2009

Will the Information Security Industry Die? Applying Social Network Analysis to Sturdy Industry Convergence

Lara Khansa
Virginia Tech, larak@vt.edu

Divakaran Liginlal
University of South Alabama, dliginlal@gmail.com

Will the Information Security Industry Die? Applying Social Network Analysis to Study Industry Convergence

Lara Khansa
Virginia Tech
larak@vt.edu

Divakaran Liginlal
University of South Alabama
dliginlal@gmail.com

ABSTRACT

In this paper, we first analyze the trends in mergers and acquisitions (M&As) activities among information security firms and other information technology (IT) firms in the US over the period 1996 to 2008. We then use social network analysis to investigate the characteristics and underlying dynamics of these M&As activities. Our results reveal an increase in cohesiveness of 200% in the network linking the information security firms and the IT firms considered in our analysis. This, in turn, implies a move towards industry convergence. In particular, we show that acquisitions of identity and access management (IAM) firms have become more central to M&As by IT firms in the US since 2004, reflecting an increasing trend among IT firms to integrate IAM technologies within their products.

Keywords

Information security, identity and access management, industry convergence, social network analysis.

INTRODUCTION

With the information technology (IT) industry shifting focus towards IT services, such as IT support and consultancy, customers have increased their expectations for more secure IT products. This demand for more secure IT has not only necessitated a marriage among IT and information security at the product level (technological integration), but it has also had repercussions at the industry level (industry convergence). Technological integration refers to "the ability of different network platforms to carry essentially similar kinds of services or the coming together of consumer devices such as the telephone, television and personal computer" (European Commission, 1997, p. 1). Porter (1985) argued that technological innovations, and the resulting bundling of innovative products, can change the boundaries of traditional industries and lead to industry convergence. The management literature (Greenstein and Khanna, 1997) defines industry convergence as the process by which two or more related industries (whether substitutive or complementary) converge over time. We found no prior research that investigates the convergence among information security firms and other IT firms, which aims at satisfying customer demand for IT products that are inherently secure. In this paper, we, attempt to fill this gap in the literature using social network analysis, which employs a set of methods and measures for the analysis of social structures.

SNA has been widely used to study social psychology and diffusion among various entities. In SNA, an actor can influence the behavior or attitudes of other actors through social relations (Pattison, 1982). The SNA methodology has also been extensively used in business, especially in marketing, where researchers have used SNA to study marketing channels and buying centers as well as consumer behavior. What distinguishes the SNA research method from other research approaches is its analysis of social actors in relation to one another, rather than as standalone entities with individual behaviors, attitudes, and beliefs (Wellman, 1988). For a complete review of the literature in this area, we refer the reader to Arabie and Wind (1994). We use two SNA concepts to study the nature of the industry convergence among security firms and other IT firms. The first concept is that of "network cohesiveness", which quantifies the strength of the ties among actors in a given social network. The second is the concept of "actor centrality", which, in SNA terms, signifies that actors are active within their network, or equivalently that actors have the highest number of ties to other actors in the network (Wasserman and Faust, 1994).

To avoid any potential ambiguity, in the remainder of this paper, we define "IT firms" as companies producing non-information security-related IT products. Further, the term "IT industry", which constitutes the basis for the Standard Industrial Classification (SIC) system, the underlying classification scheme of industry and market data in the United States (Munir and Philips, 2002), refers to the entirety of IT firms, regardless of their product offerings within IT. The notion of "sector" refers to a group of firms offering products that are related. For example, the information security sector encompasses IT firms that offer primarily information security products. Similarly, the term "segment" is used to denote groups of firms whose products and services are close substitutes for each other (Porter, 1985) and who serve the same group of customers. For example, the antivirus segment (AV) (also called 'content security') encompasses firms such as Symantec and McAfee.

We have organized the rest of the paper as follows. Section 2 presents the theory and hypotheses. Section 3 then introduces the research design, including measures and data collection. Section 4 subsequently conveys the results and their discussion. Finally, section 5 summarizes the contributions and limitations of this study.

THEORY DEVELOPMENT AND HYPOTHESES

An extensive research stream has looked at the economic benefits of acquiring firms with synergistic capabilities. For example, Cottrell and Koput (1998) found a positive correlation in the microcomputer industry between firmware variety and the price of complementary hardware platforms. Gallaugher and Wang (2002) studied the effect of cross-market complementarities on software pricing. Their analysis focused on the web server market segment and found a positive relationship between market share for browsers and the price of web servers. Brynjolfsson and Kemerer (1996) studied the computer spreadsheet industry and found that by adhering to the dominant standard, firms acquire a larger customer base and are able to impose higher prices in complementary market segments. Their study emphasized the value of network externalities and of boosting demand. Subsequently, researchers such as Economides and Salop (1992) built upon this perspective and analyzed the competition and integration among complementary products and how these products can be combined to create composite goods or systems. Yoffie (1997) observed that industry convergence and divergence have been especially predominant among digital technologies. Stieglitz (2003) analyzed the evolution of the personal digital assistant (PDA) industry and addressed substitution and complementary convergence. By differentiating between the acquisition of complementary assets or capabilities and the acquisition of substitutes, and emphasizing the "asset" side of convergence, the author attempted to define and conceptualize industry convergence. Bayus and Agarwal (2007) studied various product technology strategies that increase the survival of entrants who are targeting technologically dynamic industries, in particular the U.S. personal computer industry. They emphasized the importance, for entrants, of choosing a product technology that has the highest prospects of becoming a standard. Gao and Iyer (2006) also studied a set of alliances between companies whose products are related and found that investors are more positive when both participants belong to the same layer of the IT stack.

The information security market sector has traditionally subsisted in the shadows of the IT industry with the role of making vulnerable IT products and information systems more secure. Recently, though, firms using IT in their everyday activities have faced increasing regulatory pressures urging them to safeguard sensitive customer information amidst increasing security and privacy breaches. IT customers, especially enterprises, have voiced their preferences towards integrating information security within IT for greater ease-of-management and to comply with information security regulations (Khansa and Liginlal, 2008). Accountability is another reason why they prefer to deal with a one-stop IT shop, in case their technologies fail to keep information secure and in compliance with regulations. This demand-driven shift towards integrating security within IT has been reflected in a multitude of mergers and acquisitions (M&As) among IT and security firms. Schneier (2007) predicted the "death" of the information security industry as a separate entity. Like Schneier, we believe that IT security firms are "artifacts" stemming from the complexities and imperfections of the IT industry, and hypothesize the following:

HYPOTHESIS 1. There has been increased industry convergence among information security firms and other IT firms in the US.

Identity and access management (IAM) refers to the technologies, processes, policies, and supporting infrastructures necessary for the deployment, control, and maintenance of digital identities and their access to resources. Simply put, the objective of IAM technologies is to control access to resources based on the identities they manage. By offering solutions against data leakage and identify theft and supporting authentication and compliance-driven applications, IAM adds value at all business levels. First, at the enterprise level, IAM provides managers with the ability to streamline access to resources, thus facilitating better command and control over the corporate network. IAM technologies allow employees to have a single means of accessing all applications, using hardware tokens or a single sign-on. This results in reduced administrative costs and eliminates the need to remember multiple passwords, thus increasing productivity. The benefits of IAM extend beyond the enterprise; for example, the efficient coordination and integration of business processes with those of strategic partners permit easy and secure access to services that are housed in multiple security domains. Known as federation, this integration allows information about users, their security, and entitlement to be shared in a defined and controlled way between partners in a trusted business relationship. The growing importance of IAM has been reflected in the multitude of IAM acquisitions by IT firms. IT companies such as Microsoft, IBM, EMC, Cisco, Computer Associates, and even Google, have acquired at least one IAM firm over the past three years. For example, Cisco acquired M.I. Secure Corporation for $13 million only eight months after the start-up was initiated. According to a February 2008 Forrester Research report, the IAM market segment is expected to grow to more than $12.3 billion in 2014, from nearly $2.6 billion in 2006[1]. Given the considerable value of IAM technologies, we postulate the following:

HYPOTHESIS 2. Firms offering IAM technologies have been central to IT firms' M&A activity involving information security firms.

RESEARCH DESIGN

Not only does SNA offer a tool to visualize the relationships among entities, but it also provides an effective way of measuring the strength and other characteristics of these relationships. For example, it allows the ranking of entities according to their popularity in terms of incoming or outgoing links, in turn suggesting a more prestigious standing of some actors compared to others'. SNA also enables a researcher to perform cluster analysis and identify sub-networks within the larger scheme of things. For a thorough analysis and literature review of how SNA methods can be applied, we refer the reader to Wasserman and Faust (1994).

Network Cohesiveness

To quantify the extent of industry convergence among the information security market sector and the IT industry, we measure the cohesiveness of the network representing the M&As among them. Wasserman and Faust (1994) define cohesive subgroups as "subsets of actors among whom there are relatively strong, direct, intense, frequent, or positive ties." A frequent measure of cohesiveness is density, defined in (Scott, 2000) as the ratio of the actual number of lines in the network to the number of possible lines that would be present if all the points were connected to one another (Equation 1).

$$D \equiv \frac{L}{n(n-1)/2} \tag{1}$$

where L is the actual number of lines in the network and n is the total number of nodes.

Actor Degree Centrality

We quantify how important each information security market segment is relative to other information security market segments, using the measure of actor degree centrality as defined in (Burt, 1982). The larger an actor's degree, the higher his/her ability to directly influence other actors in the network. Burt (1982) defines the degree centrality of an actor or its "ego density", as its prominence in the network based on the ties that connect him/her to the other members of the network. As such, actor degree centrality can be computed as the ratio of the normalized actor degree by the number of vertices in the network (Equation 2).

$$C_d(n_i) \equiv \frac{d(n_i)}{n-1} \tag{2}$$

where $n-1$ is the number of remaining nodes in the network. $d(n_i)$, the degree of node n_i, is defined in (Wasserman and Faust, 1994) as the size of its "neighborhood," i.e., the number of nodes that are adjacent to it (Equation 3).

$$d(n_i) \equiv \sum_j X_{ij}$$

$$X_{ij} = \begin{cases} 1, \; if \; node \; n_j \; is\, adjacent\, to\, node \; n_i \\ 0, \; otherwise \end{cases} \tag{3}$$

where j indexes a neighboring node. Other definitions of centrality and prestige have been used in the literature, such as "betweenness" and "closeness." However, degree centrality applies more to the problem at hand because of the nature of M&A activity. Using degree centrality allows us to gauge the relative importance of the various information security

[1] http://www.freshnews.com/news/fresh-money/article_42847.html

segments throughout the time period under consideration. By comparing the degree centrality of the various sectors throughout the years, we can trace the evolution of the information security sector. The value of the degree centrality measure lies in its ability to rank the success of the various IT sectors in acquiring central information security industry segments.

Data Collection

Data related to M&As were obtained from the Securities Data Company (SDC) Thomson database, a comprehensive M&A database. We selected all M&As from 1996 to 2008 in which the acquiring firm is a public IT firm. We chose the period from 1996 to 2008 for its diversity. This period is diverse in the sense that it includes the pre-bubble years, the years of the Internet bubble, the quasi recession of 2001, the subsequent short economic recovery, as well as the credit crisis of the late 2007 and 2008. The inclusion of all these economic settings adds to the generalizability of our results. To ensure that an important merger or acquisition is not omitted, we initially collected data, in which either the target or the acquirer is an IT firm. After analyzing the raw data, which consisted of more than 54,000 M&As, we determined that many acquisitions were initiated by non-IT acquirers, including oil and petroleum firms. Further, the data included stock repurchases in which the target and acquirer are essentially the same company. Only completed transactions were included in the sample.

We then studied the product offerings of each firm in the sample and only kept M&As that related to information security targets. We allowed our sample to include both public and nonpublic information security targets to ensure thoroughness. Since our goal is to study vertical convergence, rather than horizontal convergence within the information security sector, we further specified that the acquiring IT firm cannot be security-related. Horizontal convergence is governed by different dynamics that we intend to investigate in future research.

We found a total of 7,243 M&As between noninformation security acquirers and information security targets, of which only 1,984 are mergers; the major remainder consists of acquisitions. Figure 1 suggests that after the market bubble of the years 2000, the M&A activity of IT firms in the US dropped dramatically in 2001. The number of M&As increased again in 2004 and 2005 but has dropped down sharply after 2007 because of the credit crisis and the economic recession, which started near the end of 2007. It is important to note, however, that some M&As that were announced in 2007 and 2008 might not have completed by the end of 2008, adding to the scarcity of the completed M&As in 2008, as depicted in Figure 1.

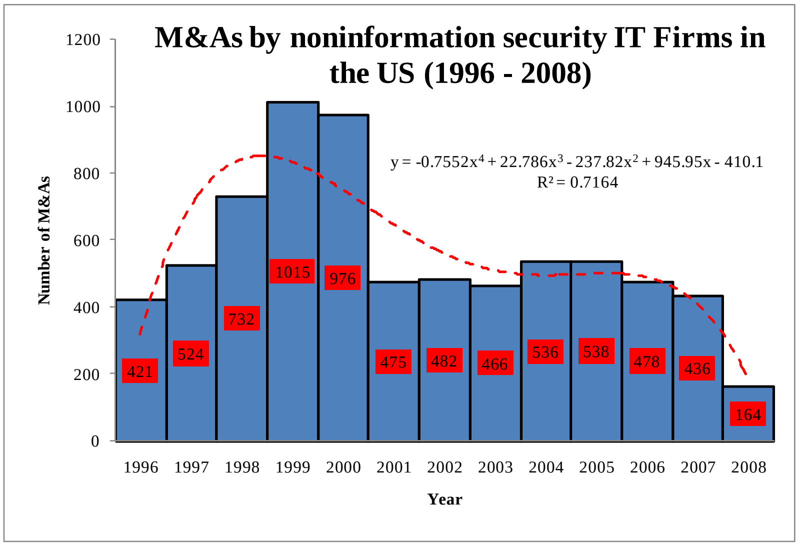


Figure 1. M&As by Noninformation Security IT Firms in the US (1996- 2008)

Our initial observation of the M&A activity of IT firms confirms the result of prior researchers, such as Gao and Iyer (2006). In their paper, Gao and Iyer (2006) only considered M&As up to 2004. They noted that "from 2001 to 2004 the number of M&As is substantially smaller, as a consequence of the economic slowdown." We agree with the authors that 2001 marked a year of economic slowdown. However, the authors claimed that only 4% of the total acquisitions from 1999 to 2004 happened in 2004, our results reveal that 2004 marked a spike in M&A activity after the quasi-recession of 2001 with 13.6%

of the acquisitions from 1999 to 2004 occurring in 2004. This difference in findings can be attributed to Gao and Iyer's incomplete data because many acquisitions announced in 2004 could have been pending at the time their analysis was done. Our results also suggest that considerably more nonpublic targets than public ones were acquired (Figure 2). Further, the results in Figure 3 suggest that ignoring international acquisitions, as Gao and Iyer (2006) did, can considerably skew the results given that the high percentage of M&As from 1996 to 2008 (over 21%) involved foreign targets.

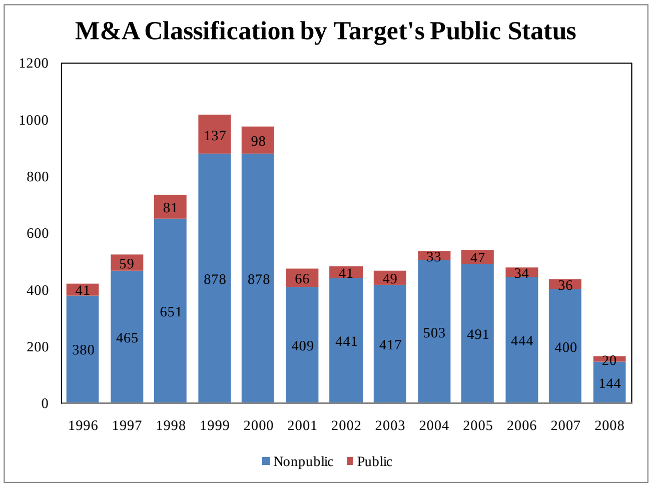


Figure 2. Categorization Based on the Target's Public Status

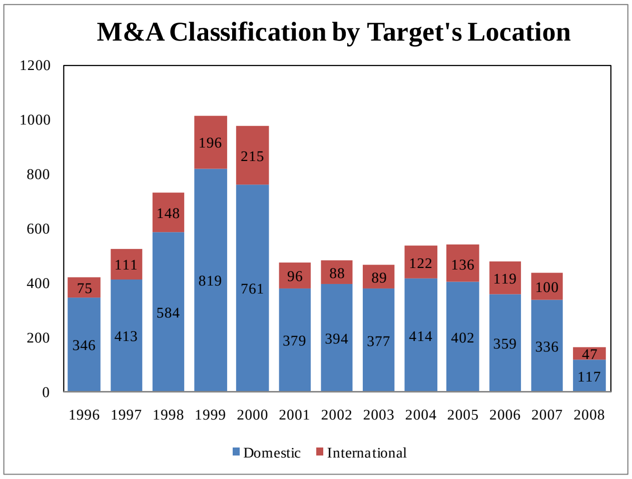


Figure 3. Categorization based on the Target's Location

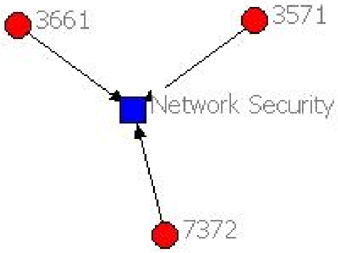
RESULTS AND DISCUSSION

In social network analysis, entities such as people, groups, or firms are represented as nodes, and the relationships among these entities are mapped as links between the nodes. In the context of this paper, the nodes in a network are the various IT sectors, represented by their corresponding SIC codes, and information security segments (antivirus security, network security, IAM, and physical security). The raw data collected from the SDC Thomson database do not distinguish software firms whose product offerings are intended for information security from other software firms. This problem arises because the data in the SDC Thomson database is based on the SIC code classification system in which a software firm, for example, belongs to SIC code 7372, regardless of the nature of its software products. To distinguish information security firms from other IT firms, we filtered the database of M&As by searching for information security keywords in the "short business description" field of the raw data. We used the built-in filtering capability of Excel 2007 to complete this filtering task. Our basis for this data filtering consists of two sources, namely the information security ontology from the national institute of standards and technology (NIST), a division of the U.S. Department of Commerce, and the IDC taxonomy of IT security (Thompson Financial Market Research, 2008). For example, to identify IAM firms, we filtered the data by using keywords that included identity management; access/account management; role management; authentication and authorization; antifraud solutions; access control/management; public key infrastructure; provisioning; Single Sign On (alternatively SSO); knowledge-based authentication (alternatively KBA); smart cards and biometrics; audit; public key infrastructure (PKI); and directory services. Network security firms were identified with keywords such as VPN, SSL technologies; network intrusion detection/prevention technologies; vulnerability assessment and real-time outbreak prevention capabilities; network security software and security monitoring software, including scanning and defensive technologies against suspicious outside traffic including malware, spyware, and DDS attacks; risk assessment technology for enterprise networks; e-mail and Web security; network encryption; firewall; standards-based network access security solutions; Internet security products; network-centric video surveillance software and hardware, etc…. Content security firms are those firms that offer antivirus products, antispyware, antimalware, and content filtering, etc…Finally, physical security firms were identified by keywords such as replication and continuous data protection; recovery and data protection; encryption; content loss prevention; data availability; etc…

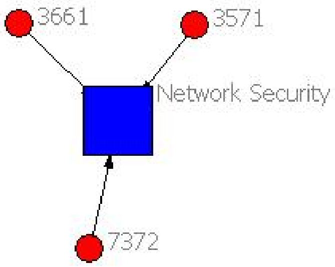
Figure 4 visualizes the evolution of the IT/information security relationships from 1998 to 2007. By studying the evolution of the resulting network, we are also able to study the progression of industry convergence between IT and information security.

The networks in the figure were drawn using the NetDraw network visualization tool (Borgatti, Everett and Freeman, 2002). The circled nodes in Figure 4 denote the acquiring IT sectors, represented by their SIC codes, and the square nodes represent the various information security segments. If a node has an incoming link, this indicates that a firm in the particular information security industry segment has been acquired by an IT firm having the SIC code of the node of origin. If a node has many incoming links, this indicates that the corresponding information security segment is highly desirable and has been the target of many acquisitions. The left side of the figure only shows what IT sector acquired what information security segment and lacks any consideration for either the number of acquisitions or the strength of the relationships. The other side of the figure provides additional information on the number of acquisitions. As such, if an information security segment is the target of many acquisitions, it is represented by a larger square. Similarly, if an IT industry, with a given SIC code, has undergone many acquisitions, its corresponding node is represented with a larger circle.

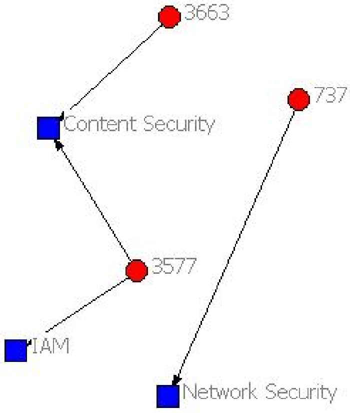
Notes and SIC code explanations for Figure 4: (1) IT firms offering electronic computers, computer storage devices, computer terminals, and computer peripheral equipment belong to the 3500's family and have the SIC codes 3571, 3572, 3575, and 3577 respectively. (2) Communication IT firms and electronic firms belong to the 3600's family, i.e., communications equipment firms (3663, 3669), semiconductors and related devices firms (3672, 3674), and electronics firms (3675, 3676, 3677, 3678, and 3679). (3) Communications services companies have the SIC codes 4813 and 4899. (4) Firms offering computer programming services belong to the 7371 family, while firms offering prepackaged software belong to the 7372 family, which includes firms such as Microsoft. Firms offering informing retrieval services, such as Google have the SIC code 7375. (5) Computer services firms, including computer rental and leasing, computer maintenance and repair, computer facilities management services, etc… are covered by the SIC codes 7376, 7377, 7378, and 7379. (6) Data processing and storage companies, such as EMC, belong to the 7374 family.



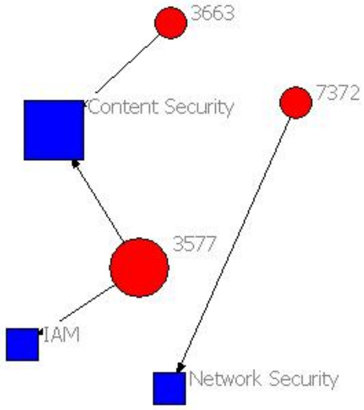
(a) Information Security Acquisitions in 1996



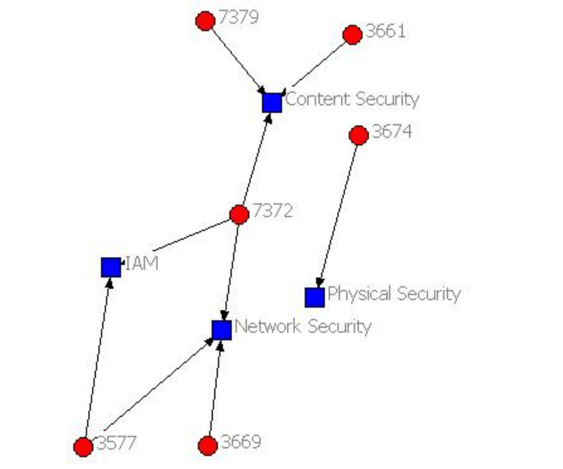
(a) Actor Centrality in 1996



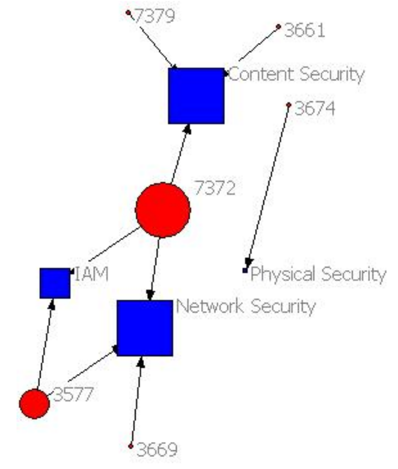
(b) Information Security Acquisitions in 1997



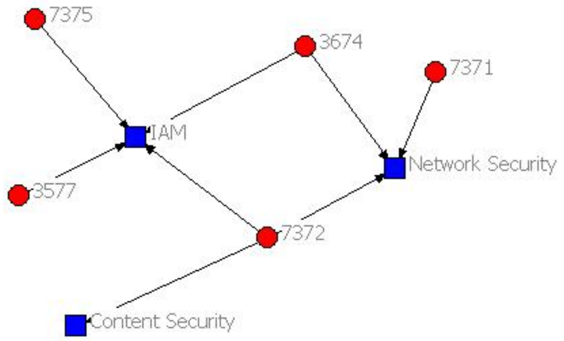
(b) Actor Centrality in 1997



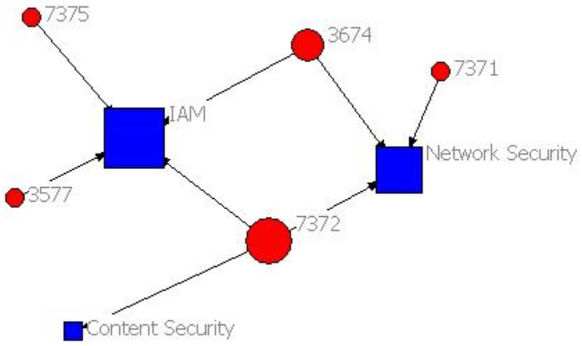
(c) Information Security Acquisitions in 1998



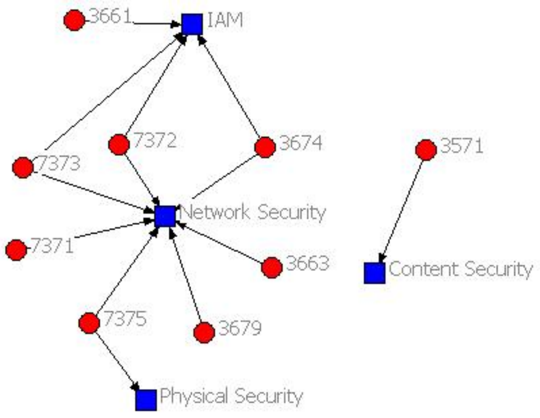
(c) Actor Centrality in 1998



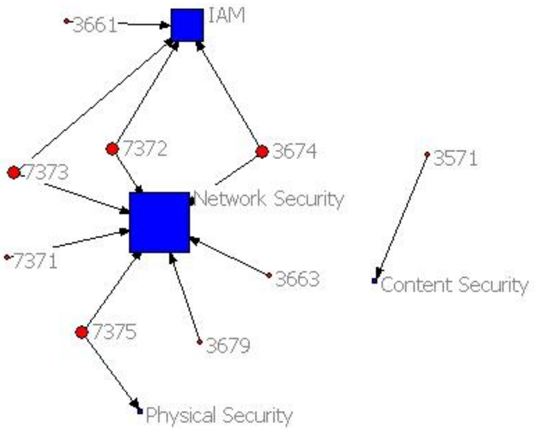
(d) Information Security Acquisitions in 1999



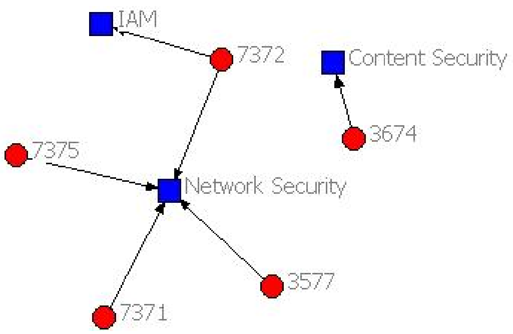
(d) Actor Centrality in 1999



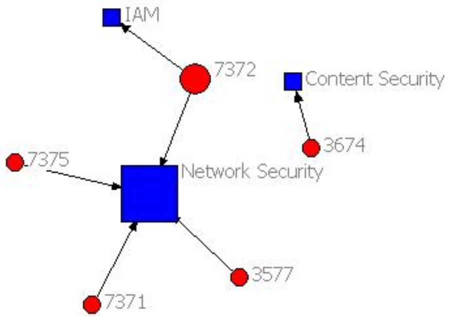
(e) Information Security Acquisitions in 2000



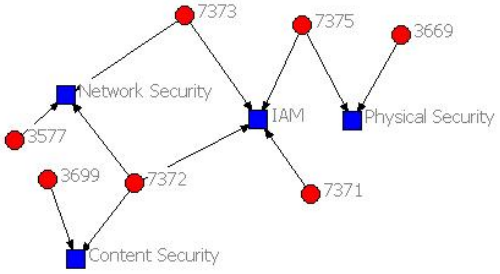
(e) Actor Centrality in 2000



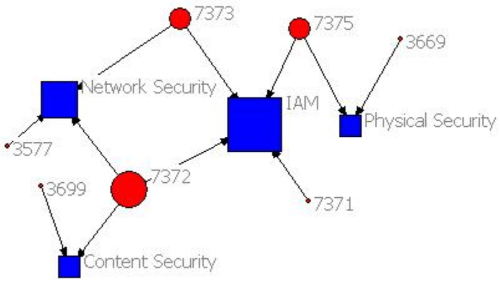
(f) Information Security Acquisitions in 2001



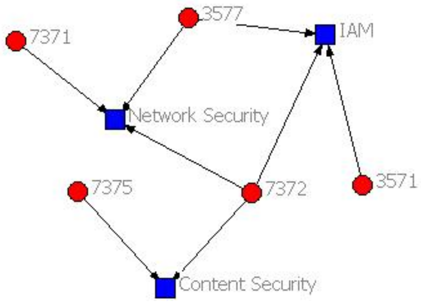
(f) Actor Centrality in 2001



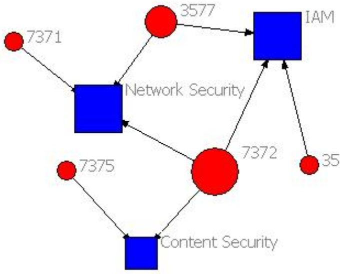
(g) Information Security Acquisitions in 2002



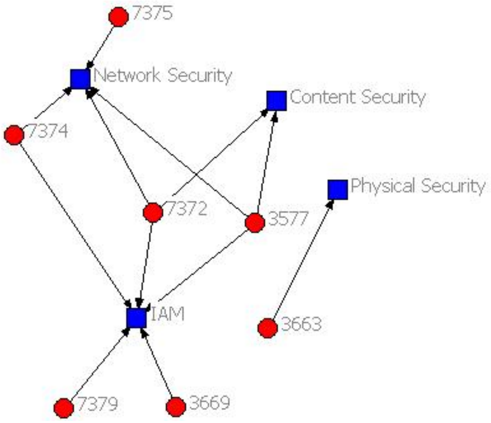
(g) Actor Centrality in 2002



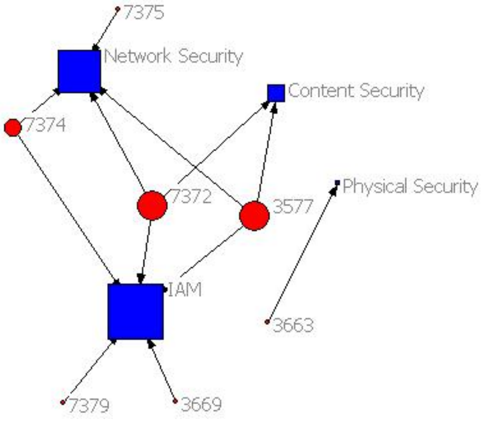
(h) Information Security Acquisitions in 2003



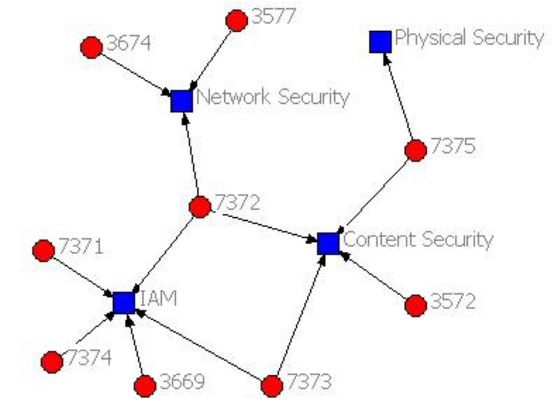
(h) Actor Centrality in 2003



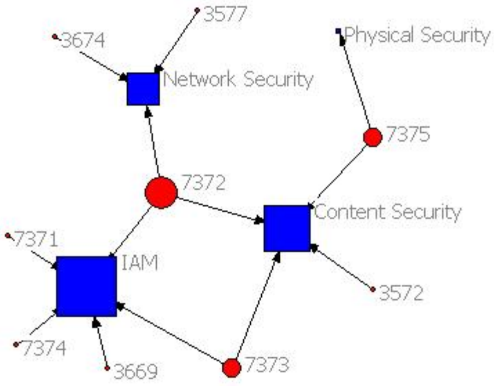
(i) Information Security Acquisitions in 2004



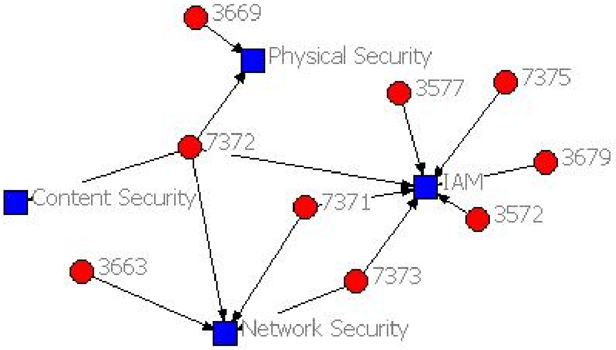
(i) Actor Centrality in 2004



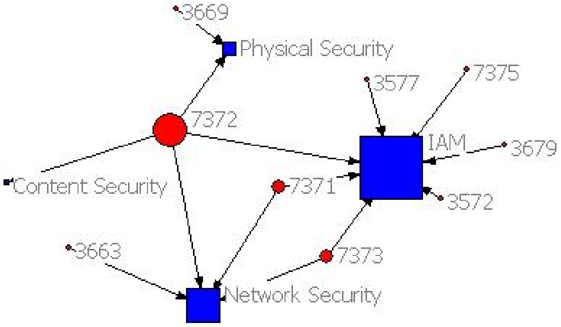
(j) Information Security Acquisitions in 2005



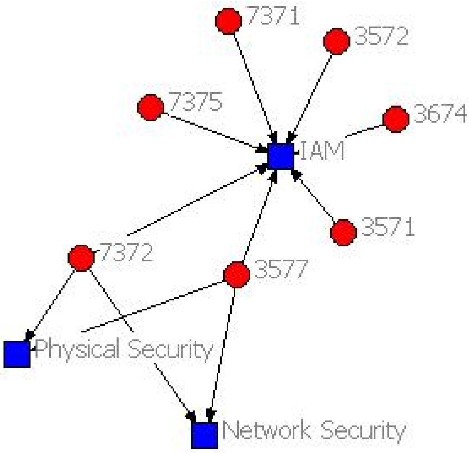
(j) Actor Centrality in 2005



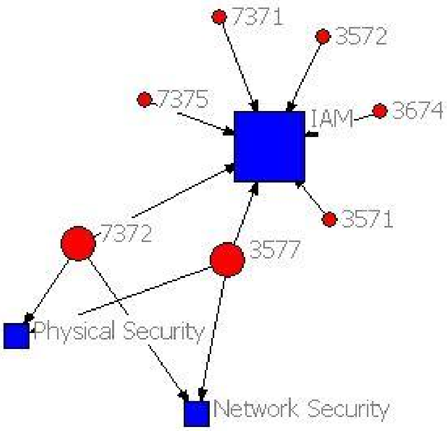
(k) Information Security Acquisitions in 2006



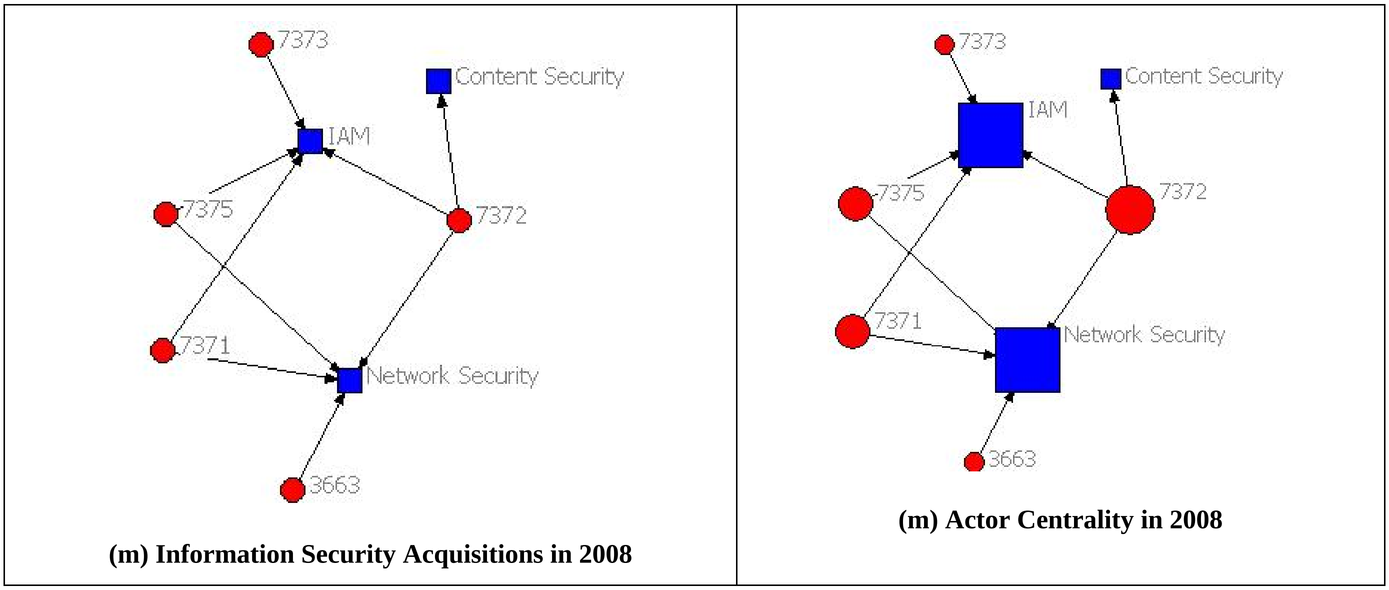
(k) Actor Centrality in 2006



(l) Information Security Acquisitions in 2007



(l) Actor Centrality in 2007



(m) Information Security Acquisitions in 2008

(m) Actor Centrality in 2008

Figure 4. Convergence among IT and Information Security Firms

Analyzing the main years of the Internet bubble from 1998 to 2000 revealed that various information security segments occupied fairly independent clusters. Firms producing prepackaged software were targeting AV firms, while business services acquired IAM firms, and communication firms were interested in network security firms. There was no apparent overlap among the various information security segments. The "prestigious" information security sectors in 1998 appeared to be network security and AV, which is understandable because this period coincides with the onset of the Internet bubble. In fact, most security products and technologies at that time consisted of products such as firewalls, antivirus products, and intrusion detection/prevention technologies, which are instrumental in defending the network from external threats. IAM capabilities were mostly needed at that time in the form of VPN for secure network access. Although 2000 saw a considerable rise in security acquisitions, the quasi-recession after the Internet bubble lasted through 2003 and was reflected negatively on the M&A activity of IT firms. After September 11, there appeared to be a noticeable increase in acquisitions of physical security firms by information retrieval and communications IT firms. Starting in 2004, acquisitions of information security firms by IT firms became more concentrated and increased in intensity. Firms offering prepackaged software (SIC code 7372), which encompasses Microsoft and IBM, and networking and communication firms, such as Cisco, Juniper, and 3Com, became the main acquirers of information security firms. The results in Table 1 further quantify the extent of the industry convergence among information security firms and IT firms in the US. In particular, the results in the second column of the table show that network cohesiveness increased by around 113% from 1996 to 2004, and by around 200% from 1996 to 2008, further validating Hypothesis 1.

Starting in 2004, IT firms also started collaborating with the goal of integrating network security and identity and access management technologies at the system, service, and enterprise levels, and developing security standards. During this period, Microsoft's trustworthy computing initiative, made public in 2002, led the operating systems giant to undertake multiple AV (antivirus, antispyware, firewall protection) and IAM (certificate and relationship management software) acquisitions. Similarly, Cisco's threat defensive initiative led the company to make several acquisitions in network security, AV, and IAM. The centrality results in Table 1 clearly confirm the dominance of the IAM market segment (in degree centrality terms), especially starting in 2004, which validates Hypothesis 2.

CONCLUSION

Khansa and Liginlal (2007, 2008) have shown that information security regulations have resulted in an increase in demand for IAM and have, in turn, boosted innovation by IAM firms and positively impacted their market value. The results of this paper demonstrate that the boundaries separating the information security sector and the rest of the IT industry have become blurred, suggesting that information security is becoming an integral part of IT products and services. In particular, the IAM market segment has become central to the M&As of IT firms in the US since 2004.

These results, interpreted in the context of results from prior literature, imply that IT firms have responded to governmental regulations and the resulting need for inherently secure IT products by acquiring information security firms, especially IAM firms. While substitutive technologies and their market segments are forced to diversify or die, niche IAM players seem to be thriving despite fierce competition from IT firms. Many alliances are currently in the works among purely IAM firms and IT firms. As of now, both IAM and IT seem to be coexisting in a symbiotic ecosystem in which innovative organizations with complementary capabilities compete and cooperate.

Our future research plans consist of investigating the implications of the shift towards integrated information security. The highly publicized acquisitions of information security firms (including IAM) reflect the fact that IT firms are concerned about security mainly because there is an urgent need for it. This open atmosphere has made it challenging for IT firms to consolidate their traditional strengths and preserve their competitive advantages. We have accordingly witnessed streaks of imitation among competing firms. For example, after EMC announced its highly publicized acquisition of RSA, IBM announced it was acquiring Internet Security, followed by Sun’s acquisition of Neogent, Cisco’s acquisition of Ironport, and HP’s acquisition of SPI Dynamics. We plan to study how these news dynamics have stirred competition among IT firms and have consequently shaped the IT landscape.

Year	Network Cohesiveness	Highest Degree Centrality (Degree)
1996	0.667	Network security
1997	0.333	Content security
1998	0.833	Network security; Content security
1999	0.917	IAM
2000	1.167	Network security
2001	0.500	Network security
2002	1.333	Network security
2003	1.000	Network security
2004	1.417	IAM
2005	2.083	IAM
2006	1.917	IAM
2007	2.000	IAM
2008	1.956	IAM; Network Security

Table 1. Network Cohesiveness and Actor Degree Centrality

ACKNOWLEDGMENTS

We thank Prof. Raj Sharman, the track Chair, and the anonymous reviewers for their valuable comments. Their suggestions were instrumental in improving the paper.

REFERENCES

1. Arabie, P. and Wind, Y.Y. (1994) Marketing and social networks, in: Advances in Social Network Analysis, ed. Stanley Wasserman and Joseph Galaskiewicz. Thousand Oaks, CA/Sage.
2. Bayus, B.L. and Agarwal, R. (2007) Pre-entry experience, entry timing, product strategies, and firm survival, *Management Science*, 53, 12, 1887-1902.
3. Borgatti, S.P., Everett, M.G. and Freeman, L.C. (2002) UCINET 6 for Windows, Harvard: Analytic Technologies.
4. Brynjolfsson, E. and Kemerer, C.F. (1996) Network externalities in microcomputer software: An econometric analysis of the spreadsheet market, *Management Science*, 42, 12, 1627–1647.

5. Burt, R. S. (1982) Toward a structural theory of action: Network models of social structure, perception, and action, Academic Press, New York.
6. Cottrell, T. and Koput, K. (1998) Software variety and hardware value: A case study of complementary network externalities in the microcomputer software industry, *Journal of Engineering and Technology Management*, 15, 4, 309–338.
7. Economides, N. and Salop, S. (1992) Competition and integration among complements and network market structure, *Journal of Industrial Economics*, 40, 1, 105–123.
8. European Commission. (1997) Green paper on the convergence of the telecommunications, media and information technology sectors, and the implications for regulation, Towards an Information Society Approach, COM, 97, 623, Brussels: European Commission. Available at: http://europa.eu.int/ISPO/convergencegp/97623.html, 19.01.2005.
9. Gallaugher, J. and Wang, Y.M. (2002) Understanding network effects in software markets: Evidence from web server pricing, *MIS Quarterly*, 26, 4, 303–327.
10. Gao, L. and Iyer, B. (2006) Using software stacks to explain complementarities: The case of mergers and acquisitions in the software industry, *Journal of Management Information Systems*, 23, 2, 121-149.
11. Greenstein, S. and Khanna, T. (1997) What does industry convergence mean? In: Competing in the age of digital convergence, D. B. Yoffie (eds.), Harvard Business School Press, 201-226.
12. Thompson Financial Market Research. (2008) IDC's *IT security taxonomy*, available at http://www.idc.com/getdoc.jsp?containerId=213072
13. Khansa, L. and Liginlal, D. (2007) The Influence of regulations on innovation in information security. *Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007)*, Keystone, CO, August 8-12 2007, Paper 180.
14. Khansa, L. and Liginlal, D. (2008) Understanding the economic impact of information security regulations: The case of identity and access management (*submitted for revision*).
15. Munir, K.A. and N. Phillips. (2002) The concept of industry and the case of radical technological change, *Journal of High Technology Management Research*, 13, 2, 279-297.
16. Pattison, P.E. (1982) The analysis of semigroups of multirelational systems, *Journal of Mathematical Psychology*, 25, 87-118.
17. Porter, M.E. (1985) Competitive Advantage: Creating & Sustaining Superior Performance, New York, NY: The Free Press.
18. Schneier, B. (2007) The death of the security industry, *IEEE Security and Privacy*, 5, 6, 88.
19. Scott, J.P. (2000) Social network analysis: A handbook, London: Sage Publications.
20. Stieglitz, N. (2003) Digital dynamics and types of industry convergence: The evolution of the handheld computers market, in: Christensen, J.F. and Maskell, P. (2003) The industrial dynamics of the new digital economy, Edward Elgar, 179-208.
21. Wasserman, S. and Faust, K. (1994) Social network analysis, Cambridge: Cambridge University Press.
22. Wellman, B. (1988) Structural analysis: From method and metaphor to theory and substance, in: Wellman and Berkowitz (eds.) Social structures: A network approach. Cambridge: Cambridge University Press, 19-61.
23. Yoffie, D. B. (1997) Competing in the age of digital convergence, Massachusetts: Harvard Business School Press.