

Friday, February 1, 2008

Cyber insurance can eliminate insecurity about IT protections

BY TRAVIS CRABTREE
SPECIAL TO HOUSTON BUSINESS JOURNAL

The media is rife with sensational stories of hacked computer systems, virus attacks, Web outages, copyright infringement, personal and private data theft and other information technology-related horror stories. In response, many insurance companies have developed cyber-insurance programs. The market and courts are still trying to determine whether this is a necessary evil in evolving business times or the undercarriage protector of the business insurance world.

A new cyber policy could be overkill because some losses may already be covered. An insurance broker and a lawyer familiar with insurance and technology losses can determine what risks are already covered and what is not. For example, does the dishonesty and fraud policy cover data sabotage from a disgruntled or recently fired insider? What if the fired employee from IT takes sensitive data with him? This is nothing more than theft which, unless expressly excluded, may be covered by dishonesty/theft coverage. Do the general commercial property terms cover invasion of privacy suits because of disclosed personal data or violations of federal or state law? Is "intangible property" excluded from the property coverage?

Often, older policies provide broader coverage with less emerging technology risks excluded because of the failure to adapt to modern hazards. Several courts have ruled that data loss is not covered under standard policies excluding intangible property. On the other hand, when renewing policies, an insured should watch

for new technology-related exclusions which should result in lower premiums for the shrinking coverage when demanded by the astute insurance purchaser.

Some insurance advisers recommend the coverage for smaller companies. They are more likely to rely on others for things such as Web hosting, credit card payment processing, tracking of inventory and sales data. The insurance provides security against the reliability, or lack thereof, of outside vendors, that may not be provided for in the typical business loss coverage. Many larger companies handle these functions in-house and therefore manage their own risk or mandate coverage from their outside vendors.

Because needs vary, prospective purchasers and insurance companies often do a risk analysis. Like smokers and life insurance, cyber-insurance policies are more expensive if the company does not have basic protections like firewalls and anti-virus safeguards. The more complex (and often larger) the business, the more in depth and costly a pre-coverage analysis can be. The cost of the insurance will be less for the widget manufacturer doing basic e-commerce transactions than the widget message board operator that collects intimate personal data for the passionate widget community. As both the insured and the insurer become more familiar with risks and losses, the process is being more streamlined.

While there are not standard market or filed rates like with other traditional coverages, in the summer of 2007, AIG was selling a small company cyber-insurance policy with annual premiums of \$1,000 for \$100,000 in coverage with a \$1,000 de-

ductible. Some analysts say that, because there is insufficient actuarial data on losses, the insurance companies have included a premium to the policies to hedge for the unknown. These same analysts say that, as the market matures, the pricing will get better as insurance companies will decrease the premium bump created by the dearth of data and claims history.

According to the 2007 Computer Security Institute survey (available at www.GoCSI.com), the average annual technology-related loss reported by U.S. companies in various industries and of various sizes doubled, from \$168,000 in 2006 to \$350,424 in 2007. Financial fraud overtook virus attacks as the source of the greatest financial loss with system penetration by outsiders on the rise. Meanwhile, only 29 percent of respondents claimed to have some type of additional cyber insurance.

As a rule of thumb, a concerned business owner should do some basic self-study to determine if cyber insurance should be considered. If a server or Web site crash, or the failure of the credit card processing service for three days, or the disclosure of data stored on the company network is not covered, the company needs to analyze whether such an incident will sink the company. If so, the cyber policy makes sense. If it would merely be a minor inconvenience that can be handled with minor adjustments and minimal losses, then cyber insurance may be as helpful as blizzard hazard coverage for Houston businesses.

Travis Crabtree is a litigation attorney with Looper Reed & McGraw (www.lrmllaw.com) who focuses on emerging media and Internet issues.