“CyberInsurance: A Market Solution to the Internet Security Market Failure”

William Yurcik[1] **David Doss**[2]

Illinois State University
Department of Applied Computer Science
Survivability-Over-Security (SOS) Research Group
<http://www.sosresearch.org>

The poor state of security on the Internet is the direct result of a market failure. Software companies have been able to institute a framework denying them liability for faulty products. In addition, time-to-market (Internet time) pressures compel software companies to release software as early as possible with lower levels of testing, if any testing at all. This combined with the increasing complexity of software virtually ensures software flaws will exist that will be exploited as security vulnerabilities. Consumers are denied information about the different levels of security for different products due to closed source (i.e., security-by-obscurity) and there is even legislation making it illegal to disclose flaws in commercial software (e.g. DMCA, DeCSS). Even if an individual consumer (“ethical hacker”) or a group of consumers (professional user group) join together to attempt to improve software products, there is little or no incentive for a software manufacturer to be responsive in developing, releasing, and distributing patches for software vulnerabilities in their products.

All would appear hopeless with corporate core assets increasingly being digital assets except it is the fiduciary duty of the officers of a corporation to protect these digital assets. Enterprises must make an unflinching assessment of their exposure to security breaches. This assessment must be a continuous process since flaws in software change dynamically and new attacks are released daily. As these on-going assessments expose potential liabilities, business leaders must decide what to do protect both their corporation and themselves. Recent Federal legislation has now instituted mandatory public disclosure of the security posture of organizations in the financial (Gramm-Leach-Blily 1999) and health care industries (HIPAA 1996).[3] In fact, there are director and officer personal liability teeth in this legislation.

Some risks of security attacks can be minimized or avoided with investment in security protection products and personnel. For those risks that cannot be avoided there are two options: (1) outsource the risk by transferring it to an external insurance company or (2) assume the risk internally via self-insurance or policy deductions. Since software security risk is relatively new, there are major impediments to risk management via insurance: (1) there is not enough data and audit procedures to quantify risk and loss potential; (2) to share this risk for affordable premiums, a wide market base must be established where is there is no base at present; (3) after 9/11 worst case terrorist scenarios are very large; and (4) insurance is not a priority of a typical technology company.

[1] corresponding author and workshop participant, Asst Professor and SOS Group Principal Investigator, Email: wjyurci@ilstu.edu telephone: 309-556-3064 fax: 309-556-3864

[2] Associate Professor and Associate Department Chair, also retired Lt. Commander U.S. Navy S.S.N.

[3] with some exceptions, this can be discussed in more detail at the workshop.

In addition to normal insurance coverage for natural disasters, traditional insurance companies have begun to issue nontraditional coverage policies to manage the risk of security breaches. These cyberinsurance policies range from coverage against hacker intrusion damage, virus infections, denial-of-service attacks, attacker extortion, identify theft, and misappropriation of proprietary data.

Small organizations that cannot afford to transfer the risk due to premium costs may decide that (1) the possibility of risk from a software security attack is low enough to assume internally, or (2) a catastrophic outcome has a low enough probability to risk exposure, or (3) a security event over an insurable threshold will be unrecoverable so insurance does not make economic sense (company cannot recover and will file for bankruptcy).

For large organizations that can afford to transfer risk externally to an insurance company, methods include solid contractual relationships, enforceable limitations on liabilities, and clearly defined warranties. There are two major actuarial problems to risk management of software security via insurance as alluded to previously:

- risks must be tangible so that they can be predicted, avoided, or mitigated

- potential loss must be identified and quantifiable

The core of the problem is that software security attacks are hard to identify (new attacks are by definition unknown) and if all possible attacks were possible to identify it would only be for a moment in time due to their dynamic nature. Potential loss is actually easier to address since analogies to natural disasters can appropriate except when considering loss of intellectual property – what is the loss of proprietary data not protected by trade secret laws.

Given that these major insurability problems are not intractable, cyberinsurance is a viable and attractive market solution to the software security problem: (1) insurance companies will facilitate standards for best practices and insurability in order to develop cyberinsurance products; (2) pressure on organizations to reduce insurance premiums provides an incentive to reduce their exposure to software security liabilities in tangible ways including demand for security information about products and “safe” software products themselves; (3) pressure on software companies to deliver “safe” products to a market demand or assume liabilities with valid warranties; and (4) pressure on software engineering practices (requirements, development, and testing) to improve in order to provide “safe” products and decrease exposure to warranty claims.

As our unique contribution to the workshop, we have data from more than a dozen different business insurance companies that provide an insight into the current state-of-the-art in cyberinsurance products. We have also had interaction with the largest personal insurance company in the U.S. (whose headquarters happens to be in the local vicinity) since, from our perspective, the next logical step is consumer insurance for home computers that have always-online broadband connections.[4]

[4] Unfortunately, this insurance company has not agreed to go on record for reasons that we can discuss at the workshop.