

Edward A. Schirick, C.P.C.U., C.I.C., C.R.M.

Cyberspace — Risks in a Networked World

Thomas L. Friedman in his The New York Times best selling book The World Is Flat, suggests that the evolution of information technology, which created cyberspace, is among the events which flattened the world, literally changing the balance of economic power among countries throughout the world.

Cyberspace, as everyone knows, is the on-line world of computer networks that has facilitated communication, accelerated the transmission of data, and revolutionized the way the world works. The long-term impacts of information technology remain to be seen. But one issue is now quite clear. Businesses will seek competitive advantages in the marketplace for goods and services by developing new ways to use the Internet more effectively. Most businesses will require employees to possess technical computer skills in order to succeed in the networked world of the future.

Camps have been quick to recognize the value of the Internet as a marketing and communication medium. Other businesses have been slower to respond. The fact is there are individuals and businesses all over the world finding new, largely beneficial, but sometimes destructive ways to use cyberspace.

Vulnerabilities

Some people see cyberspace as the new frontier. Naturally, with anything new, there are some uncertainties and risks, which may not be clear at the beginning. This has certainly been the case with the Internet. As this new online world has developed and expanded many new risks have evolved (viruses, worms, etc.). Unfortunately, some of the risks and their consequences have caught users unaware.

Consider the identity theft issue for example. How much of your personal and

business information is accessible online? Even the pioneers and leaders in cyberspace were confronted with unanticipated risks. Do you recall all of the patches Microsoft had to develop to address security issues within its various versions of the Windows operating system?

Risk Management in a Networked World

What Are Some Risks?

Risks can be categorized generally into First Party (Your Camp) and Third Party (Others).

First-Party Risks

Do you remember how you communicated and conducted business before e-mail and the Internet became so prominent in our daily lives? Fact is we have become very dependent upon our computer networks for business. Most of us can tolerate losing the use of our computer networks, or our Web site for a brief time, but a prolonged outage might jeopardize some businesses today.

Equipment Malfunction or Breakdown — Repair Expense — Loss of Income

What are the sources of the threats and risks that might cause your computer equipment to malfunction or breakdown? Generally, these threats/risks can be characterized as internal and external. Examples of internal threats/risks include manufacturing defects (usually immediately after the warranty

expires); unauthorized downloading of software by employees (which can impact system performance); vandalism (pollution or destruction of data) by disgruntled employees; and failure to maintain appropriate security for your system's resources among others.

Examples of external threats/risks include damage by lightning, power surges, brown-outs, viruses, worms, vandalism by hackers outside your organization, and other pollution of your systems by programs which spy on your systems and slow down their performance.

Third Party Risks — Acts and Omissions

Examples of threats/risks to third parties may involve inappropriate actions by camp staff, such as illegal downloading and use of copyrighted material (copyright infringement), or unintentional trademark infringement in advertising, and potential for libelous statements in electronic communications (e-mail, in official camp-sponsored chat rooms, or on camp bulletin boards).

Other third party risks include failure to protect private/confidential information about campers/parents, transmission (via e-mail) of threatening, obscene, or harassing material by campers or staff, and unauthorized creation of blogs by employees or campers. All of these actions or omissions and more may create hidden liabilities for your camp.

Other Issues

Protecting children from physical and sexual abuse has become a high priority for American society. Some of the knowledge we have about abusers is being changed by the online world. This will require new risk management approaches.

There has been a flurry of television news reports recently about predators

stalking children over the Internet. Many of these would-be abusers of children have positions of responsibility and authority in our communities, in government, and law enforcement. Most have no criminal records. Likewise you will not find their names listed in any registry of sexual abusers. They may not be known by the child, except through the virtual reality of the Internet. Under these circumstances, it is clear that businesses who wish to prevent physical and sexual abuse of children in their care must do more than just secure a criminal background check on prospective staff.

But, why do these predators feel comfortable stalking children in cyberspace? In my opinion, it is because the Internet creates a feeling of anonymity and security. Experts who have studied the motivation for abusers indicate that one of the reasons they act is they feel they won't get caught. How do you guard against a camper being stalked by a stranger over the Internet? How do we prevent a camper from being befriended by a staff person/predator who subsequently stalks them over the Internet after camp is over? Are there other concerns in light of the changing online world?

Awareness and involvement by camp management and coordination with parents is one approach that makes sense. The good news is law enforcement is aware of these predators and the risks they present to the safety and security of children. In addition, law enforcement is taking innovative action to reduce the vulnerability of children in this new online world. Children must also be educated about these risks. Parents and those who act in place of parents must be vigilant and knowledgeable. What is your plan?

Don't Assume Your Camp Insurance Will Respond

Your camp's first-party (property) insurance may respond to some of the first-party risks and losses your camp may suffer, but don't assume it will. Check into the scope of your computer insurance coverage to determine if mechanical breakdown is a covered peril. How does your insurance respond to damage from lightning, power surge, and brown out? How big is your deductible? Do you have replacement cost protection? Does your crime insurance respond to computer fraud, including electronic funds transfer fraud? How does it respond if your computer network is infected by a virus?

Liability insurance protection against third party cyberspace threats/risks is incomplete. Some versions of the commercial general liability policy covering camps specifically exclude personal injury (including libel) arising out of chat rooms and bulletin boards, for example. Likewise, some potential third party liabilities, such as failure to protect private camper and camper parent information, may involve financial losses. These losses are most likely not covered by the commercial general liability policy, which is designed to respond to bodily injury, property damage, personal, and advertising injury liability claims.

Recap

If you haven't taken the time to consider the threats/risks to your computer network resources take the time to do so in the very near future. Impacts may involve first-party (your camp) or third-party (others) interests. Realize that the risks/threats may be internal, and others may be external to your camp.

Your camp insurance program may respond to some first-party and fewer third-party threats/risks. Find out where you may be exposed. After you have identified the

risks, take appropriate action to reduce the risk of damage or destruction of your camp computer network resources. Consider establishing procedures for the use of the Internet, prohibiting those actions that might create third-party liabilities. Investigate transferring these third-party risks via insurance or other contractual risk methods.

In Conclusion

Discuss cyberspace risk management issues with your insurance brokers and computer system consultants or advisors. Partner with parents when appropriate. Integrate your — cyberspace risk management practices into the rest of your camp risk management plan. Be aware of evolving cyberspace risks and keep your camp risk management plan up to date. ■

Edward A. Schirick, C.P.C.U., C.I.C., C.R.M., is president of Schirick and Associates Insurance Brokers in Rock Hill, New York, where he specializes in providing risk management advice and in arranging insurance coverage for camps. Schirick is a chartered property casualty underwriter and a certified insurance counselor. He can be reached at 845-794-3113.

Reprinted from *Camping Magazine* by permission of the American Camp Association
© 2006, American Camping Association, Inc.