

CYBERINSURANCE: SINGING IN THE RAIN

By Sharon D. Nelson and John W. Simek

© 2005 Sensei Enterprises, Inc.

The premise is simple:

If you are going to walk outdoors in the rain, you carry an umbrella.

If you are going to run a business using technology, you carry cyberinsurance.

Most lawyers have no idea how vulnerable they are to technical disaster. Surveys have shown that most law firms believe that they are in fact covered by cyberinsurance when they assuredly are not! If a fire burns down your building, your conventional insurance policy will replace your computers. But if you were foolish enough not to have offsite data storage, what about damages stemming from the loss of your data? In the overwhelming majority of cases, no way Jose. You are on your own. Likewise, most policies will not cover damages caused by hackers, viruses, worms and data theft by disgruntled employees or identity thieves.



You have only to read the newspaper or listen to the news to know just how prevalent the dangers are. Just before we went to press, over 40 million (**40 million!**) credit card numbers had been purloined by data thieves. Mastercard and VISA are scrambling to scrub up after the mess and prevent a PR and identity theft disaster. They are on well trod ground, following in the wake of ChoicePoint and Lexis-Nexis, among many others. If the road behind is scattered with victims of cyber-disasters, the road ahead is sure to be chockablock full of them. The one thing we all know about computer security is that there's no such thing as a secure computer!

In the late nineties, insurance companies such as American International Group, Lloyd's of London and Marsh became the pioneers of cyberinsurance. At the time, there was a splash in the press and the Yankee Group predicted in 1999 that cyberinsurance would boom in coverage to \$7 billion in 2004. The market remained unimpressed. Currently, the Insurance Information Institute is predicting that cyberinsurance coverage may reach \$3 or \$4 billion by 2007. The early cyberinsurance pioneers have been joined by such firms as the St. Paul Companies, Zurich Northern America, Chubb, CAN and MediaPro.

However, the cyberinsurance business has doubled annually in 2003 and 2004. Businesses have begun to wake up – and in light of all the recent cases of data theft (ChoicePoint, Lexis-Nexis, VISA, MasterCard and scores of others), it seems certain that a lot more businesses are going to be checking out cyberinsurance.

The logic behind cyberinsurance is irrefutable. There are four ways to deal with risk: you can accept it, reduce it, ignore it or transfer it. It is beyond the pale to think that lawyers will accept the risk or ignore it. Clearly, law firms should reduce the risk by doing whatever they can to secure their data and their infrastructure. After that, they are well advised to use cyberinsurance to transfer the risks associated with today's technology to someone else.

What does cyberinsurance cover? By in large, there are six kinds of coverage currently available and they are split into first party damage (damage you suffer) and third party damage (damages that someone else suffers for which you are liable). Below are the kinds of coverages most commonly offered.

- **First party business interruption** covers revenues lost when your computing environment is down, whether through a network intrusion or through some sort of accident. Large scale electrical outages are commonly excluded.
- **First party electronic data damage** covers the cost of recovering data damaged by viruses, worms and Trojans as well as by a hacker or disaffected employee.
- **First party extortion** covers the ever-increasing frequency of ransom demands by hackers who may have stolen data or claim the ability to damage it, and furnishes the funds and resources for their capture and prosecution.
- **Third party network security liability** covers losses due to the theft and misuse of data (such as the credit information stolen from ChoicePoint and used for identity theft). Generally, such policies offer reimbursement to the victims as well as the business' recovery cost.
- **Third party (downstream) network liability** covers judgments from lawsuits filed by those harmed by such things as denial of service attacks and viruses.
- **Third party media liability** covers infringement and liability costs stemming from Internet publishing, including websites, e-mail, instant messaging and chat rooms.

The next logical question is how much you will have to ante up for this new-age insurance. No question about it – cyberinsurance is expensive. It is wise to shop around, and more than usually, because there's no such thing as standard pricing, at least so far. As a sort of benchmark, figure on paying \$12,000-\$20,000 per each million dollars of coverage if you need both first party and third party insurance. If you only need liability insurance, the costs may be more like \$7,000-\$10,000 per million.

As all lawyers know from filling out applications for malpractice coverage, the process of applying for insurance is arduous. Typically, applications for cyberinsurance will run 10-20 pages. As one might expect, the economies of scale work in favor of large law firms,

since they are more likely to have data security mechanisms in place and therefore be eligible for discounts. Small law firms may have to pay two to three times what they are paying for regular business insurance, when all is said and done. However, the costs may not seem so high when compared to malpractice insurance, which itself carries a steep price tag.

Small law firms may be able to perform their own security assessments, but large firms will almost certainly be required to have a third party perform the assessment. Companies that provide this sort of assessment include NetDiligence, TruSecure, Counterpane Internet Security, Internet Security Systems, PricewaterhouseCoopers, Ernst & Young and Deloitte Touche. Some of these firms will use their own security standards and other will use the ISO 17799 security standards.

Ten years from now it will likely become standard practice to carry cyberinsurance. In the meantime, those who do not carry it remain vulnerable. At the very least, lawyers should be cognizant of the dangers and should investigate the cost of protection. A cyber-catastrophe could devastate a law firm – is that a risk your law firm can live with? Witnessing some major companies being brought to their knees by security losses and data intrusions has been most instructive – and alarming. The time to get your cyberinsurance may be now, before disaster strikes. It's a little more complicated and expensive than grabbing an umbrella before a stroll in a spring shower. But when you are well protected, you too can enjoy singing and “hoofing” along the sidewalk even if it pours. What a glorious feeling. You're happy again.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology and computer forensics firm based in Fairfax, VA. 703-359-0700 (phone)
www.senseient.com