The Municipal
RISK MANAGER
JANUARY 2014
A Publication of the Maine Municipal Association

Secure Your Information

Our municipalities often handle personal information about residents, businesses, organizations and their own employees. Records and electronic files that need to be secure and confidential may include billing information, social security numbers, health information, human resources and public school/education data.

Using electronic communications for business transactions and providing public services is becoming a common tool, which has also caused an increase of data breach incidents. Data breaches occur for many reasons, such as a result of innocent errors, internal maliciousness actions or outside hackers.

A cyber risk generally has the potential to cause loss, injury or other damages as a result of an electronic exposure that could harm the municipality or the public that they serve. Potential activities that may create a risk of a cyber attack include:

- Online credit card payment processing and data retention
- Conducting business utilizing Web sites
- Data retention and storage (online and traditional shipping of paper records or back-up tapes)
- Third party business contractors that access confidential data
- Data held on unprotected laptops or portable devices
- Social media sites that collect and display private information, examples of which include Facebook, MySpace or Twitter.

How to minimize cyber threats:

1. **Educate Employees**. Have a written policy about sensitive data, procedures and responsibilities.
2. **Only retain required data.** Only keep the information that you need and consider the creation of a retention schedule.
3. **Safeguard Data**. Lock records in a secure location and restrict access to employees who need to retrieve private data. Implement password protection on all computers with a condition to re-logon after a period of inactivity. Use strong passwords that are required to be changed regularly.
4. **Background checks.** Conduct background and reference checks of employees and contractors.
5. **Shred and Destroy.** Shred paper files before disposing or obtain the services of a private company that specializes in the shredding and disposal of sensitive data.

Story Continued on Page 18

Workers Compensation Audit Time for Payroll Reporting

At renewal each year, members of the MMA Workers Compensation Fund are asked to provide their anticipated payroll so we can calculate the estimated workers compensation contribution for the coming year.

The projected payroll is a useful tool to evaluate future exposures and to ensure that adequate coverage is present. We understand that the actual payroll figures can vary considerably from estimates made over a year earlier. A special project may come to an end earlier than expected, a severe weather incident may occur that requires additional employees, or a position may remain vacant for a long period while

Story Continued on Page 18

Coming Soon:

Privacy and Network Security Liability Coverage

During 2014 the Property & Casualty Pool will be offering Privacy and Network Liability coverage to its membership. Privacy and Network Liability is an emerging exposure that typically encompasses the liability associated with the failure to protect the unauthorized release or disclosure of confidential personal information of customers, employees or other sensitive business information. Watch for updates!

Keep Your Cyber Defenses Up *(it is always virus season)*

In our online, mobile society, we are faced with an increasing barrage of cyber threats every day. Whether at work, home, school—virtually every part of our lives is now in some way or another connected to the Internet.

Local governments are not immune to cyber threats. A virus could shut down office computers. A disgruntled former employee could manipulate or destroy important organizational data. A malicious user could use your systems to attack other systems. Cyber security incidents can cripple computers and cause a loss of public confidence. Inadequate cyber security measures can lead to the compromise of sensitive information about organizational operations and its customers.

An organization has a responsibility to safeguard the information with which it is entrusted and to perform its business functions. Following is a list of the top ten cyber security action items recommended by the Multi-State Information Sharing and Analysis Center (MS-ISAC), designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, territorial and tribal governments.

Designate, in writing, a principal individual responsible for cyber security in order to ensure that proper policies and procedures are in place. Develop a cyber security plan and procedures for responding to cyber security incidents. Establish communication procedures so that everyone knows what, how and to whom to report a cyber security incident or problem.

1. Know how to recognize that you might have a problem, such as a slow or non-responsive computer. Your organization may be experiencing a cyber security incident if it is finding email refused (bounced back) or getting complaints from the users that the network has slow response time.
2. Understand how to deal with problems. Take infected or compromised equipment out of service as soon as practical. Notify management and other users as appropriate based on your organization's policy. Contact local law enforcement if you suspect a crime has been committed. Review your security policy and practices to determine what lessons can be learned from the incident to help you strengthen your security practices.
3. Physically protect your equipment from security threats and environmental hazards. If traveling with a laptop, never check it in at the airport; keep it with you at all times or in a secure location. Use a surge protector.
4. Protect essential hardware and software. Install, configure and use a firewall, and set your computer to automatically check for new updates. Set your computer to auto-update to ensure you have the latest security patches applied. Install spyware and virus protection software and regularly update. (A firewall does not substitute for anti-virus software.)
5. Control access. Each user must have a unique login (user ID) and password. Establish good passwords—at a minimum, a combination of eight alpha and numeric characters; avoid commonly used words, family names, or other words that can be readily associated with you. "Lock" computers when they are unattended so users are prompted to enter their user ID and password upon return. Don't allow a computer to remember any passwords. Implement an employee departure checklist to ensure account termination is performed.
6. Protect information. Information should be backed up regularly and stored offsite. Periodically test that the information can be reloaded from backups. Install operating system software patches regularly. Handle email and instant messaging with care. Use encryption for information stored on portable devices, such as flash drives. Be cautious of internet sites you visit.
7. Implement training and awareness programs. Everyone in the organization who uses a computer should be trained to practice safe computing and follow the organization's policy.
8. Develop an Internet and Acceptable Use Policy. When your employees connect to the internet or send e-mail using your organization's resources, it should be for purposes authorized by the organization.
9. Take steps to securely dispose of storage media and equipment. Hard drives and other disposable computer equipment may contain saved information even if that information has been "deleted." Run utilities and/or physically destroy the hard drive to ensure it is clear.

Welcome New Members

Workers Compensation Fund

Town of Edinburg

Unemployment Compensation Fund

Maine County Commissioners Association

Northern Oxford Regional Solid Waste Board

The Municipal Risk Manager

The Municipal Risk Manager is published seasonally to inform you of developments in municipal risk management which may be of interest to you in your daily business activities. The information in these articles is general in nature and should not be considered advice for any specific risk management or legal question; you should consult with legal counsel or other qualified professional of your own choice.

Publisher: Risk Management Services
Editor: Marcus Ballou
Layout Designer: Jaime G. Clark
P.O. Box 9109, Augusta, ME 04332-9109
1-800-590-5583 or (207) 626-5583

Pump Damage Hampers Fire Departments

Many communities in Maine do not have, or have only limited numbers of pressurized domestic fire hydrants. In some instances publicly owned water supplies are inadequately sized or do not provide enough flow water for proper fire suppression. Having water available from area streams and ponds is only helpful if the source is nearby and rapidly available. The installation of "dry hydrants" into nearby water supplies can provide a year-round water source and is a common practice in rural Maine. Correctly designed and installed dry hydrants can provide a simple, cost effective water supply option.

Regardless of the water supply, no fire pump can move water containing debris such as sand, rocks, leaves or vegetation without causing damage to the pump. Whether drafting from a pond or from a dry hydrant, the correct location of the intakes and the proper use of strainers are critical to protecting the pumps. The Property & Casualty Pool has received numerous claims involving damaged pumps due to improper drafting. As an example, while a fire department was performing pump training, they hooked onto a dry hydrant not provided with a strainer. As a result, the pump sucked up debris damaging the pump and impeller which had to be replaced. In another instance, a fire department hooked onto a dry hydrant that had been used several times prior. On this occurrence, the pump ingested sand due to the use of an improper screen that was designed to stop rocks but not sand and gravel. A third pump was damaged due to gravel being sucked from the bottom of the water source at the dry hydrant. The average cost of pump loss claims in 2012/2013 was $9400.

When a pump is damaged, not only is the repair or replacement costly, but the ability of the fire department to provide adequate fire protection while the pump is out of service may be compromised. **Helpful tips to avoid pump damage**:

- Never draft from a dry hydrant or directly from a water source without a strainer / screen, appropriately sized for the condition, in place. When training, stress the importance of protecting the pump.
- When locating a dry hydrant, the best composition for the bottom of the lake, stream or pond is sand, gravel or rock or a combination of these. Avoid decaying vegetation that can easily plug the intake screen.
- The intake should be no less than two feet below the surface to prevent a vortex or whirlpool which could allow air to enter causing the pump to cavitate or loose prime. There should be a minimum of five to six feet of water over the suction screen during low water to prevent a freeze-up of the screen.
- The strainer should be no less than two feet above the bottom of the pond so that the strainer holes will not be clogged with mud or debris.
- The selection of a proper strainer is dependent on a number of factors, including depth of the water source; type of source; flow conditions; water source fluctuations such as drought, flood or water releases; bottom type and conditions; floating and suspended debris; aquatic growth; vertical lift and desired flow rate.
- Dry hydrants require frequent inspection; quarterly is recommended. This may need to be more frequent in warm water, low flow locations. Keep records of all inspections and repairs. Hydrants should be tested with a pumper once a year and back flushed as part of a training exercise.
- When drafting from farm ponds, streams or rivers both shallow and deep or from drop tanks a floating strainers should be used. Floating strainers are available that operate below scum and debris and above sand and muck. This will strain out materials that wear impellers, packing and bearings.
- Using a dry hydrant or drawing water directly from a river or pond will introduce materials that over time can damage the pump system. When possible, following drafting operations or a water shuttle where stagnant water is used, it is good practice to drain the tank, flush valves and drains and refill he tank from a municipal water supply.

* NFPA 1142, "Standard on Water Supplies for Suburban and Rural Firefighting" provides information on planning, design and installation of dry hydrant systems.

Cold Snap = Property Damage

During the winter months our public buildings are in danger of becoming the next victim of the FREEZE. It is important that we remember to routinely inspect all buildings over winter months and especially during vacation and holiday breaks to ensure that the buildings are properly heated and that all water distribution systems including sprinkler systems are not frozen. Such inspections are critical after a deep freeze or power outage.

Remember to:

1. Inspect buildings inside and out.
2. Repair and replace broken windows.
3. Eliminate drafts in foundations and framing.
4. Insulate buildings.
5. Plan ahead and winterize all locations.

100,000 SERVED!!

In 2004, MMA Risk Management Services partnered with FirstNet Learning, Inc. to provide online safety training through the MMA website. Available at no charge to participating members of the Workers Compensation Fund and the Property & Casualty Pool, the offerings have been updated and expanded several times and now provide more than 50 course titles. As of November 30, 2013, users have taken more than 99,528 courses with a completion rate of 96.8%. We expect to reach the 100,000 course milestone to welcome in the New Year!

What's next? In mid 2014 we expect to expand the website again with the addition of employment liability, workplace ethics, public officials liability and other similar courses. If you have not utilized this valuable resource, we encourage you to visit the MMA website: www.memun.org. Demonstration courses are available to help you determine if online training is right for you.

October Safety Grants Awarded

155 grant applications were received for consideration in the October grant period. Of these, 115 were funded for a total commitment of $149,493. Safety equipment funded includes ergonomic equipment such as computer workstations; tailgate lifts and manhole cover lifters; firefighter turnout gear; traffic control signs, lights and vests; and fall prevention ice grips. 236 Safety Enhancement Grants with a total commitment of $302,561 have been approved in 2013. This program continues to be successful and well utilized by Worker's Compensation Fund participants.

To be eligible for a Safety Enhancement Grant, MMA members must participate in the Workers Compensation Fund. Grant requests must be for items that "directly enhance employee safety." Grants are a 2:1 match with a maximum of $2,000. For more information and applications visit the Risk Management Services section of the MMA website http://www.memun.org/ or call RMS, Loss Control Department at 626-5583.

Secure Your Info *(cont'd)*

6. **Digital Deletion**. Deleting files and reformatting may not be enough. You may wish to consult with an Information Technology professional and utilize software designed to permanently delete/wipe the drive.
7. **Manage Computer Usage**. Institute a policy that limits employee use of computers to business transactions. Consider Web Filtering to limit access to unauthorized Web sites and software.
8. **Software Security**. Ensure that security software is in place and current. Again, this is a time when you may wish to consult with an information technology professional for management and guidance of your antivirus and firewall protections.
9. **Data encryption**. Data encryption is a common tool utilized to protect data that is being transmitted electronically. Data encryption is also useful to protect portable media that is susceptible to loss.

WC Audit *(cont'd)*

you search for the ideal candidate. No matter the reason for variation in estimated payroll, we are committed to treating each member fairly. Therefore, the Workers Compensation Fund conducts an actual payroll audit on each member from January to April. You will be contacted by Risk Management Services who handles some audits in house, or by one of our contracted auditors at GEM Associates who will gather the data and forward it to us to process. It would be appreciated if all the necessary paperwork can be available for the auditor to review or is mailed promptly to them for review. The State of Maine mandates that all audits are completed by May 1st of each year for our Workers Compensation Fund.

If you have any questions, please contact the MMA Risk Management Services Underwriting Department at 1-800-590-5583.