Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2005 Proceedings

Americas Conference on Information Systems (AMCIS)

2005

Information Security: Is Scilence Golden?

James B. Freedman
Boston University, jfreedma@bu.edu

Information Security: Is Silence Golden?

James B. Freedman
Boston University School of Management
jfreedma@bu.edu

ABSTRACT

Investments to protect against known vulnerabilities are necessary but not sufficient to assure a firm's information security. New threats are continuously being designed and deployed to exploit vulnerabilities that defending firms have not yet discovered. Extant literature has identified the advantages for firms to share information about vulnerabilities, attacks and damages from breaches. Yet firms are hesitant to share information. I seek to understand that paradox. First I explicate the relationship between firm IT strategy and risk exposure. Next I delineate between known and unknown threats to explain organizational learning required to manage exposure. Finally I propose a relationship between risk exposure and security information exchange.

Keywords

Information Security Investment, Organizational Learning

INTRODUCTION

Information security related crime is responsible for a significant amount of financial loss to companies conducting business through the Internet (Gordon, Loeb, Lucyshyn and Richardson 2004). Attacks on corporate information assets motivated by criminal, profit-oriented intent have been increasing in number and sophistication (Tabone 2005). However, the full degree of financial loss due to information security breaches is difficult to assess because the majority of firms are hesitant to report breaches for fear of market reprisal (Campbell, Gordon, Loeb and Zhou 2003).

Firms have taken these threats seriously and have invested both technology and human resources to protect their information assets (Conry-Murray 2003). But, the pace of innovation by criminals to exploit firm network vulnerabilities has made it difficult for any single firm to be able to protect their network alone. Information security is a complex technology-based ecosystem of attackers and defenders involved in a continuous learning process. Tracing the evolution of the SOBIG virus provides an example of this learning process. Headlines published by CNET on NEWS.com January 13, 2003 claimed,

"***Sobig virus sows few PC problems***". The article stated; "*The worm also has the ability to retrieve updates of itself from the Web. The latest update contains backdoor software that could allow an attacker to access the victim's PC.*"

The central message was that the Sobig virus was not anything to really worry about. However the virus was displaying the ability to update itself from the Web, an activity that was not understood. Six months later, the June 3, headline stated,

"***Sobig worm keeps on growing***" The article quoted Vincent Gullotto, vice president of the antivirus emergency response team at computer security company Network Associates as stating "*The third variant of the Sobig worm really adds nothing new*".

Again traditional sources did not see a problem. Within weeks, researchers at MessageLabs had discovered the true nature of the intent of the SOBIG virus. Their analysis was the basis of the June 25th headline;

"***Sobig spawns a recipe for secret spam***". The article went on to state, "*While there is no concrete proof that Sobig.E has been created and released by a spammer … many bulk e-mailers are already using computers infected with a previous variant of the computer virus to avoid leaving traces*".

Armed with this new understanding of the virus, by August 20, the headline now declared,

"***ISPs: Sobig's the biggest virus so far***". The article quotes Mark Sunner, chief technology officer at MessageLabs as remarking "*This is the fastest (virus) that we have seen, The Sobig virus writer's use of an inbuilt expiry date indicates that he*

is committed to inventing new and improved versions. Each variant released so far has exceeded the previous one in growth and impact during the critical initial window of vulnerability."

A firm's ability to defend their network against attack is greatly dependent upon their capability to sense and respond to different types of attacks, some that are similar and others that are different from past threats. The Sobig story supports the argument that new threats are often interpreted based upon past experience and knowledge sources. The SOBIG threat was not considered dangerous by the traditional knowledge sources (virus protection software vendors) for more than 6 months. Insight exposing the true threat of Sobig came from a new knowledge source. In dynamic environments, a firm's ability to quickly sense and respond to unfamiliar events depends not only upon internal knowledge and expertise but also upon a firm's ability to learn from others (Cohen and Levinthal 1990). Firms gain diverse information from sources with whom they have weak ties (Burt 1992). Firm absorptive capacity which results from investments made in organizational routines to search for and access knowledge spillover (Gatignon and Xuereb 1997). Extant economic information security investment models do not explicitly address the development of firm absorptive capacity (Gordon and Loeb 2002a; Gordon, Loeb and Lucyshyn 2003; Schechter 2004). This paper incorporates strategic, economic and organizational learning theories as a foundation for future empirical research to explore the relationship between firm secrecy and information security against external attack.

THEORY DEVELOPMENT

Firm strategy affects the role that information technology plays (Henderson and Venkatraman 1993). At one extreme, emerging technology drives the strategy of the firm (Huber 1990), at the other extreme, technology is merely a necessary tool to support operations (Carr 2003). A firm's technological orientation (technological opportunism) drives investment to build the capability of identifying, assimilating, transforming and exploiting emerging technology (Srinivasan, Lilien and Rangaswamy 2002). A firm's technological opportunism determines the degree that they choose to capitalize on emerging technologies such as the Internet. Leveraging Internet technology does not come without risks, including exposure to external attack. Past literature does not explicate the relationship between firm IT strategy and risk exposure.

Risk Exposure

Information security is a form of risk management undertaken to reduce negative outcome of security breaches. (Gordon et al. 2002a)'s economic model is characterized by three parameters of a firm's expected loss due to information security breaches: the probability of a threat occurring, the probability that a threat would be successful (likelihood of a breach), and the loss resulting from a successful security breach. The model fixes the probability of a threat since it makes the implicit assumption that all threats have an equal probability of occurring and the explicit determination that the firm cannot influence the probability of the occurrence of a threat. The model also fixes the value of the expected loss as a function of the probability of a breach. This logic makes the implicit assumption that firms are concerned with an average loss, instead of an extreme case. (Schechter 2004) suggests that the probability of an attack is a function of four factors: the number of potential attackers, potential profit, attackers' perceived risk, and system resistance to attack. Neither of these studies considers the influence of a firm's technological opportunism on perception of risk exposure. (Straub and Welke 1998) identify industry susceptibility to risk, past firm actions taken to secure information systems and personal awareness of security risk as drivers for a manager's perception of risk. However, the study does not explicitly identify whether a firm's strategy influenced by technological opportunism has influence on the perception of security risk. This provides the foundation for the first proposition:

P1: A firm's level of technological opportunism influences perception of risk exposure to security breaches

Organizational Learning

Firms are influenced by experience gained from internal as well as external sources as they develop their strategy for protecting their information systems. A firm must know something about information security in order to be in a position to learn from others (Dreyfus and Iyer 2005). Firms invest in relationships to gain access to more diverse sources of information (Burt 1992). (Cohen et al. 1990) investigated how firm investment in R&D serves not only to take advantage of internal creativity, but also serves to enhance the firm's capability for understanding external sources of innovation. To succeed in ecosystems driven by technology innovation, a firm, must develop absorptive capacity that enables quick assess and incorporation of emerging unproven technology capabilities (Govindarajan and Kopalle 2003). (Gordon et al. 2003)'s model identifies the economic value for sharing information between defending firms. However, the model has several flaws; first it does not address the need to build absorptive capacity. Second, it uses the average damage or loss that may result from a security breach, when a firm may be more concerned with protecting against the extreme. But most

importantly, it does not recognize what may influence the perceived value that firm *i* would extract from sharing information with firm *j*.

I propose that firms invest in information sharing dependant upon what they expect to gain from those investments. Seeking and sharing security information has considerable costs not only in terms of human and technical resources but also in terms of perceived risk of sharing information that can be used against the firm by attackers. Decisions to share information with another firm must balance investment with perceived benefits. Exhibit 1 graphically depicts scenarios of possible benefits of sharing information between two firms.

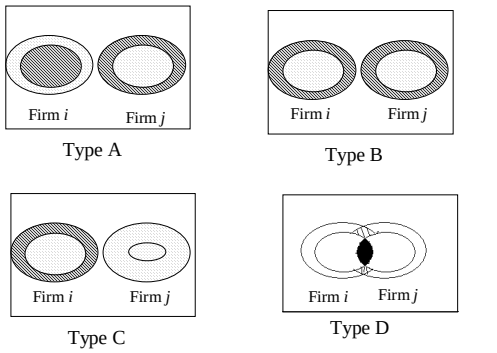

Exhibit 1 – Information Sharing Venn Diagrams

The inner circles represent the security threats for which there is a known solution, the outer circles represent security threats that are known but for which the solution is undiscovered and the blank space inside the box represents undiscovered threats. A perfect incentive exists to invest in a type A relationship because each firm possesses knowledge that is valuable to the other firm. Investment in type B relationship would provide no value to either party, since neither would gain additional knowledge. A relationship of type C would only benefit firm j. Finally in a type D relationship, each firm gains a marginal benefit. This leads to the second proposition:

P2: A firm will invest in information sharing if there is a perceived benefit.

Information Security Investment Economic Models

Firms recognize that failure to carefully weigh action to address information security is important, since the market responds unfavorably to firms that spend either too much or too little to secure their information assets (Campbell et al. 2003). The prevailing wisdom is that investments in information security have been shown to have a diminishing return, (Gordon et al. 2002a). However, the problem is complex: "*Normal tools utilized to evaluate investments such as ROI or IRR may not be appropriate*" (Gordon and Loeb 2002b).

Investment to protect against known threats is necessary but not sufficient to guarantee security. The security environment is characterized by uncertainty. Firm investment can be categorized along a continuum of firm activism. At one end firms seek to transfer the risk through insurance or outsourcing contracts (Brealey, Myers and Allen 2005). At eh other end of the spectrum firms invest proactively in dynamic capabilities as a strategy to provide flexibility to address environmental uncertainty. (Kogut and Kulatilaka 2001) identify real options or lobbying as forms of proactive investments. I define the degree that a firm invests proactively in a capability to address security uncertainty as security activism. This logic leads to the last proposition:

P3: Firm perception of risk exposure will affect the degree of firm security activism.

FUTURE RESEARCH

(Straub et al. 1998) found that firms were hampered by the lack of information that was available to them to address information security, yet they stopped short of investigating the propositions identified in this paper. I will plan to follow (Straub et al. 1998) by conducting action research of several firms extending their instruments to incorporate variables that address the propositions discussed in this paper. I will utilize this qualitative research to develop a survey instrument to gather data from an information security user group of over 600 individuals representing over 400 firms. Survey data will be correlated with archival longitudinal data indicating the extent that firm revenue is directly derived from customers utilizing

the Internet. I will utilize a process theory approach to develop rich interpretations of longitudinal data (Miles and Huberman 1994). Coding schemes will follow those developed by (Faraj, Kwon and Watts 2004).

CONCLUSION

I extend current information security literature in several ways. First I explicate the relationship between firm IT strategy and risk exposure. Next I delineate between known and unknown threats to explain organizational learning required to manage exposure. Finally I propose drivers of IT security information exchange.

REFERENCES

1. Brealey, R.A., Myers, S.C., and Allen, F. *Principles of Corporate Finance*, (Eighth Edition ed.) McGraw-Hill Irwin, Boston, MA, 2005.
2. Burt, R.S. *Structural Holes: The Social Structure of Competition* Harvard Press, Cambridge, MA, 1992.
3. Campbell, K., Gordon, L.A., Loeb, M.P., and Zhou, L. "The Economic Cost of Publicly Announced Information Security Breaches: Emperical Evidence from the Stock Market," *Journal of Computer Security* (11) 2003, pp 431-448.
4. Carr, N.G. "IT Doesn't Matter," *Harvard Business Review* (81:5) 2003, pp 41-51.
5. Cohen, W.M., and Levinthal, D.A. "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative Science Quarterly* (35) 1990, pp 128-152.
6. Conry-Murray, A. "Justifying Security Spending.," *Network Magazine* (18:3), 2003/03// 2003, p 44.
7. Dreyfus, D., and Iyer, B. "Knowledge Sharing and Value Flow in the Software Industry: Searching the Patent Citation Network," Proceedings of the 38th Hawaii International Conference on System Sciences, Hawaii, 2005.
8. Faraj, S., Kwon, D., and Watts, S. "Contested Artifact: Technology Sensemaking, Actor Networks, and the Shaping of the Web Browser," *Information Technology & People* (17:2) 2004, pp 186-209.
9. Gatignon, H., and Xuereb, J.-M. "Strategic orientation of the firm and new product performance.," *Journal of Marketing Research* (34:1), 1997/02// 1997, p 77.
10. Gordon, L.A., and Loeb, M.P. "The Economics of Information Security Investment," *ACM Transactions in Information & Systems Security* (5:4) 2002a, pp 438-457.
11. Gordon, L.A., and Loeb, M.P. "Return on Information Security Investments: Myth vs. Reality," *Strategic Finance*:November, 2002) 2002b, pp 26-31.
12. Gordon, L.A., Loeb, M.P., and Lucyshyn, W. "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy* (22:6), 2003/0 2003, pp 461-485.
13. Gordon, L.A., Loeb, M.P., Lucyshyn, W., and Richardson, R. "2004 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, San Francisco, CA, p. 18.
14. Govindarajan, V., and Kopalle, P.K. "How Legacy Firms can Introduce Radical and Disruptive Innovations: Theoretical and Empirical Analyses," in: *Amos Tuck School of Business Administration*, Hanover, NH, 2003, p. 31.
15. Henderson, J.C., and Venkatraman, N. "Strategic Alignment - Leveraging Information Technology for Transforming Organizations," *IBM Systems Journal* (32:1) 1993, pp 4-16.
16. Huber, G.P. "A Theory of the Effects of Advanced Information Technologies on Organizational Design, Intelligence, and Decision Making," *Academy of Management Review* (15:1) 1990, pp 47-71.
17. Kogut, B., and Kulatilaka, N. "Capabilities as Real Options," *Organization Science*) 2001, p 44.
18. Miles, M.B., and Huberman, A.M. *Qualitative Data Analysis: An Expanded Sourcebook* Sage, Thousand Oaks, CA, 1994.
19. Schechter, S.E. "Toward Econometric Models of the Security Risk from Remote Attacks," 2004.
20. Srinivasan, R., Lilien, G.L., and Rangaswamy, A. "Technological Opportunism and Radical Technology Adoption: An Application to E-Business.," *Journal of Marketing* (66:3), 2002/07// 2002, p 47.
21. Straub, D.W., and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly* (22:4) 1998, pp 441-469.
22. Tabone, J. "Look inside for IT threats.," *CA Magazine* (138:1), 2005/01//Jan/Feb2005 2005, p 9.