation to regulatory requirements. Demand for information security products has significantly increased ( $t$ -stat of 2.2 at a 95% confidence level) with the announcement of major regulations, especially over the past 36 months, when major regulations such as SOX came into effect.

## Further Work

This work has so far yielded two scholarly articles under review at reputed journals (*Communications of the ACM* and the *Journal of Management Information Systems*) and a conference paper at AMCIS (Khansa and Liginlal 2007), to be submitted to another leading journal after revision. The final phase of this research will involve interviews with CSOs of US firms and follow-up questionnaires. The interviews will be designed to further understand the dynamic interactions between demand for information security firms and regulations.

## References

- Adner, R., and Levinthal, D. "Demand Heterogeneity and Technology Evolution: Implications for Product and Process Innovation," *Management Science* (47:5), 2001, pp. 611-628.
- Casadesus-Masanell, R., and Ghemawat, P. "Dynamic Mixed Duopoly: A Model Motivated by Linux vs. Windows," *Management Science* (52:7), 2006, pp. 1072-1084.
- Hendricks, K.B., and Singhal, V.R. "The Effect of Supply Chain Glitches on Shareholder Wealth," *Journal of Operations Management* (21:5), 2003, pp.501-522.
- Khansa, L., and Liginlal, D. "The Influence of Regulations on Innovation in Information Security," *Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007)*, Keystone, CO, 2007, accepted.
- Kim, D., Cavusgil, S.T. and Calantone, R.J. "Information System Innovations and Supply Chain Management: Channel Relationships and Firm Performance," *Journal of the Academy of Marketing Science* (34:1), 2006, pp. 40-54.
- Wagner, S., and Dittmar, L. "The Unexpected Benefits of Sarbanes-Oxley," *Harvard Business Review* (84:4), 2006, pp. 133.