Friends of Local Government
Policy Paper Series

2016: The Changing Face of Cybersecurity & What it Means for Municipalities

Morris A. Enyeart, Ed.D.
NJLM Web & Internet Consulting Service

Volume 7, Number 3
January 2016

Preface

This is the 27th paper in NJLM Foundation's "Friends of Local Government" Policy Paper series. This paper, authored by Dr. Morris A. Enyeart, New Jersey State League of Municipalities Web Advisory Service Consultant, is entitled "2016: The Changing Face of Cybersecurity and What it Means for Municipalities."

Dr. Enyeart has authored numerous articles, given presentations and webinars on a variety of topics from 1996 to the present for the League of Municipalities. The focus of his publications have been municipal websites, e-commerce, New Jersey's Open Public Records Act, outsourcing, cyber threats, and social media. Copies of his publications are available at www.cityconnections.com/articles.html. Dr. Enyeart has also conducted website audits and training at the state, county and local government levels as well as New Jersey government associations over the past twenty years.

On behalf of the Board of the NJLM Educational Foundation, we thank Dr. Enyeart for these contributions, and believe you will find this paper informative.

About the Author

Morris A. Enyeart is a former Chief Information Officer for the International and Global Runoff Divisions of CNA Insurance. He was also the Managing Member of City Connections LLC and is the New Jersey League of Municipalities consultant for its Web and Internet Advisory Service. Dr. Enyeart also served on the North Brunswick Board of Education and the North Brunswick Township Council.

2016: The Changing Face of Cybersecurity and What it Means for Municipalities.

Governmental and private industry efforts to implement various forms of cybersecurity began with the hacking of telephone systems in the early 1970s and quickly expanded to computers. According to an October 16, 2015 overview in Forbes by Steve Morgan[1] states, "The U.S. government has spent $100 billion on cybersecurity over the past decade, and has $14 billion budgeted for cybersecurity in 2016…Cyber-attacks are costing businesses $400 to $500 billion a year…" These staggering numbers do not include the thousands of cyberattacks that go unreported because they are small or undetected, nor do they include the explosive growth in mobile use and the Internet of Things. By 2020 various estimates place the worldwide cost in the trillions of dollars. The prospect that cybersecurity will gain the upper hand over cybercrime in the next twenty to thirty years is low given the onward march of technological innovation where each advance brings with it new opportunities for exploitation. We can expect cybersecurity to continue to play catchup.

Cybersecurity Information Sharing Act of 2015

Perhaps the biggest news of the year is the insertion of the Cybersecurity Information Sharing Act (CISA) into the December 18, 2015 Omnibus $1.1 trillion Budget Bill that passed the US Senate and was signed by the president shortly thereafter. The bill that had seen multiple versions in the House and Senate had been under development for several years and was unlikely to become law on its own merits. Opponents viewed it as a seriously flawed governmental surveillance bill while proponents argued that it was a necessary tool to fight cybercrime because the tools and strategies successfully used against a company would also be used against the government and other companies. An overview of CISA[2] as it was enacted into federal law enables private entities, non-federal government agencies, state, tribal and local governments who have been victims of cyber threats to share information with any federal entity and with each other. Companies who do share information with federal entities are immune from consumer lawsuits for sharing the data.

There is a concern that this sharing of consumer information to government agencies by private entities or other third parties merely creates new targets for hackers. At the last moment, the requirement to remove or redact any personal information from data that is shared was deleted from the bill[3] resulting the further spread of personal information. Since the sharing of information under CISA is voluntary, there is currently no way to tell how effective or widespread the program will be when fully implemented.

Other Governmental Cybersecurity Clearing and Reporting Organizations

In addition to the new clearing house created by CISA, which focuses on cyber threats, there are additional clearing houses at the federal and state level that also include cyber incidents where hackers have gained access and control of private entity and governmental systems.

---

[1] The Business of Cybersecurity: 2016 Market Size, Cyber Crime, Employment, and Industry Statistics. Steve Morgan. Forbes, October 16, 2015

[2] S.754 – Cybersecurity Information Sharing Act of 2015. Congress.gov, https://www.congress.gov/bill/114th-congress/senate-bill/754

[3] A Quick Guide to the Senate's Newly Passed Cybersecurity Bill. Larry Greenemeier, Scientific American, October 28, 2015

Homeland Security established a national clearinghouse, US-CERT[4], in 2003 that tracks hacker incidents to penetrate networks and systems or propagate Distributed Denial of Service (DDoS) attacks. The US-Cert bulletins and alerts are worthwhile to subscribe to as they include alerts and patch notices used to close exposures.

Privacy Rights Clearing House[5] has a database of business, financial, educational, government including municipalities, medical and nonprofit organizations that have reported data breaches which includes reports from 2005 to 2015 that have been made public. The number of breaches is clearly declining each year in number. While no reason is cited for the decline, it is possible that the growing numbers of reporting centers is siphoning off reports to PCA.

At the State level, on May 20, 2015, Governor Christie signed an Executive Order establishing New Jersey's New Jersey Cybersecurity and Communications Integration Cell (NJCCIC)[6] as the State organization responsible for cybersecurity information sharing, cyber threat analysis and hacker incident reporting.

The New Jersey League of Municipalities[7] also works to bring awareness to the municipal level through its Issue Alerts, seminars, webinars, sample proclamations for municipalities and Annual Conference education sessions. For example, on September 29, 2015 the League alerted it 565 member municipalities on recent attempts to defraud New Jersey municipalities using false emails from the Administrator to the CFO to request wire transfers. Marc Pfeiffer, former Deputy Director of the BH Department of Community Affairs and current Assistant Director of the Bloustein Local Government Research Center, has worked with the League to raise awareness about cybersecurity issues and awareness at the municipal level.[8]

GMIS New Jersey – Association of Government IT Leaders is an association of New Jersey municipal, Board of Education, county and state governmental members that deal with technology hardware, software and system issues affecting New Jersey governmental entities. They review technology advances, investigate problems and recommend solutions including cyber threats. The GMIS New Jersey 7th Annual Technology Education Conference will be held April 7, 2016 at The Palace at Somerset Part, Somerset New Jersey.

Involving residents of a municipality. Franklin Township, Somerset County, New Jersey takes the fight against cyber threats a step further and provides information, videos and hints to raise cybersecurity awareness for residents on their website[9]. Given the electronic interaction municipalities today have with the public, arming residents with this type of information makes them partners in the fight against cybercrime and reduces the risk of accidental malware, phishing and other intrusions.

---

[4] United States Computer Emergency Readiness Team. www.us-cert.gov/

[5] Privacy Rights Clearinghouse www.privacyrights.org/data-breach/new

[6] NJCCIC. www.cyber.nj.gov/

[7] New Jersey State League of Municipalities. www.njslom.org Search cyber security

[8] Marc Pfeiffer, Keeping your Humans Secure, November 19, 2014 www.njslom.org/99thconf/conf-presentations/Secured-Humans.pdf ;
Minimum Cyber-Security Requirements: What you need to Know, March 7, 2014 www.njslom.org/presentations/League-Webinar-Minimum-Technology-Security-Requirements.pdf ;
Managing Technology Risks Through Technological Proficiency, November 2015 http://blousteinlocal.rutgers.edu/wp-content/uploads/2015/11/BLGRC-managing-technology-risk.pdf

[9] Cybersecurity resources for Residents. Franklin Township, Somerset, NJ
http://www.franklintwpnj.org/government/departments/information-technology/cyber-security-resources

Common Municipal Targets

Common municipal targets are police and court systems, financial systems, personnel records, payment systems municipal water and electric plants are all favored targets. As ballot machines become connected they will also become targets for cyber threats. Even recreation registration information is valuable information for hackers to sell.

Two main types of Cyber Threats

Distributed Denial of Service (DDoS) are brute force attacks wherein the attacker purchases access to a botnet system that directs thousands or even millions of computers to access the network, email system or website. According to Verisign Inc., one-third of website outages in 2015 resulted from DDoS attacks. The result is that the network is overwhelmed and shuts down and your normal traffic cannot get through. Your residents are left without electronic services to pay taxes and utilities online, police 911 and dispatch functions are interrupted, health departments, payroll, bill payments and more for anywhere from a few hours to several days. Systems that crash may cause data corruption problems and require expensive re-building in order to come back online. The reasons a municipality may be subjected to a DDoS attack may originate in criminal activity by gangs or individuals, political protests (think Anonymous), revenge and disgruntled employees. The attacker does not have to have highly technical skills to initiate a DDoS attack. He/she just needs to be able purchase the service on the dark web.

DDoS attacks disabled Maine.gov three times[10] in March 2015 along with the Bangor municipal website other websites. The San Jose Police Department was offline for several days due to a DDoS attack in November 2015. Rutgers University has also had departments shut down by DDoS attacks in 2015[11].

Cybersecurity vendors have taken two approaches to prevent DDoS attacks. The first is to build a firewall that analyzes incoming traffic in real time and blocks incoming traffic when certain characteristics trigger a response. Hosting and network vendors offer cloud and hardware devices that range from $500/month for three million packets per second to $2,500 per month for twelve million packets per second that would protect most municipalities. Larger cities may need the services of companies like Akamai, IBM, Microsoft and Amazon that can run into the hundreds of thousands or millions of dollars depending on the level of DDoS protection needed.

DDoS attacks are just meant to deny electronic access and functioning to the municipality. Its goal is to shut down the doors so no information can get in or out for a prolonged period. While they are certainly disruptive and inconvenient, they are not the most damaging type of cyber threat to municipalities. The vast majority of municipalities in New Jersey depend on the default services provided by their hosting company and are not prepared for a specifically directed DDoS attack.

Intrusion to municipal networks and websites

The more damaging type of cyber threat to municipalities is where hackers gain access to the municipal network, utility, systems or website. The intrusion cyber threat's purpose is to gain internal control in order to steal personal/financial information or disrupt the operation while doing maximum damage. The cybercrime of selling

[10] More Maine websites targeted on third day of cyberattacks. Craig Anderson, Portland Press Herald March 25, 2015, www.centralmaine.com/2015/03/25/cyber-attacks-targets-maine-websites-for-a-third-day/

[11] Cyber attack shuts down Rutgers online classroom site. Kelly Heyboer, NJ Advance for NJ.com. December 25, 2015 www.nj.com/middlesex/index.ssf/2015/12/ho_ho_hack_rutgers_u_hit_with_another_cyber_attack.html

stolen personal and financial information on the Internet is well-known and documented. In the event of a hacker breach a municipality may spend hundreds of thousands of dollars to rebuild and harden the network against future intrusions while limiting services to residents; and then hope it will withstand the next intrusion attempt.

The problem is, that even if the network and systems are hardened and up to date, there will be upgrades and patches to apply constantly over time. Another Trojan or malware could be accidently introduced through a trusted vendor patch or network appliance so there must be constant attention to alerts and periodic tests.

A significant portion of intrusions occur accidently due to human error. An employee opens an email and clicks on a link or opens an attached file releasing a virus, malware or a Trojan into the network as it is downloaded to the computer attached to the network. Another employee inserts a flash drive in their computer given to him/her by a vendor, a volunteer, a friend or at a conference not knowing it contains a virus. Still another employee using a personal cell phone or computer that is infected connects to the network remotely to check email, update a website, upload a file or log into a municipal system may also be introducing another virus. Employees at work accessing non-municipal systems are also at risk of introducing viruses, ransomware and Trojans into the municipal network as they check social media, personal email, and conduct personal business using the municipal workstation.

All of these scenarios can and do occur on a daily basis. These types of intrusions cannot be completely eliminated, but they can be minimized through the implementation of policies, training and controlled access methods.

What Can Municipalities Do to Minimize the Exposure to Cyber Threats

When municipalities address the issue of cyber threats they frequently follow the strategy of "lock everything down" to prevent cyber intrusions. Unfortunately, this strategy is not only expensive, it is certain to fail. Given the complexity of the myriad of hardware components and the variety of methods of accessing the municipal network it is impossible to be certain there are no holes in the network hardware and software. However, even though it is not possible to lock everything down permanently, does not mean municipalities should not take steps to ensure their network and systems are secure. Financial systems and personnel data should be encrypted. Administrative functions should be tightly controlled and strong system passwords changed every thirty to sixty days. Use password manager software like DashLane or LastPass for staff to enter passwords to systems or access the network. Access via persons using TOR as their website browser should also be blocked since it is a favorite tool used by hackers to hide their origin while hacking a network.

Hire a fulltime cybersecurity officer. With the exception of the largest municipalities, hiring a fulltime cybersecurity officer is not feasible for most municipalities due to the costs. Cybersecurity staff are in short supply and are paid more than most municipalities can afford. What municipalities should consider using a shared-service agreement to hire a cybersecurity resource to be shared across multiple municipalities. This resource could create common policies, monitor their implementation, conduct training, work with individual departments where needed and bring best practices to the municipalities at a level they can afford. They should be able to leverage

other experts in the cybersecurity field to obtain best practice information such as the Cybersecurity check list for Cities published by Lea Deesing[12], a VC3 account executive for the Municipal Association of South Carolina.

Don't make hackers jobs easier. Make sure you are not accidently making information that cyber thieves can use. If you post bill lists as part of your governing body agenda, make sure you redact the bank account numbers if they are listed. One New Jersey municipality tracked fraud back to the publication of account numbers on bill lists.

Establish a Cybersecurity Policy. Create a cybersecurity policy that is reviewed bi-annually with staff to ensure they understand all of its elements. Where policy elements apply only to a single department, hold separate meetings. Where policy elements apply to volunteers and elected/appointed officials, consider creating a video with a form/quiz that applies to their responsibilities and restrictions that can be viewed at a time that is convenient for them. A good overview of Cybersecurity for Municipalities[13] was presented at the Colorado Municipal League June 2015 Annual Conference.

The Public Technology Institute is a governmental resource that can help identify resources available to support municipal cybersecurity planning[14] such as New Jersey's Cyber-DR-COOP Assessment Tool, a 2015 PTI Solutions Award Winner.

GMIS New Jersey members conducted a workshop at the New Jersey League of Municipalities 95th Annual Conference in November 2010 which addressed specific information for IT Managers of varying size municipalities which includes a checklist for small and medium to large municipalities[15] for cybersecurity.

Create an Incident Response Plan to be implemented if a credible cyber threat is identified. Know what to do during an emergency is key to minimizing the impact. Your plan must identify participants, roles, contacts and actions for every step of the plan. An extreme example was the Incident Response Plan[16] implemented by the City of Fullerton, CA in response to attacks cyber threats from an Anonymous retaliation threat.

Follow cyber attack information resources to be kept informed about the types of attacks and use the information to help design the municipal Incident Response Plan. [17] [18]

And finally to remind yourself that cyber threats are an ever present danger, check the Norse Corporation's Net Attacks Map[19] that shows real time cyber attacks identifying the origin type of attack and target.

---

[12] What City Officials Need to Know about Cybersecurity. Lea Deesing, Western City, The Monthly Magazine of California Cities, June 2015. www.westerncity.com/Western-City/June-2015/What-City-Officials-Need-to-Know-About-Cybersecurity/

[13] Cybersecurity for Municipalities, Panelists Inga Goddijn, Paul Nelson, Jeffrey A. Wells and Ken C. Price. Colorado Municipal League Annual conference, June 2015. https://www.cml.org/Issues/Technology/Cybersecurity-for-Municipalities

[14] Webinar - PTI Resources Available to Support State and Local Government Cyber Security Planning http://www.pti.org/news/displaynews.asp?NewsID=238&TargetID=3

[15] What Technology Managers Really Need to Know About Security. Panelists Michael Esolda, John Hitrchock, Bernadette Kucharczuk and Todd Costello. New Jersey League of Municipalities 95th Annual Conference, November 2010. www.njslom.org/95thconf/presentations/What%20IT%20Managers%20Need%20to%20Know%20about%20Security.pdf

[16] Cyber Security: Surviving an Anonymous Attack. Helen Hall and Paul Underwood. Municipal Information Systems Association of California, April 7, 2015 www.misac.org/news/225416/Cyber-Security-Surviving-an-Anonymous-Attack.htm

[17] Hackmageddon Information Security Timelines and Statistics www.hackmageddon.com/category/security/cyber-attacks-statistics/

[18] NJ Cybersecurity Resources www.cyber.nj.gov/resources/

[19] Norse Net Attack Map map.norsecorp.com/