EDWARD A. SCHIRICK, CPCU, CIC, CRM

Computer Network Security — Evolving Risks

According to some experts, 2012 could be the worst year ever for computer network security breaches. In 2011, major companies were victims of massive computer network security breaches. If you listen to the news surrounding this issue, the impression you might get is that only big, publicly owned companies like SONY and Citibank are being affected.

The truth is companies of all sizes are suffering consequences from network security breaches, and if 2011 is any indication, the risk of security breach is growing and changing rapidly. Small and medium-sized businesses are also targets of increasingly sophisticated cyber thieves. Camp computer networks are at risk.

Establish an Electronic Information, Privacy, and Security Policy

Focus on managing this evolving risk by establishing an electronic privacy and security policy. Many camps already have some type of policy governing employee use of the Internet, e-mail, Facebook, and other social media. This is a good start. If these policies haven't been reviewed in a while, take some time to review these guidelines before summer. Expand on these to include some broader developing risks.

The following are some examples of issues to be addressed in your updated policy. This list is not exhaustive; consider including other risks — especially those which may be unique to your camp.

1. Use of electronic communications systems; security and privacy of electronic information; use of passwords; structure for passwords; prohibitions on downloading personally identifiable information to notebook computers or flash drives; guidelines for camper contact outside of camp.
2. Use of camp e-mail; no expectation of privacy for employee e-mail communications sent on camp e-mail systems; prohibition of offensive, hostile, discriminatory or intimidating content.
3. Internet, Intranet, or Extranet to be used solely to facilitate the conduct of the camp's business.
4. Establish guidelines for the use of social media (Facebook, LinkedIn, etc.), blogs, and other internet publications; identify prohibited conduct; emphasize the importance of using good judgment in postings; and clarify that employees have no permission to use the camp's name, etc.
5. Consequences of violating the policies — disciplinary action, which may include termination of employment.

The truth is companies of all sizes are suffering consequences from network security breaches.

Enlist your insurance broker or insurance company loss control representatives in this process. Share your current policies on these topics with them and ask for their suggestions to improve and expand your guidelines.

Your electronic privacy and security policy should be shared with every employee. Require each employee to read the policies and acknowledge with a signature that the employee has received a copy of the policy, read it, and agrees to follow the guidelines set forth in the document.

This acknowledgement should include a statement of consequences for failing to follow the company policy, such as disciplinary action up to and including termination of employment. A copy of the signed acknowledgment should be kept permanently with the employee's human resources records.

continued on page 18

Risk Management continued from page 16

What Are the Consequences of Security Breaches and Failure to Manage Privacy?

California was the first state to pass a data security breach law. Since then, forty-three other states, plus the District of Columbia, Puerto Rico, and the US Virgin Islands, have passed data security laws.

The requirements of each state law are different, but the common thread is a requirement to notify the persons whose personally identifiable information was compromised. Personally identifiable information includes name, address, social security number, gender, marital status, contact information, driver's license issue and expiry dates, credit card information, and medical history, among other things. This sounds like the very kind of information maintained in camp databases about their campers, camper families, and employees.

Forty-three other states, plus the District of Columbia, Puerto Rico, and the US Virgin Islands, have passed data security laws.

Notification costs have been quoted by various information technology industry experts to be in the $200 – $300 range per compromised data file. Not terrible, you say, but suppose your database had one thousand names, and all were compromised. That's an expense of $200,000 – $300,000 probably not covered by your camp insurance policies. If you store personally identifiable information in your camp databases, you need to be aware of your state's data security breach disclosure law.

Other consequences will most likely include civil suits, depending on the extent of any financial damages.

What Are the Types of Situations Contributing to Security Breaches?

Not all security breaches are major. In fact, some events are so minor you might not notice the event unless someone on your staff or an independent consultant is watching closely. A frequency of small events left unchecked may lead to a larger, more catastrophic event.

Security breaches may occur when passwords are stolen because unprotected wireless networks were used. Passwords should be complex and changed on a regular basis. Security may be compromised by failing to change employee login information when someone leaves. Not all former employees may be disgruntled and vindictive, but it only takes one.

Sometimes employees are fooled into clicking on links that compromise their individual work stations and jeopardize network security. Beware of clicking on a link in any e-mail that is from an unfamiliar source or that you didn't solicit. Don't click on ads that say you've "won," for example; they may download spyware that compromise security.

If you allow employees to take notebook computers or flash drives out of the office with customer information stored on the devices, you are at risk of a security breach should the device be lost or stolen. Some smart phones are also capable of storing customer information with e-mail and text applications, posing a similar security and privacy breach risk if they are lost or stolen.

I'm Safe — My Information Is in the Cloud

There are many internet service providers (ISPs) focused on the camp industry who offer directors the convenience of accessing software and storing customer information offsite on the Cloud. The Cloud in this instance is a metaphor for the Internet.

Your camp management information is accessed via the Internet from any computer, anywhere, at any time, usually through a Web browser. The experience is often the same as if the software applications and data were stored locally on the user's computer.

What about security in this situation? There are divergent views on this issue, but generally security is often as good as or better than other traditional network systems because the services are shared. As a result, these ISPs are able to devote greater resources to security than many businesses could afford on their own.

If you experience a security breach, don't expect the ISP to be responsible. Most Cloud computing contracts will contain comprehensive limitation of liability provisions, including both a financial cap on liability and an exclusion clause for indirect losses, and in most cases, a separate exclusion clause for data loss and data breaches.

Another common feature of Cloud computing contracts involves tying the financial cap in liability to the amount of fees paid by the Cloud customer under the contract, further limited to a specific time, such as the previous twelve months. This means you are most likely on your own to pay for breach notification costs and deal with any other legal consequences from a security breach.

It is recommended that directors read Cloud computing (ISP) agreements carefully and take the time to understand any limitation clauses or other provisions in the contracts that limit the ISP's liability for damages arising out of security breaches or other services.

Defensive Strategy — Protect Your Computer Network

Whether your network is wired or wireless, whether you are Cloud computing or not, and regardless if you operate just one or twenty computers, protect them by using a network router. This electronic device allows a number of computers to share the same internet connection. It also provides security for the computer's access points or ports, as well as filtering communications and blocking unauthorized access.

Wireless routers come with default administrator passwords. Unfortunately, these default passwords are not always changed before the wireless router is put into service. This increases the risk of unauthorized access and network security breaches. Be sure your camp computer network administrator is changing the default passwords in your wireless routers and using complicated passwords in their place. Also be sure that any transmitted wireless signal is encrypted.

Other suggestions for protecting your computer network and keeping private information secure include:

- Keep all operating systems up to date.
- Install and run a good antivirus and spyware scanner regularly.
- Use an external hard drive to store all information, including personally identifiable information, and disconnect it from your computer when not in use. (This practice segregates the risk and is different than backing up your systems.)
- Consider using Web-accessed e-mail.

As a practical matter, even the most savvy computer users can benefit from having an IT consultant. If you don't have such a person available to you, consider hiring one as part of your first line of defense against security breach risks and cyber thieves. This will be money well spent.

Be Prepared

In the final analysis, an effective strategy for managing the risk of computer network security involves constant vigilance. This vigilance needs to be backed up by a sophisticated information technology structure, as comprehensive as you can afford, with practical guidelines for people to follow. This approach will help to reduce the risks of privacy and security breaches. Once you've done all you can from a risk management perspective, consider buying some cyber liability insurance to protect against lawsuits alleging negligence and notification costs in the event a breach occurs in spite of your efforts.

Don't get caught unaware of this expanding and rapidly changing risk. Be prepared!

Edward A. Schirick, CPCU, CIC, CRM, is senior vice president at Schirick & Associates Insurance Brokers, a division of Bollinger Inc. in Short Hills, New Jersey, where he specializes in arranging insurance coverage and offering risk management advice for camps. Schirick is a chartered property casualty underwriter, a certified insurance counselor, and a certified risk manager. He can be reached at 877.794.3113. Visit www.campinsurancepro.com.

In the final analysis, an effective strategy for managing the risk of computer network security involves constant vigilance.