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. Benefits 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

Externalities represent a major barrier to improved cyber-security. Analogous to vaccination, positive externalities in cyber-security arise from interconnectedness – everyone reaps some of the benefit of investment in cyber-security by a single company, making other companies less likely to improve their own security. Similarly, negative externalities are associated with cyber-security. As with pollution, insecure software and hardware may impose some of their cost on the public rather than on the manufacture or purchaser. These insecure products are therefore under-priced and accordingly over-consumed. Both positive and negative externalities lead to consumption of cyber-security at lower than socially optimal levels.

Cyber-insurance increases cyber-security by reducing externalities. Insurers require some level of security as a precondition of coverage, and companies adopting better security practices 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. Insurers 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.
Second, the positive reinforcement offered by cyber-insurance – the ‘carrot’ – leads to more favorable outcomes than the negative reinforcement – the ‘stick’ – 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. The fear of ‘cyber-hurricanes’

---

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.

Normally, insurers purchase reinsurance as protection from very large potential payouts. Reinsurance providers prevent risk concentration – and the greatly increased potential pay-outs from a single incident associated with it – by diversifying their business globally. This technique is effective for ‘traditional’ major disasters, which involve a limited geographical area. Cyber-risk has a significant international component however, and reinsurers find it relatively difficult to avoid risk concentration. Prices for reinsurance for cyber-insurers are therefore relatively high, and this is reflected in cyber-insurance premiums. Reinsurers reduce their risk further by setting relatively low reinsurance limits for cyber-insurance, meaning that companies may not be able to purchase enough coverage to meet their needs.

Because cyber-insurance is a relatively new area, insurers are hampered by a lack of actuarial data with which to calculate premiums. Under-reporting of cyber-security incidents, caused by fear of negative publicity or of being viewed as a target for future attacks, contributes to this lack of data. As noted previously, uncertainty results in increased cyber-insurance 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. It is not economically feasible to insure against every possible contingency, and purchasing insurance against a well-known risk is easier for a risk manager to justify than expenditure directed at uncertain risks. A lack of data therefore makes cyber-
insurance appear less desirable to companies, while simultaneously increasing the price of cyber-insurance.

Two other traditional problems besetting insurance markets, moral hazard and adverse selection, have largely been resolved in the cyber-insurance market. Moral hazard, where those who have insurance behave more carelessly than those who do not, has been mitigated by requiring as a condition of coverage that companies maintain at least the same level of security as existed at the time when the policy was issued. Adverse selection occurs when insured parties have more information on risk than their insurer, and results in those who have the greatest risk having the greatest demand for insurance. Cyber-insurers avoid adverse selection by obtaining additional information on risk through expensive security audits. The downside to this approach is that below a certain level, the cost of auditing overwhelms the insurance policy itself. As a result, cyber-insurance tends to be impractical for small businesses.

Problems in the cyber-insurance market increase price and decrease demand, leading to lower than socially optimal rates of coverage and hampering the usefulness of cyber-insurance as a means of increasing cyber-security.

**Legislative Solutions**

Given the benefits that come with widespread 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 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,\(^5\) 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.\(^6\)

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.

The principal disadvantage of this approach is that the taxpayer is effectively providing a risk-sharing subsidy to insurance companies, which may be viewed unfavorably. However, even ignoring the national security

benefits of increased cyber-insurance rates, this risk-sharing may well turn out to be less expensive than picking up the pieces following an uninsured or under-insured major cyber-disaster, the cost of which would ultimately have to be met by the taxpayer. The other disadvantage of this action, the risk of market distortion, is minimized by limiting the term of the reinsurance program and limiting the program’s availability to primary insurance.

The large potential costs associated with establishing a full federal backstop reinsurance program may be reduced by using a revolving fund system, where reinsurance premiums and income from targeted taxes on insurance products are paid into the fund, and any reinsurance claims are then paid from the fund. While some up-front capital would still be required to seed the fund initially, and the majority of the fund would come from insurers’ contributions.

Precedent for such a scheme may be found in the Federal Aviation Act of 1958, which establishes a revolving fund to provide commercial aviation insurance and reinsurance, when insurance cannot be obtained on reasonable terms and is deemed necessary for commerce, national security or foreign policy.

This approach would help to reduce the cost of cyber-insurance by reducing supply cost and promoting market entry. However, because the amount of capital held in the revolving fund at any one time is relatively small, there is a significant risk that the fund would be unable to cover the large potential losses associated with a single cyber-hurricane incident, and so while

7 85 P.L. 726, 72 Stat. 731.
the revolving fund approach would reduce insurers’ fear of a cyber-hurricane, it would not eliminate it.

**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.” Specific types of insurance mentioned in the Regulations include workers’ compensation insurance and medical liability insurance.

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 considering the conditions already attached to government contracting. In addition, the magnitude of the federal government’s purchasing power means

---

9 48 C.F.R. § 28.301.
10 48 C.F.R. §§ 28.301(a), (b)
that the effects of this action would most likely spill over into private contracting, leading to further increases in coverage rates and security.

The disadvantage of this approach is that it imposes additional costs on government contractors in the form of new insurance premiums to be paid, with these costs ultimately passed on to the taxpayer. This might therefore be viewed as a government subsidy for insurance companies. However, that assumption ignores the direct benefits of insurance – principally transfer of risk, assurance that basic security standards have been met, and deep pockets to ensure adequate compensation for the taxpayer in the event of a problem – as well as the less direct benefits to national security that come from the adoption of cyber-insurance.

Use of federal purchasing power to require government contractors to carry cyber-insurance is supported by precedent, and would improve cyber-security while reducing risk and liability exposure to the taxpayer.

** Liability Safe Harbors

The federal government can promote cyber-security efforts by creating safe harbors or other limitations on cyber-security liability, contingent on reasonable efforts to conform to best practices.

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,\(^\text{11}\) which provides limitations

\(^{11}\) 107 P.L. 296, 116 Stat. 2135 (Subtitle G).
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.\textsuperscript{12}

This would decrease the supply cost of the liability component of cyber-insurance by reducing uncertainty and potential cost, and thereby help to decrease the price and increase the uptake of cyber-insurance. There is no cost to the taxpayer associated with this action.

However, the usefulness of this approach is questionable. At this time, but for a few specific industries there is generally little or no liability for cyber-security breaches. In light of this, and considering both the minimal impact this action would likely have on the cyber-insurance market and the unpopularity of liability relief, it is hard to recommend this action. However this action has some positive effects, and might be appropriate as part of a larger package of cyber-liability legislation.

**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.

\textsuperscript{12} 6 U.S.C. § 441 et seq.
Precedent for this approach may be found in the Year 2000 Information and Readiness Disclosure Act of 1998,\(^{13}\) 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.\(^\text{14}\)

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 policy holders to report cyber-attacks. This action would help to reduce the current under-reporting problem at no cost.

**Taxation**

The federal government can promote cyber-insurance by providing tax incentives to reduce supply cost and price, making the cyber-insurance market more attractive to insurers and consumers.

The federal government may provide an incentive to cyber-insurers by allowing losses from catastrophic events to be carried back for an extended period by cyber-insurers.

Precedent for this may be found in the Internal Revenue Code,\(^\text{15}\) which provides that losses resulting from product liability claims may be carried back

\(^{13}\) 105 P.L. 271, 112 Stat. 2386.
\(^{15}\) 26 U.S.C.
treated as a net operating loss for previous years – for the ten previous taxable years, rather than the normal two-year period.\textsuperscript{16}

This approach lowers risk barriers to entry in the cyber-insurance market, thereby increasing competition and reducing prices. This action should result in at most a very minimal distortion to the market, and will not cost the taxpayer any money for at least two years – the current carryback period.

However, this approach could potentially result in a significant loss of future tax revenue if a risk should materialize.

The federal government may also provide an incentive to cyber-insurers by allowing capital reserves set aside to cover expected losses to be deducted from taxes.

Precedent for this action may be found in the Internal Revenue Code,\textsuperscript{17} which provides that mortgage guaranty insurers may deduct capital reserves set aside to cover expected losses.\textsuperscript{18}

This would reduce the supply cost of cyber-insurance, and would therefore likely result in decreased prices and increased adoption of cyber-insurance. In addition, this approach encourages cyber-insurers to maintain adequate capital reserves to cover their losses, which could be extremely beneficial in the event of a ‘cyber-hurricane’.

However, there would be an almost certain loss of tax revenue with this approach. To offset this, conditions could be attached, such as requiring capital reserves set aside to cover expected losses to be held as government bonds in order to be deductible.

\textsuperscript{17} 26 U.S.C.
\textsuperscript{18} 26 U.S.C. § 832(e).
The federal government may provide an incentive to purchasers of cyber-insurance by offering tax credits to offset the cost of that insurance.

Precedent for this action may be found in the Energy Policy Act of 2005,\textsuperscript{19} which provides tax credits for purchases related to alternative energy sources and pollution reduction in order to promote development and widespread use of these technologies.\textsuperscript{20}

This approach would directly reduce the price paid for cyber-insurance and would therefore likely lead to significantly increased uptake and coverage rates, at the cost of some loss of tax revenue.

\textbf{Recommendations}

In response to the problems that exist in the cyber-insurance market, the federal government should:

- 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.

- 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

\textsuperscript{19} 109 P.L. 58, 119 Stat. 594.
\textsuperscript{20} 26 U.S.C. §§ 46, 48, 48A.
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. Of these two, the latter is preferred: it would be cheaper to administer, does not carry with it the risk of distorting the reinsurance market, and the loss of tax revenue from the deduction could be offset by requiring the deductible capital reserves to be held in the form of government bonds.