International Municipal Lawyers Association
2017 Mid-Year Seminar
Omni Shoreham Hotel
Washington, DC

Work Session:

Open Data, Government Transparency, Cybertheft & Individual Privacy

Benjamin E. Griffith
YMD Joint Water Management District
and Griffith Law Firm
Oxford, MS, USA
www.glawms.com

https://www.linkedin.com/in/ben-griffith-7280b79/

Sven Kohlmeier

Kohlmeier Law Firm
Berlin, Germany

www.kanzlei-kohlmeier.de

www.linkedin.com/in/sven-kohlmeier

© 2017 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2017 Mid-Year Seminar, held April 21-24, 2017 in Washington, DC. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Introduction: Scope of the Problem

Online computer system vulnerabilities in the public sector can conceivably usher in a cyber Pearl Harbor attack, given the quantum leap in the number of cyberincidents at the state and local government level and now at the national level. Over a generation ago during the early days of the Cold War, Stalin's foreign minister, Vyacheslav Molotov, remarked on a trip to Berlin, "The trouble with free elections is that you never know how they will turn out." David Remnick, *Trump, Putin and the Big Hack* (The New Yorker, January 6, 2017), at http://www.newyorker.com/news/news-desk/trump-putin-and-the-big-hack.

More recently, cybersecurity vulnerabilities have had a significant impact on the American electoral process, the exact nature, extent and cause of which is still "classified". But some of the information has been declassified and available to the American public and the world shortly before President Obama left office. In the January 6, 2017 declassified report assessing Russian activities and intentions in the 2016 U.S. elections, the Office of the Director of National Intelligence gave a detailed analysis of a vast Russian intelligence operation the extended from hacking the Democratic National Committee's computer system, cyber attacks on Democratic and Republican targets, cyber hacking of the Gmail password of Clinton staffer John Podesta, propaganda campaigns and social media disinformation. The report withheld much of the hard evidence that would have shown more of the Kremlin's fingerprints, but did conclude – without revealing a detailed evidentiary basis - that Putin's Kremlin was behind breaches of Hillary Clinton's campaign and even some state election board websites, and that the Russian hacking operations were carried out with the express intention of disrupting the American electoral process, denigrating and harming the electability of Clinton, and helping Donald Trump's election chances. *Background to Assessing Russian Activities and Intentions in Recent U.S. Elections: The Analytic Process and Cyber Incident Attribution*, ICA 2017-01D, 6 January 2017. https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

While the private sector is exposed to similar vulnerabilities, we will take a close look at how local governments – including municipalities, counties, and school districts – are in the cross hairs of cyber-attacks. These attacks have most recently taken place in connection with third-party access to county depository funds and government-owned and maintained dams. The very networks on which local governments rely to enable and facilitate many critically important aspects of our increasingly digital lives are vulnerable to cyberattack, and 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. The targets are businesses, commercial and proprietary trade secrets, critical infrastructure, and sensitive information.

How can effective tools be developed that will enable local governments, together with our national and state governments, to respond in an appropriate, proportionate and effective manner to malicious cyber-attacks and cyber-enabled activities? What credible deterrence can these governments provide that will make others refrain from engaging in similar activities? Let's take a look at strategies now being developed to combat this growing threat.

Government Surveillance – National services are watching you

In a hearing on March 12, 2013 the US senator Wyden asked the United States director of national intelligence James Clapper:
„Does the NSA collect any type of data at all on millions, or hundred millions, of Americans?"
„No sir," Clapper replied.
„It does not?" Wyden asked, somewhat dumfoundes, since as a high-ranking intelligence committee member he knows otherwise.

„Not wittingly," Clapper said. „There are cases where they could inadvertently, perhaps, collect, but not willingly." (WIRED-magazin 12-2016, page 136)

A few months later, German and European media reports said that the mobile phone communications conducted by European government members were found on an NSA list containing reconnaissance subjects. Among these government members was also German chancellor Angela Merkel. Her mobile phone number was entered in the list as "GE Chancellor Merkel". The surveillance measure was implemented by a unit called "Special Collection Service (SCS)". German media reported that the Special Collection Service operates a not legally registered espionage branch office in the American embassy located in the Berlin district of Mitte. They said that from here, NSA and CIA staff members were monitoring the communication in the nearby government quarter. (Spiegel Online, 26th October 2013, http://www.spiegel.de/politik/deutschland/nsa-ueberwachung-merkel-steht-seit-2002-auf-us-abhoerliste-a-930193.html)
The media publications also provided indications that the NSA might have collected data on a large scale also in Germany, partly in cooperation with the German Federal Intelligence Service (BND). To this end, the BND was running a project called "Joint SIGINT Activity" together with the NSA.

Furthermore – also in cooperation with the NSA – the BND operated an intelligence monitoring station in Bad Aiblingen in order to reconnoitre international telecommunication. The basis of this cooperation was an agreement for the security of information entered by the United States and the Federal Republic of Germany as well as a "top secret" classified Memorandum of Agreement (MoA). This MoA defined the terms for their joint work. Within the scope of this cooperation, BND employees were searching data diverted from an internet hub located in Frankfurt/Main, assessing them in the light of specific criteria that had been determined by the NSA – the so-called selectors. Communication was monitored based on these selectors. Due to the large amount of selectors, a specific data filter system developed by the BND – called DAFIS – was used. The NSA also provided selectors that, according the BND, were against German interests.
(Facts for the Federal Constitutional Court's decision in the so-called Organstreit proceedings (dispute between highest federal organs) between the parliamentary group of Die Linke i.a. ./. the Federal Government, 2 BvE 2/15, Rdnr. 4)

These are two examples everyone knows since internet publication of Edward Snowden. Intelligence services almost completely monitor private, administrative and official telecommunication and internet communication. In the wake of the terrible attacks of 9/11, intelligence services launched the so-called PRISM program. Its aim was to fight terror and protect national sovereignty from terrorist attacks. It can be assumed that the internet is not only being monitored by the surveillance programs operated by British and American intelligence services that became known through Snowden's revelations. State surveillance and targeted surveillance of internet communications are also attributed to Russia or China for example.

After the 2015 Paris terrorist attacks (Charlie Hebdo), the Conference of the Data Protection Commissioners of the German Federation and the German States observed the following, just as they did after the 9/11 attacks:

> "Any shift towards state surveillance and at the expense of free and unobserved actions, movement and communications of the citizens in our country must be avoided. Data protection is not an obstacle to defensive measures, but it plays a part in defining the constitutional state's identity. Or – in the words of the German Constitutional Court – it is "an elementary precondition for the functioning of a democratic community based on its members' ability to act and participate." If we encroached upon the right to informational self-determination, the terrorists would have achieved one of their aims."
> (Decision by the 89th Conference of the Data Protection Commissioners of the German Federation and the German States, March 2015)

We all know that reality is different. In light of comprehensive state surveillance, the protection of our right to informational self-determination, personal data as well as professional and trade secrets is only given if individuals take proactive measures to protect their data.

In 2014, the German Bundestag voted for the establishment of a parliamentary committee of inquiry to investigate the scale and background of the spying activities carried out by foreign intelligence services in Germany.

To determine the extent of monitoring through foreign intelligence services, the parliamentary committee of inquiry requested information from the Federal Government for example about the NSA's selector lists and search criteria.

In its decision 2 BvE 2/15 of 13th October 2016, the Federal Constitutional Court rejected the request. In its headnote the Court said:

> "The government's interest in non-disclosure outweighs the parliamentary interest in information, as the same NSA selector lists are not subject to the Federal Government's exclusive power of disposal due to international treaties. Constitutionally, there are no objections to the Federal Government's assessment according to which handing over the lists in disregard of assured confidentiality and without the approval of the United States of America would significantly undermine the functioning of the German intelligence services as well as their ability to cooperate. In that regard the Federal Government, in consultation with the Committee of Inquiry into NSA Activities, took account of the request for submission as specifically as it could have done without disclosing secrets."
> (Decision by the Federal Constitutional Court concerning the so-called Organstreit proceedings (dispute between highest federal organs) between the parliamentary group of Die Linke i.a./. Federal Government, 2 BvE 2/15, headnote no. 5)

Until today, the public still does not know to what extent and with which keywords (selectors) foreign intelligence services have monitored communication in Germany.

Privacy interest in a global surveillance world

Is there still privacy safeguard in our electronic communication e.g. emails, chats, whats app and similar?

In Germany protection of personal data and privacy is a fundamental right. Regulation of privacy interest and decision of the Federal Constitutional Court protects the privacy interest. Article 2 of the German Basic Law protects the so called "informational self-determination", Article 10 of the German Basic law protects the privacy of correspondence, posts and telecommunications. In many cases, in particular in legislation against the terror and for national security the Federal Constitutional Court in Germany constitutes a corrective institution for the measures implemented by the legislator, and it safeguards time and again the right to informational self-determination, the privacy of correspondence, posts and telecommunications and the right of lawyers to protect their communication.

For Europe defines article 4 of the General Data Protection Regulation (Regulation (EU) 2016/679) as follows:

> 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The General Data Protection Regulation passed the European Parliament on 27th April 2016 and is directly valid law in all EU member states from 25th May 2018. This Regulation is intended to contribute to the accomplishment of

an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons (Whereas No. (2)). The Regulation applies to the processing of personal data from companies or authorities in the European Union. The Regulation does not apply tot the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

In 2016 the Court of Appeal in New York decided, that Microsoft don't has to transfer emails stored in Dublin (E.U.) to American servers so U.S. investigator can use the data in a narcotics case. Early 2017 the court voted not to revisit the decision. A lot of technology businesses, privacy advocates and Associations welcomed that decision. (Case 14- 2985, Microsoft v. United States, http://digitalconstitution.com/wp-content/uploads/2016/07/Decision-opinion.pdf)

In February 2017 a U.S. judge has ordered to Google to comply with search warrants seeking customer emails stores outside the U.S. That decision is fully opposing to the decision Microsoft vs. United States. The Judge in Philadelphia ruled that transferring emails from foreign server so FBI agents could review them locally as part of of a domestic fraud probe did not qualify as a seizure. "Though the retrieval of electronic data by Google from its multiple data centers abroad has the potential for an invasion of privacy, the actual infringement of privacy occurs at the time of disclosure in the United States.", the Judge Thomas Rueter wrote. After the decision Google publishes an announcement to plan to appeal the decision. (http://www.reuters.com/article/us-google-usa-warrant-idUSKBN15J0ON)

Protection of privacy means not alone personal privacy: Most of us don't want that third persons or authorities knowing the pictures of your child you send via email to your mother or grandmother. Most of us don't want that third persons or authorities knowing what you write in private to your spouse or best friend. For good reasons there is a private area in our life. Just because you are using emails or chats don't mean that you open your frontdoor of your privacy to everyone. Compared with you private property or house: not to use a fence don't mean, that everyone can walk into your house and look around. Privacy remains privacy regardless of whether you are not using a fence or don't lock your frontdoor.

Protection of your privacy means the company or attorney interests as well. As a lawyer you have to observe the lawyer-client-privilege.

The attorney-client privilege in Germany is protected both by the Rules of Professional Practice and the Federal Lawyers' Act.

> § 43a Federal Lawyer's Act
> Basic duties of a lawyer
> (2) A lawyer has a duty to observe professional secrecy. This duty relates to everything that has become known to the lawyer in professional practice. This does not apply to facts that are obvious or which do not need to be kept secret from the point of view of their significance.

Also in other countries, the law protects the attorney-client privilege and confidentiality.

In the US, the attorney–client privilege is a recognized evidentiary privilege that protects certain communications between a client and their lawyer. The attorney-client privilege protects the attorney from being forced to disclose the communication conducted between him and the client. The attorney-client privilege is one of the oldest privileges granted to safeguard confidential communication.

The United States Supreme Court has stated that by assuring confidentiality, the privilege encourages clients to make "full and frank" disclosures to their attorneys, who are then better able to provide candid advice and effective representation. See *Upjohn Co. v. United States,* 449 U. S. 383, 389 (1981).
From lawyers view it is only possible to defend criminal proceedings successfully if the client can be sure that information exchanged between him and the lawyer will not be disclosed. In commercial cases, it is of substantial business interest for companies that information known to the lawyer will not be made public or known to competitors. Clients with a strong public presence, such as politicians, artists or business leaders, trust that information given to the lawyer are not made public or known to other parties.

Last but not least, for U.S. companies who want to make businesses in the E.U. they must to this in accordance with the E.U. data protection regulations or guarantee the protection of personal data. After the court decision Bloomberg headlined an article "A new reason for foreigners to avoid Google and Facebook" (https://www.bloomberg.com/view/articles/2017-02-07/a-new-reason-for-foreigners-to-avoid-google-and-facebook). It's an economic argument as well to protect privacy interest, to protect our personal data.

State of Cybersecurity in Local, State & Federal Government

A nation'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. During his tenure, President Barrack Obama warned that the United States nation was not devoting enough resources or attention to the nation's cybersecurity interests and that the infrastructure provided vulnerable targets for cyber-attackers whose attacks could lead 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.
These concerns were echoed in The Ponemon Institute's study of The State of Cybersecurity in Local, State, and Federal Government sponsored by Hewlett Packard Enterprise, which 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.
A major challenge at both the local and state level as well as the federal level is the lack of skilled personnel. Lack of budgetary resources is a key issue, leading to the unfortunate dilemma for state and local governments being unable to share as much intelligence about threats as they should.
Top security threats for local government range from failure to patch known vulnerabilities, negligent insiders, and zero-day attacks. State and local governments need to be prepared to deal with cybersecurity threats, yet their agencies and political subdivisions have yet to achieve an optimal level of maturity in their cybersecurity initiatives.

Reasonable Cybersecurity Actions Based on Threat Profile

One question for a local government entity concerned about cybersecurity centers on what reasonable cybersecurity actions the local government should take in light of that entity's particular threat profile. In short, what is the local government entity's risk appetite? Answering that questions compels local government leaders – and local government attorneys – to consider many interrelated cybersecurity issues.

Interrelated Cybersecurity Issues

Among the cybersecurity issues that have a direct impact upon municipalities, counties, school districts and other local governments and the citizens they represent, are 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.

U.S. and E.U. Not On Same Page in Privacy v. Security

The United States and the European Union are moving in different directions in the debate over "privacy" vs. "security." They do not have a uniform approach to cybersecurity problems that are international in scale, and time is running out for them to start singing from the same cybersecurity page. Some of these cyber-nightmares, such as the recent Segate ATM theft and the Ramnit financial fraud debacle that was recently shut down, can only be resolved through international cooperation and sharing of governmental and law enforcement information that includes public-private partnerships, discussed in detail *infra*.

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. An October 16, 2015 report said 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 that cost businesses $400 to $500 billion a year, little if any mention is made of 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

It has been projected that by 2020, the worldwide cost for essential cybersecurity protection will approach trillions of dollars. Is this a game in which cybersecurity will continue to play catchup for the next two to three decades, with no real prospect of gaining the upper hand over cybercrime? 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 four 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 cyber intrusion 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 claimed 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.

The exponential growth in these numbers and the boldness of the cyber-attacks demands a coherent strategy and response.

Attack against German Telekom Internet routers

In November 2016, about 900,000 internet routers from Deutsche Telekom were not able to connect to the internet and crashed. Thus, users were no longer able to establish an internet connection. Unknown hackers intended to install malware on the internet routers to make them function as part of a botnet, that means to serve as a remote-controlled infrastructure for further attacks. German Telekom routers were attacked through the remote maintenance port that is normally used to provide updates. Although no malware was installed, the repeated attacks against the routers made them crash by exploiting a security issue. Users were able to re-establish an internet connection by restarting their device. Deutsche Telekom, however, had to acknowledge that "it is impossible to guarantee 100% security for any IT component. We must therefore ensure to close known security gaps as quickly as possible."
https://www.telekom.com/de/medien/details/13-fragen-zu-angriff-auf-router-445088

Strongest DDos-attack with Mihai-malware

The attack against Telekom routers is seen as part of a large-scale DDoS attack (Distributed-Denial-of-Service attack) carried out in October 2016. Twitter, Netflix, Paypal, Spotify, and Amazon were no longer accessible for millions of users. The hackers were using a huge amount of Internet-enabled home appliances such as printers, routers, baby monitors, TV receivers etc., infecting them with malware and connecting millions of infected devices to establish so-called botnets. Criminals are then able to monitor and control such botnets from one central location and use them for DDoS attacks. Experts from the FBI and the Department of Homeland Security were alarmed, as they were worried that a similar attack could possibly target the online voting system used for the US presidential elections. Thirty-one federal states and the District of Columbia in Washington allow internet voting for overseas military and civilians. Alaska allows any Alaskan citizen to do so. It was feared that an attack could keep citizens from submitting votes either because they feel uncertain or because voting would be even impossible due to an DDoS-attack.
https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?smprod=nytcore-iphone&smid=nytcore-iphone-share&_r=3

Attack on Cellebrite with theft of 900 GB of data

Even companies specialized in monitoring and reading out mobile data have been exposed to cyber attacks. The Israeli company developed the "Universal Forensics Extraction Device" (UFED) tool that is used for example by the Federal Criminal Police Office (Bundeskriminalamt) and the German customs authorities to gain access to smartphones. The company promotes the product as the "all-in-one solution that enables logical and physical extraction of invaluable evidentiary data including encrypted and deleted mobile data." In the attack, customer data including login credentials and passcodes, databases and various technical information about Cellebrite products were stolen.
http://www.cellebrite.com/Mobile-Forensics/News-Events/Press-Releases/cellebrite-statement-on-information-security-breach

Cyber attacks on the German Armed Forces

In the last few years, about 47 million unauthorized or malicious attacks were said to be carried out on the German Armed Forces. In 2016, 9 million attacks were classified to have a "high risk level", while in 2015, 8.5 million attacks were classified to have the same high risk level. On foreign missions of the German Armed Forces, 58,000 attacks were detected, with 21,000 of them being regarded as particularly dangerous. Attacks are classified as having a "high risk level" if the attack cannot be repelled using conventional anti-virus or firewall systems. According to the German Ministry of Defence, no damage or losses have occurred so far.
https://www.heise.de/newsticker/meldung/Ueber-47-Millionen-IT-Angriffe-auf-die-Bundeswehr-im-Jahr-2016-3595632.html

Cyber Attack on the German Bundestag

In the last few years, the German Bundestag has been exposed to repeated cyber attacks. Early in 2015, and then again in May and August 2016, the German Parliament's IT infrastructure and some political parties were the targets of several cyber attacks. At first, the offenders intruded the computers of members of parliament or their staff by using ordinary malware. Then, they were able to move freely in the intranet of the parliament using admin rights in the network domain. The German parliament's IT infrastructure could not be used for several days until complete reinstallation of the systems. The German Federal Agency for Internal Security is supposed to have evidence that this might have been an attack "controlled by a foreign secret service". In August 2016, security agencies detected a targeted attempt to attack various German politicians and organisations. These targets received an e-mail from the "NATO Headquarters" which was infected with malware. The Federal Office for Information Security feared that hackers were trying to gain access to internal documents of politicians and political parties in order to exploit them for revelations to be made in the upcoming election campaign – similar to the attack on the Democratic Party in the US presidential election campaign.
https://netzpolitik.org/2016/wir-veroeffentlichen-dokumente-zum-bundestagshack-wie-man-die-abgeordneten-im-unklaren-liess/

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, and Europol's efforts proved it. 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/

Let us turn now to the local government vulnerabilities.

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

Former President Obama's fears about the vulnerabilities of U.S. infrastructure were justified. 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

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

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, the motivations behind these cyberattacks can be identified:

> 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.

IT-Department: How the Berlin Authorities Protect Themselves Against Cyber Attacks

According to federal security expert reports, more than 400 attacks on the government networks are said to have taken place every day in the first half of 2016. These attacks could not be detected using commercial protection solutions and merely twenty highly specialized attacks were detected by performing manual analysis. According to security authorities, one such attack per week is launched as part of secret service activities.

The federal state of Berlin protects its authorities’ and government’s IT infrastructure by using their own IT Department Center (IT security report, parliamentary printed document 17/3160 of House of Representatives, www.parlament-berlin.de). In 2013, the IT Department Center (ITDZ) assumed that no targeted cyber attacks have been geared towards specific authorities (parliamentary printed document 17/12194 of House of Representatives, www.parlament-berlin.de). It was nevertheless concluded that about 10% of external communication attempts with the Berlin state network have to be regarded as “random attacks” using malware, for example through e-mails. However, as the examples of cyber attacks show over and over again, viruses, Trojans and malware can infect a system because unknown file attachments are opened and e-mails are received carelessly.

The ITDZ is connected to all regional authorities, as IT equipment and IT security are to be controlled and managed from one central location. The ITDZ is also responsible for the information security with the Berlin authorities.

The ITDZ creates and implements IT security concepts. It monitors the implementation, effectiveness and compliance of security measures. Furthermore, it carries out training initiatives concerning information security.

Out of 72 dependent authorities, 65 have so far submitted a written concept, while seven authorities are currently developing such a concept. When we look at these numbers, we notice the lack of sensitivity with the authorities. At the same time, the fact that not all authorities have developed such a security concept, also poses a threat to these authorities.

Every authority is supposed to have one IT security officer. Nevertheless, four authorities still do not have any IT security officer in place. Also, the process controlling the implementation, effectiveness and compliance of security measures needs further improvement. Only twenty-two authorities have so far implemented this procedure completely, whereas it is only partially implemented with 45 authorities.

The ITDZ is deploying so-called Computer Emergency Response Teams (Berlin-CERT) with legally defined powers. The warning and information service collects and processes IT security incidents occurring in the Berlin authorities. The authorities are legally obliged to report any security-related incidents immediately to the ITDZ. The ITDZ collects and evaluates notifications about security gaps, malware, successful or attempted attacks on the infrastructure and the methods applied therein, and it issues warnings and gives recommendations for action. This makes the ITDZ in Berlin a central office detecting cyber and harmful attacks and developing protective measures for the authorities’ network.

As the ITDZ announced, no targeted cyber attacks on specific Berlin authorities were detected in 2015. The major risks for the authorities’ network include mistakes and negligence of staff members and malware imported by viruses and infected file attachments. Cyber attacks can only be prevented if staff members are sufficiently trained.

And last but not least, authorities and the heads of authorities have to take the increasing risks of cyber attacks seriously.

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 Plans

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

The cat-and-mouse game that seems to be taking place constantly between the perpetrators and victims of cybersecurity breaches, practices and measures is daunting. It has spawned a number of practices that can be implemented by municipalities to help protect their networks and systems. Some of these practices have been implemented by the private sector and 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

A number of best practices for municipalities were identified in *Cybersecurity for Municipalities*, a program presented at the Colorado Municipal League's 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.

Best-practice plus: protect your personal and business data and observe the attorney-client privilege

a. Protection of Internet-router/internet-devices

With easy measures you schould protect you internet router against cyber attacks. First of all change the admin-password of the internet-router. Most of the devices use a standard password like 0000, the password is the same on thousands of devices. It's very easy for attacker to know that standard password as well. Change that password to an individual one (see also page 29: "Effective password management"). Furthermore change the password to access to the wifi-connection. It's almost the same on the devices from one manufactor. The best wifi-protection is WPA2. Some of the devices comes with a connection-button called WPS (Wireless Protected Setup), like a wifi-repeater. Attackers could find out the connection pin number, because the pin number is calculated by an algorithmus. Switch of the remote access of your router or internet device. Most of us never use the remote access to connect from underway. Most of the router attacks use that remote access. And for sure, please update your device tot close security gap or backdoors.

b. Internet use

All of us and the government use the Internet. We google information, read the news, do online seminar, look up for the code of law online and legal cases, research information, read comments and look up for the functionality of objects and much more. And, since you are sitting in your office, nobody will notice it. Don't run away with that idea! Every search query, every website you visit is sent around the world. Your search queries and visited websites cannot only be recorded easily by secret services and other government agencies. By tracking your IP address, your Internet provider knows exactly from which connection you access the Internet. The Internet provider knows what search queries you are running and saves so-called cookies on your computer. These cookies save the search queries that you have entered.

Looking at your browser history, third parties can easily see the websites you have visited.

Your computer saves sufficient data in order to analyse later what search queries you have been running and what websites you have visited.

And I don't want to mention the various possibilities to monitor everything you do by means of hackers or espionage.

So I have some additional advices to help you protect the government data, while benefiting from the use of digital media.

c. Internet usage via the TOR network and VPN-Connection

The TOR-software (https://tor.eff.org) provides anonymous browsing and is free of charge. The Tor network allows to establish an anonymous connection to the Internet. Using the Tor browser you log in to a so-called Tor node and from this point, your entire connection is encrypted. The server you are calling cannot track the location it was called from. The advantage of this system is that you can act fully anonymously on the Internet and almost no one can track or surveille you. But for sure, I never heard that local und public government is using the TOR-Software. Instead of using TOR, the most governments using own and secure communication networks like VPN (virtual privat network). With the VPN the government user exchange data across public networks as if the user devices were directly connected to the private network. It's not only for inner-governement-communication important to use. It's also important for employers and government staff who get access to the computers from their home or with their own private device. If you are allow your staff do home office, a common working modell, make sure, that you only connect via VPN to the governements network and datas. Using the public internet connection without VPN

allows third parties, cyber thefts and government surveillance to see and steal your data and control everything you are doing.

d. Internet usage with LiveCD

Every time you use the Internet, you leave behind traces on your computer that are still there even after rebooting your computer. Such traces can be found both in the browser history and in the co-called cookies (small files provided by the website operators intended to “improve the quality”). If you don’t want that, you can use a so-called LiveCD. You can find it online, but also as a supplement to IT magazines. When you use this LiveCD, your system does not boot from your hard drive, but from a memory device, such as a CD-ROM, DVD-ROM or flash memory. After rebooting your system using the LiveCD, you can for example use the Internet. Following a new restart, no data collected through using the Internet before can be tracked or found anymore, as this constitutes only a temporary session. Your browser history, cookies or any other data can no longer be read out. By using a LiveCD system, you can prevent your browser history from being read out, search queries from being saved etc. However, your IP address can still be identified, if you do not browse anonymously. Using LiveCD-Systems in government daily work isn’t really common. But it’s an example to safeguard your personal use of the internet.

e. Internet usage with a different IP address

If you or your clients don’t want the connection used to access the Internet to be tracked, you can use so-called anonymization services. Using this kind of service, you are not browsing with your own IP address, but with an IP address taken from a large address pool. In addition, the IP address changes periodically as you are browsing the web. Your IP address is like the house number of your Internet connection. By tracking your IP address via the telecommunications provider, it can be identified what connection this IP address belongs to. And, of course, from the perspective of the attorney it may neither be useful nor advisable to browse with your own IP address.

f. Email usage

Everyone knows that an unencrypted email is like a postcard. Everyone who has access to the data transfer can also read the email, and everyone who has access to the recipient’s computer can read the email. The IT departments in government and enterprises are able to read any unencrypted emails, or colleagues may even have access to them. At this point, I don’t want to mention that of course also government authorities or criminals may have access to your Internet traffic and as such to your emails, too.

In my opinion, unencrypted emails pose one of the biggest risks for the lawyers’ confidentiality. They are a menace also to the attorney-client privilege. In this presentation we presented a lot of examples were emails were stolen and publishes. Most of them were not for publicity, the press or the opposite party. In my opinion, unencrypted emails pose one of the biggest risks for the government secrets and the data of local population theire data you store.

It is true that only very few people wish to communicate by using encrypted emails. There is communication that can be facilitated using non-encrypted email. However, government and local state lawyers should conduct their sensitive communication only in an encrypted manner.

I therefore support communication with encrypted emails using end-to-end encryption. There are companies on the market that provide encryption, and there are also open source providers. I recommend using open source solutions, such as Open PGP. With PGP solutions provided by commercial businesses, you can never be fully sure if there isn’t another backdoor, allowing emails to be sent unencrypted. For Open PGP solutions, many independent programmers work together, and anyone can read and verify the source code. This minimizes the risk of a backdoor, for example as is used by government agencies. There are PGP solutions for every email programme, even the user-friendliness of these programmes is much better today. This way, you take a large step towards a better protection of your clients’ data.

g. Cloud services

Using cloud services as DropBox or other services it is easy and convenient to use unlimited storage space and be able to share folders or documents with third parties, for example administration customs or clients.

In their general terms and conditions, many cloud services reserve the right to disclose data to third parties upon request, for example due to search warrants, subpoenas, court or government orders or by order of government or judicial authorities. This way, it is possible that your data will be disclosed to third parties such as government authorities or forein surveillance.
Some terms and conditions also contain provisions concerning the place of jurisdiction, which is often where the cloud provider is based. This means that you would have to assert your rights in the US if the cloud provider is based in San Fransisco. For foreign users it may turn out difficult to enforce their rights in such a case.
Who do the data saved in the cloud belong to, for example in the case of the cloud service provider's insolvency? How can you access your data if a liquidator continues to operate the business or accompanies the insolvency proceedings?

I therefore recommend government staff using cloud services only if these provide a very high level of privacy protection and ensure that no information or data will be disclosed to third parties at any time. Using a Dropbox is of course a tremendous help for the staff's everyday work to exchange documents, files and data. However, what good does it do if such a tool does not ensure professional secrecy, because data from the cloud are falling in the wrong hands in a targeted or accidental manner? If you make use of cloud services, you should only save data that are not under a particular obligation of confidentiality and that are not of particular importance or value.
Alternatively, you can choose a provider that grants a particular degree of privacy and data security or you are using the cloud services who are recommended by your government management. The best way would be using a own state or government cloud, which is only and fully under technical control and support of your authority or a trustful authority or IT-department.

h. Network technology and computer repair works by external service providers

If you want your computer technology to be repaired or maintained by third parties, you should definitely agree on a privacy statement with your provider. In my opinion, this does not apply if you give your computer containing your data to an external service provider outside the governements roof.I therefore recommend that you have your data systems repaired in your government IT-department only.
Also in the case of remote maintenance services, that is access of service providers to your PC through the Internet, you have to make sure that the service provider does not become aware of your government or authority data or documents.
In addition, you will want to make sure your employees observe the government data protection rules. I therefore recommend prohibiting the use of USB flash pens or external hard drives for the office's hardware. By using USB flash pens and external hard drives, criminal or surveillance malware may easily be introduced to your system, or USB flash pens may contain key loggers that log every keyboard input, running of programmes and every website you call without you noticing it.

State and Local Government Cyber-exercises

The future is not entirely bleak. Many valuable state and local government cyber-exercises have taken place across the United States, demonstrating successful public-private partnerships and substantive sharing of information and cyber technology. See Brian Nussbaum, *Thinking About State and Local Government Cybersecurity Exercises* (Center for Internet and Security, May 29, 2015), accessible at http://cyberlaw.stanford.edu/blog/2015/05/thinking-about-state-and-local-government-cyber-security-exercises-insights-incibe. Planning, preparedness and cyber-hygiene efforts are part of the toolkit of many state and local governments, and their focus on use of tabletop exercises and simulations is remarkable in its scope, practicality and level of effectiveness. A few examples provide encouraging evidence about potential best practices that may be developing at the state and local government level:

●In Delaware, the state's 2012 version of its annual cyber security and continuity of operations exercise was sponsored in part of the Delaware League of Local Governments and involved technical participants from a number of local governments.

●In Kansas, the scenarios used for a 2009 continuity of operations exercise related to cyberattacks were recently published, revealing the results of exercises designed for cities and other local governments, entailing a series of hacking attacks with serious consequences for local government operations and questions that were designed to help local officials work through the scenarios.

●San Francisco's 2014 Bay Area Cyber Tabletop Exercise was sponsored in part by the San Francisco Police Department and the Northern California Regional Intelligence Center.

●The City of Huntsville, Alabama conducted a day-long joint cyber exercise with state, local and non-governmental sponsors, including the Huntsville-Madison County Emergency Management Agency and Cyber Huntsville, focusing on cross-sector information sharing and infrastructure interdependence.

●The New York Independent System Operators hosted the New York State Critical Infrastructure Cybersecurity Exercise in 2014, with participants from electric and gas utilities and state, local, tribal and neighboring territorial government entities participating, leading to the planned formation of a New York State Security Working Group with both governmental partner and utilities.

●Hawai'i conducted a "tip of the spear" exercise in which its 2015 Po'oihe cybersecurity exercise looked at cyber impacts of a potential hurricane on the state, sponsored in part by the University of Hawai'I at Manoa, the state I.T. Services Department.

● On February 6, 2017, the ABA House of Delegates adopted Resolution 108 as proposed by the Standing Committee on Disaster Response and Preparedness and the Section of State and Local Government Law, urging federal, state, local, territorial and tribal governments to adopt standards, guidance, best practices, programs, and regulatory systems that make communities more resilient to loss and damage from foreseeable hazards and enhance the disaster resilience of communities. Central to the community resilience initiatives urged in this report, now official ABA policy, is the common theme: governments, businesses, the nonprofit sector, and the legal community should adopt standards, guidance, programs, and best practices, and consider regulatory systems that will make communities more resilient to loss and damage from foreseeable hazards and enhance the disaster resilience of communities. Included in such foreseeable hazards are broad-ranging damage and losses attributable to cyber-intrusions and cyberattacks on public and private infrastructure, for which emergency managers at all levels of government and in the private sector share responsibility. The amended Report accompanying R. 108 recognized this in the clearest of terms:

> Like natural disasters, cyber-attacks are a modern-day threat to national and local, economic and societal importance. Today, a single attack on the country's data system does not damage an isolated device, rather, attacks target critical infrastructure that is integral to protecting our economy, national security and daily life. While cybersecurity has been traditionally considered the responsibility of our country's information security and technology communities, preparing against cyber-attacks has now become a shared responsibility among emergency managers at all levels of government and among the private sector. Such efforts must involve *collaboration and information sharing* between government agencies, as well as between the private sector and government. *Cyber-specific incident plans* are critical and persons at all levels must be properly educated and trained with regard to his/her role before, during, and after an attack. *Continuous education and incident plan improvement* is also essential. This could include *monthly cyber-preparedness meetings* to discuss recent threats and to review the incident plan. *Routine cyber exercises* would also be effective.

CONCLUSION

There is no silver bullet solution to public sector computer system vulnerability and cyber-intrusion 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, sharing of information and technology with state, federal and non-governmental partners, 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.