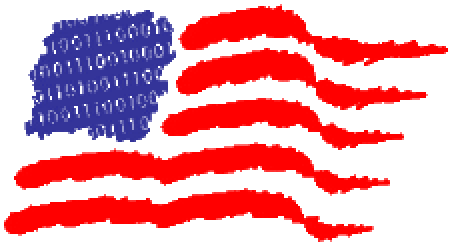

The National Strategy for Securing Cyberspace

Version 5.1

Defending America's Cyberspace

Insurance Sector

The insurance sector – in particular, those insurers that provide insurance to cover "cyber losses" -- can play a vital role in protecting the nation's critical infrastructure from cyber risks. These insurers are in the unique position to educate and motivate companies to reduce their exposure to potentially catastrophic cyber-related losses, as well as to help protect companies from serious operational and financial impairment should they experience a cyber loss event. Preventing and mitigating cyber losses, especially a mass event impacting critical systems or a multitude of companies, is essential to the smooth operation of today's system-reliant economy and avoiding an undue burden on the taxpayers, who may be called upon to bail out companies forced to the brink of insolvency.

The insurance sector has years of experience in helping companies assess and manage their risk to an incredibly broad range of volatile exposures. The industry's technical expertise has lead to practices that have helped to reduce the risk of workplace injuries, auto accidents and consumer product-related injuries, to name a few examples. Insurance companies have also provided guidance in management responsibilities in numerous areas such as environmental and employment related legal obligations. Insurers often are the first to see an emerging pattern of loss vulnerability due to their close relationships and regular contacts with clients, as well as their loss experience data collection methodologies. As a result, insurers are among the first to develop and promote new best practices and standards through general educational and awareness programs as well as specially designed training programs to individual corporate customers.

As with other types of exposures, companies that employ good risk management programs and standards that decrease their vulnerability to cyber-related losses may be rewarded by greater access to insurance products, lower insurance costs, and other preferred insurance terms and conditions. This could lower a company's cost of risk, reduce its exposure to litigation brought by injured parties, as well as angry shareholders and regulators, and even generally improve its operational efficiency. When a company improves its risk profile, it may also become a better investment in the eyes of shareholders as well as lenders.

Unfortunately, no matter how much companies spend on IT security, they will still not be fully protected from hackers, criminals and terrorists who chose to wreak havoc on corporate e-commerce and information systems. These individuals are constantly seeking ways to infiltrate and compromise company systems. As soon as a new type of security system is created and installed, they will find ways to get around the safeguards. While companies would be foolish not to invest in these systems, they also would be foolish not to have a safety net should a security failure still occur.

Emerging cyber insurance products will provide the financial mechanism to enable companies to continue and restore their operations as soon as possible following a disaster. In addition to providing this mechanism, insurers possess the expertise to assist their clients to plan for such disaster and implement those business continuation and recovery plans quickly.

Physical and other cyber threats facing our nation, both domestically and internationally, show no signs of abating. The expanding universe of cyber threats have led the insurance and reinsurance sectors to focus on education and awareness of cyber threats and provide guidance in support of superior cyber risk management techniques, with emphasis in the following areas of risk management decisions:

1. Identifying and assessing risk and the potential impacts that e-business activities present to organizations;
2. Identifying common obstacles encountered when applying traditional insurance products to these new or magnified exposures;
3. Leveraging the cyber risk assessment process to support decisions to mitigate known vulnerabilities, to defend against threats that are likely to disrupt business activities or impair the financial and reputational position of the organization;
4. Determining how the purchase of specialized cyber risk transfer insurance coverage can provide the necessary balance sheet protection to their organization;

5. Design and implement business continuation plans, including decisions to purchase cyber risk transfer products that provide funds to implement those plans;

While the cyber insurance marketplace is still a niche market for many insurers, it continues to grow in terms of the number of insurers and customers. However, several barriers have prevented the marketplace from growing as quickly as it could. These include lack of: (1), awareness of the value of insurance, (2), a sizeable reinsurance marketplace to support insurers products, and (3), available data to price and model cyber risk exposures. With these in mind, the following recommendations have been proposed:

Sector Action #1:. ***The insurance sector should consider providing specialized cyber insurance product.*** These products typically include broad financial risk loss transfer protection directed toward cushioning the financial impact of damage to, destruction of or denial of access to web sites, systems and data, and any resulting litigation, among other exposures. These products also provide post-incident support funds for the repair and reconstruction of web sites, systems and data and crisis communication services to restore confidence in consumers, employees, shareholders and other stakeholders of the insured company. Finally, in concert with providing this insurance, insurers should consider incorporating affordable loss prevention services. Specifically, the services provided can include:

- *Assessment and Understanding*: Analysis. Assessing the underlying processes, procedures, people, technology and cyber-financial management.
- *Loss Prevention, Education, Awareness and Business Recovery*: Taking proactive steps to strengthen our customers' capacity to prepare for, defend against, and recover financially and technologically from enterprise wide and systemic cyber attacks.
- *Detection and Response*: Building and implementing strategies for detection, early warning and incident response to cyber attacks on the technological tools, software, data, critical infrastructure, proprietary network configurations and intellectual property of our customers.
- *Reconstitution and Restoration*: The insurance and reinsurance sectors play a vital role to fund our customers' ability to recover and restore technological and financial services and functions to their normal state of operation.
- *Financial Risk Management*: The insurance mechanism provides the balance sheet protection to our customers so as to withstand and smooth the unexpected, catastrophic financial impact of cyber attacks.

Sector Action #2: The government should encourage the use of insurance as well as other risk management techniques to mitigate the potential of cyber losses from occurring in the private sector and mitigate the financial losses of a cyber attack if one does occur. Companies whose products or services directly or indirectly impact the economy or the health, welfare and/or safety of the public should be encouraged to purchase specific cyber risk insurance programs from financially strong insurers.

Sector Action #3: Develop an awareness campaign through a joint public/private partnership for education and outreach to directors, officers, and key stakeholders of the publicly traded enterprises. Directors should take an active role in the management of cyber risk just as they did during the Y2K crisis. The security of the nation's critical infrastructure cannot be obtained without active involvement of companies boards of directors. Directors and offficers liability (D&O) insurers can assist in the education of boards and, when appropriate, modify applicable terms and premium of their D&O policies to be consistent with the level of the board's management in this area.

Sector Action #4: Partner with the Executive and Legislative Branches to remove the legal and economic obstacles to robust information sharing between the public and private sectors, and within the private sector, essential to the security of the nation's cyberspace and critical infrastructure. These obstacles include the potential application of Freedom of Information Act to information shared with the public sector and federal and state antitrust laws to information shared among private sector companies and the potential for legal liability arising out of disclosing such information. Lessons learned from legislation enacted for Y2k disclosures can be especially useful. Accordingly, Congress should be encouraged to enact disclosure legislation on FOIA, antitrust and liability issues similar to those passed for Y2k.

Sector Action #5: The private and public sectors should collaborate on and fund research to develop the data and risk models necessary to quantify and control cyber loss exposures, and hence, enable insurers to adequately price and offer cyber insurance products. This information is particularly important to reinsurers, who would protect insurers from the financial impact of a large cyber exposure emanating from one or more insureds. Without a robust reinsurance marketplace for cyber risk, insurers will either not enter the cyber insurance marketplace or will greatly restrict the scope of the coverage they offer.

Quantification of cyber risks is vital for the efficient allocation between expected losses due to known cyber vulnerabilities versus unexpected, infrequent and potentially catastrophic, systemic, cyber loss events.

Quantifying the economic consequences of cyber risk loss events creates the opportunity for scarce homeland security resources to be efficiently allocated to those infrequent, unexpected, events that threaten the nation's economic and national security.

Accordingly, Congress should appropriate sufficient funds to the appropriate federal agencies to institute a continuous process of data collection, as well as promote research and development in the areas of network security risk and risk management.

As government is a likely repository for myriad components of useful data, albeit scattered throughout its vast infrastructure, collaboration with insurers and other private sector participants is necessary to identify existing insightful data. Once data is mined and scrubbed, the government can assist insurers with developing a methodology to model cyber exposures, similar to the models insurers and reinsurers have developed for traditional physical perils. This assistance has become far more critical post-9/11, since already limited technical resources have been diverted to quantifying and modeling the suddenly critical risks of physical terror.

Sector Action #6: The Federal Government with Insurance sector support, should encourage education and enhanced awareness of both the risk and the value of a robust risk transfer insurance market for cyber inasmuch as both can be more quickly achieved with public sector support. Accordingly, both the Executive and Legislative branches should be encouraged to voice support for a cyber-insurance market in manners and in forums as and when appropriate.

Summary:

With the continued partnership of the Federal Government and the critical infrastructure sectors, the insurance and reinsurance sectors can focus on the implementation of the stated sector actions.

We believe that the Executive Branch can set the appropriate tone at the top for the boards of directors of publicly traded companies by encouraging boards and executive management to make cyber security a subject of continual and active management attention. We also believe that the competitive insurance market-mechanism will increasingly value and reward superior cyber risk management on the part of private organizations as technology becomes more vital to the delivery of their goods and services.

In an effort to implement these sector actions, we have identified four overarching principles to guide the insurance and reinsurance sector's efforts to mitigate and transfer cyber risk in support of achieving the goal of national and economic security:

- *The insurance and reinsurance sectors, specifically, those in the business of insuring cyber risk, in partnership with customers, brokers and government should identify and assess cyber threats and known vulnerabilities to loss and/or service disruption that that gives rise to potentially catastrophic systemic risk.*
- *The owners and operators of our nation's critical infrastructure, and those companies who directly or indirectly impact the health, welfare, or economic viability of the nation should participate in efforts to achieve a consistent level of infrastructure assurance by applying sound risk management, business and security practices and by instituting an action plan which incorporates optimal levels of risk retention, risk mitigation and risk transfer.*
- *Owners and operators of our nations critical infrastructure should be encouraged to mobilize to defend and protect against systemic cyber risks, including cyber terrorism in a coordinated matter.*
- *The Federal government should work in partnership with our customers (the owners and operators and other third party service providers), as necessary, to defend and respond to systemic cyber attacks that threaten to disrupt the nation's economic security.*

This framework reflects the insurance and reinsurance sector's continued focus as a market driving force to educate, encourage, and reward sound business practices, information security principles and superior cyber risk management policies.