Cyber-Insurance Metrics and Impact on Cyber-Security

"Sometimes we can . . . be a little bit more vigorous in using market-based incentives, working with the insurance industry, for example. . ."

DHS Secretary Michael Chertoff, April 29, 2005

"The Insurance industry has a pivotal role in play [in protecting our national infrastructure], particularly by developing cyber-insurance policies. This may be easier said that done…But carriers must begin…Somehow it can be done."

Paul B. Kurtz, Homeland Security Council, 2003

Overview to Cyber-Insurance

What is Cyber-Insurance?

Cyber-insurance is an insurance product used to protect businesses from Internet-based risks, and more generally from risks relating to information technology infrastructure and activities. Risks of this nature are typically excluded from traditional commercial general liability policies. Coverages provided by cyber-insurance policies may include first-party coverage against losses such as data destruction, extortion, theft, hacking, and denial of service attacks; liability coverage indemnifying companies for losses to others caused, for example, by errors and omissions, failure to safeguard data, or defamation; and other benefits including regular security audits, post-incident public relations and investigative expenses, and criminal reward funds.

The Benefits of Cyber-Insurance

Cyber-insurance increases cyber-security by encouraging the adoption of best practices. Insurers will require a level of security as a precondition of coverage, and companies adopting better security practices often receive lower insurance rates. This helps companies to internalize both the benefits of good security and the costs of poor security, which in turn leads to greater investment and improvements in cyber-security.

The security requirements used by cyber-insurers are also helpful. With widespread take-up of insurance, these requirements become de facto standards, while still being quick to update as necessary. Since insurers will be required to pay out cyber-losses, they have a strong interest in greater security, and their

requirements are continually increasing.

As well as directly improving security, cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping to businesses to return to normal and reducing the need for government assistance.

Finally, insurance allows cyber-security risks to be distributed fairly, with higher premiums for companies whose expected loss from such risks is greater. This avoids potentially dangerous concentration of risk while also preventing free-riding.

Advantages over Governmental Regulation

Cyber-insurance has a number of advantages over governmental regulation as a means for improving cyber-security. First and foremost, government standard-setting is simply not suitable for a rapidly evolving area such as cyber-security. Standards produced by organized bodies are based on compromise, and government involvement in the process stifles innovation further. Closely related to this is the threat of regulatory capture attendant with any system of governmental regulation.

Positive reinforcement is generally the more effective behavior modification technique, as individuals naturally prefer reward to punishment. Fear of legal sanctions can force companies to maintain a set of minimum standards, as cyber-insurance does, but unlike cyber-insurance it does not provide any incentive to do better. Governmental regulation results in an emphasis on meeting basic minimum standards, whereas insurance results in companies striving to adopt – and improve upon – best practices. Finally, because the risk is global, United States regulations alone cannot effectively manage it. However, worldwide regulation is impractical because international organizations move even more slowly than national governments. Widespread use of cyber-insurance will produce better security than a system of governmental regulation and standard-setting.

Problems with the Market for Cyber-Insurance

Despite the benefits of cyber-insurance, the market for cyber-insurance is adversely affected by a number of problems.

First and foremost, insurers are afraid of a "cyber-hurricane" – a major disaster resulting in great number of claims. Cyber-hurricanes represent an uncertain risk of very large losses, and as such are very difficult for insurers to plan for. Because computer systems are interdependent and standardized, they tend to be especially vulnerable to correlated losses of this nature. This fear increases

insurance premiums, because insurers naturally focus on worst-case estimates of the expected loss from such an event so that they can maintain underwriting profitability.

In addition, "cyber-hurricanes" raise a barrier to entry to the insurance market, because an insurer may be wiped out if a major event occurs before they have built up sufficient cash reserves. Prices for private market reinsurance for cyber-insurers is extremely high as the fear of a "cyber-hurricane" is felt most by the reinsurance community.

Second, because cyber-insurance is a relatively new area, insurers are hampered by a lack of actuarial data with which to calculate premiums. In addition to increasing price, a lack of data leads to problems with the risk analysis undertaken by companies when deciding whether insurance against a particular risk is worthwhile. A lack of data also makes cyber-insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance. .

Legislative Solutions

Given the public policy benefits that come with widespread adoption of cyber-insurance and the current obstacles to the widespread creation and adoption of cyber-insurance, the federal government should act in order to help counteract the current market failure in the cyber-insurance market. The federal government has a number of measures at its disposal that it may use to improve the market for cyber-insurance, and by doing so help shore up domestic and international cyber-security.

Federal Purchasing Power

The federal government can promote the use of cyber-insurance with its strong position in the marketplace, by requiring government contractors and sub-contractors to carry cyber-insurance. This would directly stimulate the cyber-insurance market by increasing demand for cyber-insurance. Further down the line, companies carrying cyber-insurance to meet federal contracting requirements would be able to use their insurance as a selling point when bidding on private contracts, leading to further uptake of cyber-insurance by their competitors to nullify this advantage.

Precedent for this action may be found in the Federal Acquisition Regulations, which require government contractors “to provide insurance for certain types of perils.”

The principal advantage of this approach is that it would directly increase the adoption of cyber-insurance, and thereby improve cyber-security, while imposing an additional regulatory burden that is truly minimal.

In addition, the magnitude of the federal government's purchasing power means that the effects of this action would most likely spill over into private

contracting, leading to further increases in coverage rates and security.

Cyber Safety Act

The federal government can promote cyber-security efforts by creating a Cyber Safety Act that provides safe harbors or other limitations on cyber-security liability, contingent on reasonable efforts to conform to best practices. Liability would be generally capped at the amount of insurance purchased and there would be requirements to purchase adequate amount of insurance. This would provide a powerful incentive to adopt effective security measures. It would also make the regular security evaluations associated with cyber-insurance especially valuable. Precedent for this action may be found in the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002, which provides limitations on liability and damages for claims against sellers of anti-terrorism technologies arising out of the use of anti-terrorism technologies, contingent on having liability insurance.

A cyber-Safety Act would increase the supply of the liability component of cyber-insurance and reduce its premium cost by reducing uncertainty and potential cost. There is no cost to the taxpayer associated with this action.

Encourage Information-Sharing

The federal government can promote the sharing of cyber-security information by establishing an antitrust exemption to allow insurers to pool data on vulnerabilities and attacks. This would allow insurers and risk managers to create better actuarial models for cyber-risks, reducing insurance premiums and making cyber-insurance more attractive to companies, and therefore increasing the adoption of cyber-insurance. Precedent for this approach may be found in the Year 2000 Information and Readiness Disclosure Act of 1998, which provides a limited exemption from federal antitrust law and the Freedom of Information Act for the sharing of vulnerability information related to the Year 2000 bug. This action would result in the production of a comprehensive and detailed compilation of cyber-security information at no cost to the taxpayer. By reducing the uncertainties currently associated with cyber-risks, it would tend to drive down the supply cost of cyber-security insurance and reinsurance, leading to lower prices and increased coverage rates. Insurance companies are best placed to compile this data, and already require policyholders to report cyber-attacks. This action would help to reduce the current under-reporting problem at no cost.

Federal Government as a Reinsurer

The federal government can increase the supply of cyber-insurance by providing

reinsurance to cyber-insurance companies for a limited time. This would increase the adoption of cyber-insurance by reducing prices, with price reduction caused both by decreased supply cost and increased competition in the cyber-insurance market.

Precedent for this action may be found in the Terrorism Risk Insurance Act of 2002, which for a limited period provides compensation for insurers who suffer sufficiently large losses resulting from designated acts of terrorism, subject to recoupment through risk-spreading premiums on other insurance products. This action solves the most important problem with the cyber-insurance market, the fear of a cyber-hurricane". With this obstacle lifted, supply and adoption of cyber-insurance will increase. In addition, the availability of guaranteed reinsurance with large limits may allow insurers to offer large amounts of cyber-insurance coverage to companies who require it. By the time the reinsurance program ends, insurance companies will have built up sufficient reserves to cope with a "cyber-hurricane" unaided. If no covered risk materializes during the time period covered by the reinsurance program, this action has no cost to the taxpayer. In the event that a covered risk does materialize, the taxpayer would be able to recover at least some of their costs.

Insurance Underwriting
Standards of Due Care for Network Security Risk

It has been said that the insurance industry is in a uniquely motivated to understand and communicate to its insureds what are the standards of due care appropriate for the management of network security. The reason for this is simple. Only the insurance industry has "skin in the game". That is to say, in the event of a loss it is the insurance company that will pay, excess of any self-insured retention, any damages to third parties as well as reimburse the policyholder for any loss of business and additional expense associated with the event.

The exact tools and metrics used by a cyber-insurance carrier is proprietary to that carrier and might differ from carrier to carrier. However, much of the criteria used is generally common among carriers and is known to the industry.

Cyber-insurance carriers must seek to understand:

1. The frequency or likelihood of a loss event will occur to a particular company,
2. The frequency or likelihood that such an event will cause damage to the company or to others for which the company is legally liable,
3. The severity or insured cost of such a loss event should it occur, and finally

4. What steps of prevention and/or mitigation a company employs to either avoid (largely impossible) or reduce (definitely possible) any of the above 3.

To do this, carriers use a number of tools including an application for insurance, an online security assessment (based mostly on ISO 27001), telephone call between the carrier's technical expert and the company's CISO and, if deemed necessary, an on-site security assessment. Any previously conducted network assessment or regulatory review is also analyzed by the underwriters.

Typically, an underwriting analysis will include a review of the following:

1. General risk exposure of the industry and business activities,
2. General risk exposure of the size of the company,
3. Loss History,
4. Years in business,
5. Financial condition
6. Extent of use of outsourced network security services
7. Dependency on third parties networks
8. In depth analysis of network security pursuant to standards such as ISO 27001

Each of the above can now be discussed.

<u>General risk of exposure based on company industry and size and business activities</u>

The general risk exposure based on industries focuses on industries that have one or more of three characteristics: (1) the extent and type of data used, (2) the extent of dependency of network systems in a company's daily operations and (3) the extent the company is subject to regulation. For this reason, industries such as financial institutions and healthcare and retail which employ highly sensitive data are generally considered to be of a higher exposure industry. These industries are expected to have higher levels of network security best practices and those that do not can fail to obtain insurance. A review is made of a company's business activities activities. How dependent are their on their systems. What is their systems used for? (e.g. communications only, order taking, inventory, data exchange, etc.) The more central the use of their systems to their business activities the greater the exposure. Finally, since larger companies tend to have larger losses arising from the same errors, large companies usually command higher premium levels than smaller companies.

<u>Loss History, Years in Business and Financial Condition</u>

Underwriters will inquire as to the extent of prior computer attacks. This is usually done after a dollar threshold of damages since all companies suffer attacks on a daily basis. Substantial prior losses will result in an increased intensity of questioning on what steps the company has taken to reduce such losses in the future. Failure to respond adequately to these questions will result in a lack of insurability with the carrier recommending the adoption of certain actions or recommending a third party to conduct a formal network assessment before any underwriting decision can be made. In general, younger businesses are deemed to be more inexperienced and thus more likely to have losses than older businesses. Finally, an underwriter will review a company's financial condition (balance sheet, income statement, cash flow statement). Underwriters understand that companies in poor financial condition tend to "cut corners" with security often being one of the corners cut.

Third Party Exposure and Outsourcing

Underwriters recognize that our economy is based on the interdependence of networked computers. As a practical matter, a company's systems can be endangered by the systems of others that it is connected with. Underwriters inquire into what due diligence a company has made into the quality of the networks of its partners/distributors/etc systems. Company who have successfully made such assessments will enjoy lower premiums that those who do not.

Underwriters also recognize outsourcing of network security. Outsourcing can raise or lower a company's premium. Underwriters will look at the country where the outsourced services are too recognizing that certain countries pose greater risk than others. Small companies will be expected to outsource generally and will be penalized if they represent that they do all IT work internally. In contrast, large companies will be expected to have robust internal IT specialists including a chief information security officer with experience.

Membership in information sharing organizations is encouraged.

Network security quality

The most sizable premium credits and debits are reserved for the underwriter's analysis of the quality of the company's network security. While there is some difference between underwriters, most will use methods following the standards illustrated in ISO 27001. This assessment will take one or more forms: Written application for insurance, Online security assessment, Telephone calls between the underwriter's technology expert and the company's CISO and On-site security assessments. Technology, process and people will be reviewed. Among the issues that might be looked at are:

- Incident Response,
- Business Continuity and Disaster Recovery Plans, (very important)
- Vulnerability and Security Event Management,
- Data Retention and Protection, (very important)
- Vendor and Service Provider Management
- Software Security Development
- Network Security Design
- Identity and Access Management (very important)
- Cyber Regulation and Law Compliance (very important)
- Security Training

Recommendations

- Require government contractors to carry cyber-insurance. Doing this would improve cyber-security among government contractors, with a chance that private industry would adopt a similar requirement, resulting in high cyber-insurance coverage rates and a corresponding increase in cyber-security generally. The regulatory burden of added by such a requirement would be minimal, and the cost to the taxpayer would most likely be low.

- Create a Cyber Safety Act that provides safe harbors or other limitations on cyber-security liability, contingent on reasonable efforts to conform to best practices.

- Establish an antitrust exemption to promote the sharing of information and data relating to cyber-security. This actuarial data would allow the risks and benefits of a particular cyber-insurance policy to be calculated more accurately, allowing insurers to charge lower premiums and allowing and making cyber-insurance more attractive to risk managers. There would be no associated cost to the taxpayer.

- Consider a measure aimed at reducing the fear of a "cyber-hurricane" among insurers. The two best options for doing so are providing backstop reinsurance for cyber-insurers, and offering a tax deduction encouraging insurers to increase the capital reserves used to pay out cyber-insurance claims.