



Business Advisors and Certified Public Accountants

Farmington, CT • New London, CT
Springfield, MA

Pond View Corporate Center
76 Batterson Park Road
Farmington, CT 06032-2571

Main Line: (860) 678-6000
Toll Free: (800) 286-KRCCO
Fax: (860) 678-6110
Web: www.kostin.com

Municipal Entities: The Importance of Information Security ***Michelle Syc***

Most records or files of state and local agencies are available to the public for inspection or copying. Should municipal entities require the same standards of security as corporations in the United States of America?

While it's true that most information in local agencies is public in nature, there is still a need to secure information because identity theft is a major issue. It's true that the majority of data in a local government falls under the classification of public information, but data classification is something very different from information security. Data classification is the act of determining the level of security of data. Information security is the act of protecting information from unauthorized access. These two concepts are mutually exclusive. An entity can house public data and still have a secure information system. An entity can have confidential data and be lacking in information security. Regardless of the level of data classification, municipal entities should still have secure information systems.

The reason can be better explained by the following example. If Hacker Bill wishes to attack a well-known organization, let's say Amazon.com, he can gain access to the poorly secured information system of a municipal entity, let's say Municipal Entity A, and use this to propagate an attack. Amazon.com would see an attack being initiated from Municipal Entity A. Hacker Bill would still remain anonymous while siphoning credit card numbers, or the like, from Amazon.com. Municipal Entity A and its poorly secured network is what ultimately allowed Hacker Bill to perform the hack. Municipal Entity A not only would have its reputation damaged, but could face some serious penalties. Hacker Bill, in true hacker style, remains anonymous and moves onto his next big gig while Municipal Entity A takes the fall and Amazon.com cleans up the mess. If Hacker Bill uses your municipal network to attack and hack another organization, why would Amazon.com pursue the hacker, who has much less financial backing and will be harder to find to persecute?

Municipalities should have the proper security in place to prevent hackers from using their networks as a launching pad for attacks. Based on Kostin, Ruffkess & Company, LLC's experience at our clients, the majority of security issues can be fixed with very little cost. All too often we focus on the technical aspects to manage data risks and forget that people, policies, and processes are just as, if not more, important. Education is the key when it comes to security. No technical devices will ever protect the information system better than a user who understands the risks.

The best place for a municipal entity to start is by having a very clear and concise data security policy. Write your security policy in terms that an end-user will understand and keep it



focused on specific items. For example: lock the screen when you walk away from the computer. Once this guideline has been implemented, follow through with a random audit, jot down the number of exceptions, and re-perform the random audit at a different point in the future. Be sure to benchmark your results.

Host a ‘lunch-&-learn’ or breakfast seminar to educate users on email risks. Most municipal organizations have implemented firewalls and email attachment scanning to protect against outside threats. However, the majority of attacks arise in the form of phishing emails with links that trick users into visiting a malicious site. A visit to these sites can install malware and other unwanted viruses on the computer, causing technical support issues, down time, and frustration on both the end-user and technical staff. A 15 minute seminar that addresses these risks can better educate your users, secure your network, and preserve technical resources for the job they were hired to perform.

Create a long term and short term plan and advocate! IT Departments are still viewed as a “help desk” function in the municipal world. The majority of the time spent by the IT departments in the municipal sector is reactive in nature as it is focused on fixing problems, with very little resources left for proactive activities such as planning for increased usage, more storage space, quicker connectivity, or better security. The IT manager in a municipality is focused on running the operational aspects of the infrastructure and department. As technology becomes more incorporated into local governments, the IT manager is going to become more involved in the tactical and strategic aspects of information technology, such as effectively implementing new technologies, discovering and promoting the capabilities of the information technology function, and researching more diverse technological choices. In short, the role of the IT manager is changing in the municipal world from a day-to-day operations manager into more of a strategic planner.

Ensure the availability of documentation of the network. Most documentation we receive during our audits is, at best, out of date. Usually, there is none. Make sure the network diagram is up-to-date. A network diagram, presented to management in the proper way, can also be an excellent tool for depicting the complexity of the technology environment and advocating for more resources. A list of all applications in use by the municipality can help to ensure IT employees are leveraged adequately. A documented backup procedure and backup log is a great start for a disaster recovery plan. Workflow diagrams that depict what information is flowing into and out of each application can help when evaluating new technologies or attempting to integrate applications.

Review firewall logs and access logs on a periodic basis. This is a fundamental control for a municipal environment to ensure that unwanted visitors are not stealing your bandwidth or resources. Know who’s accessing your system and why, even if your network is managed by a third party provider. Technology can be outsourced to a third party; security can not. A municipal entity is still responsible for the security of its information system, regardless of who manages the technology operations. If you are using a third-party technology service provider, make sure the contract includes a right-to-audit clause because the risk appetite of a municipal entity may be different from its third-party technology service provider.



Patch! Software vendors release patches to their products to fix vulnerabilities or to enhance the usability of the product; both of which are important to securing and optimizing your system. Make sure operating systems and applications are up-to-date on patches. Web servers and email servers, since they interface with the internet, are critical to keep patched.

Use strong passwords. Most all security issues, both internal and external, pare down to one thing: lack of a complex password, yet this is the easiest and cheapest way to force data security. Passwords should be 8 characters and require the usage of alphanumeric and special characters. Passwords should also be changed on a frequent basis (between 30 and 90 days depending on the sensitivity of the underlying data).

Physically secure all network equipment. Many times physical security is overlooked, but it's one of the easiest ways for a malicious intruder to get onto a municipal network and begin causing trouble. Make sure server rooms are locked and perform a periodic inventory analysis of hardware, software, and software licenses.

Municipal entities should still understand that information security is a necessity. The aforementioned security-fixes are meant to help municipal IT directors better safeguard their network.

Michelle D. Syc, a certified ethical hacker and certified information system auditor, heads the Information Technology Assurance Service Group at Kostin, Ruffkess & Co. LLC, with offices in Farmington and New London, Conn., and Springfield, Mass. She is responsible for evaluating information systems, identifying vulnerabilities and recommending solutions. You can reach her at MSyc@kostin.com.