CIRMA

Municipalities and public schools may be targeted for cyber attacks due to the vulnerable and open nature of their operations

Cyber Security

CIRMA
Member Owned
Member Governed

Connecticut Interlocal Risk Management Agency
900 Chapel Street
New Haven, Connecticut 06510
www.CIRMA.org

April 2017

Cyber risks, while often serious, can be managed through appropriate risk management techniques

"In this complex, interconnected world, no enterprise can think of its security as a standalone problem."

Critical Security Controls for Effective Cyber Defense
Center for Internet Security

A Pervasive Threat to Public Entities

According to the 2016 Verizon Data Breach Report, public entities experienced 47,237 known data breach incidents. In the past, scattershot, broad-based attacks were often more about causing mischief than stealing confidential or financial data; however, the threat has changed. Targeted, malicious, and persistent attacks are designed to acquire valuable information, often for financial gain, and can cause significant disruption.

Because local governments store and maintain an extraordinary amount of personal and sensitive information, they are a prime target for cyber criminals to launch malware or data-retrieval attacks. As a result of cyber attacks, government agencies have lost millions of citizen records since 2009. Although the responsibility for cyber security may seem overwhelming and sometimes bewildering, as with any exposure, it can be managed through appropriate risk management techniques and specialized insurance programs.

Identify and Prioritize the Risks

To begin the risk management process, municipalities and school leaders should identify and prioritize the risks. Ask:

- Which systems, networks, computers and servers are **most critical** to maintain the mission of the municipality and school district?
- Which data systems and databases contain the **most sensitive** information?

Questions to Consider

As you proceed through the risk management process, there will be many issues that should be considered and questions to be answered; for example:

- What are the rules that will govern the use of Town or School resources? (i.e. computers, smartphones, tablets, etc.)
- What training should be available to staff, and how will it be delivered?
- If there is a cyber event (malware, spyware), who should be contacted in the organization?
- What is the policy on bringing personal devices into the workplace?
- What devices are allowed to connect to the organization's system and could they device infect the system?

Hazards and their Effects

The next step for municipalities and school districts should be to analyze how cyber hazards would affect daily operations. A cyber-attack may result in:

- Unauthorized access to servers and computers.
- Unauthorized access to software, hardware, and networks.
- Loss of data.
- Deletion or modification of data.
- Unsecured portable devices and computers.

The Risk of Human Error

After risks to the computers and network systems from outside threats, one of the most common and costly cyber risks to most municipal and school operations comes from unsafe cyber practices used by their own employees and vendors. Even the best security systems can be compromised by an employee who clicks on a link in a phishing email or accidentally installs malicious pieces of software, such as ransomware, that can take over a network, computer, or communication

Portable devices pose special risks

The use of portable devices, whether personal or organization-owned, increase the risks of:

- Data loss when the device itself is lost,
- Data exposure when sensitive data is exposed to the public or to a third party without consent,
- Increased exposure to network-based attacks between the network system and the device over the Internet.

An effective enterprise-wide training program should take a holistic approach

system. It is estimated that **one-in-five employees** will inadvertently click on a "bad" link.

Human error remains a major point of vulnerability and one that municipalities and schools should address early on. There are some simple best practices should be put into place to reduce the risk of staff letting in nefarious malware:

> "The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise."
>
> *The CIS Critical Security Controls for Effective Cyber Defense*
> Center for Internet Security

Recommended Best Practices

- Implement a password policy; this is one of the **most** important best practices.
- Train and test staff regularly and repeatedly so that they understand and fully appreciate their role in maintaining a cyber-safe work environment.
- Institute strong security rules for vendor access to systems, facilities, and equipment.
- Develop strong policies concerning employee access to sensitive information, especially at separation of employment.
- Train employees not to use "plug-in" devices, such as thumb drives, from unfamiliar sources.
- Train employees to "lock" their computers when not at their desks.
- Institute a strong acceptable-use policy for electronic communication devices equipment.
- Restrict employee access based on their job descriptions and responsibilities.
    - Separation of administrative vs. employee access.
- Implement a strong Bring-Your-Own-Device policy.
- Implement a strong incident reporting protocol for all employees.
    - The best way to support your municipal or school cyber security defenses is to ensure that your organization reports incidents through the appropriate channels as soon as they are discovered.
- Monitor employee behavior to ensure compliance.

> "To be effective in both cost and outcome, security training should be prioritized, focused, specific, and measurable."
>
> *Critical Security Controls for Effective Cyber Defense*
> Center for Internet Security

Implementing a Strong Password Policy

Why do strong, unique passwords matter? Stolen, weak, or default passwords are involved in about 63% of confirmed data breaches according to the Verizon Data Breach Report. Although cyber security experts recommend the use of strong, unique passwords as a top priority, unfortunately this remains one of the *least* followed recommendations. Strong, unique passwords are crucial for several reasons.

The first reason is that every day cyber attackers compromise websites and online accounts, and post lists of usernames, email addresses, and passwords online. This not only exposes people's passwords, it exposes them with information that uniquely identifies the user, such as an email address. That means that a malicious actor can look for other accounts associated with that same person, such as work, personal social media, or banking accounts. Then they can try with the exposed password, and if the password has been reused, they can gain access.

Secondly, when malicious cyber threat actors can't easily find or a guess the password, they can use a technique called *brute forcing*. This is a technique where they try every possible password until the correct password is identified.

Addressing human factors includes a implementing a strong password policy

"...Empowering people with good cyber defense habits can significantly increase readiness. "

Critical Security Controls for Effective Cyber Defense

Center for Internet Security

Computers can try thousands of passwords per second, but for this technique to be worthwhile, the malicious cyber threat actor needs the password to be easy to identify. The stronger the password the less likely brute forcing will be successful.

For instance, when faced with choosing a password that fits these requirements, most users will pick a word, put the uppercase letter first, and end the password with the number and symbol. Alternatively, many people will replace common letters with a number or symbol that represents that letter. This changes a common password, such as "password," into the only slightly more complex password of "p@ssw0rd," which is still an easy-to-guess pattern.

Recommendations for creating strong, unique passwords
Consider using a password manager, which is an application that can run on a computer, smartphone, or in the cloud, that securely tracks and stores passwords. Most password managers can also generate strong, random passwords for each account. As long as the password to access the password manager is strong and unique, and two-factor authentication is being utilized, this technique can be affective. However, if the company running the cloud-based password manager is compromised, or a vulnerability in their software is discovered and leveraged by an attacker. It is possible that all of the passwords could be compromised. If you choose a password manager that is local to your computer or smartphone, your passwords may be compromised if malware gets on your computer or you lose your smartphone. When choosing a password manager, ensure it is from a known, trustworthy company with a good reputation.

Another technique to assist in building strong, unique passwords, is to choose a repeatable pattern for your password, such as choosing a sentence that incorporates something unique about the website or account, and then using the first letter of each word as your password. For example the sentence: "This is my January password for the Center for Internet Security website" would become "TimJp4tCfISw." This password capitalizes five letters within the sentence, swaps the word "for" to the number "4," and adds the period to include a symbol. The vulnerability in this technique is that if multiple passwords from the same user are exposed it may reveal the pattern. Variations on this technique include using the first letters from a line in a favorite song or a poem. Employees should be reminded that Post-It notes, index cards, etc. aren't secure from attackers even if they might be out of sight under the keyboard.

Reducing Risk from Independent Contractors/Third Party Vendors
Additional cyber risk exposures stem from business partners and other third party resources.

Municipalities often use third parties to handle aspects of their information technology infrastructure, control systems, and security. It is critical that municipalities understand the security services that their contractors provide. Municipalities and school districts should take the following steps to enhance their network security while allowing these third parties access:

Recommendations for reducing risk from third-parties:

- Ensure all contracts and agreements contain appropriate hold-harmless and indemnification language.

"Attackers, who can be located anywhere in the world, are continuously scanning the address space of target organizations, waiting for new and unprotected systems to be attached to the network."

Critical Security Controls for Effective Cyber Defense

Center for Internet Security

- Municipalities should ask their internet service provider about the various levels of security they offer, including protection from distributed denial of service (DDoS) attacks.
- Ensure that transfers of the data are properly protected and that the vendor only has the necessary access in the network to maintain and protect confidential information.
- Be sure to draft requests for proposals (RFPs) that include requirements that support and consider your security policies.
- When possible, ask vendors about the security characteristics of their products.
- Implement a strong incident reporting protocol for all vendors.

Protecting Town and School Websites

Municipalities and school districts communicate information through their websites. These websites may also contain employee portals as well as student portals, which allow users to access to sensitive or even confidential information.

A website can be thought of as a office building with an unlocked front door and an office safe that is wide open: the information in the safe is accessible to anyone looking for it. This is why municipal and school leaders should take every precaution to protect data that is posted on or accessible through a website. Cyber thieves are invisible and fast, searching website for details of vendor accounts, staff information and student records, especially identifying information that can be used in scams or identity theft.

Theft is not the only thing on the mind of a hacker: data destruction or ransom is a major motivator as well. Cyber criminals may want to destroy records, manipulate websites to redirect the town or school's information or deny internet service (DDoS).

Because the threat is changing rapidly, municipal and school leaders should take steps to prevent these types of attacks on their websites. Even the most basic protection will discourage many cyber criminals enough to make them go elsewhere. While there are not any guarantees that your organization won't be attacked, following these eleven basic principles will assist in protecting your website and electronic data from cyber criminals.

Recommendations for protecting websites:

- Ensure all areas of the website are updated.
- Toughen up access control.
- Tighten network security.
- Install a web application firewall.
- Install security applications.
- Hide admin pages.
- Limit file uploads.
- Use SSL.
- Remove form auto-fill.
- Back-up frequently.

Unsecured website and web portals can act as an open door to cyber thieves.

> "Deficiencies in security logging and analysis allow attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without protected and complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers."
>
> *Critical Security Controls for Effective Cyber Defense*
>
> Center for Internet Security

Avoiding Business Email Compromises

The FBI estimated that from 2013-2015, Business Email Compromises (BEC) related losses affected 22,143 victims in 79 countries, with estimated losses of $3,086,250,090. A business email compromise is an exploit in which the cyber criminal gains access to a municipal or school district email account and spoofs the owner's identity to defraud the entity and its employees, residents, or partners of money. In some cases, the con artist may simply create an account with an email address that is very similar to one on the municipal or school district's network. BECs are also referred to as "man-in-the email attacks."

In a BEC exploit, the criminal can use the identity of someone on a network to trick the target or targets into sending money to the actor's account. BECs may involve malware, social engineering or a combination of the two. The most common use of BEC are to obtain wire transfers or ACH payments from their targets. Cyber criminals may further use a compromised account (especially those of HR employees) to gain more personally-identifiable information (PII) for later use in defrauding the company or its clients.

The U.S. Department of Justice Federal Bureau of Investigation, Office of Private Sector, published a bulletin on BECs that highlighted preventative measures to protect entities from these attacks, they are:

BEC Preventive measures a for IT & financial security:

- Establish more than one communication channel to verify significant transactions.
- Use digital signature on both sides of transactions.
- Immediately delete unsolicited email (spam) from unknown parties.
- Forward emails and include the correct email address to ensure the intended recipient receives the email.
- Keep alert to sudden changes in business practices; encourage employees to question and report any suspicious or sudden change in business practices.

BEC Preventive measures for general operations:

- Avoid free web-based email, if possible.
- Establish a website domain and use it to establish email accounts for town and school business use.
- Be careful what is posted to social media and entity websites.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Separate computer devices from Internet of Things (IoT) devices.
- Disable the Universal Plug and Play protocol (UPnP) on your router.

Additional measures to prevent BECs:

- Employee education.
- Phone verification of payment changes.
- Secondary sign-offs for payment changes. And,
- Keeping an eye out for irregularities in email communications.

Cyber Security Risk Management Planning

After the risks have been identified, municipalities and school districts will

“Telltale signs of a potential *phishing* email or message include messages from companies you don’t have accounts with, spelling mistakes, messages from the wrong email address.”

Center for Internet Security

have a holistic understanding of the exposures. This will allow you to move forward with an Enterprise Risk Management approach that uses best practices to build a secure cyber environment that will protect your data, community, and employees.

To reduce the likelihood of suffering from a catastrophic attack, municipalities should implement a formalized cyber security plan. This implementation should be a shared responsibility by all departments within the municipality. The municipality’s ability to identify what online activities by their employees put their digital information at risk is crucial in developing the policies and trainings needed to reduce the risk of human error. Learning about the dangers online and taking action to protect your organization will make the internet a safer place for all municipalities.

While there are not any guarantees against malware and other cyber attacks, such as ransomware, by having a strong backup protocol in place, your municipality or school district can be back online in a timely fashion.

“The CIS Critical Security Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state.”

Critical Security Controls for Effective Cyber Defense
Center for Internet Security

Appropriate backup protocols will vary depending on your entity’s tolerance for how much data you are willing to lose (known as a “data deductible”). However, there are several simple practices that can be implemented, regardless of your specific tolerance for risk/data loss:

- Implement a data backup protocol.
- Physically separate backup systems from networks and servers once data is saved.
- Implement redundant backup systems.

Center for Internet Security’s Critical Security Controls

To further assist public entities in defending themselves from cyber-attacks, the Center for Internet Security (CIS) has established a list of Critical Security Controls (CSCs). The CSCs are informed by actual attacks and effective defenses, and reflect the combined knowledge of experts from every part of the cyber world (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and from many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to develop the consensus list of Controls. The Controls represent the best defensive techniques to prevent or track attacks. The Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The Controls not only work to block an initial system compromise, they also help to detect already-compromised machines and preventing or disrupting attackers’ follow-on actions. The defenses identified through the Controls deal with reducing the initial attack by hardening device configurations, identifying compromised machines to address long-term threats inside an organization’s network, disrupting attackers’ command-and-control of implanted malicious code, and establishing an adaptive, continuous defense and response capability that can be maintained and improved.

Municipal and school leaders can download the CSCs for free from the Center for Internet Security at www.cisecurity.org.

As previously mentioned, one of the most effective preventative measures a municipality or school district can take is regularly communicating and

For additional information on this topic, please contact George Tammaro, Risk Management Services Manager, CIRMA, 203-946-3076, or at gtammaro@ccm-ct.org.

training all computer users in cyber security best practices. This training can be accomplished by implementing protocols to review the entity's policies and protocols when password changes are required.

After an Incident: Response and Mitigation

Local law enforcement should be contacted when an attack, breach, BEC, ransomware or other cyber-attack is experienced. Law enforcement may be able to provide guidance and consult with resources to assist in response to the attack. Communicating with law enforcement also allows for an open exchange of information and may assist with other investigations currently being conducted. This information may be valuable in stopping future attacks.

CIRMA Liability-Auto-Property members should report Cyber incidents to CIRMA as soon as it is discovered by following the instructions on the CIRMA website at www.CIRMA.org/Claims Reporting button.

Sources

2016 Verizon Data Breach Report. https://www.entrepreneur.com/article/241620

Center for Internet Security. www.CISECURITY.ORG. https://www.cisecurity.org/critical-controls/documents/CSC-MASTER-VER61-FINAL.pdf

Margaret Rouse, TechTarget.com, Business Email Compromise (BEC, man-in-the-email attack),

U.S. Department of Justice Federal Bureau of Investigation, Office of Private Sector

State of Connecticut Department of Emergency Management and Homeland Security https://msisac.cisecurity.org/newsletters/2016-03.cfm

The Connecticut Interlocal Risk Management Agency, CIRMA, is Connecticut's leading provider of municipal risk financing and risk management services. A member-owned and governed agency, CIRMA provides high quality insurance for municipalities, school districts, and local public agencies. CIRMA operates two risk pools, the Workers' Compensation and the Liability-Auto-Property pool. It also provides Heart & Hypertension claims services and claims administration and risk management services to self-insured municipalities. CIRMA's financial strength enables it to provide assured rate stability, open availability, and expert risk control and claims services.

Cyber Security

This publication is intended for general purposes only and is not intended to provide legal advice. If you have questions about particular legal issues or about the application of the law to specific factual situations, CIRMA strongly recommends that you consult your attorney.