



## Cyber Insurance Analysis from Treadstone 71

Although 1.5 years old, the CIP Report on Cyber Insurance still rings true with respect to several areas. Before discussing these areas, let's take a look at the general theme of the report.

According to George Mason University, the market for cyber insurance is at \$350M. Many organizations use cyber insurance as another layer of defense in their efforts to combat threats to their computing environments. As data grows exponentially and the systems used to house, process and transmit this data expands in equal amounts, so too does the level of risk.

Insurance firms use historical data to predict risk, mining actuarial tables gathered from proven statistics. These same firms find it very difficult to provide a comprehensive product when the data available is not complete and the risk is difficult to measure. What the insurance firms face is exactly what information security and assurance professionals face; the inability to accurately predict probability of occurrence and subsequently, the associated risk. Cyber insurers have not progressed very quickly due to the lack of industry data. Insurers look at historical data to predict future issues. Without this, they are betting blind. Sites like [datalossdb.org](http://datalossdb.org) can provide some of this data but this is only what is reported. Cyber crime statistics are still limited since only what is known (not necessarily reported) is captured. Risk models are difficult to create without the necessary data.

Cyber Insurance covers many different areas such as data theft, external hacking, 1<sup>st</sup> and 3<sup>rd</sup> party risks, internal sabotage and theft, computer malfunctions, web content liability, viruses/malicious code, copyright infringement, business continuity, crisis management, network outages, network congestion, and other areas related to technology (George Mason University School of Law, 2007). These areas protect against liability lawsuits related to the loss, disclosure, modification, destruction, and or interruption of systems and information. There are federal regulations and nearly 45 state laws concerning data and data breaches. Many federal regulations have been in a hold pattern for several years (George Mason University School of Law, 2007) forcing states to establish laws of their own.

Like most insurance companies, reinsurance is important to sustainability. Reinsurance is insurance for the insurance companies should losses exceed forecasted or expected yearly totals.

### ***Liabilities and Risks***

The liabilities and risks that drive companies to purchase cyber insurance are no different than the issues information assurance professionals face. Organizations face liabilities that can impact shareholders and investors for failure to identify, and report internal controls deficiencies and weaknesses. The failure to create and maintain regulatory compliance programs and the inability to execute due care towards third parties and customers are liabilities that can lead to risks such as civil

and class action suits. Regulatory enforcement actions and unwanted external audit activities can lead to adverse publicity and reputational injury. In a cascading fashion, the suspension of business activities due to data loss or disclosure such as the loss of trade secrets or intellectual property can have long term effects on any firm.

## ***Traditional Insurance***

The reason we need cyber insurance is because traditional insurance does not provide strong coverage for civil suits arising out of security and privacy breaches nor does it provide any coverage for regulatory enforcement actions. There is very little in the way of case law for precedents in technology-related insurance claims. It is also not uncommon for policies to come with four or five pages of single-spaced exclusions to the coverage. There are several areas where traditional insurance falls short (George Mason University School of Law, 2007):

- No coverage for defense of a regulatory enforcement action
- Criminal acts exclusion may bar coverage for security breaches related to employees
- Data protection issues may fall outside the definition of professional services
- Privacy coverage does not address the full exposure related to gather and use PII
- Coverage is not worldwide
- Electronic data is not considered tangible property
- Malicious code and computer network attacks are excluded under property policies
- Crime policies cover stealing things not data

## ***Cyber Insurance***

Most cyber insurance is geared towards high compliance industries such as healthcare and financial services with limits up to \$50M in coverage. Coverage can include:

- Third Party Privacy Suits
  - These is monies the insured is obligated to pay (including defense costs) as a result of claims made as a result of a breach of privacy under defined regulations such as HIPAA, GLBA or state privacy laws.
- Employee Privacy Civil Suits
  - This is no different than the Third Party Privacy policy except the plaintiff is an employee.
- Regulatory Fines and Penalties
  - Should a privacy breach be proven, this covers defense and payments of fines.
- Crisis Management
  - Public relations costs associated with brand protection related to a claim as covered under the policy.
- Network Security Liability
  - Liability and costs for claims associated with attacks caused by security failures including data loss, identity theft, negligent transmission of malicious code, and denial of service

issues. This also covers insiders and an interesting section covering 'failure to warn' obligations as required by many state laws such as SB1386 from California.

## ***Analysis of Coverage and Premiums***

Some analysis that may be of interest here is that the amount of coverage sought was \$50M in coverage in order for the program to be effective. With \$10M set aside for incidents described above, the company sought assurances through cyber insurance to cover over and above any cash reserves. What was discovered:

- No insurer at the time offered over \$10M in coverage;
- One of the insurers listed used one of the other insurers to supplement the \$10M coverage;
- Programs differed greatly in coverage's' offered and no one insurer covered everything we sought;
- Each provided questionnaires for IT and Security teams to complete;
- Not all required onsite assessments; those that did offered it as a cost to validate and prove findings prior to a final premium determination;
- The onsite assessments could be from a third party with costs ranging into the hundreds of thousands depending upon corporation size and locations;
- The questionnaires were not very expensive and not related to an industry standard such as ISO27001/2;
- ISO27001 or SAS 70 Type II certifications had no bearing on the policy or premium;
- One insurer provided only up to \$5M in coverage;
- Terrorism was an afterthought and an add on for up to 5% of the total premium with many exceptions;
- Coverage for business continuity was a completely separate policy;
- Since this review, one of the insurers no longer offers this type of coverage due to financial problems associated with the current financial crisis;
- If you wanted \$50M in coverage, you had to stack policies from multiple vendors and pay over a million dollars in premiums;
- Premiums average around \$400K for a \$5M policy (with many exceptions and exclusions).

## **Summary**

Analysis would indicate that cyber insurance is still a growth area in need of years of historical data, data that can be related back to regulations and statutes. Since the creation of regulations and statutes is still a moving target, it is difficult for insurers to adequately predict risk and offer cost effective solutions that cover enough of the areas required by companies seeking another layer in their defense-in-depth, security strategy. Historical data on actual breaches and subsequent losses is difficult to gather since it is assumed that many organizations do not disclose their breaches. Since many breaches are not disclosed, costs cannot be associated to the breach since the non-disclosure leads to a lack of fines and regulatory enforcement.

Additionally, the number of listed exceptions and required definitions indicated a lack of understanding of the threat/vulnerability environment and overall risk issues associated with insuring IT environments.

Legal precedent is very limited since there is not much in the way of case law available. Cases such as TJX and the ongoing Hannaford case are kept secret in many ways due to the potential embarrassment issues associated with alleged negligence by the target companies. This further limits the availability of information for insurers upon which to determine risk. An interesting offering from one vendor is coverage for 'failure to warn' in the event of a breach. Based upon what we know of the marketplace, this option could be attractive to many firms who do not disclose in a timely fashion or choose not to disclose at all.

Depending upon your cash-on-hand and your overall coverage requirements, policies may not be broad enough or offer enough coverage based upon the premiums. The overall risk should be examined for every corporation to determine if cyber insurance has matured to the point where it is cost effective with the appropriate amount of coverage.

On the other hand, large companies have security budgets that range in the millions. Spending from \$500K to \$1M could add a significant layer of protection that comes from a budget other than IT or Security. This coverage could provide a level of comfort that should such a breach occur, dollars are available. Should the security posture in question be at issue, the target corporation may not be able to adequately pass a risk assessment performed by the insurer therefore rendering the premiums too high and the operation unattainable.



Copyright 2002 **Treadstone 71** [info@treadstone71.com](mailto:info@treadstone71.com) 1-888-687-8450 Office - 508.519.0363 Fax

---

George Mason University School of Law. (2007, September 17). *Critical Infrastructure Protection Program - Cyber Insurance*. Retrieved January 21, 2009, from Critical Infrastructure Protection Program - George Mason University School of Law: [http://cipp.gmu.edu/archive/cip\\_report\\_6.3.pdf](http://cipp.gmu.edu/archive/cip_report_6.3.pdf)