WORLD JURIST ASSOCIATION BIENNIAL CONGRESS, BARCELONA, SPAIN

INTERNET: CHALLENGES TO PEACE AND FREEDOM

Panel 1: Justice, Civil Service and the Internet

Hacking Municipal Government: Best Practices for Protection of Sensitive Local Government Data

May 20, 2016

Benjamin E. Griffith* and Gerald Waltman III**

Introduction: Connect the Dots

There is a growing public awareness that online computer system vulnerabilities in the public and private sector can conceivably lead to a cyber Pearl Harbor attack. The number and extent of cyberincidents continue to grow at a geometric pace, and our elected leaders at the federal, state and local level are focused like a laser on "The Next Big Attack." Nonetheless, there are still many of us who measure life in terms of pre- and post-9/11, and collectively we have an uneasy feeling that our government may be failing to connect the dots … again.

Local Government in the Cross Hairs

We are living in the information age where almost every part of our daily lives is in some way inextricably interwoven with the Internet. Local government – including municipalities, counties, and school districts – are finding themselves in the cross hairs of cyber-attacks, most recently in connection with third-party access to county depository funds and government-owned and maintained dams. The problem is that those very networks on which we rely to enable and facilitate many critically important aspects of our increasingly digital lives, governments and systems of commercial activity are vulnerable to cyberattack. Not a day passes when malicious cyber criminals, hacktivists and other highly motivated but misdirected actors are launching attacks that originate beyond our national borders. They are targeting our businesses, commercial and proprietary trade secrets, critical infrastructure, and sensitive information. The toughest challenges lie in developing effective tools that will enable our national, state and local governments to respond in an appropriate, proportionate and effective manner to malicious cyber-attacks and cyber-enabled activities, and to provide a credible deterrence that will make others refrain from engaging in similar activities. Some countries have already begun efforts to confront these growing threats by malicious cyber attackers and cyber actors, but countries must work together to develop strategies for combatting this growing threat.

State of Cybersecurity in Local, State & Federal Government

A country's infrastructure is one of its most essential elements, and, as more infrastructure becomes dependent on the Internet, infrastructure is becoming one of the ripest targets for cyber attackers. "Securing the Electricity Grid", http://massoud-amin.umn.edu/publications/Securing-the-Electricity-Grid.pdf. United States President Barrack Obama believes that the United States is not devoting enough resources or attention to the nation's cybersecurity interests. This lack of resources and attention could make the country's infrastructure vulnerable targets for cyber-attackers, and those attacks could subject U.S. citizens to massive power outages, widespread denial of services, and compromised confidential information. "Obama warns of power grid's lagging cyber defenses", http://thehill.com/policy/cybersecurity/258588-obama-warns-of-power-grids-lagging-cyber-defenses.

In the Ponemon Institute's study of The State of Cybersecurity in Local, State, and Federal Government sponsored by Hewlett Packard Enterprise, the report concluded that government is the target of cybercriminals and state-

sanctioned attackers. See State of Cybersecurity in Local, State & Federal Government at http://www.ponemon.org/library/the-state-of-cybersecurity-in-local-state-and-federal-government

At both the local and state level as well as the federal level, a key challenge is the lack of skilled personnel. This is a major challenge at the state and local level. Lack of budgetary resources is a key issue. State and local governments may not be share as much intelligence about threats as they should.

Top security threats for local government can fall in the category of failure to patch known vulnerabilities, negligent insiders, and zero-day attacks. State and local governments are not prepared to deal with cybersecurity threats, and often their agencies have achieved a less than optimal level of maturity in their cybersecurity initiatives.

Reasonable Cybersecurity Actions Based on Threat Profile

For a local government entity concerned about cybersecurity, one key question centers on what reasonable cybersecurity actions the local government should take in light of that entity's particular threat profile. In other words, what is the local government entity's risk appetite? Local government leaders, and attorneys, must consider many interrelated cybersecurity issues in answering this question.

Interrelated Cybersecurity Issues

In this presentation, we will explore cybersecurity issues that have a direct impact upon municipalities, counties, school districts and other local governments and the citizens they represent. Among these are issues relating to the following:

1. Vulnerability to attacks: address known vulnerabilities and implement a system to monitor and update it.
2. Understand why hackers exploit local government websites and networks: whether a malicious attack by a disgruntled employee or an opportunistic attack by a third party, strengthen the local government entity's resilience through constant assessment and enforcement of best practices.
3. Greatest vulnerabilities and need for protection: consider whether cyber insurance, which may require the insured entity to undertake certain predefined tasks during a security breach.
4. Best cybersecurity practices: realize that it is not a matter of whether, but when, a cyber-attack or security breach will occur; be prepared through training, an effective response process, periodic testing, and adequate recordkeeping for central and secure storage during a cyberincident; and maintain a strong communication link with law enforcement, including a trained and staffed forensics team.
5. Hacking vulnerabilities of vehicles and mandatory security standards: Understand the "Internet of Things" – the linking of many previously non-Internet connected devices such as video cameras – to computer systems and the web. This makes it all the more important to segment networks and eliminates the "weakest link in the chain" so that a compromise of one device or sector will not translate into exploitation of the entire system.
6. Feasible means of preventing local governments from becoming gateways to federal and state hacking: make sure that the governmental entity creates network boundaries and segments that enable it to enforce detective and protective controls within its infrastructure.

Scope of the Problem

The United States and the European Union are apparently moving in different directions in the debate over "privacy" vs. "security" and do not have a uniform, coherent approach to cybersecurity problems that are international in scale. Time is running out for them to start singing from the same cybersecurity page, so to speak. Some of these problems, such as the recent Segate ATM theft and the, recently shutdown, Ramnit financial fraud debacle, can only be resolved through international cooperation and sharing of governmental and law enforcement information that includes public-private partnerships. We will discuss those in detail.

Projected Costs for Cybersecurity Protection

In the early 1970s, the government and the private sector implemented various forms of cybersecurity in response to the hacking of telephone systems later expanded to computer systems. One analyst reported in an October 16, 2015 article that the U.S. government had spent over $100 billion on cybersecurity over the past decade and had budgeted $14 billion for cybersecurity in 2016. With cyber-attacks costing businesses $400 to $500 billion a year, these figures to not take into account the thousands of cyberattacks that go unreported because they are small, undetected or do not include the explosive growth in mobile use and the internet. Steve Morgan, *The Business of Cybersecurity: 2016 Market Size, Cyber Crime, Employment, and Industry Statistics*, Forbes, October 16, 2015.

Advances in Technological Innovation vs. New Opportunities for Exploitation

Some have projected that by 2020, the worldwide cost for essential cybersecurity protection will approach trillions of dollars. This is a game in which cybersecurity will continue to play catchup, with no real prospect of gaining the upper hand over cybercrime for the next two to three decades. As we witness advances in the relentless march of

technological innovation, cyber criminals match each step forward with a giant step backward as new opportunities surface for exploitation. *The Changing Face of Cybersecurity & What it Means for Municipalities*, Morris A. Enyeart, Ed.D. Jan. 2016.

A Quick Look at the Numbers

As of three years ago, the number of cyber intrusions by various actors was running at a gallop:

- BP claimed to have suffered 50,000 attempted cyber intrusions per day.
- The Pentagon reported 10 million attempts a day.
- The U.S. Energy Department's National Nuclear Security Administration recorded 10 million hacks a day.
- The United Kingdom reported 120,000 cyber incidents per day.
- The State of Utah claims to have 20 million attempts per day, up from 1 million per day two years before.

Brian Fung, *How Many Cyberattacks Hit the United States Last Year?* National Journal, March 8, 2013.

These numbers and the boldness of the cyber-attacks have grown exponentially.

Segate's $55 Million ATM Cashouts

In June 2015, the U.S. began prosecuting Ercan Findikoglu, a Turkish citizen known as "Segate," for allegedly orchestrating one of the largest cyber bank heists in American history. Segate masterminded a series of Oceans 11-type ATM heists that led to the theft of over $55 million by hacking bank computers and withdrawing millions in cash from ATMs. Findikoglu allegedly organized "ATM cashouts" by hacking into networks of several credit and debit card payment processors, enabling the intruders to simultaneously lift the daily withdrawal limits on numerous prepaid accounts for each processor and dramatically increase the account balances on those cards to allow ATM withdrawals far in excess of the legitimate card balances. The criminals cloned the cards and sent them to co-conspirators around the globe, who used the cards at ATMs to withdraw millions in cash in the span of just a few hours. These "unlimited operations" relied on the manipulation of withdrawal limits, and the cybercriminals were able to steal virtually unlimited amounts of cash until the operation before being shut down. See A Busy Week for Ne'er Do Well News, Krebs on Security, http://krebsonsecurity.com/tag/ercan-segate-findikoglu/

Europol Cross-Border Cooperation

International engagement on cybersecurity is essential, as proved by Europol's efforts. In June 2015, Europol investigators announced the arrest of five Ukrainians suspected of developing, exploiting and distributing banking Trojans, the ZeuS and SpyEye malware that were used to steal hundreds of millions of dollars from consumers and small businesses.

The cybercriminals specialized in creating malware, infecting machines, harvesting bank credentials and laundering the money through money mule networks. Through digital underground forums, they actively traded stolen credentials, compromised bank account information and malware, while selling their hacking 'services' and looking for new cooperation partners in other cybercriminal activities, according to Europol. Their criminal activities entailed work in countries across all continents, infecting tens of thousands of users' computers with banking Trojans, and subsequently targeting many major banks. See http://krebsonsecurity.com/2015/06/a-busy-week-for-neer-do-well-news/#more-31368.

The Europol operation resulted from a successful coordination of an international team of investigators to bring down a destructive cybercriminal group, and it demonstrated that it was possible to combat cybercrime in a sustainable way if the investigative judges and judicial authorities coordinated and cooperated across the borders in the fight against threat brought about by malware. *Major Cybercrime Ring Dismantled by Joint Investigation Team*, June 25, 2015, https://www.europol.europa.eu/print/content/major-cybercrime-ring-dismantled-joint-investigation-team

Ramnit: Public-Private Collaboration to Enhance Cybersecurity

In February 2015, a joint operation by Europol, FBI and Symantec and other technology companies and international law enforcement agencies struck against the Ramnit botnet, a prominent financial fraud botnet that had been in operation for over five years. Before Europol and Symantec dismantled it, Ramnit harvested banking

credentials and other personal credentials from its victims, infecting over 3.2 million computers. Prepared testimony of Adam Bromwich, Vice-President, Security Technology and Response, Symantec Corporation, Emerging Cyber Threats to the United States, at 7, U.S. House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure and Security Technologies, Feb. 25, 2016.

Ramnit provided attackers with multiple ways to defraud their victims once their computers were compromised, by monitoring their web browsing sessions, stealing banking credentials, stealing website cookies that allowed cyber attackers to impersonate the victim, taking files from the victim's hard disk, granting the attackers remote access to the computer, and allowing them to infiltrate stolen information or download additional malware. http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation.

Financial Malware

Before it was shut down, Ramnit became a fully-featured cybercrime tool, featuring standard modules that provided attackers with multiple ways to compromise a victim, including a spy module that monitored the victim's web browsing and detected when they visited online banking sites at which point it could inject itself into the victim's browser and manipulate the bank's website, making it appear that the bank was asking the victim for additional credentials such as credit card details that could then be used to facilitate fraud.

Aside from the spy module, Ramnit featured (1) a cookie grabber that allowed the attacker to hijack online banking sessions, (2) a drive scanner that could steal files from the computer's hard drive and ferret out sensitive information like passwords, (3) an anonymous FTP server through which the attackers remotely accessed the compromised computer and browsed the file system, using the server to upload, download, or delete files and execute commands, (4) a virtual network computing (VNC) module that gave the attackers another means to gain remote access to the computer, and (5) an FTP grabber that allowed the attackers to gather login credentials for a large number of FTP clients. See https://nakedsecurity.sophos.com/2015/02/27/europol-takedown-of-ramnit-botnet-frees-3-2-million-pcs-from-cybercriminals-grasp/

Chelan County, Washington v. Bank of America Corporation

County depositories are not immune from cyber theft and security breaches. A recent example from Washington State tells us why. The county treasurer of Chelan County, Washington was required to hold and disburse funds for the county medical center. Unauthorized payments by third parties totaling over $1 million were made from Chelan County's main operating account and its direct deposit account, with access being gained to a county medical center employee's computer via a computer virus or malware. The county's claims against Bank of America alleging liability for the bank processing of the fraudulent fund transfer requests, survived a motion for summary judgment. Chelan County, Washington v. Bank of America Corporation et al, 2015 WL 4129937 (E.D. Washington July 9, 2015), accessible online at http://scholar.google.com/scholar_case?case=13940983776102082 16&q=related:2KNnkxbVWBMJ:scholar.google.com/&hl=en&as_sdt=3,25

The main operating account held the county's tax receipts and other deposits, including deposits from the county medical center. The direct deposit account was used to directly deposit funds into employees' accounts using Bank of America's Automated Clearing House account services. Bank of America informed the county that its software was converting to a new online banking platform called CashPro, which county medical center employees could use to process payroll payments by logging in to the CashPro platform with a unique user ID, a company ID, and a password. The county used a manual transfer procedure by which a county medical center employee with proper authorization could select the Direct Automated Clearing House transfer module to create a payroll payment order. Three payment orders were made using the unique login information of a county medical center employee to sign in to Cash Pro, resulting in an overdraft of the account for $1 million. The fraudulent transfers were not discovered until after all of the payment orders were processed, and only a fraction of the transferred funds were recovered by the county when it issued reversals to the receiving banks.

The U.S. District Court for the Eastern District of Washington denied Bank of America's motion for summary judgment because it concluded that there were material factual disputes regarding the commercial reasonableness of the overall security framework agreed upon by the bank and the county, regarding whether the bank acted on certain security procedures in good faith, and regarding whether the bank offered the county alternative reasonable security measures that the county refused.

Iranian Cyber Attacks Targeting New York Dam

The President's earlier mentioned fears about the vulnerabilities of U.S. infrastructure appear to be well grounded. During a three-week period in 2013, hackers linked to the Iranian government launched cyber-attacks on multiple targets, one of which was the Bowman Avenue Dam, a flood-control dam north of New York City. Officials cite the incident as a warning and a "shot across the bow" that U.S. infrastructure such as power plants and water-treatment facilities are vulnerable to cyber-attacks. The Attorney General of the United States noted that the hacking of this dam could have posed a danger if the facility had not been shut down for maintenance. The dam cyber-attack followed the imposition by the U.S. of sanctions on the Iranian government and a cyber-attack on Iran's nuclear program utilizing the Stuxnet virus, discussed below.

The Bowman Avenue Dam was about 20 miles north of New York City, built in the 1940s, and is 119 feet long and 13 feet high. According to the U.S. Attorney for the Southern District of New York, Preet Bharara, the security breach at the dam represented "a frightening new frontier" for cyber-attacks. According to the indictment that were unsealed in March 2016, Hamid Firoozi repeatedly obtained unauthorized access in 2013 to a computer that controlled the supervisory control and data acquisition of the Bowman Avenue Dam, repeatedly obtained information about the dam's status and operation, including water levels and temperature and the status of the gate that controlled flow rates. Although access to the system would have typically permitted a remote user to operate and manipulate the sluice gate, unbeknownst to Firoozi, the dam's management had manually disconnected the sluice gate control earlier for maintenance. New York Senator Charlie Schumer urged the U.S. to begin a probe to determine if critical infrastructure is vulnerable to cyber-attacks and emphasized that state and local governments and companies need to beef up computer security, noting that "[h]ackers can come in, as these Iranian hackers did, and hurt our critical infrastructure. What if they open the sluice gates of a dam with a whole lot of people behind it?" *Iranians Hacked From Wall Street to New York Dam, U.S. Says*, Bloomberg Technology, March 24, 2016, http://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

Stuxnet

As noted above, a possible motivation for the Iranian-led cyber-attack on a New York dam in 2013 may lie in events several years before surrounding the Stuxnet virus. Stuxnet had completed its mission by the time it was discovered. TA human intelligence agent seeded those Iranian facilities with Stuxnet-infected USB drives that were picked up by engineers and used with their personal laptop computers first introduced him Stuxnet virus into Iranian nuclear facilities. The Stuxnet laptops were used to update software that was in turn used in the computerized controllers that directed the centrifuges. Once the laptops were plugged into maintenance ports, they infected the hosts, and the delivery was complete. Stuxnet ran successfully, and the Iranian nuclear program was set back several years. See Chris Inskeep, Managing Attack Vectors to Disrupt Cyber-Attack Delivery (Advances Protection Strategies) ('Managing Attack Vectors').

The level of sophistication in cyber-attacks and the methodologies behind them has grown significantly since the delivery of the Stuxnet virus gave other state-sponsored actors the incentive to orchestrate multi-stage attacks, spear phishing, DDS (distributed denial of service), encrypted malware, stub-viruses, masquerading through keystroke logging malware and replay of stolen logon credentials. New and emerging threats are coming from the Stuxnet Family viruses. See Managing Attack Vectors.

Spearphishing

One form of direct social engineering attack is spearphishing, delivered by e-mail and designed to exploit human vulnerabilities. Spearphishing exploits a weakness in the e-mail system technology: the sender address is assumed correct, hence, the addressee routinely opens e-mails that purport to have originated with colleagues, business associates, acquaintances, and friends. It the attackers can spoof a credible sender's address information; the

recipient will be more likely to open the message. The attack delivery would be disrupted and the attack would fail if spurious e-mails were not delivered by the e-mail system, as when the e-mail recipient has an easily available means to verify the origin of the message. Spearphishing is enabled when the recipient is unable to easily verify the message origin or guarantee of origin, and its success reveals serious shortcomings of current e-mail technology. Managing Attack Vectors.

Disruption of Attack Delivery

Many multi-stage cyber-attacks begin with spearphishing that uses e-mail as the attack vector, with credible messages that the victim will likely open and respond to positively. Message credibility is a critical factor in such an attack. If the recipient of the message is aware that the message was not from a guaranteed origin, that is, not from whom it purported to be from, message credibility could become a significant hurdle for the attacker.

Multi-Stage Attacks by State-Sponsored Actors

In 2011 and 2012, hackers attached Coca-Cola Corporation with what began as a spear phishing targeting of a senior corporate executive with a malicious e-mail purporting to be from the CEO. Contained in the e-mail message was a link to a malicious website that performed a drive by download of keystroke logging malware. The goal of this attack was the theft of data relating to Coca Cola's acquisition of another company, but the attack may have had grander designs. Malware compromised the logon credentials and enabled unauthorized but unrestricted access to the corporate resources on the network. The attackers used stub viruses, a new strain of remotely updatable malware with new capabilities. The company did not detect the theft of sensitive data was undetected for a lengthy period. Managing Attack Vectors.

Aramco attack

The Saudi-owned Aramco was subjected to a viral attack in 2012 that killed up to 30,000 desktop computers. The hackers apparently worked with or paid off an Aramco insider who was sympathetic to Iran and who helped plant the virus in the Aramco network. The virus destroyed computer hard drives, and it did so effectively. The virus disrupted Aramco's operations while the virus was being contained and the network was being disinfected. Managing Attack Vectors.

Zeus Virus and Masquerading

Conventional wisdom tells us that viruses spread through propagation, and behavior malware detection software detect viruses. When a virus does not exhibit expected behavior, according to this conventional wisdom, the effectiveness of anti-malware protection controls can be seriously challenged. This brings us to the field of malicious software of a particularly problematic type: The Zeus Trojan Horse Virus.

Stealing Confidential Information from Compromised Systems

The Zeus virus is a keystroke logging software delivered by drive by download, through a Zeus Trojan. It runs on versions of Microsoft Windows and steals information by man-in-the-browser keystroke logging and form grabbing. Zeus is designed to steal confidential information from the computer systems it has compromised and does so by specifically targeting system information, online login credentials, and banking information. It has also been used to install the CryptoLocker ransomware and is spread through drive-by-downloads and phishing schemes. The Zeus Trojan can be customized to gather social security and credit card numbers.

Wide Array of Targets in and Outside Government

Zeus was initially identified in July 2007 when it was used to steal information from the U.S. Department of Transportation. By June 2009, Zeus had compromised over 74,000 FTP accounts on websites at the Bank of America, NASA, Monster.com, ABC, Oracle, Cisco, Amazon and BusinessWeek had been compromised.

Inability to Remove All Versions from Operating Systems

While there are many forms and versions of the Zeus Trojan, it appears that no utility can effectively detect and remove all versions of it from all operating systems. Some estimates indicate that as of 2009, Zeus had infected 3.6 million personal computers in the United States, and security firms proactively advised businesses to continue to offer training to users to implement such practices as not clicking on hostile or suspicious links in e-mails or websites and to keep their antivirus software current. While some vendors represent that their software protection can prevent some infection attempts, none claim the ability to prevent infection under all circumstances. See *Removing the Zeus Malware Virus*, Cox Tech Solutions, January 21, 2016, at

http://www.cox.com/residential/support/internet/article.cox?articleId=9e960f50-c2ae-11e4-52f6-000000000000; Zeus (Malware), at https://en.wikipedia.org/wiki/Zeus_(malware)

Replay Masquerades

Logging user IDs and passwords is performed so the credentials can be used later to gain access to otherwise inaccessible systems. Reusing stolen logon credentials is known as "replay", and the attacker who uses replay "masquerades" as the legitimate owner of the replayed credentials. The highest level of masquerading is compromise and replay of the logon credentials of privileged users, since it opens up the resources of corporate information systems and networks to compromise.

Protection Methodology

The protection methodology against this is two-fold: first, disrupt the implanting of keystroke logging malware, just as one would disrupt drive by downloads and detect malware before it could be implanted. Second, design a one-time credential that cannot be replayed. Options for preventing replay are one-time passwords and adding a second factor to the authentication credential such as a one-time value like the one provided by the RSA SecureID device.

Cat and Mouse

Response to a cyber-attack can depend largely the ability, talents and knowledge the attacker has about the human factors and human vulnerabilities of the target. Attack response can become a game of cat and mouse as defenenders strategies are roll out as quickly as attackers modify their attack strategy.

Attack Vectors

A successful cyberattack requires an attack delivery as an essential step. If the cyberattack cannot be delivered, the attack fails, and the danger to the target is averted. The path that a cyber attacker uses to deliver an attack is an attack vector.

Attack vectors are poorly understood and seldom addressed. That may be changing, since the conventional method of attacking was usually through the wired network, but more and more attention is being given to disruption of attempts at attack delivery. To put it another way, protection from and prevention of attacks can and should include detecting the attack vector that a cyber attacker plans to use and preventing the attack from being delivered. Managing Attack Vectors.

The Cybersecurity Information Sharing Act (CISA)

The Cybersecurity Information Sharing Act (CISA) was quietly inserted into the $1.1 trillion December 18, 2015 Omnibus Budget Bill that was passed by the United States Senate and signed by the President. Its opponents saw CISA as a seriously flawed governmental surveillance bill while CISA's proponents said it was a necessary tool to fight cybercrime, their rationale being that the tools and strategies successfully used against a private sector business would also be used against the government and other companies.

CISA includes sections about Internet monitoring that modify the Internet surveillance laws, and it broadens the powers of network operators to conduct surveillance for cybersecurity purposes. In so doing, CISA dramatically expands those powers in significant ways, the extent of which is still unknown. See S.754 – Cybersecurity Information Sharing Act of 2015. Congress.gov, https://www.congress.gov/bill/114th- congress/senate-bill/754; Larry Greenemeier, *A Quick Guide to the Senate's Newly Passed Cybersecurity Bill*, Scientific American, October 28, 2015.

Immunity from Consumer Lawsuits

One of CISA's key features is that it 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.

Some have expressed concern that such sharing of consumer information to government agencies by private entities or other third parties will create new targets for hackers. Shortly before CISA was voting on by the Senate, the requirement to remove or redact any personal information from data that is shared was deleted, and some critics say this will result in further spreading of

personal information. Sharing of information under CISA is voluntary, so one cannot tell how effective or widespread the data sharing program will be when it is fully implemented.

Governmental Cybersecurity Clearing Houses and Measures at Federal and State Level

The new clearinghouse created by CISA focuses on cyber threats. In addition, there are additional clearinghouses at the federal and state level that include cyber incidents where hackers have gained access and control of private entity and governmental systems.

On May 20, 2015, Governor Chris Christie signed an Executive Order that set up New Jersey's New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) as the State organization responsible for cybersecurity information sharing, cyber threat analysis and hacker incident reporting.

New Jersey League of Municipalities Cybersecurity Awareness Efforts

The New Jersey League of Municipalities is bringing awareness to the municipal level through its Issue Alerts, seminars, webinars, and sample proclamations for municipalities and Annual Conference education sessions. See New Jersey State League of Municipalities. www.njslom.org Search cyber security.

Awareness at the Municipal Level

On September 29, 2015, the NJLM alerted it 565 member municipalities about recent attempts to defraud New Jersey municipalities using false emails from the Administrator to the CFO to request wire transfers. These efforts raised awareness about cybersecurity issues and specifically awareness at the municipal level. 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

Education and Outreach at N.J. Local Government Level

On April 7, 2016, GMIS New Jersey held its 7th Annual Technology Conference in Somerset, N.J. GMIS 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. Included in the conference will be a review of technology advances and investigation of problems and recommended solutions including cyber threats. Id.

Franklin Township's Fight Against Cyber Threats

Franklin Township in Somerset County, New Jersey is taking the fight against cyber threats a step further by using its website to provide information, videos and hints to raise cybersecurity awareness for residents. This effort is a reflection of the level of electronic interaction that many municipalities have with the public, and it is a feasible means of arming residents with critical cybersecurity information that will make those citizens partners in the fight against cybercrime, while reducing the risk of accidental malware, phishing and other intrusions. See Cybersecurity resources for Residents. Franklin Township, Somerset, NJ

Japan's Efforts to Prepare Cyberattack Countermeasures

The 2012 London Olympics official website was attacked about 200 million times, and Japan is bracing for even more cyberattacks in 2010. Its concerns are well-founded. In May 2015, the Japan Pension Service, which operates Japan's public pension program, was hit by cyberattacks that led to the leakage of 1.25 million people's personal data.

As Japan's government plans for the 2020 Tokyo Olympics, it is increasing the number and scale of exercises designed to counter cyberattacks. The drills are to be held six times a year and will involve ministry and agency officials, increasing to 10 and then expanded to include local governments trailing in cybersecurity measures. See *Japan to boost drills to counter cyberattacks ahead of 2020 Olympics*, KYODO, JAN 2, 2016.

Japan's central government believes prefectural and municipal governments lack experience in the cybersecurity field and plans to give higher priority to training municipal officials in remote areas, since they cannot rely on

specialists in urban areas if their computer systems are attacked. This means that for Tokyo Olympic organizing committee officials, Japan's central government will run drills involving simulated attacks on the ticket sales system of a mock official website, and by having local government officials in charge of computer systems and others join the drills; the number of participants is expected to increase to 2,000 from the present 300 now. Japan will also send officials to Rio de Janeiro, which will host the 2016 Games, to collect cybersecurity information and will seek to bolster security after the May 2015 series of electronic breaches.

Municipal Targets of Cyber Threats

Police and court systems, financial systems, personnel records, payment systems for municipal water and electrical plants are common municipal targets. From the Chelan County, Washington case discussed above, we know local government bank depository accounts are not immune from cyber intrusion and theft by third parties. Moreover, from the Howard Avenue Dam breach by an Iranian-backed hacker, we know that local government-operated and maintained dams can be targets.

As ballot machines and voter registration databases become more and more digitally and electronically cyber connected, they too will become targets for cyber threats. It has already been reported in many local and state jurisdictions as well as abroad, from theft of devices holding political data to sensitive voter data and donor information, and that is only the beginning. The following accounts were noted by Bev Harris in a January 7, 2016 Election Watch blog by Black Box Voting.org entitled *Voter Data Breaches*, http://blackboxvoting.org/voter-data-breaches/?doing_wp_cron=1460585370.1178429126739501953125

(1) In July 2012, the Democratic Party headquarters in Harrisburg, Pennsylvania was burglarized, and thieves took two laptops and a camcorder, along with all the data contained those devices contained.
(2) Earlier in 2012, presidential candidate Mitt Romney's campaign had two iPads, two laptops, two handheld radios and a briefcase stolen out of its rented SUV.
(3) At the local government level, in June 2012, the mayoral campaign office of Manhattan Borough President Scott Stringer was broken into, and two laptops containing sensitive campaign and donor information were stolen.
(4) In July 2012, the campaign office of South Carolina state senate candidate Deedee Vaughters was burglarized, and the campaign's laptop computer was stolen.
(5) In June 2014, a midnight burglar removed the video surveillance camera for a cluster of offices housing Oklahoma Governor Mary Fallin's campaign office, along with other politically related offices including former Senate president pro tem Glenn Coffee, who was representing several state officials on various legal matters. The burglar spent over six hours going from office to office, entering computers, and rifling through paperwork, and stole a laptop from Gov. Fallin's campaign office.
(6) In 2012, personal information for 553,000 eligible voters in the province of New Brunswick, Canada was appropriated when two Elections New Brunswick computers were stolen, one containing names of voters with their drivers' license numbers.
(7) In Uruguay, intruders cut the barbed wire protecting the campaign office of the main opposition candidate in a presidential election, took the closed circuit cameras, erased the entire security system, and stole every computer, hard disc, DVD containing digital data.
(8) In 2012, an intruder forced open a door at Labour leader Ed Miliband's suite of offices in Great Britain and stole 25 laptops and scores of iPads and mobile phones.

Better Security with Slot Machines than Computer Voting Systems?

More recently, a charge has surfaced in connection with the 2016 Arizona primary election that Las Vegas slot machines have far better security than the Arizona computer voting systems. Specifically, following the 2016 Presidential Preference Election in which the Democratic and Republican parties held primary elections in the State of Arizona, amidst complaints that voters were forced to stand in lines for five to six hours due to an inadequate number of voting centers and inadequate planning, a suit was filed in the Superior Court of Maricopa County, Arizona on April 8, 2016 by an Arizona citizen against the Arizona Secretary of State and several county governing boards in which it was alleged that, according to a "Hivecomm" twitter feed, an anonymous group had test-hacked

the Arizona central voter registration database prior to the primaries, that Voice-by-Mail ballots could be gamed with impunity and that the tabulator for those ballots was hackable and could be pre-programmed to alter batches of ballots without being detected by random hand-count audits. *Brakey v. Reagan et al*, Superior Court of County of Maricopa, State of Arizona, Case No. CV2016-002889, accessible at http://archive.azcentral.com/persistent/icimages/politics/ElectionContestlawsuit04082016.pdf

DDoS: Distributed Denial of Service

DDoS is a form of brute force attack in which the attacker buys access to a botnet system that directs thousands or even millions of computers to access the network, email system or website. It has been estimated that in 2015 one-third of website outages resulted from DDoS attacks, the result of which was that networks were overwhelmed, shut down, and normal traffic could not get through. This left municipal residents without electronic services to pay taxes and utilities online, interrupted 911 and emergency dispatch functions, and delayed communications with and essential functions of health departments, payroll departments, online facilities for payment of bills, for hours up to several days. Systems that crash due to DDoS attacks may in turn have data corruption problems and require expensive re-building in order to come back online.

Purchase of DDoS Service on the Dark Web

Why would a municipality be subjected to a DDoS attack? This might originate with criminal activity by gangs, political protests, revenge, or disgruntled employees. The cyber attacker need not have sophisticated technical skills to initiate a DDoS attack, but only needs to purchase the service on the dark web.

A few examples illustrate the range of this kind of attack.

►The Maine.gov website was disabled by DDoS attacks three times in March 2015 along with the Bangor, Maine municipal website and other websites. Craig Anderson, *More Maine websites targeted on third day of cyberattacks*, Portland Press Herald, March 25, 2015, www.centralmaine.com/2015/03/25/cyber-attacks-targets-maine-websites-for-a-third-day/

►As a result of a DDoS attack in November 2015, the San Jose Police Department was offline for several days.

►Departments at Rutgers University were shut down by DDoS attacks in 2015. Kelly Heyboer, *Cyber-attack shuts down Rutgers online classroom site*, 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

Approaches to Prevent DDoS Attacks

Distributed Denial of Service (DDoS) attacks are designed to deny electronic access and functioning to a municipality. They shut down the city's doors so no information can get in or out for a prolonged period. While they are not the most damaging of cyber threat to municipalities, they are disruptive and can cost valuable taxpayer dollars in times of limited local resources.

Cybersecurity vendors have used several approaches in an effort to prevent DDoS attacks on municipal governments, but these are not the only form of attack.

1. Cybersecurity firms can 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.
2. Policies, procedures and controlled access methods can be developed and implemented to minimize the risk of such everyday cyber threats as

(a) Exposure of municipal networks and websites by which hackers gain access to the municipal network, utility systems, or website, and the intrusion cyber threat seeks to gain internal control in order to steal personal/financial information or disrupt the operation while doing maximum damage.

(b) Theft of personal and financial information on the Internet, through which the hacker's breach may force the municipality to spend hundreds of thousands of dollars to rebuild and harden the network against future intrusions while limiting services to residents, and then hope the system, will withstand the next attempted intrusion.

(c) Despite constant attention to alerts and periodic tests, and even if the municipality's network and systems are hardened and up to date, there will be upgrades and patches to apply constantly over time, and another Trojan or malware could be accidently introduced through a trusted vendor patch, an employee's flash drive or similar network appliance, or human error as when an employee opens an e-mail and clicks on a link or opens an attached file that releases a virus, malware or a Trojan into the network as it is downloaded to the computer attached to the network, or when an employee accesses a non-municipal system that risks introducing viruses, ransomware, or Trojans into the municipal network as he or she checks social media, personal e-mail or conduct personal business using the municipal work station.

Grass Roots Approach to Cyber Security

Cyber-attacks affect more and more organizations in both the public sector and the private sector. While interconnectedness through the internet, the cloud, mobile devices, and social media has increased productivity and commerce, these trends also are making businesses, governments, and individuals more vulnerable to cyber-attack. The federal government and large corporations constantly seek news ways to fortify their enterprises against attack. However, what is overlooked in cyber-security planning and responses are local governments and small businesses. A "grass-roots" approach to cyber-security is required to compliment the efforts of large enterprises and governments.

Recognizing the Problem

The first step in this grass-roots approach is the recognition of the importance of cyber-security by local leaders to include mayors and town councils, chambers of commerce, school boards and civic groups. Such leadership has the ability to raise awareness of cyber-security among their respective constituencies. They can direct the attention of citizens to the importance of cyber-security. Leaders should use their respective forums to discuss cyber-security at given opportunities.

One recent example and the constructive advice that can be provided is the official-sounding tech-support scheme, in which a cyber hacker tries to access a computer or sensitive information stored in it by offering to "fix" the computer. In a blog by Andrew Johnson, Division of Consumer and Business Education for the FCC, entitled *Official-sounding calls about an email hack,* April 6, 2016, at https://www.onguardonline.gov/blog/official-sounding-calls-about-email-hack, this latest form of hacking takes place when a person gets a call from a person identifying himself or herself as representing the Global Privacy Enforcement Network, in which they claim that the person's email account has been hacked and is sending fraudulent messages. The scammers then tell the person they will have to take legal action against the person until he or she lets them fix the problem right away. The scammers have given out phone numbers of actual Federal Trade Commission staff and have sent people to the actual website for the Global Privacy Enforcement Network, an organization that helps governments work together on cross-border privacy cooperation. Recommendations for responses in case a person gets this kind of tech support case are simple and clear:

1. Don't give control of your computer to anyone who calls you offering to "fix" your computer.
2. Never give out or confirm your financial or sensitive information to anyone who contacts you.
3. If you are getting pressure to act immediately, that is a sure sign of a scheme. Hang up.
4. If you have concerns, contact your security software company directly. Use contact information you know is right, not what the caller gives you.

Coordinated Governance via a Cyber-security Governance Committee

Following efforts to raise citizen awareness of the importance of cybersecurity, the next step is for local governments to develop cyber-security committees to bring together stakeholders for the following purpose:

- Raise awareness among citizens;
- Improve cyber-security posture of local government institutions;
- Share best practices with local businesses and organizations;
- Develop a cyber-security curriculum for local schools;
- Coordinate law enforcement response options to reported cyber-crimes.

Through a cyber-security governance committee, plans can be developed, implemented and monitored to meet these objectives.

Engaging Stakeholders

To meet these objectives, the committee should consist of at a minimum the following individuals:

- Cyber-Security Expert: Municipalities can recruit a volunteer through their local ISACA chapter (www.isaca.org). Service on such a board can count as continuing education credits to maintain good standing as a Certified Information Systems Auditor (CISA).
- Head Law Enforcement Official: This individual will be able to assist in creating mechanisms for reporting cyber-crime.
- Member of Council: This individual assures that planning aligns with local strategic vision and facilitates the approval of resolutions to support the effort.
- Municipal Information Technology Professional: This individual's knowledge of systems, data and access levels are necessary for risk assessments, implementation, and monitoring.
- Municipal Manager or Administrator: This individual brings strong knowledge of functional processes in the local government that aid with both risk assessments and implementation and monitoring.
- School Board Representative: This individual assists with improving the school district's cyber-security posture and provides insight into developing a cyber-security curriculum.
- Government Sub-unit Representative(s): These are individuals representing any independent or quasi-independent agencies that have separate information technology systems. Industrial automation in utilities is a focus of these individuals.
- Educational Institutional Representative(s): These individuals represent colleges or community colleges in the municipality to assist with awareness and educational development.
- Business and Labor Representative(s): These individuals represent business groups and labor organizations in the municipality. These individuals can assist with awareness and dissemination of best practices.

Smart Cities and Protection of Citizens from Cyberattacks

Ultimately, all governments have a duty to protect their citizens. As with any other type of crime, any decrease in cyber-attacks represents an increase in quality of life and a boost to economic development. Cyber-attacks represent a new threat from which citizens require protection, at the same time, as cities are moving toward the smart city technology market. Poul Nielsen, Smart City Security and Cyber Attacks, Feb. 25, 2016, http://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks/.

Ironically, the adoption of high tech innovations and improvements by major cities around the world has given rise to Smart Cities, whose internet technology initiatives range from smart traffic lights, to knowing exactly what time public transportation will arrive, to paying for public services with the touch or swipe of a credit card or a personal device. Everything seems to be connected in the Smart City, from local government services to utilities, financial and transportation services. Smart Cities are facing significant security concerns as their infrastructure becomes increasingly dependent upon internet technology. The weakest link in a Smart City's IT infrastructure must be protected, and therein lies the problem. The increased vulnerability that comes with this increased technology raises security concerns about Advanced Persistent Threat (APT), which are targeted attacks executed by a hacker or group of hackers, perhaps using malware, in which the attackers are motivated not by financial gain so much as by political gain or "hacktivism."

The Smart London Initiative is the focal point of an analysis cited above, Poul Nielsen, Smart City Security and Cyber Attacks, Feb. 25, 2016, http://www.informationsecuritybuzz.com/articles/smart-city-security-and-cyber-attacks/, in which a troubling scenario is outlined for a city of over 8.5 million people in which a critical service is attacked and many operations dependent on that service malfunction or shut down. The targeted attack is carried out by hackers who know which city services are essential to the function of the city, placing the entire city at risk of complete standstill, leading to the failure of the economic infrastructure within 48 hours, loss of economic transactions and problematic maintenance of law and order during the time needed to restore or replace the infrastructure, not to mention loss of public confidence.

Optimal security of the smart city's IT infrastructure would require constant monitoring from end-to-end, including end-user devices where the system is most vulnerable. To put this in perspective, one estimate by the Gartner analyst firm in November 2013 indicates that there were an estimated 2.5 billion connected devices, mostly mobile phones, PCs and tablets, in 2009, and by 2020 that number will skyrocket to over 30 billion devices connected.

End-users will be accessing an increasing amount of smart services with their devices, and they will make easy targets for malware and hacktivist intent on reaching the heart of the smart city's infrastructure where the most damage can be inflicted. This points to the need for smart cities to develop and implement solutions to monitor their IT infrastructure and end-user endpoints, the weakest link in the IT security chain with the greatest vulnerability. An additional layer of protection for the smart city can also be provided by IT analytics solutions that provide alerts on suspicious activities and behavior, a form of pre-warning for such attacks. In order to stop or prevent a cyberincident from causing too much damage, these security measures will require smart cities to initiate greater levels of proactivity in the detection of abnormal activities and maintain constant enforcement of security compliance standards with information that is both real-time and accurate.

Post-Ferguson DDoS Attack

The susceptibility of a city to a cyber-attack may coincide with a major adverse event that draws an extreme level of public attention and focus to the city.

Following the fatal shooting of Michael Brown by a Ferguson, MO police officer on August 9, 2014, the City of Ferguson found itself at the epicenter of worldwide attention, including that of hackers with a sociopolitical agenda. In an excellent article by Colin Wood entitled *Unmasking Hacktivism and Other High-Profile Cyberattacks,* Government Technology, August 28, 2015, accessible at http://www.govtech.com/public-safety/Unmasking-Hacktivism.html

According to Wood, the hactivists at Anonymous engaged in a "shotgun approach to retribution" by mounting a vigilante assault that began with the online release of the home address, phone number and photo of the house of the St. Louis County Police Chief, shortly after which photos of the Chief's daughter and wife began circulating on Twitter. This was only the beginning of their furor as Anonymous expressed its indignation over what its minions perceived as a violation of its moral code. Its online efforts led to others making veiled threats against the safety of the Chief and his family. Anonymous launched DDoS attacks, SQL injection attacks and a phishing campaign against the Missouri state government's digital infrastructure and that of law enforcement agencies and regional governments not directly related to Michael Brown's death. The collateral damage to those targeted by this cyber-attack was extensive, and the State of Missouri was not fully prepared.

Similar cyber-attacks had been launched by Anonymous as far back as 2008, when it "cut[] its hactivist teeth" in online attacks against Sony, PayPal, Visa, MasterCard, the Motion Picture Association of America, ISIS, Koch Industries, the Westboro Baptist Church, the New York Stock Exchange, and the federal governments of the U.S., Australia, Uganda, Israel, Canada, Tunisia and Egypt. Each target has somehow been selected by Anonymous based on a perceived transgression of its sense of moral propriety.

According to the chief information security officer for the state of Missouri, as Wood explained, the state had not completely implemented its security plan at the time the cyber attacks took place, although overall the state did a good job minimizing their impact. There were several things the state would have done differently when it was subjected to the three forms of attacks in the middle of the night on a weekend. These consisted of DDoS attacks that disabled websites, SQL injections that infiltrated databases and a phishing campaign that sought to obtain security credentials. Some of the large DDoS partners were hard to reach, and some of the state's vendors wanted an emergency setup fee of $20,000 to $40,000. While the cyber-attacks actually helped improve the state's security posture, the state has now contracted with several new vendors to manage security operations, uses a managed DNS provider, and has in place border gateway protocol and application-layer protection to mitigate DDoS attacks.

According to Woods,

> Groups like Anonymous attack their enemies to prove a point. They want to show the government, or whomever, that evil deeds do not go unpunished. It is out of a perceived lack of legitimate recourse that hacktivists disable websites and make personal threats, but of the 10,000 arrows fired, many land on innocent villagers. Roling did not shoot anyone, but he and the rest of the state's IT team are the ones left picking up the pieces. The more time and money the state spends on its cybersecurity, the less taxpayer funding there is left for citizen services. The people Anonymous wants to advocate for are the same ones footing the $40,000 emergency setup fees and new vendor contracts. Anonymous might mean well, but pestering the state will not stop the next race riot. It is just another thing that poorly funded state and local governments must worry about.

The post-Ferguson cyber-attacks on the State of Missouri demonstrate graphically that governments do not have the option of doing nothing, unless they relish the idea of being pounded repeatedly as "easy, soft targets" and allow citizens' trust in their government to be sacrificed on the altar of cost-control.

Understanding Hactivists' Motivation, Means, and Opportunity

There are ways to prepare for hactivist attacks like those spearheaded by grass roots political movements like Anonymous, and they begin with an understanding of motivation, means, and opportunity. As Wood notes, preparing for hacktivism differs little from other forms of cyber defense. Control frameworks as outlined by the National Institute of Standards and Technology are good road maps for governments, Brasso said. Even if organizations are not ready to implement every piece of the framework, they can know where they stand compared to where they should be. Tools include things like firewalls, advanced malware protection, intrusion prevention tools, vulnerability assessment tools, and education to prevent simple mistakes by employees.

Encrypted iPhones and the Battle for Encrypted Data Access

Encrypted handhelds, iPhones, cell phones, and other products allow users alone to access their data. In the wake of the Charlie Hebdo attacks in Paris and the terrorist attacks in San Bernardino, California, the law enforcement's fears that critical information about the violent attacks are hidden in the terrorists' encrypted mobile devices are being realized. In its most recent pitched battle with Apple over access to encrypted data stored on a suspect's iPhone, in this case of one of the San Bernardino attacker's county-owned device, the FBI argued that encrypted messaging applications could hinder its ability to uncover terrorism. In that battle, Apple claimed a First Amendment right of privacy bars governmental access to the data, and the FBI argued that it needs immediate access to the contacts made by the terrorist in the last hours of his life. See Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

The San Bernardino iPhone encryption controversy is not the only time that Apple has locked horns with the government over encryption recently. In 2014, authorities seized an iPhone 5s that they believed had encrypted information that would aid in a drug investigation. A federal magistrate judge recently declined to order Apple to comply with the government's access requests. Despite Apple previously complying with approximately seventy similar requests, Apple resisted in this case after Judge James Orenstein, the federal magistrate judge, disputed whether the All Writs Act, the statute the government argued gave them the authority to access the devices, was

applicable to this type of encrypted information. Apple Wins Ruling in New York iPhone Hacking Order, Feb. 29, 2016 http://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html?_r=0 The FBI has appealed Judge Orenstein's ruling. "Apple fires back at FBI in New York iPhone case", http://thehill.com/policy/cybersecurity/276525-apple-fires-back-at-fbi-in-new-york-iphone-case

Device management feature lacking

According to the Washington Post, the county could have purchased a device management feature what would have given the FBI easy, immediate access to the encrypted data. See Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html. When city officials have the opportunity to invest in cyber security, they should remember that those investments could be tremendously valuable to their constituents and law enforcement.

Going Dark

According to Segal and Grigsby, U.S. law, enforcement has expressed concern over "going dark" since the 1990s, meaning its inability to access encrypted data, even when armed with a court order.

Encryption Backdoors

To prevent future terrorist attacks, tech giants like Apple are being urged to incorporate "backdoors" or "front doors" in their products that will assure the technical ability to decrypt communications pursuant to a warrant. Apple and other tech manufacturers claim that if someone other than the owner of the data is allowed to decrypt communications, criminals and state actors, weakening security for everyone, could exploit such a flaw. There is a technological workaround, however, through which the encrypted devices can be broken into, and the government is actively seeking to compel cooperation by the tech companies.

The choice need not come down to an absolutist immediate, on-demand decryption capability or caving in to business interests that favor going dark. On the contrary, there are existing solutions that would enable law enforcement to gather the evidence it needs without creating encryption backdoors.

1. Congress can empower law enforcement to have the legal ability to hack into a terrorist suspect's handheld or computer with a court order, exploiting existing security flaws in communications software to access the data it needs. As Segal and Grigsby point out,

> It's no secret that software is riddled with security flaws. …[S]ome prominent computer security experts have argued such lawful hacking would allow authorities to use existing vulnerabilities to obtain evidence instead of creating new backdoors. Although this would entail law enforcement adopting the same techniques as criminals, tight judicial oversight would ensure that lawful hacking is employed responsibly, much like the restrictions that already apply to wiretapping. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

2. A national capacity to decrypt data for low enforcement purposes should be explored by the Executive Branch. The challenge of "going dark" affects state and local law enforcement the most: They are the least likely to have the resources and technical capabilities to decrypt data relevant to an investigation. Creating a national decryption capability, housed within the FBI and drawing upon the expertise of the National Security Agency, would provide assistance to state and local law enforcement, similar to what the FBI provides for fingerprint and biometric data. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

Law enforcement needs to ramp up its tech literacy. Just as law enforcement in the 1990s dealt with a problem similar to "going dark" when organized-crime suspects began using disposable phones that hampered wiretaps, it adapted its procedures, and arrests and prosecution of organized-crime suspects continued.

While the San Bernardino iPhone issue is moot after a third-party contractor was able to access the information, Judge Orenstein's reluctance to order Apple to comply with the demonstrates that judges may not be willing to order technology companies to help the government access information related to investigations or prosecutions.

If technology companies refuse to create "backdoors" and are reluctant to comply with court orders relating to accessing information on devices and courts are reluctant to issue the orders in the first place, then it is unlikely that law enforcement officers will be able to access information through judicial intervention. If law enforcement believes that accessing such information is critical to investigations, which it is very likely that they will continue to do, then it will likely take affirmative legislation to prompt courts to require such things. Judge Orenstein's disapproval of using the All Writs Act as a skeleton key for digital information is indicative that new legislative action is needed if law enforcement want a consistent ability to access encrypted information.

Apple Wins Ruling in New York iPhone Hacking Order, Feb. 29, 2016 http://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html?_r=0

Alternative Avenues to Encryption: Cloud Backup

Encryption of data can occur on a device when data is transmitted and stored in the cloud, but this does not automatically mean the evidence trail will go cold. Encryption in one avenue does not necessarily mean other avenues will be encrypted. It an encrypted iPhone had been backed up to the Apple's cloud storage system known as the iCloud, Apple can still access the content of the encrypted iPhone if it has been backed up to iCloud.

As Segal and Grigsby note,

> Recognizing how and when encryption occurs, and the different security offerings of the more popular service providers, may help law enforcement access data. Better tech literacy might have avoided the current Apple-FBI fight. The FBI could have obtained more information from the San Bernardino attacker's iPhone if it had not hastily ordered the county to reset his iCloud password. Adam Segal and Alex Grigsby, 3 ways to break the Apple-FBI encryption deadlock, The Washington Post, March 14, 2016, at http://www.syracuse.com/opinion/index.ssf/2016/03/3_ways_to_break_the_apple-fbi_encryption_deadlock_commentary.html

While these proposals may not be fully acceptable to law enforcement or the tech sector, and while it is unlikely that a one-size-fits-all solution will be forthcoming, the time is rapidly approaching to consider and develop realistic solutions.

Albuquerque P.D. Going Dark

The City of Albuquerque, New Mexico, is considered a leader in open data and transparency. In August 2014, after members of the Albuquerque, N.M., Police Department fatally shot a mentally ill homeless man who had been camping in the wilderness, the Police Department's website went dark on the heels of cyber-attacks from Anonymous. Some police personnel as tests of how well the city had been maintaining its security program saw the attacks.

The cyber-attacks brought down the APD's website for a few hours, but unlike Missouri, the city was able to mitigate the attacks by working with such groups as the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the FBI. While it may be problematic to predict when the threat of hacktivism will surface, whether arising from a police officer's use of force or something that a group sees as social injustice, there are still practical considerations for maintaining a robust social media presence, and promoting city information, but the trick is to "be smart about what's being publicized." In light of emerging technologies like police body cams, moreover, amidst growing public demands for open data and transparency, the line between good practice and threat to the public servant can become a thin one. "[I]n the online world, everything that has a good motive also can be exploited."

Essential Preparation and Planning

According to the digital services coordinator for Evanston, Ill., one of the best things governments can do when it comes to any disaster is to prepare and plan.

> Make sure you have a robust social media presence up and running, because a lot of these government agencies are slow to adopt and waiting until after that natural disaster hits to start a Twitter account, [but] it's too late….You want to build up those relationships ahead of time." http://www.govtech.com/public-safety/Unmasking-Hacktivism.html

Basic measures local governments can take

Among the basic measures local governments can take are getting verified status on Twitter and using two-factor authentication. According to an official with the FBI's Cyber Division, state and local governments should expect DDoS attacks and have a mitigation plan and vendor relationships in place. They should monitor how often their networks are being pinged so they can quickly recognize when an attack has begun. Once due diligence has been performed, the most realistic advice may be that offered by Robert Louis Stevenson, author of Treasure Island, who once wrote, "Our business in life is not to succeed, but to continue to fail in good spirits."

Developing Nations' Reach for Cyberspying Capabilities

The norms of behavior by nation states in cyberspace like the Peoples Republic of China and the USA may set a lofty standard, but less technologically advanced countries may lack the skill or motivation to follow that lead. Instead, increasing literature indicates a mounting interest among these less sophisticated countries in acquiring cyber espionage capabilities. At a time when governments are trying to curb the volume of hostile activity occurring in cyberspace, the media have revealed instances of suspected U.S. global surveillance and China's rampant commercial cyber espionage. These and similar episodes that unfortunately resemble the old days of Mad Magazine's *Spy vs. Spy* cartoon, have given rise to serious discussions about how and in what manner to establish a baseline for accepted actions for governments to take in cyber space. China, Russia, and the United Nations Governmental Group of Experts on Information Security have developed proposals addressing these concerns.

Cyber Sanctions

Coupled with this trend for nation state cyber responsibility, the President of the United States in an April 1, 2015 Executive Order established "cyber sanctions" that granted authority to the U.S. Department of Treasury to sanction "individuals or entities" that pose a cyber threat to the "national security, foreign policy, or economic health or financial stability of the United States." This was the first sanctions program to allow the Obama administration to impose penalties on individuals overseas who engage in destructive cyber-attacks or commercial espionage in cyberspace. *Executive order: Obama establishes sanctions program to combat cyberattacks,* The Washington Post, April 1, 2015, cyberspyinghttp://apps.washingtonpost.com/g/documents/world/executive-order-obama-establishes-sanctions-program-to-combat-cyberattacks-cyberspying/1502/

As the President put it when he signed this EO, "Starting today, we're giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit." *Our latest took to combat cyberattacks,* https://www.whitehouse.gov/blog/2015/04/01/our-latest-tool-combat-cyber-attacks-what-you-need-know

The rationale underlying this executive order is that malicious cyber actors often rely on U.S. infrastructure to commit the acts described in the EO, and they often use U.S. financial institutions or partners to transfer their money. By sanctioning these actors, the U.S. can limit their access to the U.S. financial system and U.S. technology supply and infrastructure. Basically, sanctioning them can harm their ability to both commit these malicious acts and to profit from them.

In a landmark agreement in November 2015, governments of the 20 leading global economies – including China – pledged not to engage in cyber-enabled commercial espionage for profit.

FinFisher

FinFisher Gamma Group in Munich has developed and produced a sophisticated, user-friendly spyware that is sold exclusively to government agencies and police forces. It has risen in popularity with government agencies across the world, and over 32 countries – including our host country for this Congress - have been identified as users. FinFisher's software can remotely control any computer it infects, read and copy encrypted files, intercept Skype

calls, log keystrokes, and activate webcams. The software has been touted as a way to "help government law enforcement and intelligence agencies identify, locate, and convict serious criminals."

In August 2015, a data breach placed FinFisher's business practices and clients under scrutiny. Stolen files and client information of 33 customers was placed on the web, and some of it suggested that FinFisher was being used for activities beyond tracking criminals. The other activities entailed spying on high-profile Bahraini activists. According to some reports, it was believed that dissidents, law firms, journalists, and political opposition in Bahrain and from Ethiopia had been monitored through FinFisher.

Yet despite this progress, revelations exposed with the Gamma breach, as well as the one suffered by Italy's Hacking Team in July 2015, continue to demonstrate that states desire to acquire offensive cyber surveillance capabilities, even if they can't develop them indigenously. Some of the customers identified in data were notably states that are neither considered cyber powers, nor considered leading economies. Some of the governments identified in data taken from the breach include Bangladesh, Kenya, Macedonia, and Paraguay. In two of these cases, the intelligence agencies of the governments were linked to FinFisher products.

While these states may not use these capabilities in order to conduct cyber espionage, some of the governments exposed in the data breach are those that Reporters without Borders have identified as "Enemies of the Internet" for their penchant for censorship, information control, surveillance, and enforcing draconian legislation to curb free speech. National security is the reason many of these governments provide in ratcheting up authoritarian practices, particularly against online activities. Indeed, even France, which is typically associated with liberalism, has implemented strict laws fringing on human rights. In December 2013, the Military Programming Law empowered authorities to surveil phone and Internet communications without having to obtain legal permission. After the recent terrorist attacks in Paris, French law enforcement wants to add addendums to a proposed law that blocks the use of the TOR anonymity network, as well as forbids the provision of free Wi-Fi during states of emergency. To put it in context, China, one of the more aggressive state actors monitoring Internet activity, blocks TOR as well for its own security interests.

Cyberspace has been called "the great equalizer" because it is an environment that can be leveraged by smaller, less industrialized nations in order to compete with larger ones. The Snowden document leaks and rampant, unchecked cyber espionage have created an environment in which all governments—regardless of size—want a modern, relatively inexpensive capability indicative of their ability to keep pace with the times.

Despite the lead taken by larger governments to reach consensus on some unacceptable actions in cyberspace, Pandora's Box may have reached an aperture too great to close. Whether these poorer nations use the tools they obtain for legitimate national security or law enforcement reasons, or to oppress and keep populations in check will largely rest on perception and interpretation.

What City Officials Need to Know About Cybersecurity

In the wake of highly publicized data breaches and cybersecurity attacks, city officials have begun looking at historically underfunded municipal cyber-defense programs. See Lea Deesing, What City Officials Need to Know About Cybersecurity, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html

Lea Deesing paints an all-too realistic scenario for a municipal government that has been subjected to a well-orchestrated cybersecurity attack. In her hypothetical scenario, the signs of a cyber-attack are everywhere:

►city staff unable to log in to their computer network,

►fire and police departments forced to rely solely on radio communications rather than mobile data systems to receive and respond to incidents,

►city staff is limited to communicating through text using the phone numbers in their personal smartphones since the telephone and e-mail systems are down,

►no city employees receive their electronic paycheck via direct deposit the night before payday,
►counter staff does not know how to handle manual transactions and cannot log in to their systems,
►staff who attempt to call the IT department help desk do not even get a dial tone, ►massive lines begin to form in the planning, permitting and cashiering departments, and
►residents and business owners who need to conduct business with the city are getting frustrated.
In addition, all of this has taken place on a Friday.

IT staff finally determine that many city servers have been compromised through a well-organized cybersecurity attack. Weeks later the IT Department discovers the cause of the chaos was a Trojan horse virus that had been transmitted via a city staff member's personal flash drive. Lea Deesing, What City Officials Need to Know About Cybersecurity, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html

Deesing notes that recent cybersecurity breaches in both the private and public sectors have captured the attention of local government agencies. Highly publicized data breaches and cybersecurity attacks raised awareness of these challenges, and consequently many city officials are looking at historically underfunded municipal cyber-defense programs.

Cybersecurity Awareness Training

Cyber Hackers usually hit the easiest targets first, much like thieves operating in a neighborhood during the holidays. A common breach can occur after a user clicks on a link in a spam or phishing email, and whether such an attack is financially motivated, or an attempt to cause mayhem in the city, or an act of revenge by a terminated city employee, it must be confronted and effectively mitigated.

Cryptolocker

A well-designed trojan horse virus writing like Cryptolocker can generate for its writers millions of dollars in revenue by encrypting the target's data and holding it for ransom until the target pays a fee. According to one cybersecurity expert, top coding talent is being recruited to write some Trojan horse viruses that lie undetected until a future date and contain malicious code that can carry out a specific action when the hacker signals the software. The cyber hacker has the choice of trying to breach a $20,000 security device or convincing someone to insert an infected $5 thumb drive.

Cybersecurity Awareness Programs

Among the simplest ways to mitigate, the risk of such cyberattacks is a good security awareness-training program. Prevention of internal breaches can be much more effective through utilization of low cost end-user security awareness videos that are available through private-sector security organizations. Preparation measures can combine with good awareness training, a cybersecurity policy in place that deals with unknown media, and suspicious calls or online messages that try to get staff to visit a website, e-mails with suspicious attachments.

End-User Education

It is no longer sufficient for local governments to continue to rely on anti-virus and firewall protections along while ignoring end-user education.

Security Audits, Penetration Tests and Monitoring

Local government can implement security efforts in the form of security audits and penetration tests. These measures call for paying ethical hackers to try to breach the local government's system and reporting their findings. The government officials can use this information to take pre-emptive action. Officials, from the highest to the lowest levels, must understand the long-term cost of a data security breach, and they must understand, in context, the great expense of a security audit or audits. They must count the cost not only in monetary terms, but officials must also count it in terms of the loss of trust that citizens and customers have in their governments. Further, officials must decide whether an annual or biennial security audit is sufficient in the present and future cyber landscape. Attention should be given to such emerging trends as hiring 24/7 managed professional security service providers. These professional can operate from remote security operations centers with fully dedicated certified security teams. The teams watch the local government's network, inside and out, and can identify real time security

threats and help develop preventive counter measures. It is not cheap, but its cost in relative terms may make it a bargain.

Security Information and Event Management (SIEM) Tools

Managed security service providers often use special Security Information and Event Management (SIEM) tools. These tools provide a dashboard view into security and server logs that the local government's IT staff likely does not have time or capability to monitor. The IT staff may view these security and server logs after an incident has already occurred, but usually not before.

Continuity of Operations Plan

Officials must prioritize systems in advance through a continuity of operations plan. This is the scenario described by Lea Deesing in *What City Officials Need to Know About Cybersecurity*, June 23, 2015, at http://www.govtech.com/opinion/What-City-Officials-Need-to-Know-About-Cybersecurity.html.

Officials can vet continuity of operations plans through departmental meetings

> where questions are asked, such as, "What would happen if your computer system went down for two hours? A day? A week? A month?" It is surprising what occurs when you have these discussions with departmental staff. They may say, "I never thought it would be possible for systems to be down that long. If we simply take this extra step, in advance, we will be as prepared as possible when the systems fail." For example, a payroll team saves the last successfully run payroll in a PDF format and stores it in a secured location, along with blank check stock. On the day of a disaster, all checks are printed and signed, and required payroll adjustments are made after system recovery.

Questions for Local Government Leaders to Consider

Security measures and security efforts may already be underway in a local government's IT department, but they should give consideration to supporting and implementing the current cybersecurity efforts in a collaborative way and take steps to require that policies be written and be grounded upon executive sponsorship.

1. Questions the human resources department on whether it can help support a security awareness-training program.
2. Give support for new hardware, software, or services.
3. Perform assessments, within the limits of funding, at the executive management level regarding the amount of risk the local government is willing to mitigate or simply accept.

4. Make the backup and recovery plan a good as the government can afford, since a cyber attacker with the time and desire will gain access one way or another.

BASIC CYBERSECURITY BEST PRACTICES

Notwithstanding the daunting cat-and-mouse game that seems to be taking place constantly between the perpetrators and victims of cybersecurity breaches, practices and measures exist which municipalities to help protect their networks and systems. The private sector is already implementing some of these practices, and they are listed in a 2015 report from Online Trust Alliance (OTA). According to OTA, if the affected organizations and entities had implemented basic cybersecurity best practices, they could have prevented 90% of recent breaches. See Security & Privacy Best Practices (Jan. 21, 2015), https://otalliance.org/resources/security-privacy-best-practices.

OTA recommends all organizations implement these best practices:

1. Effective password management policies, using best practices for password management:
   a. multi-factor authentication;
   b. unique password for external vendor systems;
   c. strong passwords comprised of an 8-character;
   d. login abuse detection system monitoring connections, login counts, cookies, and machine IDs;
   e. Avoid storing passwords;
   f. Remove or disable all default accounts from all devices and conduct regular audits to ensure that inactive accounts can no longer access your infrastructure; and
   g. Remove access immediately for any terminated employees or any third parties or vendors that no longer require access to your infrastructure.

2. Least privilege user access (LUA).3. Harden client devices by deploying multilayered firewall protections.
3. Conduct regular penetration tests and vulnerability scans of infrastructure.

4. Email authentication on all inbound and outbound mail streams.

5. Mobile device management program, requiring authentication to unlock a device, locking out a device after five failed attempts, using encrypted data communications/storage, and enabling the remote wiping of devices if a mobile device is lost or stolen.

6. Continuous monitoring in real-time the security of the organization's infrastructure.

7. Deploy web application firewalls to detect/prevent common web attacks.

8. Permit only authorized wireless devices to connect to the network.

9. Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log in authentication and data collection.

10. Review server certificates for vulnerabilities and risks of domains being hijacked.

11. Develop, test, and continually refine a data breach response plan.

Best Practices for Municipalities

Similarly, a number of best practices for municipalities have been identified in a program on *Cybersecurity for Municipalities* presented at the Colorado Municipal League at its June 2015 Annual Conference, accessible at https://www.cml.org/Issues/Technology/Cybersecurity-for-Municipalities. Among these best practices are the following:

1. Encryption: Financial systems and personnel data should be encrypted.
2. Control over Administrative Functions: Administrative functions can be tightly controlled.
3. Strong Passwords: Strong system passwords can be changed every thirty to sixty days, using password manager software for staff to enter passwords to systems or access the network.
4. Blocked Access for Hackers: 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.
5. Cybersecurity Staff: A full time cybersecurity officer may be hired by the largest municipalities, although this is not feasible for most municipalities due to cost. Further, qualified cybersecurity staff members are in short supply and are paid more than most municipalities can afford.
6. Shared Service Agreements: Municipalities can 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.
7. Cybersecurity Policies: Municipalities can establish a comprehensive cybersecurity policy that is reviewed twice a year with staff to ensure they understand all of its elements, including holding separate meetings where policy elements apply only to a single department, and creating a video with a form quiz where the policy applies to volunteers and elected/appointed officials, providing them with a good overview of their responsibilities and restrictions.

ICS-CERT: Cybersecurity Measures for Water and Wastewater Industry

Return for a moment to the Howard Avenue Dam cyberattack by the now-indicted Iranian-backed hackers. Are there feasible, established, vetted, and available best practices and training measures for reducing the risk of such attacks, mitigating the vulnerabilities, and improving the resiliency of such systems? In short, is there a way to lessen the likelihood of a similar cyber-attack on a water supply system, water storage facility, or wastewater site in the future? WaterISAC in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI and the Information Technology ISAC has developed a compendium of 10 Basic Cybersecurity Measures, setting forth best practices to reduce exploitable weaknesses and attacks in the U.S. water and wastewater sector, accessible online at . https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf

These measures collectively provide a front line of defense against avoidable data breaches and cyber-attacks Summarized, the ten basic cybersecurity measures are as follows:

1. Maintain an accurate inventory of control system devices and eliminate any exposure of equipment to external networks. "Never allow any machine on the control network to talk directly to a machine on the business network or on the Internet."
2. Implement network segmentation and apply firewalls, classifying and categorizing IT assets, data, and personnel into specific groups and then restricting access to those groups.
3. Use secure remote access methods.

4. Establish role-based access controls and implement system logging.
5. Use only strong passwords of at least eight characters, change default passwords, and consider other access controls.
6. Maintain awareness of vulnerabilities and implement necessary patches and updates.
7. Develop and enforce policies on mobile devices.
8. Implement an employee cybersecurity training program.
9. Involve executives in cybersecurity.
10. Implement measures for detecting compromises and develop a cybersecurity incident response plan that includes such measures at intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), antivirus software and logs to help detect compromises in their earliest stages.

CONCLUSION

There is no silver bullet solution to public sector computer system vulnerability, and the reality for local governments is inescapable: It is not a matter of whether, but when, a cybersecurity incident, breach, or attack will occur. Local governments can best serve their citizens by implementing best practices similar to those listed above, and combining them with strong training programs, clear cybersecurity policies, consistent enforcement of those policies, and good faith transparency and openness with the citizenry through social media and other news media outlets. With these measures, local governments can rebound, recover, and minimize the long-term damage from cyber-attacks.

---

*World Jurist Association National President for USA; Adjunct Professor, University of Mississippi School of Law; ABA House of Delegates; International Committee Chair, ABA Section of State & Local Government Law; International Steering Committee Chair, International Municipal Lawyers Association; principal, Griffith Law Firm, Oxford, MS

** President, Treasurer, and Senator, Law School Student Body Association; Editor-in-Chief, University of Mississippi Business Law Newsletter; Executive Online Editor, Mississippi Law Journal v. 85; Staff Editor, Mississippi Law Journal v.84; Alumni Coordinator, Mississippi Law Journal v. 85; Member, Trial Advocacy Board; Member, Dean's Leadership Council. Graduating 3L, University of Mississippi School of Law, J.D. May 2016.