Risk Reporter
for Camps and Conference Centers
Summer 2014 | Vol. 8 issue 2
A quarterly publication by Church Mutual Insurance Company

Act now to reduce cyber breaches

If a large retail chain can't avoid being hacked, can your camp?

That's the question camp administrators should be asking after a 62 percent jump in breaches over the past year.[1]

"There is no 100 percent foolproof way to avoid cyber problems, but there are ways to make it harder," said Chad Quiring, director of CircuiTree Products, a technology division of Kanakuk Kamps.

Recognize it *can* happen to you

Big corporate stories make the news, but small businesses are vulnerable too. In 2012, companies with fewer than 250 employees made up 32 percent of all attempted cyber attacks.[2]

Educate employees

"Data protection isn't solely an IT issue," stressed Tom Widman, president and CEO of Identity Fraud Inc., a company that provides identity fraud solutions and cyber insurance for organizations. "Sound technical controls are important, but data security requires a comprehensive approach that involves all employees."

Employees should know to never view, open or copy an email attachment unless they know who sent it *and* expect the file or link. They also should update passwords regularly and use a complex one with both letters and numbers.

Install virus software and firewalls

"Skilled hackers can get into any system, but basic defenses can limit their return on investment and make you a less appealing target," Widman said.

Security expert, Symantec Corporation, recommends your security includes:

- **Antivirus and behavioral malware prevention.** Malware is designed to disrupt your computer's operation; these stop a malicious threat from executing.
- **Bi-directional firewalls.** Filter both incoming and outgoing traffic and protect vulnerable applications/services on your computer.
- **Browser protection.** Protect your system from web-based attacks.
- **Reputation-based tools.** Check reputation/trust of a file or website before downloading.

(See Cyber breaches, Page 2)

[1] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
[2] http://windows.microsoft.com/en-us/windows/end-support-help

Inside

cont.

(Cyber breaches)

Update, update, update

Update old versions of software, web browser and operating systems. Set up your system to automatically check for updates; only use those that come directly from your vendors. Still using Windows XP? Replace it. As of April 8, 2014, updates were no longer provided.[3]

Limit email attachments

Symantec suggests configuring mail servers to block or remove any email that includes a file attachment-type used to spread viruses, such as .BVS, .BAT, .EXE, .PIF and .SCR.

Control data access — and only collect and retain the data you need

"Have the 'owner' of the area — say, the head nurse for medical staff — verify an employee needs data access to do his or her job," Quiring said.

"Anyone having access needs proper background screening before he or she touches sensitive data," Widman added.

Many camps have temporary employees who need access to sensitive data but only for a short time. "Create a login to use while they're on site and disable it afterward," Quiring said. "Make it a policy to routinely check and disable old logins."

Keep data collection to a minimum. "Only collect the data you need to deliver your services and do your job," Widman said.

Create two data networks

"Use one network for sensitive data, and limit employee access," Quiring said. "The other is a guest network that allows staff and visitors to use the Internet."

If you accept credit cards at your campground, ensure your point-of-sale terminals only link to your secure network.

Choosing third-party vendors

Most camps use a third-party vendor to manage camper applications, health information, payments and similar. Learn how your vendor protects and limits data access.

- **PCI-compliance.** PCI DSS is the Payment Card Industry Data Security Standard, and all companies that process, store or transmit credit card data should meet it. "Ask to see the vendor's PCI compliance," Quiring said. "Ask if they store credit card data. If they do, verify that it's encrypted, and ask how they do it."
- **External scans.** Make sure your vendor has had — and passed — a third-party scan conducted by one of PCI's Approved Scanning Vendors (ASVs). "This checks for site vulnerabilities, and PCI requires it quarterly," Quiring said.
- **Security permissions.** Choose a provider that lets you control security permissions for various data categories.

Back up your data

The Small Business Administration recommends backing up your data daily or weekly depending on how active you are in generating new data and files. "Make sure your backup method is secure — many will let you encrypt your contents," Quiring said.

Should you use the cloud?

Using the cloud — which means storing and accessing data and software through the Internet rather than your computer's hard drive — has become increasingly popular. The cloud can't be beat for file sharing or protecting data if your camp is damaged, and it is an affordable way to update software. But what about security? Is it easier to hack the cloud?

"The important thing to keep in mind is the sensitivity of your data," Widman said. "You *are* relinquishing some controls when your data moves into the cloud. Also, review the terms and conditions of any contract with a cloud provider, and recognize that if the cloud is compromised, the liability and responsibility of responding to the breach will still most likely rest on your shoulders."

"Confirm that a vendor's data center is PCI-compliant," Quiring said.

Be wary of mobile and personal devices

"Mobile devices offer great efficiencies, but they also introduce a whole new frontier of exposure," Widman said. "Your staff should only access your business network if their devices have been scanned for vulnerabilities and approved for use."

Hacking isn't the only way to compromise data

"Fraud, social engineering, lost and stolen equipment, misguided emails and accidental website postings are major contributors to data loss," Widman said.

Instruct employees to lock up any hard copy printouts of data, log out of unattended computers, secure their hardware and shred all vulnerable paper data.

Responding to a breach

Develop an incident response plan *now* that dictates the steps you'll take if a breach occurs and identifies your response team and their roles. This should include: a forensic analysis to determine if a breach occurred and which data/machines/devices were affected; steps you'll take to ensure you're meeting all legal requirements for notifying and protecting affected people (46 states require notification), how you'll resolve breach issues and whether you'll offer credit or identity monitoring services to those whose data was compromised.

Church Mutual now partnering with Identity Fraud Inc.

Church Mutual is working with CMIC Specialty Services and Identity Fraud Inc. to offer a cyber liability insurance and data breach services program to our customers. For more information, please contact your Church Mutual representative or agent.

[3] http://windows.microsoft.com/en-us/windows/end-support-help

Managing Your Risks

Ladder Inspection Checklist and safety posters

Ladder-related slip-and-fall accidents are a significant cause of claims to Church Mutual. During 2009-2013, employees, volunteers and even some guests and campers were involved in 870 ladder accidents costing more than $13.8 million. Injuries to maintenance workers were responsible for the biggest share of the workers' compensation claims and associated dollar losses.

Trimming trees, painting, repairing roofs and changing light bulbs are just a few of the tasks that often require using a ladder. Because ladders are used frequently, it's easy for employees and volunteers to overlook potential hazards when using them.

To help address the proper use of ladders and related safety concerns, Church Mutual developed a new ***Ladder Inspection Checklist***. The brochure outlines five key steps for using ladders safely:

- Choosing the right ladder
- Inspecting the ladder
- Correct set up
- Climbing and descending
- Using safe work practices

The brochure includes four tear-out copies of the checklist. There also are four *Danger — Damaged Do Not Use tags* that can be attached to a defective ladder to warn others about its condition and to indicate it is "out of service."

Six new safety posters were added to the risk control resources available to Church Mutual customers. These posters provide helpful tips for employees and others about preventing back injuries, kitchen accidents, strains and sprains and slips and falls on walking surfaces and from ladders. Also, information on making ergonomic adjustments to computer workstations is covered in one of the posters. To view, download or print copies of these and other safety resources, please visit our website at www.churchmutual.com.

Edward A. Steele
Risk Control Manager

Seasonal Spotlight

Steps to improve vehicle and driver safety

As your camp prepares to transport buses and van loads of excited, energetic campers, the following can help improve safety and limit camp liability.

Require proper licensure. Anyone who drives a commercial motor vehicle is required to have a commercial drivers license (CDL). Those who operate school buses and vehicles that can carry 15 or more (plus driver), must pass written and road tests and secure the appropriate endorsements placed on their CDL. Each driver must have a CDL for the state where your camp is located.

Match the driver to the vehicle. "The vehicle type and capacity determine required licensing and training," said George Coleman, founding director of Coleman Family Camps in Merrick, N.Y. and chairman of the transportation committee for the New York State Camp Directors Association. "You can't pull seats out of a 16-passenger van and say the driver doesn't need a CDL."

Require a road test and abstract of every person who drives for your camp. Coleman uses the New York DMV test for his camp's drivers; an abstract summarizes the driver's history (license, tickets, accidents, etc.). "Verify everyone's abilities — even the errand person," Coleman said.

Conduct vehicle inspections. "Have all vehicles inspected annually by a competent mechanic, use a checklist and have this signed off by the camp director or designee," Coleman said. "Hold all vehicles transporting campers or staff to school bus standards."

Coleman Family Camps rents the buses it uses and requires all buses are four years old or newer. "But the mechanical condition is more significant than vehicle age," Coleman stressed.

Follow a pre- and post-use checklist. Before every trip, Coleman recommended the driver walk around the vehicle, check the tires and wipers, verify lights and signals work and mirrors are intact and functioning, check windshields for cracks and determine seatbelts are operable. "At the end of the run, check every seat to make sure all passengers are off," Coleman stressed.

Have staff on board. "Even if you're using an outside company for vehicles and drivers, staff who know the kids should also be on board," Coleman said.

Consider installing vehicle monitors. These show mileage, location and speed; some include video cameras. "These are becoming more common on rented buses (as school districts become more insistent) and are a good proactive risk management tool," Coleman said. "They've been helpful to us to prove a driver wasn't in a certain location and was traveling at a safe speed."

- **Resource:** For more information — including a pre-trip inspection video and checklists — visit www.churchmutual.com/transport.

Q|A

A Perspective

When an employee is hurt on the job, filing an insurance claim might seem low on your list of priorities. But there are a number of reasons why it's critical to report the injury to your insurance company within one business day. Risk Reporter recently spoke with Jennifer Wolf Horejsh, executive director of the International Association of Industrial Accident Boards and Commissions (IAIABC), to learn more.

Founded over a century ago, the IAIABC was created to improve the efficiency and effectiveness of workers' compensation systems around the world. Additional information can be found at iaiabc.org and OSHA has a useful worksheet on workers' compensation at https://www.osha.gov/Publications/safety-health-management-systems.pdf.

Risk Reporter: **Why do injuries go unreported?**

Jennifer Wolf Horejsh: An employee might think the injury is no big deal, fear being reprimanded or worry co-workers will think differently of them. A company might believe reporting an injury will cause its insurance rates to go up. One thing that's become clear over the history of IAIABC is that it's best practice to report every injury.

Risk Reporter: **IAIABC research shows costs start to go up if reporting is delayed even a week. Why?**

Jennifer Wolf Horejsh: A delay can exacerbate a medical problem and complicate treatment. It can also hinder the accident investigation process, which could increase the chance of a workers' comp claim denial and lead you to incur costs in the dispute resolution process. If the injury was the result of a dangerous situation, more people might be hurt because the problem wasn't resolved. Delayed reporting can also slow return to work. Research shows the longer an employee is out of work, the less likely they are to return to work. Delaying return to work will drive up indemnity costs, and delaying appropriate medical treatment could compromise employee recovery. Delays could also lead to fines or penalties from your state.

Risk Reporter: **What are some things to be aware of during the return to work process?**

Jennifer Wolf Horejsh: Work with the claims adjuster, the employee and his or her medical provider to understand a reasonable timeline for returning and if accommodations will be necessary to avoid reinjury. Research supports the value of returning to work, but it must be done appropriately.

Risk Reporter: **Please address the importance of a safety culture.**

Jennifer Wolf Horejsh: This must be integral to your organization. Work to ensure employees understand safety rules and best practices — discuss them frequently and regularly. An accident is a good time to revisit your safety protocols. Talk about the accident in a neutral environment, and use it as a learning lesson. Determine if protocols are appropriate. Do you provide the staffing and support needed to follow them? Employees must know they can't be fired for filing a workers' comp claim — it's a no-fault system and their injuries will be covered even if the accident was their doing.

Church Mutual Insurance Company | **www.churchmutual.com**
3000 Schuster Lane | P.O. Box 357 | Merrill, WI 54452-0357

Interim Editor: Patrick M. Moreland | (800) 554-2642 Ext. 4833 | pmoreland@churchmutual.com
Risk Control Advisor: Edward A. Steele, CSP, ARM | (800) 554-2642 Ext. 4403 | esteele@churchmutual.com
Writer: Vicky Franchino | **Layout:** Dan Kaminski