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

Blanket Building And Blanket Personal Property Coverage

Many of the participating members of the MMA Property & Casualty Pool have blanket building and blanket personal property (contents) coverage. This means that at the time of any covered building loss, the total amount of the values listed for all of the buildings included in the blanket coverage is added together and that total amount is available to draw upon for the reconstruction or repair of the damaged or destroyed building. By the same process, at the time of any covered loss to contents, the total amount of the values listed for all of the contents included in the blanket coverage is added together and that total amount is available to draw upon for the replacement or repair of the damaged or destroyed contents.

Blanket coverage for buildings and blanket coverage for contents gives the member additional protection against the possibility of inaccurate property value estimates. It is important to note that it is the responsibility of each member to provide accurate information about their building and personal property insurable replacement cost values. A requirement for each member that has blanket building and blanket contents coverage is a Statement of Values, signed by the member that stipulates that the building values shown on the property schedule are 100% replacement cost values.

The Loss Control Department through their use of the Marshall & Swift building valuation computer program is able to produce estimates of insurable value for member-owned buildings that they have surveyed. The Marshall & Swift estimates of insurable value are provided to the Underwriting Department. The Underwriters then review the member's current scheduled building values and compare the two numbers. If there is a significant discrepancy, the Underwriter will work with the member to reconcile the values. It is important to remember that the Marshall & Swift computer program may not have a comparable schedule to suit buildings of unusual construction. Such buildings would need to be appraised by a licensed appraiser to determine the actual replacement cost. Overall, however, the program offers valuable assistance to the Underwriters

Story Continued on Page 21

More on Online Training

In the July Risk Manager we announced the three-year extension of a service agreement with FirstNet Learning, Inc. to provide online safety and risk management courses to participating members of the Worker's Compensation Fund and Property and Casualty Pool. The MMA Risk Management Services Online Training courses are provided at no cost to members of the Fund and Pool. Upgrades to the website are underway and courses addressing property, casualty and liability exposures will be added throughout the next three years, expanding the current offering of more than 50 courses. Titles that we expect to add include:

- Ethical Decision Making,
- Sexual Harassment Prevention (Supervisor),
- Harassment Prevention,
- Workplace Bullying and Violence Prevention,
- Discipline and Discharge,
- Guide to Interviewing,
- Ethics in the Workplace,
- Information Security and Privacy Awareness, and
- Lawful Hiring.

Watch the Risk Manager for announcements of new courses and visit the website to preview courses and the online university at: http://www.memun.org/InsuranceServices/RiskManagementServices.aspx

Welcome New Members

Property & Casualty Pool

Town of Sebec

Unemployment Compensation Fund

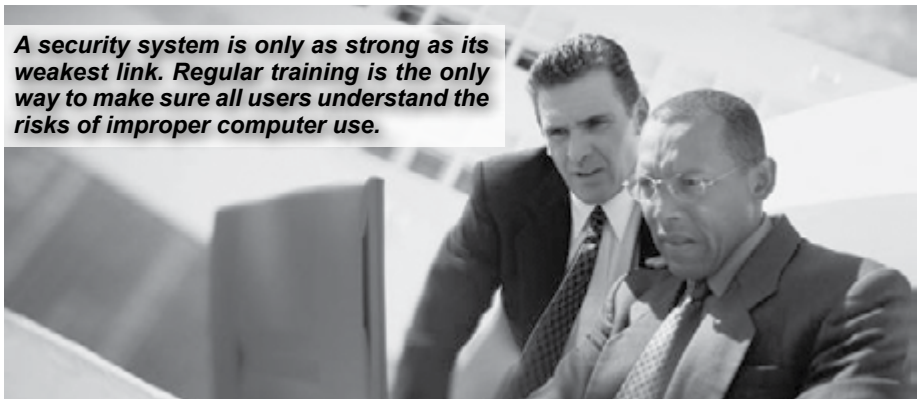
Town of Palermo

Is Your Town's Data Secure?

Municipalities need to develop sound policies to protect public information and their computer networks from a variety of threats

By Marc Pfeiffer, Assistant Director, Blaustein Local Government Research Center; member; NJ-GMI

Reprinted with the permission of the Editor NJ Municipalities Magazine.



A security system is only as strong as its weakest link. Regular training is the only way to make sure all users understand the risks of improper computer use.

Why do we need information security? We need information security because in the digital world we trust data we know little about. Without protections, data can easily enter our computers from untrustworthy sources.

Are your computers protected? An unprotected computer is one that *does not:*

1) have antivirus or spyware protection software installed and updated regularly;

2) have installed hardware or software firewall to manage communications between and among networks;

3) require the user to use a password to log on (known as authenticating);

4) have operating system and software patches installed and regularly updated.

To be considered protected your computers and networks should meet all four criteria!

What can happen when we trust data from unauthenticated sources? We can unknowingly install destructive programs on our computer network or confidential information could be accessed. For example, if a keystroke logger (a type of software that records keyboard strokes) were unknowingly installed (perhaps following a click on a link from a malware infested email), it could capture keystrokes with logons to websites, like a bank site, and then use your logon credentials to steal your money.

This type of information theft can be prevented by making sure any computer used to access bank accounts is only used for that purpose, and not for any other. That computer should not be used for reading email or web surfing. I recommend that every municipality take this precaution.

Hacker attack computer systems for many reasons, including political espionage, retaliation, internal threats, "just because I can," or more importantly, financial gain. And sometimes, "black-hat" hackers use tools used by "whitehat" security workers.

For example, popular websites have information that helps the good guys, but can be abused by bad guys. Some web sites include techniques on how to break into a password-protected computer (and how to prevent it from happening to you) and how to crack a wifi password.

How can we protect our systems and ourselves? It's a never-ending process that begins with implementing a sound policy. Towns should also invest in quality "best of breed" anti-cyber theft technology solutions. Once the policy and technology is in place the final keystroke to cyber security is ongoing education of everyone who uses the system

What should we consider when developing cyber security policies? Every organization with computers needs a cyber security policy. The depth and detail of the policy depends on the scope and structure of organization.

Generally speaking, there are five things a cyber security policy should do. The first is to put someone in charge of cyber-security. This individual should be responsible for developing and implementing plans and policies. Second, make sure you maintain and keep the plan up-to-date. Third, promote the use of security precautions and provide ongoing training. A security system is only as strong as its weakest link. Regular training is the only way to make sure all users understand the risks of improper computer use.

We can unknowingly have destructive programs installed on our computer network or confidential information could be accessed.

The fourth item is to communicate the critical role your organization and its employees play in protecting both public and internal information. Fifth, establish communication procedures so that everyone knows what to do when faced with

Story Continued on Page 21

Cyber Security *(cont'd)*

a cyber-security incident or problem. They must know how to react and to whom they should report problems.

What should be included in an effective cyber security plan?

There are many elements to a sound information security plan. One is an ongoing effort to identify risks, threats, vulnerabilities and consequences and take appropriate action to prevent or mitigate them. This effort includes enforcing password policies (including password strength and requirements for regular updates), and risk-manager review of appropriate insurance coverage. Another activity that has spin-off benefits is to ensure hardware and software asset inventories are maintained.

What about disaster recovery? Finally, prepare for the inevitable by supporting a robust disaster recovery planning process, including protecting the availability and recoverability of the organization's information.

What should you do? Unless your organization already has a sound plan, the first thing the person in charge of technology in your municipality should do is download: "Cyber Security-Getting Started: A Non Technical Guide" from msisac.cisecurity.org/resources/toolkit/oct13/documents/Getting_Started_Print.pdf.

Read it; see how it applies in your municipality; adapt it, then implement it. Then talk to your risk manager to see what else you should be doing. If you like the guide, the MS-ISAC organization has additional non-technical information and guides at: http://msisac.cisecurity.org/resources/guides/.

If all this is done, will all security problems go away? No! No security system is 100 percent perfect, since threats are always evolving. Keeping up on viruses, malware, and intrusions through regular software upgrades and education is the cornerstone of stopping web attacks, bank theft, and key loggers. Keep your protection services and operating systems updated and design them to be easily updated and simply distribute them in your environment. Finally, if you run your own system with servers, etc., the folks in charge should join MS-ISAC, a federally sponsored organization focused on cyber security for government agencies (msisac.cisecurity.org). MS-ISAC also has links to sample government cyber-policies. mba.

Basis Technical Safeguards

There is no single thing that can protect a computer or network from intrusion. Staying cyber-safe requires a combination of hardware and software tools. The following tools are used by most organizations.

Firewalls: Every computer connected to the internet needs its firewall turned on. What's a firewall? A system designed to prevent unauthorized access to or from a private network. A firewall is the first line of defense; just as, in another context, the US Border Patrol works to prevent unauthorized access to the country. All Windows computers have a built-in software firewall that should be turned on all times.

Anti-virus, - spam, and - malware software: These are programs that scan potentially suspicious emails and files the way the Border Patrol agents inspect vehicles or people acting suspiciously. Even the best anti-virus software will flag a good email from time to time because of possible suspicious behavior. All systems should have active and regularly updated anti-virus software, which includes anti-spam, malware, and related protections.

Every municipality that has its own direct internet connection needs its own "gateway" (similar to a border crossing) protecting its system. This can be done through software, hardware devices, or a third party service providing gateway protection. Each has its own advantages, disadvantages, and costs.

Cyber Security Terms

Data electronically stored information, regardless of format

Authenticated - you know the source of the information. If you're not sure, it's unauthenticated.

Firewall a security system that uses hardware and/or software to prevent unauthorized users from accessing an organization's internal computer network.

Malicious Software software used or programmed by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. This includes spyware, adware, viruses and general malware.

Software Patches software that corrects a problem.

Blanket Coverage *(cont'd)*

and the members in estimating insurable values.

If you would like further information on the topic of Blanket Building and Blanket Personal Property Coverage or would like to have a review of your entity's coverage, please contact the Member Services Department at (800) 590-5583 and ask to speak with Marcus Ballou or Judy Doore.

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

MMA Delivers the Goods

Risk Management Members' loyalty is rewarded

All of us at MMA Risk Management Services (RMS) would like to recognize the extraordinary efforts and continued commitment of our membership. We are pleased to announce that the

The Property & Casualty Pool distributed $550,000 in Dividends to its Members in 2014.

The Workers Compensation Fund distributed $650,000 in Dividends to its Members in 2014.

Property & Casualty Pool and Workers Compensation Fund have awarded dividends to their respective members. Through the efforts of our membership, sound management, responsible underwriting and the favorable loss histories of the Property & Casualty Pool and Workers Compensation Fund, RMS has awarded **$1,199,223** to its membership in 2014.

Readfield Town Manager Stefan Pakulski.

Fryeburg Rescue Shanna Walker and Bill Kane.

Fayette Town Manager Mark Robinson and Clarissa-Jean Herrin.

Kittery Town Manager Nancy Colbert Puff.

Cyber Liability Coverage Now Available

MMA's Risk Management Services is pleased to announce the introduction of Cyber Liability & Data Breach Expense coverage to members of the Property & Casualty Pool. Today's technology makes it easier to store, steal or lose personal information. An entire pickup truck of social security numbers, credit card numbers or health records can fit onto a pocket sized flash drive.

Cyber Liability Coverage:

- Covers liability arising out of the failure of network security, including unauthorized access or unauthorized use of municipal systems, a denial of service attack, or transmission of unauthorized, corrupting, or harmful software code to your computer system.
- Cyber Liability will cover losses arising out of your failure to protect sensitive personal information in any format.

Data Breach Expense Coverage:

- Reimbursement for expenses incurred due to a data breach, including but not limited to:
- Forensic services to determine the scope of the breach
- Notification of potentially affected customers
- Crisis management services
- Legal aid
- Credit monitoring services

Coverage Highlights:

- Cyber Liability - $1,000,000 limit per wrongful act
- Data Breach Expenses - $50,000 aggregate limit
- $1,000,000 Aggregate limit per member
- $1,000 minimum Deductible
- No additional cost (with completed application and subject to Underwriting review)

Please contact a member of Risk Management Services Underwriting staff at 1-800-590-5583 for questions or additional information.

YOUR MONEY IS WAITING Safety Grant Application Deadline Approaches

The Maine Municipal Association has been awarding safety grants to members of their Workers Compensation Fund since 1999. The grant program has assisted municipalities by bestowing **over $2,000,000 to their safety programs** through the funding of Safety Enhancement Grants and Scholarship Grants.

Grants are awarded in May and October of each year. To be eligible for the **May awards**, your application must be received between **October 1 and April 30.** Applications for the **October** awards must be received between **May 1 and September 30.**

For more information about any of the Maine Municipal Association Risk Management Service programs, including Safety Enhancement Grants eligibility and applications, please visit our website at **www.memun.org** and click on the Risk Management Services link, or call us at 1-800-590-5583.