

A Framework for Using INSURANCE FOR CYBER-RISK MANAGEMENT

Seeking to protect an organization against a new form of business losses.

The use of the Internet has significantly increased the vulnerability of organizations to information theft, vandalism, and denial-of-service attacks, thereby bringing information security issues to the forefront of the agenda for corporate executives. The importance of this agenda item is highlighted by a 2002 survey conducted by the Computer Security Institute and the Federal Bureau of Investigation. The CSI/FBI survey reported that 90% of respondents detected a computer security breach within the last year and the average estimated loss (for organizations that provided estimates) was over \$2 million per organization [7]. Moreover, 74% of the survey's respondents reported their Internet connections were the points of frequent attacks.

Organizations have long been concerned with protecting their proprietary information, maintaining the integrity of their databases, and ensuring timely access to information by authorized users. Nevertheless, the increased vulnerability to substantial economic loss from attacks through the Internet is causing many executives to seek additional tools to manage information security risk. One new tool is the use of recently developed cyber-risk insurance policies (that is, policies that provide coverage against losses from Internet-related breaches in information security). By insuring losses from information security breaches,

a firm may hedge its potential losses from cyber crime. A framework for using insurance as a tool for cyber-risk management related to information security is described here. We begin by establishing some background explanation of the unique characteristics of insurance related to cyber-risk management.

Much of the potential risk from conducting business on the Internet is not fundamentally new. For example, a firm would incur liability risk of copyright infringement or defamation of character whether the information is distributed through the Internet or through television, radio, or magazines. Similarly, a firm would suffer

ILLUSTRATIONS BY PETER HOEY

a loss of business whether an interruption is caused by a fire, a flood, or by a hacker's denial-of-service attack.

While the business risk of being connected to the Internet is analogous to many traditional business types of risk, some characteristics of Internet-related (cyber-) risk are unique, in terms of location, degree, and visibility. For example, a perpetrator of information theft or property damage may be thousands of miles away from the business location when committing the crime via the Internet.

The damages from a virus can go beyond the effects on the data and software of the targeted business, causing the initial targeted business to incur a liability. Additionally, since the commodity on the Internet is information, security breaches (such as the theft of the firm's strategically sensitive information) often go undetected.

Firms traditionally carry insurance to safeguard against various business, natural, and political risks. However, traditional policies do not comprehensively address the additional risk firms face as a result of being a part of the digital economy. The growth of the Internet has therefore created a demand for new insurance products that hedge some of the risk of connectivity [2]. Thus, insurance companies (including American International Group, Chubb, Fidelity, and Deposit, Marsh, Lloyds of London, and J.S. Würzler) introduced new policies covering varying aspects of cyberspace risk.¹ In designing these new policies, insurance companies addressed issues related to pricing, adverse selection, and moral hazard. Although each of these issues is common to all forms of insurance, the cyber-risk situation creates different concerns as discussed here.

Pricing. Pricing of insurance products traditionally relies on actuarial tables constructed from voluminous historical records. Since the Internet is relatively new, extensive histories of e-crimes and related losses do not exist. The repositories of information security breaches that do exist (see www.cert.org) do not cover many years, and suffer from the fact that firms often will not reveal details concerning a security breach.

The previously described situation notwithstanding, insurance companies have made pricing determinations for their cyber-risk policies. Hence, they have quantified what some claim is unquantifiable risk. However, given the high uncertainty involved with calculating the actuarial value of cyber-risk insurance policies, it remains to be seen whether these pricing schemes are correct. In this regard, Radcliffe [8], quotes the vice president of e-business solutions at Fidelity and Deposit as stating, "These insurance

products are so new, that the \$64,000 question is: Are we charging the right premium for the exposure?"

Adverse Selection.

As noted previously, cyber-risk insurance policies also must be designed to take into account the problem of adverse selection. Adverse selection refers to the problem that arises because a firm (or person) choosing to insure against a particular loss is likely to have private information not available to the insurance

company at the time of contracting. For example, a person who does not feel well would be more prone to purchase health or life insurance than an average person shown in actuarial tables. To deal with the adverse selection problem for health and life insurance, underwriters require physical examinations, discriminate by lifestyle characteristics (such as smokers vs. nonsmokers), and require a period of time to pass before the policy is effective.

For cyber-risk insurance, the adverse selection problem manifests itself in terms of the likelihood of a security breach. Firms with a higher likelihood of an information security breach would be more prone to buy this policy than firms with a low likelihood of such a breach. To protect themselves from the adverse selection problem when offering cyber-risk policies, insurance firms typically require an information security audit before issuing a policy. Another response to the adverse selection problem is for insurance firms to identify high-risk users and differentiate the premium for such users. For example, J.S. Würzler, an insurance firm offering a policy to cover loss from hackers, apparently adds a surcharge to firms using Microsoft's NT software in Internet operations [1]. Thus, Würzler treats the use of NT software as a precondition,

A TRADE-OFF EXISTS BETWEEN THE AMOUNT A FIRM SHOULD INVEST IN PROTECTING AGAINST SECURITY BREACHES OCCURRING AND THE AMOUNT IT SHOULD SPEND ON CYBER-RISK INSURANCE.

¹See www.gauntlettlaw.com/insurance.htm for contact information for many firms providing cyber-risk insurance coverage.

much like a life insurance policy treats smoking or high blood pressure.

Moral Hazard. While adverse selection deals with the insured's private information prior to contracting for the insurance, the moral hazard problem deals with the lack of incentives by the insured to take actions that reduce the probability of a loss subsequent to purchasing the insurance. For example, a firm with fire insurance may be less inclined to take fire safety steps than a firm without such insurance. One way insurance policies can address the moral hazard problem is through the use of deductibles. By using deductibles, the insured will suffer some loss should the occurrence (such as a fire or security breach) be realized. Thus, the deductible provides a monetary incentive for the insured to take actions that reduce the likelihood of the loss actually occurring.

Another way of addressing the moral hazard problem is for policies to offer premium reductions for taking actions that reduce the probability of a loss. For example, a homeowner's policy may provide discounts for having smoke detectors to reduce the probability of a major fire. Similarly, firms offering cyber-risk insurance offer discounts for firm's taking specified security measures. For example, Bryce [1] has noted that AIG offers discounts for firms using Invicta Network's security device for shifting Internet Protocol addresses and Lloyds of London provides a discount for firms using Tripwire's Integrity security software [11]. Another feature found in cyber-risk insurance is partnering, whereby the producer of a product/service offers the purchaser the option to buy a particular insurance policy at a discount. In this latter vein, Hewlett-Packard teamed up with J.S. Wurzler to offer insurance for revenues lost because of a security breach to users of HP-UX systems [4]. AT&T teamed up with Marsh to offer e-business insurance to firms using AT&T's Internet data centers and Web hosting services [5].

What Cyber-Risk Insurance Covers

A plethora of cyber-risk insurance policies exists in the marketplace. Trade names include Chubb's Cyber Security, AIG's NetAdvantage Security, Hiscox's Hackers Insurance, Legion Indemnity's INSUREtrust, Lloyd's e-Comprehensive, Marsh's NetSecure, and St. Paul's Cybertech.² These policies cover first-party and/or third-party cyber-risk poten-

tial arising from a firm's Internet-related activities.

First-party risk occurs when the insured faces the possibility of loss of profits due to such things as: theft of trade secrets, destruction of the insured's property (including software, hardware, and data), and extortion from hackers. Third-party risks are those faced by the insured because of damages caused, directly or indirectly, to another firm (or individual). Third-party risk includes liabilities for such events as: a computer virus inadvertently forwarded, failure to provide products (as contracted) because a hacker or virus stopped the insured's delivery system, contents placed on the company Web site (including infringement of copyrights), and/or theft of information held about a third party, such as credit card records.³

Since cyber-risk insurance is a new product, under-

writers are generally reluctant to offer large policies (relative to traditional insurance). However, Lloyds offers limits for its e-Comprehensive policy of \$50,000,000, and gives custom quotes up to \$200,000,000 [11]. As more experience is gained in this area, we expect to see these limits raised. Additionally, we

expect insurance firms to offer alternate policies providing high limits in combination with substantially raised deductibles. Thus, firms will be able to secure higher total coverage by combining policies from multiple insurers (for example, having one policy cover the first \$20,000,000 of losses and another policy cover losses over \$20,000,000).

Cyber-Risk Management Framework for Information Security

Risk management related to information security is "the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk" [6]. Thus, organizations should begin by assessing the threats and vulnerabilities associated with their information systems. The value of the information vulnerable to threats also needs to be considered at this stage of the process. In this latter regard, a value-vulnerability grid that helps identify which information should receive the security resources could be developed. This grid would cate-

| | | V U L N E R A B I L I T Y | | |
|-----------------------|--------|---------------------------|--------|-----|
| V A L U E | | High | Medium | Low |
| | High | 1 | 2 | 3 |
| | Medium | 4 | 5 | 6 |
| | Low | 7 | 8 | 9 |

Figure 1. Value-vulnerability grid.

²A chart summarizing the main features of these, and some other policies, is provided in [9].

³For more discussion of first-party and third-party risks, see [10].

gorize information from high to low for both value and vulnerability, as shown in Figure 1. In order to effectively leverage scarce information security resources, information falling into boxes 1, 2, 4 and 5 should generally receive the largest share of the information security budget.

Next, organizations should reduce information security risk to an acceptable level. This level will vary from organization to organization, based partly on the location of the information in the value-vulnerability grid. To reduce risk to an acceptable level, organizations should take the following two steps. First, an organization should invest in protecting against the risk of actual security breaches occurring. This protection would include the installation of firewalls, encryption, and access control techniques. However, even with the best protection, detection, and correction systems, losses from security breaches will likely occur. Hence, the second step is the acquisition of cyber-risk insurance. This insurance is a management tool for reducing the risk of financial losses associated with Internet-related breaches.

A trade-off exists between the amount a firm should invest in protecting against security breaches occurring and the amount it should spend on cyber-risk insurance. For a given level of information value-vulnerability, higher levels of security protection will require lower levels of cyber-risk insurance (and vice versa). When allocating resources to lower the overall risk exposure to an acceptable level, the trade-off between investing to reduce the probability of security breaches and investing in insurance to reduce the financial losses (should breaches actually occur) should be viewed in cost-benefit terms. This cost-benefit trade-off between reducing the risk of security breaches and buying insurance will also affect the level of residual risk (that is, the remaining risk after taking steps to protect and insure against security breaches) deemed to be an acceptable level.

Once the acceptable level of residual risk is determined, that level should be maintained. Thus, orga-

nizations should invest in intrusion detection systems and have contingency plans in place for correcting potential breaches. The cyber-risk management process described here is illustrated in Figure 2. The phases of the risk management process

shown are sequential and iterative.

After recognizing the potential need for cyber-risk insurance, a decision plan of action is needed. One such plan, based on four steps, includes: conducting an information security risk audit, assessing current coverage, examining available policies, and selecting a policy.

Figure 3 illustrates our four-step cyber-risk insurance plan. In presenting this plan, we highlight some key issues discussed earlier. As will become clear, we view the insurance decision plan of action as a mechanism for reviewing and assessing the firm's entire cyber-risk management strategy.

The first step is to conduct a thorough audit of current information security risk (that is, review the entire risk management process described in Figure 2). This audit should uncover the firm's information security risk exposure and place a dollar value on that exposure. Even full insurance cannot financially protect a firm from a security breach, if the breach cannot be documented. Therefore, an essential aspect of the

audit is to assure that intrusion detection systems are in place to provide such documentation.

The next step is to assess current coverage. Corporate executives should thoroughly review existing property and liability insurance policies. This review should focus on gaps in Internet-related coverage in the current policies. Many insurance companies have recently added cyber-risk-related exclusions to their traditional policies in order to limit the underwriter's

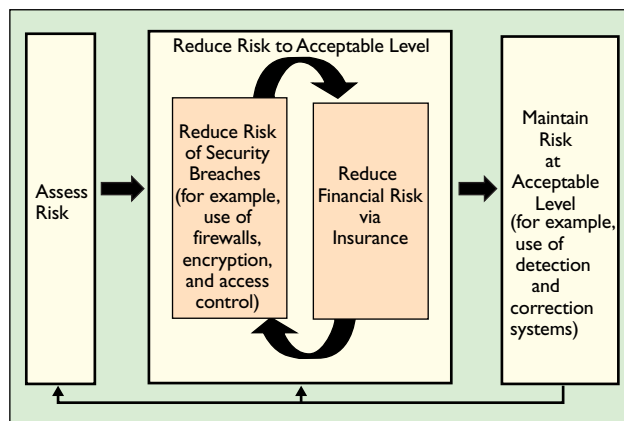


Figure 2. Cyber-risk management framework for information security.

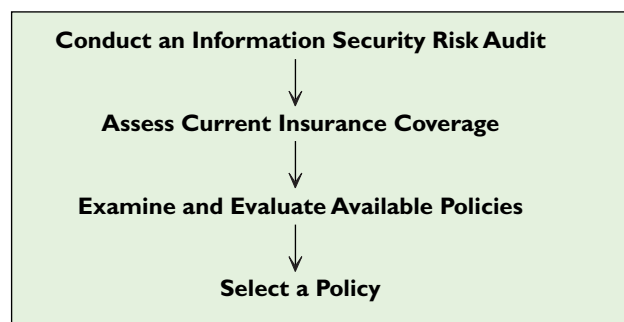


Figure 3. Cyber-risk insurance decision plan.

risk exposure. Some view the growth in such policy amendments as the insurance industry's way of forcing businesses to buy their more profitable cyber-related products [3]. By examining existing policies, financial executives will become aware of existing coverage gaps, and therefore will be in a position to negotiate with their current insurance providers.

The third step is to examine and evaluate available insurance policies. Cyber-risk insurance has recently been developed, and policies differ widely in coverage and price. The information security audit, combined with the review of current policies, allows management to focus on policies that cover existing gaps. For example, does a particular firm require coverage for losses due to: a crash of the firm's Web site, a denial-of-service attack, potential liabilities from third parties, or libelous statements appearing on the company's Web site?

Recall that insurance companies design cyber-risk insurance policies to handle adverse selection and moral hazard problems. Thus, in evaluating a policy, it is important to consider a firm's potential losses and the security measures in place. For example, firms that pose a low moral hazard threat should carefully analyze insurance policies that are cheaper for firms exhibiting this feature.

The fourth step is to select the policy appropriate for the unique circumstances of a given company. In making such a selection, the policy should have the desired additional coverage at an acceptable price. The trade-off between reducing the risk of security breaches and the cost of insurance also must be considered at this point. Additionally, companies should determine the portion of financial risk they want the insurance company to cover and the residual portion they are willing to bear. Hence, a company's risk tolerance is a key determinant of the appropriateness of a particular insurance policy. Finally, since cyber-risk insurance is so new and insurance companies are uncertain about how to price these products, there is often considerable room for negotiating prices with brokers and/or agents.

Conclusion

Information security risk has been highlighted by several hacker attacks on high-profile U.S. Web sites, a series of computer viruses, and electronic thefts that caused considerable financial damage. Companies, therefore, have invested heavily in numerous information security measures. Unfortunately, no amount of security can prevent all breaches. Hence, a viable market has emerged for cyber-risk insurance to protect against financial losses from information security breaches. We have described a generic framework for using cyber-risk insurance for helping

to manage information security risk. This framework is based on the entire risk management process and includes a comprehensive four-step cyber-risk insurance decision plan. **C**

REFERENCES

1. Bryce, R. Insurer considers Microsoft NT high-risk. *Interactive Week* (May 28, 2001), 11–12.
2. Gauntlett & Associates. Insurance Products Review. (Aug. 15, 2001); www.gauntlettlaw.com/insurance.htm.
3. Gold, J., Anderson, K. and Olick E-business insurance: Insurance coverage for e-business claims. (Aug. 16, 2001); www.andersonkill.com/Publications/Alerts/EBAAlert/winter2001.asp.
4. Madden, J. HP to offer e-business insurance policies. *PC Week* (Feb. 16, 2000), 15–20.
5. Marsh Company. Marsh, AT&T unveil innovative e-business risk solution. (Aug. 15, 2001); www.marshweb.com/home/homepg.nsf/afb6ac060ccea991852567af004d1b3a/e2047f2bf3af5f6685256a850055209a.
6. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12, 1995.
7. Power, R. 2002 CSI/FBI computer crime and security survey. *Computer Security Issues and Trends* 8, 1 (Jan. 2002), 1–22.
8. Radcliff, D. Calculating e-risk. *ComputerWorld* 35, 7 (Feb. 12, 2001), 34.
9. Rossi, M.A. International Risk Management Institute. Standalone e-commerce market survey. (July 2001); www.irmi.com/expert/articles/rossi004chart.asp.
10. Rossi, M.A. New standalone e-commerce insurance policies for first-party risks. (Feb. 2001) International Risk Management Institute; www.irmi.com./expert/articles/rossi006.asp.
11. Tripwire named loss-control tool of choice for e-comprehensive insurance. *Business Wire* (June 24, 2000), 7–9.

LAWRENCE A. GORDON (lgordon@rhsmith.umd.edu) is Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance at the Robert H. Smith School of Business at the University of Maryland.

MARTIN P. LOEB (mloeb@rhsmith.umd.edu) is a professor of Accounting and Information Assurance, and a Deloitte & Touche Faculty Fellow at the Robert H. Smith School of Business at the University of Maryland.

TASHFEEN SOHAIL (tsohail@rhsmith.umd.edu) is a Ph.D. student in Accounting and Information Assurance at the Robert H. Smith School of Business at the University of Maryland.

Support for this research was provided in part by the Laboratory for Telecommunication Sciences (within the Department of Defense) through a contract with the University of Maryland Institute for Advanced Computer Studies.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.