

Security of Information Technology Assets and the Diffusion of Cyber Insurance

Term Paper

By

Prasanna Karhade

Introduction

Modern information technology (IT) environments are growing in complexity. In spite of these growing complexities and the challenges associated with successfully implementing Information Systems, firms in different industries are investing in IT assets to conduct their business online (Jonathan 2000). The recent trade press indicates that the number of security threats and successful attacks is increasing at an alarming rate (Russ 2000; Hartwig 2002; Anat and John 2003; Joanne 2003; Anat and John 2004). In spite of widespread adoption of electronic commerce internet applications, cyber risks are not yet well understood (Dave 2004). Thus one key challenge in successfully using IT assets lies in ensuring that these IT assets are secure and not vulnerable to security violations (Orlowski 1996; Smith 2004).

As a result of the growing potential and threat of security violations, IT managers are making non-trivial investments to secure their IT assets (Mears 2004). In terms of investments, to reduce the risk and damage from successful security violations, IT managers can pursue several choices, including (1) investments in IT security technology products and infrastructure (Abrams and Joyce 1995) (2) investments in developing and enforcing IT controls, including security training of employees, developing and enforcing acceptable use policies, raising awareness regarding IT security issues or (3) outsource

the IT security tasks to reputable vendors (Desouza, Awazu et al. 2004; Endorf 2004; Goodwin 2004; Blum 2005). A more recent investment opportunity IT managers are pursuing is (3) to invest in cyber insurance (Gordon, Loeb et al. 2003; Lynn 2004).

Cyber Insurance: An IT innovation

Cyber insurance (Amanda 2000; Anonymous 2001; Anonymous 2005) aims to reduce cyber risks by providing extended insurance coverage especially when compared to traditional business insurance (Gordon, Loeb et al. 2003; Mark 2003). This extended coverage includes insurance against virus attacks, business continuity interruption due to security attacks (Eric 2001), network intrusion insurance, data corruption and violations (Erin 2001). Clearly there are diminishing returns (Yurcik and Doss 2002) to investments in all these three IT security investments options discussed above (Kate 2000; Kate 2002). The IT technology related security products are themselves evolving. Though raising security awareness and developing acceptable use policies are immensely helpful, monitoring if such policies are being implemented on a daily basis can be exorbitantly costly. Thus an ideal mix of investments along these three dimensions discussed above is likely to be more efficient to minimize security related risks.

Cyber insurance (Radcliff 2000), as an industry, is still rather nascent (Peter 2002; Steven 2005) and the process of obtaining cyber insurance is itself complicated. A focal firm's cyber insurance premium critically depends on the firm's internet presence, its online IT assets and the extent of internet enabled IT transactions it wishes to insure. A given firm's insurance policy (premiums and deductibles) will be determined by a cyber insurance provider after an audit or inspection of the firm's investments in IT security

and controls. The insurance provider will assign a firm a security rank (a risk-level in terms of its IT security investments) and insurance premiums and deductibles will depend on this security rank.

Since the cyber insurance industry is rather nascent, the option of using cyber insurance to reduce risk is *itself* risky (Bohme 2005). From the perspective of the firm buying cyber insurance (Sarah 2000), potential sources of risk are the following: (1) Right now, the variance in cyber insurance policies (in terms of premiums and deductibles) is very high. (2) Since cyber insurance policies are essentially incomplete contracts, the exact nature of incidents or security violations covered by cyber insurance policies are not entirely formulated or articulated clearly yet.

From the perspective of the cyber insurance provider (Mark 2003), potential sources of risk are the following: (1) since there is no historical data available on cyber insurance policies and security violations, insurance providers find it difficult to accurately predict insurance premiums and deductibles (2) Auditing a given firm's IT investments in IT security is challenging as standard security profiles have not yet emerged in the IT security industry (3) Like all other insurance policies, cyber insurance claims can be fraught with problems associated with hidden information and hidden action problems.

In particular, as firms continue to invest more in IT security, they will have more knowledge in IT security management, and thus would ideally need less cyber insurance (Kesan 2005). But if firms that invest in IT security related technologies might opt to get insurance, because based on their high investments in IT security infrastructure, their cyber insurance premiums and deductibles are likely to be low. But as firms gain more

knowledge and expertise in IT security, they can act opportunistically, especially if their profits die down, and can be expected to make fraudulent claims. This possibility does exist and is a non-trivial risk for the insurance providers, especially assuming that most security violations come from within the firm.

The relationship between rates of adoption cyber insurance and industry type (Anonymous 2000; Anonymous 2005) is also interesting to study. Both the financial and healthcare industries are highly regulated (Goodwin 2004). Is it likely that firms in the healthcare industry or financial industry are likely to adopt cyber insurance more readily? Firms competing in these industries have to comply with several laws which are constantly being revised. In the past, security violations by firms operating in these regulated industries have been punished very severely. Thus it is likely that firms operating in highly regulated industries are more likely to readily adopt cyber insurance as a risk mitigating technique (Garg, Curtis et al. 2003).

Alternatively, the innovation of cyber insurance could apply more specifically to industries that are adopting e-commerce (Lai 2002). Are firms that are likely to adopt (or have already adopted) internet based, e-commerce applications ideal candidates for adopting cyber insurance? These are interesting empirical questions that need to be tested.

The Business Case for Cyber Insurance

In most modern industries that have adopted electronic commerce, protecting the security, privacy and confidentiality of electronic resources is critical, thus investing in cyber insurance is justifiable (Gordon, Loeb et al. 2003; Kesan 2005). In some industries

taking steps to insure and protect technology resources present on the internet can be perceived as a *strategic differentiator*. Adopting cyber insurance to protect and insure security related violations can help differentiate and thus could lead to some strategic advantages (Daughtrey 2001).

Making investments in cyber insurance can also be justified (Ogut, Menon et al. 2005) because owing to the interconnectedness of IT applications on the internet, fates of most companies adopting electronic commerce are intertwined. Here is a scenario: In an outsourcing relationship, based on entirely vendor's mistakes (due to under investments in IT security) the outsourcing firm can pay a heavy price. Thus even though the outsourcing firm makes sizeable investments in IT security technology based products, it can suffer tremendous losses if the IT vendor does not invest in IT security products. Thus investing in cyber insurance makes economic sense for the outsourcing firm.

A growing number of experts believe that uncertain sharing of liability and inadequate or ill-defined accountability for security flaws exacerbates network externalities (Hartwig 2002) and thus represents core obstacles to improving IT security. US case law, also, has not yet clarified who bears responsibility for losses when a breach of IT network security occurs upstream from the damaged party (Ashish, Jeffrey et al. 2003). Consider the following scenario. Consider a scenario when a hacker exploits a security weakness at site A to launch an attack over backbone network B through Internet service provider C which results in damages to company D's information stored on a server maintained by company E. Now, to what extent are A, B, C or E liable for D's damages? If no such liability exists for Firm A, B, C or E, then these parties will not invest in IT security beyond their own direct needs nor purchase third-party insurance

with attendant incentives to improve security for firm D. This is the basic externality issue which can lead to a familiar scenario known as the ‘tragedy of the commons’.

Expenditures or investments in IT security activities are driven not only by rational economic analysis (NPV based cost-benefit analysis) but also by other forces like a given firm's past investments in IT security, best practices in the industry (Gordon, Loeb et al. 2003). For IT security investments, often times conducting a formal cost-benefit analysis is difficult. Benefits of a particular IT security investment are very often difficult to quantify.

The process of procuring cyber insurance proceeds as follows. Before granting an insurance policy, the insurance provider will conduct a security audit of a firm seeking cyber insurance. Due to the possible lack of IT security-related capabilities, the insurer is likely to hire the services of independent *IT security auditor*, to evaluate the level of IT security preparedness of the firm that chooses to insure itself. This level of preparedness, is likely to depend of several factors including (a) the level of investments made by the given firm in IT security related technology products (b) the nature of IT security related processes and acceptable use policies instituted within the firm (c) the level of training and IT security related awareness within the firm. More investments along these three dimensions state above are likely to result in a high level of IT security preparedness. From the point of view of the insurer, firms that have made sizeable investments along the above state three dimensions are likely to be evaluated as being less risky. Thus, such firms are likely to be granted an insurance policy and their premiums are likely to be low.

Owing to rapid changes in IT security related technologies, insurance providers are likely to expect insured firms to continually invest along the three dimensions stated above *to maintain their insurance policies*. The cyber insurance providers are also likely to provide insured firms with IT security related investment advice. Cyber insurance providers are likely to provide with yearly audits of the insured firms based on their evaluation of the insured firm's IT security infrastructure. In order to maintain a cyber insurance policy, insured firms are expected to continually invest in IT security related technology, training and processes.

In the event of a security violation or a security "*accident*", the insured firm is most likely to file a claim. Since insurance claims are likely to be ridden with agency problems, the insurer is most likely to validate or authenticate all such insurance claims. Again, owing to the possible lack of such capabilities, in this context, the insurer is again likely to seek the services of IT security consultants, or IT forensic experts to authenticate the validity of insurance claims.

Thus the diffusion of this IT innovation, cyber insurance, is likely to spawn the growth of several other related markets including the market for IT security auditors, IT security vendors, IT security consultants and IT forensic service providers.

Barriers to the diffusion of the cyber insurance

A review of the literature (Baer 2003) indicated that several forces are preventing the diffusion of cyber insurance:

(1) Lack of Agreement on Basic Policy Definitions and Language: Constant developments in IT environments result in ambiguity about (a) what is insured, (b) what risks are covered, and (c) how losses will be assessed. Law involving IT security is also

changing, thus cyber insurers are likely to minimize their risk by narrowly defining coverage on new policies. Thus, lack of standard policy language is preventing the expansion and maturity of the cyber insurance market.

(2) Lack of Underwriting Experience: Insurers have little experience with IT security claims on which to base premiums, because (a) cyber insurance is relatively new, and more importantly (b) firms have resisted revealing losses resulting from security breaches. Anecdotal evidence indicates that Clients' do not file claims as they fear the damaging publicity if their IT vulnerabilities are revealed. This client reluctance to file claims works to the insurers' advantage, in the short run, but it also means that insurers have little experience to refine their policies, and to develop more complete contractual language.

(3) Lack of Adequate Reinsurance: Insurers' concerns about their inability to judge the level of future exposure is compounded by the lack of a strong reinsurance market to lay off IT security risks. In other fields of property/casualty insurance, underwriters commonly purchase reinsurance to protect themselves against unusual, extreme losses. But the limited nature of claims experience for IT security is restricting the growth of the related reinsurance industry.

(4) Policy Exclusions: Like other property/casualty policies, those covering breaches of IT security typically exclude claims resulting from acts of war, riot, civil commotion and similar disasters known as *force majeure*. Yet these may be precisely the risks that businesses fear most and want to insure against.

The future of cyber insurance: The following things are likely to happen as more firms choose to use cyber insurance as a means of reducing their IT security related risk (Gordon, Loeb et al. 2003; Sally 2003). Developing a business case for cyber insurance Kesan (2005) have proposed the following three consequences of cyber insurance: (1) As more firms adopt cyber insurance, firms are likely to invest more in IT security to reduce the cost of their insurance premiums. These investments are likely to make firms less vulnerable to security violations. (2) As more and more firms adopt cyber insurance, IT security profiles are likely to be standardized within the industry. In other words, more reliable IT security related benchmarks are likely to emerge. (3) As more firms buy cyber insurance, cyber insurance providers will have access to more data and will be able to more economically assign ranks to various security profiles of different firms. Based on the nature of claims filed by firms whose IT assets were damaged by security violations, insurance companies are likely to gain a better understanding of what security violations can be covered and which ones can not be covered economically in the future.

A scenario in which a firm chooses to reduce IT security risk by just buying more cyber insurance and not continually investing in IT security related technology is also clearly not economically conducive for the cyber insurance market. This will lead to insurance providers bearing all the risk, which will not keep insurance premiums low (Ogut, Menon et al. 2005). Continuously maintaining sufficiently high levels of investments in IT security is thus critical to minimize the insurer's risk, which will in effect also reduce insurance premiums.

Research on diffusion of innovations tries to answer the following research question: “What Determines the Rate, Pattern, And Extent of Diffusion of an Innovation across a Population of Potential Adopters?” Based on the analysis of the literature I have fleshed out some of the parameters used in the classical diffusion model in the context of the cyber insurance innovation.

Components of the Classical Diffusion Model

Definition of diffusion: Firms buy an insurance policy to cover damages from IT security related violations on the internet.

Typical Diffusion Pattern: Certain key firms, with significant IT assets vulnerable to security violations are likely to opt to buy cyber insurance first. Given that the amount of costs involved in procuring insurance increase with size, it is not sure if large firms will necessarily be the early adopters. But right now, the business press indicates that cyber insurance rates are too costly for small or medium sized firms to adopt this means as a risk reducing technique.

Innovation Characteristics: Before granting a cyber insurance policy, the insurance provider firms will want to audit a given firms IT security infrastructure. Based on this evaluation, firms with more investments in IT security are likely to be granted a cyber insurance policy with lesser premium as compared to a firm with fewer investments in IT security.

Adopter Characteristics: Firms that invest in IT security are likely to adopt cyber insurance. As firms invest in IT security infrastructure and technology security solutions, they are likely to have relationships with reputed IT security vendors. A firm that has an ongoing relationship with a reputed, IT security vendor is likely to procure a cyber

insurance policy with smaller premiums. There are likely to be partnerships between IT security infrastructure vendors and cyber insurance providers to encourage simultaneous investments in IT security infrastructure and cyber insurance.

Adopter decision stages: Cyber insuring a modern multinational enterprise that has a lot of ongoing outsourcing relationships with software vendors across the globe is understandably an exorbitantly expensive endeavor. The decision to adopt cyber insurance is thus most likely to progress in stages. A firm could choose to cyber *insure a particular, strategically important relationship* with a particular IT service provider or vendor to start with. Thus firms are likely to not cyber insure their entire operations, but choose to insure just the relationships they perceive as being critical to their strategic position.

Opinion leaders and change agent: Certain key firms, located at key locations in certain key supply-chains can serve as opinion leaders. Once these key firms adopt cyber insurance as a risk mitigating technique, other firms in similar supply-chains are also likely to be motivated to adopt the cyber insurance innovation.

Several forces could lead to the widespread adoption of diffusion of the cyber insurance innovation across most modern industries that have adopted e-commerce. As more firms opt to use cyber insurance, premiums are likely to reduce or at least stabilize and converge to the optimal price. As more firms adopt this innovation, more data will be available for insurance companies to better estimate insurance premiums. Insurance providers are also likely to have access to more information on security violations, security attacks and incidents, and thus this information is likely to be used to write more

detailed, essentially more complete policy contracts for the future. It is not just the current high cyber premiums that are preventing firms from adopting cyber insurance but it is also the large variation in these cyber insurance premiums. These premiums are likely to stabilize only as more firms adopt this innovation.

Measure of Adopter Innovativeness

Earliness of Adoption: A firm could be first in a particular industry to adopt cyber insurance when compared with other firms in the same industry. A firm could also be the first in a given supply-chain to adopt cyber insurance. Thus based on different strategic groups that a firm belongs to, this measure can be developed for a given firm.

Internal Diffusion: Most large modern corporations are multinational, multi-location firms. Thus the extent to which each division or each branch of the given firm has adopted this innovation could be used to measure the internal rate of diffusion. Thus adopting cyber insurance could be a two stage process where one division chooses to adopt this innovation as a risk mitigating technique for one its critical projects or strategic outsourcing relationships. This could then be followed by a company wide diffusion of this innovation.

At this stage, the costs, benefits and risks associated with adopting the cyber insurance innovation are not clear. Insurance policies are essentially incomplete contracts. All contingencies under which security violating will be covered by the policy are often not clearly articulated. Based on the popular press and anecdotal evidence, right now cyber insurance is very expensive for most small and medium sized firms. Thus the diffusion of cyber insurance is going to require considerable amounts of collaboration between the IT

security technology vendors and insurance companies. This collaboration can be in terms of actual discounts, for instance: a firm investing in a security technology of a particular vendor is likely to be given some discounts on their cyber insurance policy.

Proposition One: Collaboration between IT security vendors and insurance providers is likely to lead to the diffusion of the cyber insurance innovation

The process of procuring and maintaining a cyber insurance policy is also very complicated right now. More yearly audits, familiarity with auditing related assessments, are likely to help, and more standard profiles and practices are likely to emerge. Most IT security auditor firms possess the capabilities to offer IT security related security advice. Likewise, IT security consultants also possess the capabilities to conduct IT security related audits. Thus, IT security audit and consulting firms are likely to benefit from the diffusion of cyber insurance. Assuming the auditor independence property does not exist, more cyber insurance adopters can also lead to more consulting opportunities for IT security consultants and auditors.

Proposition Two: Collaboration between IT security auditing/consulting firms and insurance providers is likely to lead to more diffusion of the cyber insurance innovation.

References:

1. Abrams, M. D. and M. V. Joyce (1995). "New Thinking About Information Technology Security." Computers & Security **14**(1): 69-81.
2. Amanda, L. (2000). "Hacker attacks spur web liability products." National Underwriter **104**(11): 3.
3. Anat, H. and D. A. John (2003). "The impact of Denial-of-Service attack announcements on the market value of firms." Risk Management and Insurance Review **6**(2): 97.
4. Anat, H. and D. A. John (2004). "The Impact of Virus Attack Announcements on the Market Value of Firms." Information Systems Security **13**(3): 32.
5. Anonymous (2000). "Cyber insurance coverage." The Controller's Report(12): 15.
6. Anonymous (2001). "Chubb unveils CyberSecurity--unprecedented protection from Internet-related losses for financial institutions." Forensic Accounting Review and Computer Security Digest **17**(7): 2.
7. Anonymous (2005). "CYBER-INSURANCE." New Scientist **186**(2505): 30.
8. Anonymous (2005). "A directory of markets for cyber insurance." American Agent & Broker **77**(7): 52.
9. Ashish, G., C. Jeffrey, et al. (2003). "The real cost of being hacked." The Journal of Corporate Accounting & Finance **14**(5): 49.
10. Baer, W. (2003). "Rewarding IT Security in the Marketplace." Contemporary Security Policy **24**(1): 190 - 208
11. Blum, D. (2005). "Don't lose control with outsourcing." Network World **22**(45): 61-61.
12. Bohme, R. (2005). Cyber-Insurance Revisited. Workshop on the Economics of Information Security (2005), Kennedy School of Government, Cambridge, MA, USA.
13. Daughtrey, T. (2001). Costs of Trust for E-Business
<http://sqp.asq.org/pub/qualityprogress/past/1001/qp1001daughtrey.pdf>.
14. Dave, L. (2004). "Cyber risks not well understood." Business Insurance **38**(46): 32.

15. Desouza, K. C., Y. Awazu, et al. (2004). "The Risks of Outsourcing." J@pan Inc.(60): 32-37.
16. Endorf, C. (2004). "Outsourcing Security: The Need, the Risks, the Providers, and the Process." Information Systems Security **12**(6): 17-23.
17. Eric, L. (2001). "E-surance fills in the gaps when business is down." Information Management & Computer Security **9**(2/3): 138.
18. Erin, E. A. (2001). "Hackers, viruses prompt growth of e-surance policies." Barron's **81**(31): 12.
19. Garg, A., J. Curtis, et al. (2003). "The financial impact of IT security breaches: What do investors think." Information Systems Security **March-April 2003**: 22-33.
20. Goodwin, B. (2004). "Regulations are pushing users to outsource security management." Computer Weekly: 6-6.
21. Gordon, L. A., M. P. Loeb, et al. (2003). "A framework for using insurance for cyber-risk management." Communications of the ACM **46**(3): 81 - 85
22. Hartwig, R. P. (2002). The Long Shadow of September 11: Terrorism & Its Impacts on Insurance and Reinsurance Markets, http://server.iii.org/yy_obj_data/binary/632700_1_0/sept11.pdf.
23. Joanne, W. (2003). "Computer viruses seen as big threat to many businesses." Business Insurance **37**(44): 3.
24. Jonathan, F. (2000). "Cyber insurance to cover E-business." The Internal Auditor **57**(4): 13.
25. Kate, G. (2000). "ASPs to insurers: 'Cover me'." Tele.com **5**(8): 13.
26. Kate, M. (2002). "Demand for cyber insurance pegged as high-growth market." Memphis Business Journal **23**(49): 7.
27. Kesan, J. P., Majuca, Ruperto P. and Yurcik, William J. (2005). "The Economic Case for Cyberinsurance" . SECURING PRIVACY IN THE INTERNET AGE,. Available at SSRN: <http://ssrn.com/abstract=577862>, Stanford University Press.
28. Lai, E. (2002). Cyber-insurance gaining popularity due to high-tech risks, MSNBC. Reuters. <http://stacks.msnbc.com/local/rtor/m23000.asp?cp1=1> [2002, April 5].

29. Lynn, L. (2004). "Cybercrime insurance may be coming to a business near you." The Mississippi Business Journal **26**(51): 25.
30. Mark, A. H. (2003). "Cyberrisk exposures challenge insurers." Business Insurance **37**(47): 12.
31. Mark, G. (2003). "Cyber safety: The latest tool in the risk management arsenal - 'cyber insurance'." Bank News **103**(10): 26.
32. Mears, J. (2004). "Is security ripe for outsourcing? (Cover story)." Network World **21**(34): 1-80.
33. Ogut, H., N. Menon, et al. (2005). Cyber Insurance and IT security investment: Impact of Interdependent Risk, The University of Texas at Dallas.
34. Orłowski, S. (1996). The changing face of information technology security. Information Security and Privacy. **1172**: 1-13.
35. Peter, K. (2002). "Cyber-risk assessors chasing \$2B market." Philadelphia Business Journal **20**(50): 4.
36. Radcliff, D. (2000). "Got Cyber Insurance." Computerworld **34**(34): 44-45.
37. Russ, B. (2000). "Attack of the cyber villains." World Trade **13**(8): 46.
38. Sally, R. (2003). "Greater understanding of cyber exposures fuels growth of coverage." Business Insurance **37**(48): 3.
39. Sarah, V. (2000). "Many U.K. companies lack cyber cover: Survey." Business Insurance **34**(25): 24.
40. Smith, G. S. (2004). "Recognizing and Preparing Loss Estimates from Cyber-Attacks." Information Systems Security **12**(6): 46.
41. Steven, T. (2005). "Cyber-Coverage Potential Boundless." National Underwriter, P & C **109**(34): 43.
42. Yurcik, W. and D. Doss (2002). CyberInsurance: A Market Solution to the Internet Security Market Failure. Workshop Economics of Information Security, 2002