YMCA Safety INSIGHTS
SAFETY and RISK Management News & Notes from YMCA OF THE USA Consulting

Volume 1 - Issue #8

If You Collect It - Protect It

YMCAs face data loss and security issues every day. Data theft is a growing risk for Ys and other businesses across the nation. The impact touches the organization at all levels and from many directions. Studies on the total cost of identity theft suggest that it costs U.S. businesses and consumers $56.6 billion in 2005. The loss or theft of just one laptop can cost a company as much as $90,000 or more in fines, credit monitoring for victims, public relations damage control, and class action litigation. The US Department of Justice reports that identity theft is now surpassing drug trafficking as the number one crime in the nation.

Data loss occurs when the organization allows information to become available unintentionally or through mismanagement. Data theft occurs when security measures are not in place or are breached by an outside party. Staff dealing with data storage and security must work together, and the organization must set data protection as a priority.

Along with the financial implications from such an incident comes the damage to an organization's reputation. A study conducted by Unisys reports that 69 percent of consumers would stop using a Web site that lost their personal information. The negative effects of identity theft or a breach of information can have long-term and far-reaching ramifications. It should be a priority for YMCAs to heighten their awareness of identity theft, and the financial and image costs of a data loss.

Many Ys utilize outside services for data protection such as secure transaction portals and online back-up. Most incidents seem to occur when practice does not follow policy. Recent incidents of data theft or loss occurred where old hard-drives were not disposed of and where monthly child care payments were kept on a standalone system. YMCAs must make every effort to secure all their data consistently.

Both data theft and loss can be prevented. Strategies and resources for protecting and securing information are available throughout this issue and by visiting www.ymcaexchange.org; click on the "Operations" tab and scroll to the Technology Management page. ◆

Data and Responsibility

This issue of *Safety Insights* focuses on data security and the need to treat member and staff information safely and responsibly. YMCAs have the responsibility to prevent data loss and theft. It shows good stewardship, ensures public trust and is consistent with our values and mission.

Knowing and accepting this responsibility is often easier than actually accomplishing the goal. This newsletter shares information that will assist Ys of all sizes to manage confidential information appropriately. Data comes in many forms: written, electronic and verbal to name a few. Whether you have a sizable computer network or a simple laptop, you can learn how to safely and securely manage data. Please read the various articles, visit the referenced Web sites and take a few moments to access the resources on www.ymcaexchange.org. All this information will assist your security efforts.

YMCAs must respect the tremendous power that data commands, care about this power, honestly assess their management capabilities and then develop procedures to responsibly manage and control personal data. Our core values and our members demand it of us. ◆

YMCA of the USA CONSULTING | 101 North Wacker Drive | Chicago, Illinois 60606 | 800.872.9622 | www.ymcaexchange.org

YMCA Safety INSIGHTS
SAFETY and RISK Management News & Notes
from YMCA OF THE USA Consulting

Data Security Standards

The PCI Security Standards Council has developed a set of comprehensive requirements for enhancing payment account data security. The PCI Council is a cooperative effort that was founded by the nation's leading credit card institutions to help facilitate the broad adoption of consistent data security measures.

The PCI standards include requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations protect their customers proactively. The council provides a group of principles and accompanying requirements, around which the specific elements of the security standards are organized.

The PCI Security Council recommends the following twelve standards for data security:

1. Install and maintain a firewall to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to networks and cardholder data
11. Test security systems and processes regularly
12. Maintain a policy that addresses information security

More information on these security standards can be found at www.pcisecuritystandards.org or by visiting www.ymcaexchange.org; click on the "Operations" tab and scroll to the Technology Management page. ◆

Data Breach Disclosure Laws

Many people may be familiar with common privacy practices that are followed by large financial institutions. These practices, required by several laws including the Gramm-Leach-Bliley and Fair Credit Reporting Acts, are Federal laws designed to protect private personal data from misuse.

Most states have passed similar laws related to disclosure by a company that has experienced a data loss or theft. These Data Breach Disclosure Laws vary by state; however, most require an organization to provide notice if there is a breach of the security of unencrypted computerized data, electronic media or electronic files containing personal information. Notice is usually not required if the breach will not likely result in harm to the individuals. Depending upon the type of information accessed, YMCAs may be required to comply with disclosure laws in their state. Also keep in mind that these requirements may be different if the YMCA is under contract to a government entity.

YMCAs should become familiar with the reporting requirements in their state. Ys should develop a breach response policy and communicate it to all appropriate employees.

Continued on page 3

YMCA Safety INSIGHTS
SAFETY and RISK Management News & Notes from YMCA OF THE USA Consulting

Tips for Preventing Data Loss

Data loss prevention efforts should focus on two areas: computer system controls and the implementation of responsible information handling practices. The tips below will assist YMCAs in preventing data loss and theft.

- Adopt a comprehensive privacy policy that includes responsible information-handling practices.
- Store sensitive personal data in secure (encrypted) computer systems.
- Ensure that wireless networks are protected with the proper security settings.
- Dispose of documents properly: shred paper with a cross-cut shredder, "wipe" electronic files, destroy old computer drives and CD-ROMs, etc.
- Conduct regular staff training, including new employees, temporary employees, and contractors.
- Conduct privacy "walk-throughs" and make spot checks on proper information handling. Afterwards, reward employees and departments for maintaining "best practices."
- Limit data collected to the minimum needed.
- Put limits on data display and disclosure of Social Security numbers.
- Restrict data access to staff with legitimate need to know.
- Conduct employee background checks, especially for individuals who have access to sensitive personal information.
- Limit, control and safeguard mobile devices that contain sensitive personal data.
- Notify law enforcement, customers and/or employees of computer security breaches (note: most states have adopted security breach notice laws).
- Develop a crisis management plan for data theft or loss.
- Conduct and document regular policy and practice compliance audits.

All staff must be aware of practices and be able to ensure that personal information is handled responsibly. ◆

Risk Management Discussion Board

YMCA of the USA has a discussion board available for all those interested in safety and risk management. The board allows for timely discussion on a variety of topics related to safety and risk management efforts. Users may pose questions, share information or simply search the board for more information. Various staff members monitor the board, facilitate discussion and assist where appropriate. To join the discussion board, interested volunteers and staff may go to www.ymcaexchange.org. From the top of the home page, select Discussions, then "Create an Account." ◆

Disclosure *continued from page 2*

Whether the Y is legally responsible for disclosure of data breach will affect their policy as will any moral obligation. Any suspected or confirmed compromise of protected electronic data should be reported to the Y's management and immediate steps to secure the system should be implemented.

YMCAs should consult with local legal counsel about pertinent disclosure laws. More information is also available at www.consumersunion.org/campaigns/Breach_laws_May05.pdf ◆

YMCA Safety INSIGHTS
SAFETY and RISK Management News & Notes from YMCA OF THE USA Consulting

Training and More

Healthy & Secure Computing is a Webinar designed to help program staff who perform IT tasks routinely at their Ys but have little or no IT background. This Webinar can help you answer important questions like the following: Does your YMCA regularly backup important files on all desktop computers and your server? Do you regularly update the antivirus and spyware protection on your computers? If you're an "accidental techie" and you're not sure about the answers to these questions, join in on this free workshop provided by Tech Soup. Please visit www.techsoup.org/hsc/page7475.cfm to register.

Data Breach Response and Planning is a Webinar available from First Data that provides direction on preventing and responding to data loss and theft. First data also provides a data protection guide available for download. For more information go to www.star.com/data_breach_response_and_planning.aspx

The Desktop Security Audit offered by CompuMentor's is designed to help nonprofits audit their desktop computers against a security standard that is appropriate for most small- and medium-sized organizations. Secure computing environments are critical to productive use of technology and the integrity of your organization's data. For more information please visit www.compumentor.org/hsc/resourcesandtools/

Raptor Ware provides background check services and software that can help a YMCA track visitors to their facilities. Originally created for educational institutions, V-Soft is a web-based software application that aids in tracking visitors, members and staff. V-Soft not only provides an effective, efficient method for tracking, but also goes beyond conventional applications by utilizing available public databases to help control security. Service contracts can provide unlimited annual access for a YMCA's screening needs. Recently, V-Soft has been successfully implemented in several YMCAs. For more information please visit www.raptorware.com.

The Occupational Health and Safety Administration (OSHA) has collaborated with the University of South Florida to develop new materials designed to assist trainers in conducting Spanish-language training for employees. YMCA-applicable topics include hazard communication, bloodborne pathogens and use of personal protective equipment. For more information please visit www.consultationconnection.org/oti. ◆

Healthy & Secure Computing Workbook Available

The Healthy & Secure Computing (HSC) Workbook has been designed to help YMCAs make decisions that increase the reliability and security of their information technology (IT) infrastructure at minimal cost. Intended for use by the person responsible for technology at your YMCA, this workbook initially sets minimum hardware and software specifications that apply to any YMCA. It then provides an extensive set of worksheets and templates that can be used to record IT inventory, identify technology objectives and priorities, and track current documentation and policies.

To obtain a copy of the workbook please visit www.ymcaexchange.org, click on the "Operations" tab and scroll down to the Technology Management page. ◆

Safety Insights is produced on a monthly basis for Y-USA Consulting by Safe-Wise Consulting, LLC.

YMCA staff and volunteers may subscribe to the newsletter distribution list by sending an email request to: safety.insights@ymca.net

Past issues are available at www.ymcaexchange.org and www.safe-wise.com ◆