MANAGING TECHNOLOGY RISKS THROUGH TECHNOLOGICAL PROFICIENCY

Guidance for Local Governments

Issue Paper #3 | November 2015
Bloustein Local Government Research Center

Marc H. Pfeiffer, MPA
Assistant Director and Senior Policy Fellow
Bloustein Local Government Research Center
Edward J. Bloustein School of Planning and Public Policy
Rutgers, The State University of New Jersey

MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND • MEL •
jif
RUTGERS
Edward J. Bloustein School
of Planning and Public Policy

The Bloustein Local Government Research Center

New Jersey is served by more than 1,500 distinct local government agencies: municipalities, school districts, utilities, counties, and more. Yet, even with this wealth of opportunity, precious little substantive research has been done within the local government environment to inform some of our state's most pressing policy issues.

The **Bloustein Local Government Research Center**, or **Bloustein Local** ***http://blousteinlocal.rutgers.edu/***, serves as a focal point and engages in a range of services, including:

- Encouraging and conducting applied and academic research on local government fiscal and administrative issues, emphasizing application and support to New Jersey local government.
- Developing resources that can assist others in conducting research and analysis.
- Organizing and hosting conferences and symposia on New Jersey local government fiscal and administrative issues.
- Supporting New Jersey local government fiscal and administrative policy development, implementation, and analysis through contract research and on-call advice for organizations and institutions that engage in local government policy setting and policymaking.
- Promoting and increasing public understanding of local government issues by partnering with and supporting civic and media organizations that inform and educate the public on local government matters.

A list of the Center's current projects may be found online at ***http://blousteinlocal.rutgers.edu/projects/***.

About the Author

Marc H. Pfeiffer retired in 2012 from a 37-year career in New Jersey local government administration, having served as a municipal administrator in several municipalities, and 26 years of service in the State's local government oversight agency, the Division of Local Government Services. At DLGS he served as Deputy Director for 14 years, and periodically as Acting Director.

Marc has broad experience in many areas of local government policy and administration, including specific expertise in areas such as finance and property taxation, public procurement, shared services and consolidation, records management, technology, energy, labor relations, and general government administration. He also has deep experience in the legislative process and as a regulatory officer. He is currently engaged in research concerning the use of technology in local government.

In addition to participating in Bloustein Local, Marc makes his extensive government experience available as a guest lecturer at the Bloustein School and other collaborative efforts. He is also assisting the Rutgers School of Public Affairs and Administration with the State's Certified Public Manager Program in curriculum development and instruction. He can be reached at marc.pfeiffer@rutgers.edu.

READ THIS FIRST!

Why this Study is Important to Local Government Officials

Local government agencies face risks from their use of technology.

Today's technology is embedded in most government activities, and it is increasing because the public expects it.

There are three types of technology:

- **Information:** computers, smart phones, and tablets
- **Communications:** voice, video, and data that move over wires and wirelessly
- **Operational:** video cameras, water and sewer process controls, meters, sensors, etc.

Risks stem from the things that people do (or do not do), the failure of technology systems, the failure of management and operational processes, and the disruptions created by external events (e.g., natural disasters).

There are six interrelated categories of risk: ***cyber security, legal, operational, financial, reputational, and societal***.

To manage these risks, organizations need to be technologically proficient. They can accomplish this by establishing and institutionalizing practices related to governance, planning, cyber hygiene, and technical competency.

The study shows how to assess an organization's technology risk maturity (a measure of risk) and technology profile (a way of defining its use).

The detailed report analyzes government technology risks and how to apply the four elements of technological proficiency. It is accompanied by four sets of Best Practices and Resources Guides, one for each of four technology profiles: Basic, Core, Managed, and Sophisticated.

Set your organization on the road to achieving technological proficiency now!

The study was conducted by the Bloustein Local Government Research Center at Rutgers University on behalf of the Municipal Excess Liability Fund. All the study material can be found at **blousteinlocal.rutgers.edu/managing-technology-risk** *and at* **http://tinyurl.com/NJMEL-Tech-Risks**.

Executive Summary

Only the smallest of organizations and an ever-shrinking number of individuals do not use contemporary digital technology in their daily activities. Today's technology permeates our personal and work environments. Mornings can start with a digital alarm clock, progress to smartphones and continue to GPS-enabled cars (or devices in them) that connect to wireless internet services providing local traffic reports. Our commutes include security cameras on digitally controlled traffic lights as well as streaming and downloadable entertainment (music, games, and videos). We have adopted fitness tracking devices that monitor our levels of activity and the location of our workouts. We use household devices that run on wireless networks. At work, we utilize tools and equipment that require the newest technologies. There are digital sensors built in to physical devices that report constantly on the conditions and operations of the power grid, our water supply systems, worker productivity, air and water quality, crop conditions, and almost every other human enterprise.

Digital technology surrounds and envelops us. Even if you are paying only scant attention to news stories (which are now identified, written, photographed or video recorded and then delivered through digital technology), there is a general awareness that this new world poses risks and challenges to the people who manage it and to those who use it. While cybersecurity (data and personal information theft, and denial of access in particular) gets the lion's share of public attention, those responsible for managing their organization's technology face a range of other risks affecting their organizations, employees, customers and clients.

What we do and use carry risks. Organizations face risks created by their use of technology. When it comes to using digital technology, cybersecurity is high on the list, but it is also essential to consider and plan for operational, legal, financial, reputational, and society-driven liabilities and exposures. Each government agency needs to manage its risks, which can vary by technological profile and risk management maturity.

Further complicating the development and use of government technology, is an increasing public expectation of 24/7 access to government information and services, on mobile devices, without regard for how government develops, manages and pays for that access and those services.

This research project looked at local government technology use from a risk management perspective. It suggests that to identify, assess and manage technology risks, organizations need to be technologically proficient. It concludes that agencies can become **technologically proficient** by establishing and institutionalizing four practices:

1) Technology governance that is driven by senior elected and appointed officials;
2) Planning that is integrated with governance and budgeting;
3) "Cyber-hygiene[1]" is institutionalized with employees, and
4) Development of technical competency that is needed to drive the management and delivery of the organization's technology.

The analysis suggests that all four practices comprising technological proficiency must be present for organizations for successful technology risk management. The challenge is in managing and overcoming institutional and practical barriers to it. This report includes several Best Practice and Resources documents, and a Leadership Summary to assist organizations in developing their technological proficiency. The results of a survey of New Jersey local government technology activities that informed the study is described in Appendix A. All study material is online at blousteinlocal.rutgers.edu/managing-technology-risk and http://tinyurl.com/NJMEL-Tech-Risks.

[1] See the "National Campaign for Cyber Hygiene sponsored by the Center for Internet Security at www.cisecurity.org/about/CyberCampaign2014.cfm

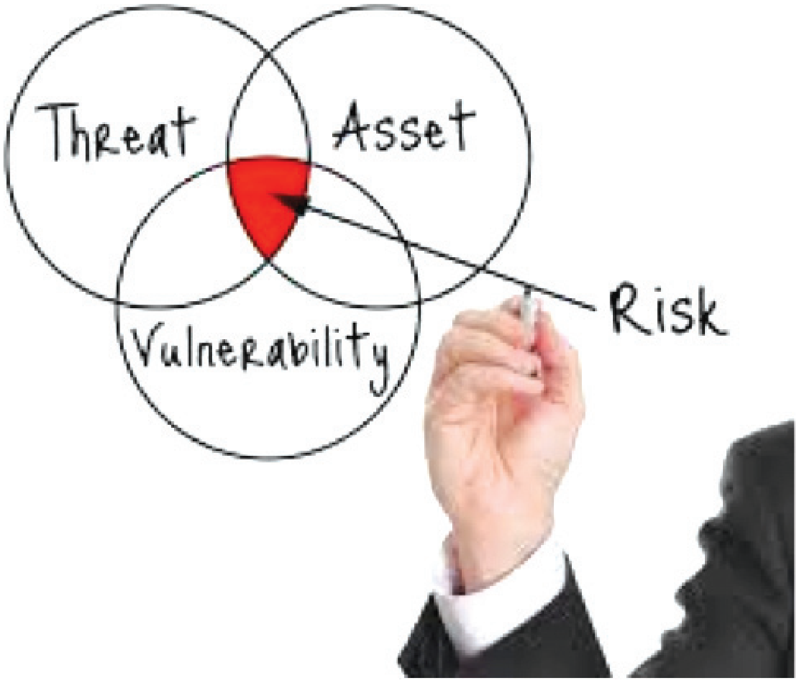
Preface

Readers of this report, you are at risk. If your organization manages a network, has an internet homepage or uses social media, it is at risk. If you have email, own a smartphone or drive a car, you are at risk. Constantly.

Events of July 2015 are instructive: a criminal data breach at the U.S. Office of Personnel Management caused an enormous leak of personal and confidential information belonging to over 24 million current, former, and potential federal employees. The crash of the New York Stock Exchange computer systems forced the suspension of trading for four hours due to a failed software upgrade; and the entire United Airlines flight system ground to a standstill because a bad router stopped moving information. In addition, the Wall Street Journal home page crashed, most likely because investors overwhelmed it by wanting to know what was happening on the NY Stock Exchange. These events highlight the risks society faces from cyber-attacks, software failures, hardware failures, and the unanticipated consequences of user behavior.

Information technology risk is usually discussed in terms of cybersecurity, i.e., the situation in which computers and/or network are under attack from hackers. In this scenario, individuals or organizations want to steal information. Computers have it, and have access to data, or that access can lead them to other sources of desirable data. However, the risks are greater than any one sequence of security events.

These risks stem from everything technology-related, particularly from our inescapable use of digital technology. This report examines the risks that local governments (and other organizations)[2] face because of their use of technology. It recommends what they can do to become *technologically proficient* in order to manage and mitigate these risks.



[2] The focus of this report is on New Jersey local government agencies. This should be broadly interpreted as municipalities, counties, local authorities and fire districts; for literary purposes, the report refers to them collectively as local governments, organizations, or agencies. Additionally, the principles suggested likely affect all kinds of other government and non-government organizations.

Part One–The Opportunities and Risks of Technology

WHAT IS THIS DIGITAL TECHNOLOGY THING?

"Isn't 'technology' just another word for computers?" "Don't we just have to buy them every few years?" "And why is 'digital technology' different from the technology we have used in the past?" Many elected and appointed officials often ask these questions. And understanding the answers to them is at the root of understanding risk.

Digital technology is used to describe **microprocessor**-based equipment, the software programs (applications) that run on them, ancillary devices that connect to them (printers, displays, sensors), and the communication networks that move information between them (Ethernet, the Internet, telephone networks, and cellular and other wireless communication technologies). Microprocessors are the so-called "computer on a chip" – a powerful computing device that can be the size of a fingernail, or smaller.

Today's microprocessor technology is found almost everywhere: in cars, traffic lights, medical devices, coffee makers, appliances, planes, and of course, desktop and laptop computers, tablets, and smartphones. While microprocessors appear in many forms, they have at their core a common element; they ultimately process information and instructions through a complicated series of 0s and 1s, the basic elements of computer processing.

Digital technology is often subdivided into several major application categories:

- **Information technology (IT)** represents the equipment and services that process, transform, move, store, convert, and present information (stored as 0s and 1s and translated by the technology to be useful).
- **Communications technology (CT)** transfers voice, video and data over wired and wireless networks from one point to individual or multiple destinations. Information and communication technology are often grouped together as ICT.
- **Operational technology (OT)** refers to devices such as video cameras (e.g., police body and dash cameras) chemical process controllers (e.g., water and systems), sensors, meters and related technologies that enable human activities. They even include the latest innovation – drones that can take photos now, and in the future may deliver products. OT also encompasses the **Internet of Things (IoT)** (or as some call it, the Internet of Insecure Things because of its mostly limited security protections).

This report will refer to all of these simply as technology.

What does this mean? For every MINUTE of the day during 2014[3]:

- 204 million emails were sent;
- 4 million searches are conducted on Google;
- $83,000 in sales were processed by Amazon;
- 26,380 reviews were posted on Yelp;
- 72 new videos were uploaded to YouTube;

and every day, 1 million new computer viruses or other malicious software programs were released.

These numbers increase constantly as more people around the world become digitally enabled with new and lower cost devices and access to networks. This ever-increasing usage has meaning for local governments that face challenges when adopting and using new technologies.

[3] Source: Domo, "Data Never Sleeps 2.0" https://web-assets.domo.com/blog/wp-content/uploads/2014/04/DataNeverSleeps_2.0_v2.jpg, and http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/

CHALLENGE OF DIGITAL TECHNOLOGY IN LOCAL GOVERNMENT

Since the 1960s when computers started becoming cost-effective, local and state government adoption of new technologies has always lagged behind private sector adoption. In local government, technology (usually information technology) was something to make government more efficient and reduce costs (usually personnel costs). Because decisions involving spending are something elected officials focus on, and technology is usually something new, the tendency had been to wait for costs to come down.

In the early years of mini-computers and PCs, IT was a cost-saver designed to lower expenses in areas such as accounting and payroll systems, and by replacing administrative support staff. IT drove efficiency in what was a relatively static work environment.

Now, for the first time, the use of new technology by consumers (i.e., citizens) has increased public expectation for government to move faster in order to meet their technology demands. This is contrary to most government behavioral patterns and instincts, and does not always meet the expectation of technology investment as an offset to other spending. It appears in new technology: the use of websites, social media, police mobile data terminals and shot-spotter systems (they help identify gunshot locations) that provide new and useful public services, but incur new costs without the offset of budget savings, and that may even add new, ongoing expenses.

Managing information security is another new technology-driven cost. Today's technology has enabled people who want things (money, power, and data) owned by others to use illegal means to obtain them. To prevent that, organizations need to learn how to protect their technology assets. When internet-based services started, security was a secondary issue. However, as technology has evolved to drive virtually all business processes, individuals seeking to access valuable information belonging to others have caused organizations to spend additional resources of time, attention and money to prevent this.

While new technologies still add efficiencies to operations (e.g., online recreation program registration, mobile device-driven inspections) and conveniences (e.g., tablets for use at governing body meetings) they are also occurring at a time of increased public scrutiny of government spending. This leads to the challenging paradox of public demands for lower taxes and increased services at the same time!

These changes have resulted in technology management opportunities and challenges; they require the integration of new technologies into a government environment that includes:

- **Cost/tax/fee pressures:** today most New Jersey elected officials focus on controlling costs because of statutory limits on appropriations and property tax levies. There are few options for other revenue raising tools.

- **Varying and changing public expectations:** it is widely accepted by elected and appointed municipal and county officials that the public wants more services and does not expect to pay more in taxes for them. Alternatively, some people want government to do less. This paradox comes from a developed lack of trust in government, well-known examples of abuse of government by a small number of elected officials and public employees, and changes in demographics as the workforce evolves (i.e., the rising importance of the millennial generation as baby-boomers move toward retirement while remaining active citizens with longer life expectancies.)

- **Political dynamics that work against long-term planning:** Turnover in elected officials prevents long-term In addition to the political implications of the two previous items, technology decision-making can be compromised by a belief that deferring a technology program "for just one year (or several)" in order to reduce the budget for the current year will not cause a problem. Elected officials or senior managers who take this position can frustrate (or destroy) efforts to develop and execute technology planning. With today's rapid changes in technology, plans of three to five years can be considered "long term," with plans of three years offering an appropriate project horizon when accompanied by annual reviews to address year-to-year changes.

Combining these three elements with political pressure to keep property taxes stable, and a perception that technology should save money, not cost more, results in an environment that inhibits the development of technological proficiency.

These are the challenges local officials face when managing their technology:

- Determining what is needed, wanted, and can be afforded; when and how to get it; how to manage it.
- Understanding that technology is more than just information technology; it also includes operational and communications technologies. All three have a range of risks to manage.
- Knowing that managing technology and its risks is an ongoing process, not a journey or destination; technology management is an ongoing, evolving process that does not stop with the purchase of the newest and best product or service.

ABOUT TECHNOLOGICAL RISK

The field of risk management provides guidance to meet these technology challenges and opportunities. Risk management tools focus on key actions to minimize threats and risks. There are four general elements:

- Identify the risks;
- Assess their likelihood;
- Treat them by protecting the organization from the risks (e.g., buying insurance) and by mitigating them (i.e., taking actions to reduce the risks); and,
- Monitor them by regularly reviewing your risk management plan to ensure that it is working and that is consistently enforced.

Every organization uses technology differently and therefore, has a different risk profile; that profile drives different solutions. Understanding the causes of technological risk will help frame the challenge.

What causes technology risk? **A Taxonomy of Cyber Security/Operational Risks**[4] has identified four primary causes:

- **Actions of People** – activities that people either perform or fail to perform that cause harm. These people can be insiders or outsiders; their actions can be inadvertent or deliberate, or the result of no action at all.
- **Systems and Technology Failures** – reflects the abnormal or unexpected functioning of technology. This can include hardware, software or integrated systems.
- **Failed Internal Processes** – the failure of internal processes to perform as needed or expected. This comes from poor process design or execution, or faulty process controls.
- **External Events** – events that are generally (but not always) outside the organization's control; these include disasters, infrastructure failure, legal issues, business issues, and service dependencies.

[4] Adapted from: A Taxonomy of Operational Cyber Security Risks, December 2010, By James J. Cebula, Lisa R. Young, Software Engineering Institute, Carnegie Mellon Institute

Table 1 – Taxonomy of Operational Risk

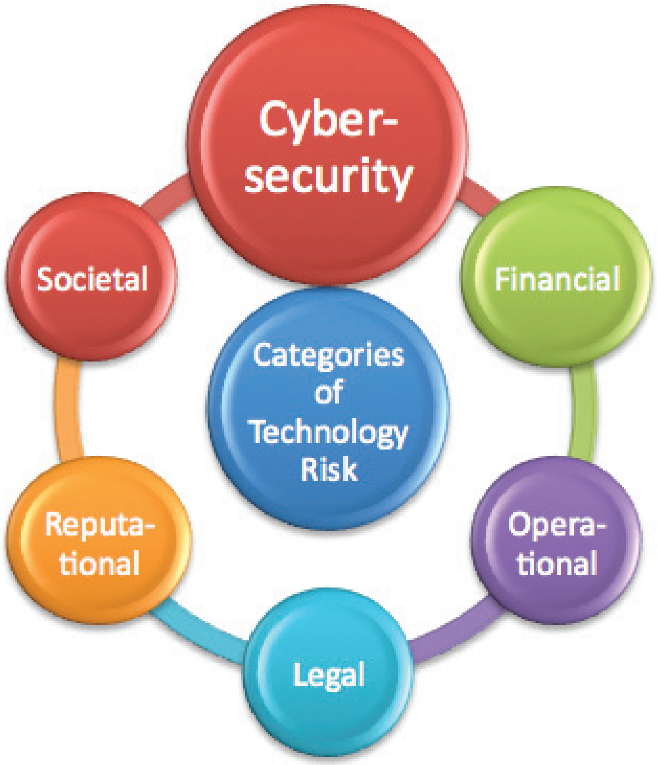
1. Actions of People	2. Systems and Technology Failures	3. Failed Internal Process	4. External Events
1.1 Inadvertent	**2.1 Hardware**	**3.1 Process design or execution**	**4.1 Disasters**
1.1.1 Mistakes	2.1.1 Capacity	3.1.1 Process flow	4.1.1 Weather event
1.1.2 Errors	2.1.2 Performance	3.1.2 Process documentation	4.1.2 Fire
1.1.3 Omissions	2.1.3 Maintenance	3.1.3 Roles and responsibilities	4.1.3 Flood
	2.1.4 Obsolecence	3.1.4 Notifications and alerts	4.1.4 Earthquake
1.2 Deliberate		3.1.5 Information flow	4.1.5 Unrest
1.2.1 Fraud	**2.2 Software**	3.1.6 Escalation of issues	4.1.6 Pandemic
1.2.2 Sabotage	2.2.1 Compatibility testing	3.1.7 Service level agreements	
1.2.3 Theft	2.2.2 Configuration mgmt.	3.1.8 Task hand-off	**4.2 Legal issues**
1.2.4 Vandalism	2.2.3 Change control		4.2.1 Regulatory compliance
	2.2.4 Security settings	**3.2 Process controls**	4.2.2 Legislation
1.3 Inaction	2.2.5 Coding practices	3.2.1 Status monitoring	4.2.3 Litigation
1.3.1 Skills	2.2.6 Testing	3.2.2 Metrics	
1.3.2 Knowledge		3.2.3 Periodic review	4.3 Service dependencies
1.3.3 Guidance	**2.3 Systems**	3.2.4 Process ownership	4.3.1 Utilities
1.3.4 Availability	2.3.1 Design		4.3.2 Emergency services
	2.3.2 Specifications	**3.3 Supporting processes**	4.3.3 Fuel
	2.3.3 Integration	3.3.1 Staffing	4.3.4 Transportation
	2.3.4 Complexity	3.3.2 Funding	
		3.3.3 Training and development	
		3.3.4 Procurement	

While the taxonomy focuses on cybersecurity, this study concludes that it also applies to technology risks in general. Table 1 takes these four areas and breaks them down into more detailed subdivisions; their applicability to a broad range of technologies should be clear.

SIX CATEGORIES OF TECHNOLOGY RISKS

After studying the literature on technology risks, the bulk of the research was found to have focused on cybersecurity and matters of internal control. Other research focused on specific areas such as legal or financial issues, but nothing was observed that integrated and analyzed the larger technology view from a risk management perspective. While the author concludes that the six risks described below cover the range of risks, the specific risks that fall under each one may overlap and intersect (i.e., cybersecurity risks can also involve financial, operational, and legal risks), and will evolve (i.e., the assessment of risks related to drone technology is in its infancy).

Figure 1- Categories of Technology Risks



Cybersecurity risks: The most complicated and pervasive of technology risks, cybersecurity is composed of a variety of threats. Cybersecurity risk is highly visible, creates news, and can have a debilitating personal and financial impact on individuals whose financial credentials or personal information has been stolen, which leads to identity theft. For organizations that find themselves specifically attacked, their technological resources are jeopardized, and their ability to deliver services is compromised. Threats to cybersecurity can be broken down into several discrete categories:

- Banking incursions – i.e., fraudulent electronic funds transfer
- Data breach/theft that results in:
    - o Disclosure of Personally Identifiable Information (PII)[5] via malware-based access, device theft or data theft by an employee
    - o Data loss or corruption
      Example: Medical records are worth 10 times more to hackers than credit card numbers. According to experts, hospitals often utilize low-level security measures, which make them prime targets for patient data theft. In that case, a patient's policy numbers, diagnostic codes and billing information could easily be accessed. The number of medical cyber-attacks has doubled in the last four years. Stolen health credentials can go for $10 each, about 10 or 20 times the value of a U.S. credit card number.[6]
- Network breaches, where a network is used as a remote host that the intruder can control. In this case, computer resources are used to attack or breach other systems (a.k.a., "botnets").
- Access to networked environmental control systems. This can compromise vital power, air and water systems, and serve as a launching platform to attack other systems.

[5] PII generally consists of an individual's driver's license number, date of birth, social security number, health care ID number, and biometric data such as fingerprints or handprints.

[6] www.consumerfraudforum.com/why-hackers-now-prefer-your-medical-records-to-credit-card-information/

- Credit card security system compromise. Thieves obtain credit card credentials that are then misused.

- Cyber-extortion (DDOS, Cryptolocker/ransomware). These kinds of attacks represent a category of risks that can prevent access to agency websites and/or can result in data loss. In some situations, the perpetrator may want something in return in order to end the attack.

- Website/social media attacks. These intrusions can result in the defacing of websites, the loss of access to social media sites, or some form of content compromise to both. These attacks can also result in the temporary inability of the organization to deliver services.

It is fair to label individuals who attempt to create data and network breaches as criminals. Some will quibble with this label, as they prefer to identify themselves as "political activists" (a.k.a., "hacktivists"). However, while they may see their motives as political in nature, their actions are legally classified as crimes.

A cyber threat that jeopardizes a government organization can also be classified by the type of threat it represents. Is the agency a specific or general target? Most local government agencies are not usually the intended targets of cyber threats, but someone who holds a grudge against an organization may attack them, or an agency may become a target of interest if something goes wrong. For example, organized hackers may create specific threats when a government agency acts badly or provokes a public event that attracts attention.

As a case in point, in the aftermath of the tragic shooting in Ferguson Missouri, not only was the city's website defaced and brought down, hackers digitally attacked city officials. The hackers disclosed their personal information (social security and health insurance account numbers, cellphone numbers, names, addresses and other private information. They found the information on the internet in available and hidden databases and on social media websites, and then posted the data online. This internet-based practice of researching and broadcasting personal information is known as **doxing**.

However, local governments, like any entity on the internet are subject to mass attacks. In these cases, hackers look for vulnerabilities in the organization's systems. When discovered, these poorly protected areas are probed to see what PII or network insecurities (easily guessed or insecure passwords, unprotected servers) can be found and exploited. These vulnerabilities most often stem from successful email **phishing** (phony emails designed to get the recipient to click on a link that inadvertently gives the sender access to the organization's systems) and other **social engineering** techniques. These efforts focus on obtaining access to personal or organizational financial accounts and/or access to personally identifiable information (for either an individual or a group). They may also result in forcing the organization's technology to attack other systems, thus creating a botnet.

Technology contractors may also inadvertently allow cyber criminals to breach the security of organizations for whom they provide services as hackers may be able to breach the un- or under-secured systems of contractors that hold agency data or that can access agency resources. This must lead agencies to require that their contractors employ policies and practices that protect the agency as well as themselves. The well-known Target store and the US Office of Personnel Management data breaches started when the credentials of contractors with access to the primary system were stolen or compromised.

Finally, employees may be a cyber-threat to their organization; employees can be fooled into clicking on a deceptive link or opening an infected file, which can lead to a breach. People are susceptible to phishing or social engineering attacks. In addition, as employees, they can commit fraud (i.e., a payroll employee can steal and sell the PII of other employees), while overworked employees and understaffed agencies can result in poor technology administration practices that can lead to breaches.

To summarize the risk: there are many ways in which bad actors try to manipulate individuals into divulging personal or business information, or trick them into schemes that ultimately defraud the organization.[7]

Recent commentary has pointed out that these risks are amplified in local government for four reasons:[8]

- The increasing complexity and intensity of cyber threats; the phrase "advanced persistent threats" is now commonly used to reflect the 24/7/365 nature of cyber-attacks.
- The funding for cybersecurity initiatives is insufficient; the increasing threats require new financial resources to fund protective techniques and personnel to manage them.
- The lack of cybersecurity visibility and control – cybersecurity activities have historically been buried deep in an organization's structures; this is changing, however, with the advent of a function (and sometimes a position) called Chief Information Security Officer (CISO), and the public attention paid to very public breaches.
- The ability to maintain compliance with a growing array of regulations; as more is learned and attacks increase in sophistication; lawmakers attempt to "fix" the problem by imposing new regulations and requirements on technology systems.

And lest it is thought that large businesses are better prepared, a recent cybersecurity report noted that:

> *Size just doesn't matter. That's the word from RSA, which found that the size of an organization is not an indicator of cybersecurity maturity. In its inaugural Cybersecurity Poverty Index, the company assessed the maturity of cybersecurity programs… and found that 83% of organizations surveyed with more than 10,000+ employees are not well prepared for today's threats. Overall, nearly 75% of all businesses lack the maturity to address cybersecurity risks.*[9]

To close this discussion of cybersecurity risk, four summary points are offered:

1. Cybersecurity is a never-ending battle against changing adversaries with evolving techniques, requiring ongoing and increasing resources of time, attention, and money.
2. Agencies can adopt policies and practices that improve security for themselves and that will reduce the loss and damage done by cyber intrusions and exploits.
3. More effective sharing of cybersecurity information and the development of greater expertise in protection and resilience can improve cybersecurity.
4. There is always more that can be done; this is something that will not end.

Legal risks: While risks from cybersecurity events have legal implications, technology drives other legal risks, most of which relate to litigation and the costs that come from that. They also divert the time and attention of management and legal practitioners from other matters. These risks include:

- Liability risks: third party individual, joint and several liability claims resulting from technology failure.
- Discrimination: individuals who are deprived of employment or access to services stemming from technology failure or misuse.

[7] For more details on these issues, see www.microsoft.com/security/online-privacy/scams.aspx

[8] www.routefifty.com/2015/05/cybersecurity-issues-state-local-governments/112081/

[9] www.infosecurity-magazine.com/news/cybersecurity-maturity-lacking/

- Litigation against technology contactors: this related to failure to perform or litigation addressing a breach of contract by either party for cause.
- Public records (OPRA), records retention and electronic discovery compliance failure: if agency technology and practices fail to meet expected standards leading to a lack of compliance, litigation and costs often follow.
- Non-compliance with federal and state regulations – ADA/Sec. 508 accessibility: if technology prevents disabled individuals from accessing resources to which they are entitled, legal action can ensue.
- Criminal Justice Information System abuse: agencies that maintain criminal justice information (CJI) in dedicated or centrally administered systems require confidentiality and limited access. If breached or inadequately maintained, these systems may fail to work as expected. If an individual claims harm because of such a breach, litigation can result.
- Employee misuse: individuals who misuse an agency's technology resources can can be subject to disciplinary actions with legal cost implications. Their conduct may also lead to criminal enforcement actions and liabilities related to the impact of the misuse.
- Theft of information: The unauthorized appropriation of PII and the accompanying harm to individuals often lead to expenses for legal defense
- Transparency access: more and more citizens expect that information maintained in technology systems is publicly available. If systems fail to meet expectation or legal requirements, litigation may ensue.
- Defamation: permitting public comment on websites and social media can lead to slander/liable charges; agencies need to ensure that they adopt policies and enforce them fairly; failing to do so leads to legal costs.

Operational risks: These risks occur when technology failure compromises government operations; services cannot be delivered because the needed technology fails to work or is unavailable. Some examples of these risks include:

- Loss of capacity to manage day-to-day activities: the loss of network access prevents work order assignments and tracking, the inability to process transactions or conduct business (e.g., financial, over-the-counter customer service, police records, inspections data, GIS access).
- Project management and project failures occur when management fails to oversee and properly manage the development of installation of mission critical projects.
- Compromised physical security of technology resources: i.e., server room environmental failures (heat, air conditioning) or compromised physical access that results in unintended or intended hardware or other equipment damage.
- Failure of electrical distribution systems to provide reliable power needs.
- Failure of third parties to provide network connections.
- Failure of backup and disaster recovery systems to work as expected (which could stem from lack of attention to regular testing).
- Data loss stemming from poorly maintained or tested hardware.
- Loss of network access to operational technology, particularly during emergencies or critical incidents; e.g., traffic control devices, water/waste water management systems, and surveillance cameras.
- Communications and video resources that fail due to communications network loss or system failure/compromise.

Financial risks: Technology risks have an accompanying monetary component, and this list highlights those risks:

- Cost of cyber insurance: cyber insurance is sold to protect organizations from the expense of responding to and litigation that stem from data breaches. The market is evolving as technologists, insurers and courts assess the costs of responding to breaches and assigning liability, as well as the costs of safeguarding individuals whose data has been compromised.
- Costs of responding to breaches and operational failure: while cyber insurance may reimburse an organization for the impact of incidents that fall under its coverage, insurance does not cover all breaches and failures. There are often direct financial costs, in addition to the loss of productivity that stems from a breach or operational failure and the accompanying reputational impact. These costs include the purchase of new services or equipment needed to protect the organization's systems from future breaches and their consequences. Being proactive or defensive in technology planning and spending is becoming more of a priority.
- Costs of defending liability suits[10] and liability damage awards: while cyber insurance may cover data breach events, operational failures can lead to the same kind of litigation, with costs of liability defense and damage awards falling to the responsible agency along with its tax and rate payers.
- Unanticipated technology costs: while technological advancements often bring improved and increased local government capacity, they do not always save money; often the full cost of the service will not be initially apparent (or discussed). Agencies adopting new or evolving technologies need to carefully study, assess and present the full costs of change to decision makers.
- Procurement risks: traditional government procurement models are not well suited to the purchase of technology goods and services.[11] New Jersey government procurement laws need to be refreshed to permit the purchase of complicated technology goods and services in an efficient manner that ensures integrity in public procurement processes.
- Capital vs. operating expenses: in the past, government traditionally bought its technology through capital purchases. Changes in technology markets, the move to cloud computing, and the increase in the purchase of services (apps) and software licenses over hardware are driving increases in operating budgets. As noted earlier, in New Jersey, this complicates the budgeting process as local governments face caps on operating costs (tax levy and appropriation caps), but not on capital spending.
- Higher costs of financing government activities: bond markets are starting to assess the exposures created by technology and the ways in which governments manage them as part of their bond rating reviews. Rating agency and bond market perceptions of poorly planned technology management can lead to higher borrowing costs (also a reputational risk).

Reputational risks: Local governments operate in a very public environment and how they manage their technology can affect public and media perception of the competency and capability of their managers; missteps attract attention. The new world of social media adds complexity to the perception of local governments and their officials by the public. These risks include:

- Public trust: success (new or improved services) and failure (ineffective or abandoned projects or security breaches) affect the public's trust in their officials. For elected officials this may have a negative impact on their ability to win future elections; for appointed officials it may call into question their continued employment.
- Media risk: technological success or failure can attract media (print, electronic and online) attention where it is seen not only by residents, but also by potential future residents, and businesses that make location decisions.
- Social (i.e., Facebook, Twitter) and website

[10] In this case, "resources" include the time and attention of management, which is taken away from other activities, as well as the costs of prosecution or defense of litigation.

[11] See www.govtech.com generally for searchable articles on "procurement" and "problem" or "innovation" for many articles on this challenge. Also www.codeforamerica.org/blog/2013/09/27/the-state-of-local-government-procurement/

content: These tools are becoming increasingly important as the way in which residents engage with their government. The ability of local governments to meet the needs of their online customers plays a major role in the reputation of the community and its officials.

- Response to technology failures: How the government responds to data breaches and/or improper or hacked online postings can affect the personal reputation of affected or attacked individuals. If the government responds in a clear and comprehensive manner, its reputation is enhanced; a failed response garners distrust and public insecurity.
- Political risk: well-run and capably administered technology enhances election prospects and public confidence in elected officials. The impact of the opposite is self-evident.
- Rating agency and bond market perspective: as noted above, when government agencies issue debt, their technological proficiency is measured as part of their bond rating and influence how bond markets respond to agency issued debt.

Society driven risks are the most challenging type of risks, as they are neither static nor quantifiable. Examples of these include:

- Employment pattern changes: this reflects changes in the values and expectations of employees of different generations. Newer employees (millennials) who grew up with technology, have different expectations of their workplace environment than their older (baby boomer) peers. These differences can lead to the early retirement of current employees who are less comfortable with emerging processes and technologies, and a higher turnover of younger employees when their workplace expectations collide with the relatively slow pace of change in government workforce management practices.
- Globalization of local government: this phenomenon has introduced a wide variety of languages and cultures into local governments across the country. New residents and new cultures bring new service demands, and the expectation that government will communicate in more than one language. This affects technology services from web site design and construction to social media policy. With that comes the need to manage the risks of communicating in multiple languages in a way consistent with cultural norms.
- Technological driven processes often outpace the government's ability to manage them: the needs of technology investment now exceed the tradition of most governments to simply update desktop computers and servers every few years. The speed of technology change and the increasing expectations of residents for technology-based services are driving technology-spending decisions.
- Pressures for increased government transparency complicate how we respond to risk.
  - o National (and international), state, regional, and local organizations of citizens, businesses, and civic interest groups are promoting increased access to public records, improved and regular access to government data and enhanced participation in decision-making (through online tools and video access to meetings).
  - o These efforts require the increased use of technology, which is often advocated without regard to costs, an organization's capacity to manage the technology, or its ability (or inability) to manage risks, both known and unanticipated.
  - o The release of data sets believed to be anonymized brings new challenges as the new science of "re-identification" of data can compromise personal privacy.
- Public perceptions: The public's lack of trust in, increased frustration with, and antipathy toward the perceived high costs of government, as well as the challenges faced by decision-makers thinking

“Government officials cannot throw up their hands and run away; opting out is not an option. The challenges of technology risk must be confronted.”

about the short- and long-term implications of their alternatives is an additional risk factor facing officials.

These technology risks are complicated, challenging, evolving, and troubling. They are also new, as is the explosive growth rate of new technological opportunities. Local government officials have never before faced challenges with this level of risk (perhaps the introduction of electricity is a parallel). We are in a time where technological change has an inexorable pull that is resisted at one’s political and economic peril. For the first time, it is the public (by whatever term: citizens, residents, voters, customers, clients, constituents) who have increased expectations for their government and who are pulling government toward their expectations.

Government officials cannot throw up their hands and run away; opting out is not an option. The challenges of technology risk must be confronted. To help address them, the concept of technological proficiency is suggested as an approach to managing technology risks.

The Special Risks of Water and Fire

WATER AND WASTEWATER OPERATIONS

Government activities that distribute, collect, and/or treat potable and wastewater face information and communication technology risks similar to all other government organizations. Consequently, the elements of technological proficiency fully apply to these groups. They have, however, a significantly greater risk of operational technology failure through their use of process control devices, digitally enabled equipment and networks of sensors that regulate, report, and control elements of those systems.

This specialized technology niche is exposed to increased cybersecurity risks when the control systems are connected to the internet. Therefore, these organizations must pay special attention to mitigating those risks. The exposures must be appropriately assessed and managed to ensure these vital elements of local and national security remain operational and protected.

Specialized resources have been developed to help these organizations manage their risks. All agencies engaged in these activities should access the following resources; they are in addition to the material in the profile-based Best Practice Guides that accompany this report.

- American Water Works Association - Process Control System Security Guidance for the Water Sector www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx This guide goes beyond a discussion of the threats posed by unsecured information technology, and focuses on water specific operational technology risks. The cybersecurity practices included in the guide provide a set of recommendations for improving the security posture of the process control systems (PCS) used by potable and waste water utilities.

- Agencies should join the WaterISAC, https://www.waterisac.org in order to collaborate with other water sector professionals. This organization provides a way for members to share information on natural disaster preparedness, security threats, and other hazard response practices. Like the MS-ISAC, which provides cyber security resources to all government agencies, basic membership is free.

- The ICS-CERT (the Industrial Control System Cyber Emergency Response Team) is sponsored by the Department of US Homeland Security and focuses on cyber threats to control systems such as those used by potable and waste water systems. Membership in MS-ISAC or the WaterISAC provides access to the ICS-CERT's resources https://ics-cert.us-cert.gov/

FIRE SERVICE TECHNOLOGY

The research examined technology risks related to those organizations that provide community fire safety. In New Jersey, municipalities and independent fire districts provide fire protection and suppression services though the use of paid, partially paid and volunteer departments. However, regardless of how fire safety services are provided and managed, the elements of technological proficiency apply. The research highlighted that the use of digital technology by fire service personnel, more so than by most other agencies in the public sector, is spread widely across all three forms: information, communications, and operations.

Examples of fire service technology show its range and depth:

Information technology

- Preplanning, incident training and response data
- Recordkeeping applications to manage personnel and track training schedules
- Training resources that use learning management systems, as well as discrete online services and products
- Resource inventories that list equipment and supplies, and track their use
- Tools for incident recording and applications that track resources and report events
- Agency public communications policies and practices (i.e., websites and social media)
- Technology resources that aid in predicting weather events and assess their impact on operations

Communication technology

- Immediate access to online data sources: e.g., assistance in vehicular extractions, medical data for EMS services, hazardous material reports, construction material information, building plans, and access to preplanning resources
- GPS/GIS systems used to access incidents and deploy resources
- Personnel tracking devices and personal safety gear
- Voice radio and fire-ground communications equipment; traditional, digital (RF, WiFi and Bluetooth), software-based, and those with interconnection capability
- Remote controls on fire apparatus and mechanisms for managing water streams
- Video streaming to command posts in order to relay information regarding current conditions and personnel

Operation technology

- "Internet of Things" sensors and monitoring equipment in facilities that become useful during an incident
- Discrete devices that are microprocessor-driven and have communication capability. Such devices are used to provide information during incidents (e.g., infrared sensors, oxygen supply capacity, video cameras).
- Drones used for the detection of infrared hot spots and cameras that provide situation overviews; robotics used for search and rescue missions

This range, diversity of purpose and current limited integration of various firefighting technologies amplify the need to assess and intelligently manage technology risks especially in light of the agencies' purpose – saving lives. This service has added challenges, as risks and threat assessments will vary by the nature of how the service is delivered: paid operations will have different risk profiles than volunteer groups.

Thus, fire service organizations need to pay special attention to their adoption of technology in order to develop proficiency in its use and ensure effective risk management.

Part Two–Managing Risks Through Proficiency

WHAT IS TECHNOLOGICAL PROFICIENCY?

Up to this point, this paper has highlighted the technological challenges and risks that face local governments. These challenges and risks vary according to the size of the government entity, the technology used, and the way in which a government administers that technology. These variations make it clear that there is not a single solution to managing technology risks. What can be identified, however, are essential practices that can lead an organization through a process of technology risk management, and in doing so, bring them to a level of **technological proficiency**.

How will an organization know if it has achieved such proficiency? At the end of the day, a technologically proficient organization should be able to demonstrate that it:

- Recognizes the links between its business processes and its technology
- Understands its technology needs and risks;
- Has attained a level of proficiency that will allow it to feel confident that the technology will work when it needs to, including in routine and emergency situations; and,
- Is capable of defending itself against compromise and risks, including protecting and responding to those posed by cyber threats.

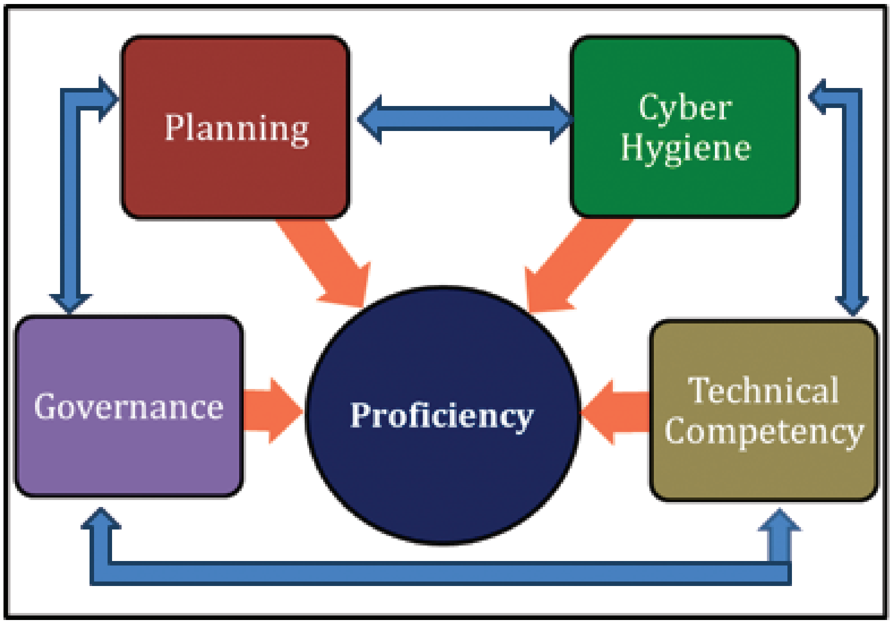
Technological proficiency safeguards the ability of a government organization to fulfil its various societal and legal missions; it is a way to manage the risks that technology introduces into the organization's business processes.

> “Technological proficiency safeguards the ability of a government organization to fulfil its various societal and legal missions; it is a way to manage the risks that technology introduces into the organization's business processes.”

This paper concludes that there are four essential practices of technological proficiency:

1. **Governance:** Governance: the governing body and executive management provide overall technology policy goals and guidance, make risk management decisions, approve and fund plans, and monitor activities.
2. **Planning:** government officials and technology managers combine to approve a technology plan that implements the long- and short-term goals of the organization and recommends risk management strategies.
3. **Cyber Hygiene:** all employees understand and practice the safe use of technology and receive ongoing training to prevent technology compromise.
4. **Technical Competence:** staffing, management attention, and the financial resources necessary to ensure sound technology practices are properly and adequately deployed to fulfill the plan.

Figure 2 — Elements of Technological Proficiency



Furthermore, like the risks discussed above, these four elements are interrelated and not discrete; each practice has an impact on the others, and to the extent that there is vulnerability in one, they all are vulnerable.

1. Governance

Public and private organizations are realizing that elected and appointed governing boards cannot ignore their organization's technology risks, nor can they delegate its key elements; it is clear that the duty of directors requires oversight of crucial business elements.[12] The legal system is becoming attuned to the importance of technology risk to the tactical operation and strategic path of organizations. Courts are concluding that governing boards cannot divorce themselves from risk oversight responsibility, legally or otherwise. Ignoring a red flag is a sign of organizational mismanagement and is rife with potential legal liability. Like finances, elected officials cannot ignore technology risks nor can they completely delegate key elements.

This does makes sense. Reputational and financial risks cannot be delegated to employees. While the fluid and challenging nature of technology adds to the burden of governing (especially for part-time, low paid or volunteer positions), there may be a desire to "make it someone else's problem." To do so would lead to arbitrary and capricious criteria for making decisions. In the end, technology risks, like all risks, reflect back on the governing board that makes decisions about spending, staffing and policy.

Governing bodies and chief executives must engage with their organization's technology, which means they must establish a decision-making process; they must create a process for technology governance. The governance process must result in the governing body making key decisions regarding an appropriate technology plan and then approving it (discussed below). This is much like how land use, open space acquisitions, or insurance coverage decisions are made. Now, they must understand technology risks and recognize to mitigate them.

The governance process should include not only representatives of the governing board and executive leadership, but depending on the **technological profile** of the organization (discussed below) it should also include technology managers, fiscal staff, public safety officials and operations personnel. It may also include responsible and knowledgeable citizens who volunteer their time to assist the municipality.

[12] www.governing.com/columns/smart-mgmt/col-cybersecurity-organizational-culture-risk-management.html, and https://en.wikipedia.org/wiki/Corporate_governance_of_information_technology

> “Governing bodies and chief executives must be engaged with their organization’s technology, which means they must establish a process for decisions to be made.”

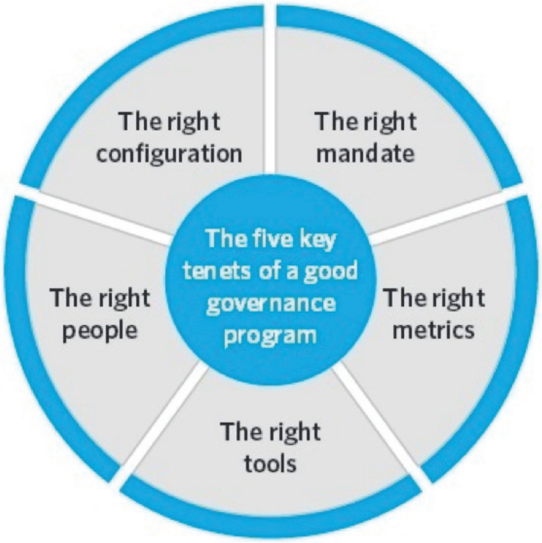
Organizationally, the governance process needs to set the tone from the top and:

- Ensure ongoing awareness and accountability of the governing body.
- Understand and approach technology as an enterprise-wide risk management issue, not just a technology issue.
- Appreciate the impact of a suspension of business process in the event its technology is attacked or there is a system failure stemming from a man-made event or natural disaster.
- Have adequate access to technology expertise, and ensure there is time for adequate discussion of issues.
- Establish agency technology goals and missions.
- Include the legal implications of technology, as well as the financial, reputational and cyber risks as they relate to their organization’s specific circumstances.
- Understand the roles and importance of all four technological proficiency practices.
- Develop risk management processes commensurate with the organization’s level of risk and complexity; discuss which risks to avoid, accept, mitigate or transfer through the purchase of insurance, as well as approve specific plans associated with each approach, managing risks both today and tomorrow.
- Adopt organization technology policies for implementation; minimum critical policies include:
    - Data breach/network attack response plan
    - Password strength
    - Social media use
- Establish a technology planning process that will be integrated into the organization’s routines, especially budgeting.
- Ensure that reports to elected officials are meaningful and timely, and that they focus on the institution’s vulnerability to technology risks and their potential impact on operations.
- Be able to communicate the critical nature these activities to the public.

Each organization will have variations to their approach. Small organizations may have a task force that consists of one governing body member, the municipal clerk, one or two interested citizens and a staff leader who uses technology. Larger, more sophisticated organizations may have a larger group, possibly adding a contractor, network manager or chief technology or information officer, and department users.

The key is that governing boards have to establish their own process, support it and address the issues brought to it. Once established, the process needs to identify

Figure 3 — Tenents of a Good Governance Program



This “wheel” is another way of looking at the governance component of proficiency.

and assess technology risks, determine how the organization should address them, and gain governing board approval. Regardless of the structure, it must also integrate its activities with the technology planning process that follows.

2. Technology Planning

A technology plan is an essential part of technology governance. As part of technology governance, the planning process needs to include those involved in governance (they may make up the core of the planning process).

Like any other municipal plan, a technology plan determines the extent to which technology supports each business process, how resources are allocated, and the way in which they will be administered and funded. It inherently supports and must be is integrated with the governance process since key decisions in the planning process come from governance decisions. There are many templates for creating technology plans (dozens of books have been written on the subject and examples abound on the internet), but they have to be customized to the needs of each organization. Generally, key elements can include:

- Business Processes:
    - Coordinating the organizational goals to technology goals.
    - Matching and assigning business processes to the appropriate technology.
    - Establishing plans to implement the goals.
    - Gaining the approval of the plan by the governing body.
    - Providing for an ongoing review of the plan by all concerned parties.
- Technology needs:
    - An assessment/inventory of the organization's technology assets, services and resources (hardware, software, networks, contractors, facilities, people), and an evaluation of their adequacy to meet goals.
    - A determination that the organization's technology is able to ensure the continuity of operations and continuity of government as well as the reliability of its disaster recovery plans.
    - A scan of the technology "horizon" and local needs to identify priorities for changes in technology solutions and activities.
    - A plan for a practical time horizon: three years is the maximum window of time given the rate of technological change, but an annual plan tied to the budget process may be practical. In all cases, periodic mid-year reviews are appropriate.
    - The assignment of responsibility to execute the plan to appropriate staff members and,
    - The integration of the plan with the organization's budget and the governance process, so that relevant spending decisions are tied to technology planning.
- Risk Assessment and Management:
    - An assessment of technology risks and a way to address them (for review through the governance process and for governing board approval).
    - An understanding of the information security management framework and the policies and resources available to address cybersecurity risks.
    - A method to address "make or buy" decisions, which services are provided by staff, which are purchased from contractors.
    - The establishment of a data breach plan that includes: an initial assessment, analysis, a determination of the scope of the breach, notification(s) (who is notified and how to do it), and an understanding the consequences of the incident so appropriate actions can be taken. Test the plan periodically.
    - An attorney to review the plan.

Matters of Compliance and Data Breaches

Agencies have the responsibility to comply with laws, regulations and contractual requirements in order to ensure the integrity of all digital information pertaining to an individual's personal and financial information. While local government agencies regularly deal with compliance and enforcement of state and local laws, technology management presents specialized risks that require agencies, based on their technology use, to comply with a set of specialized standards. Failure to meet cybersecurity compliance standards can result in fines and related legal, financial, reputational and societal damage.

These areas include:

1. **Personally Identifiable Information (PII)** – laws require notifications and actions if there is a disclosure of, or unauthorized access to PII. PII held by government agencies generally includes an individual's Social Security number, driver's license, health insurance account number, date and place of birth, mother's maiden name, and/or biometric records (which include finger and handprints).

2. **HIPPA** – this federal law addresses confidentiality of an individual's health care information, and specifies actions that must be taken in the event of a disclosure or security breach.

3. **Criminal Justice Information System information (CJI or CJIS)** – standards for law enforcement agencies to properly handle data necessary for performance of their mission, including but not limited to biometric, identity, history, person, property, and case/incident history data.

4. **Payment Card Industry (PCI)** – standards and requirements used to secure data stemming from credit or debit card transactions.

Agencies that use technology to manage data in these areas have the responsibility to ensure that their risk management practices specifically address how they handle compliance with these requirements.

Forty-seven states, including New Jersey, have enacted their own data breach laws requiring private and government entities to notify individuals of security breaches that involve information pertaining to personally identifiable information. In general terms, the New Jersey law (N.J.S.A. 56:8-161 et seq., P.L. 2005, c.226) requires:

- Disclosure of the breach to those affected in the most "expedient time possible and without unreasonable delay" consistent with needs of law enforcement. The agency must also take actions to determine the scope of any breach that included access to data by an unauthorized person.

- Disclosure of the breach to the State Police in advance of a public disclosure; notification can be delayed if immediate notification of the breach will impede a criminal or civil investigation, and the agency requests a delay.

- Notices sent to those affected by the breach. These can be written or sent electronically to the injured parties, or a "substitute" notice may be employed if the cost of individual notices exceeds $250,000 or more than 500,000 people are involved, or, if the agency does not have contact information for those damaged by the breach. A substitute notice can be communicated by media, email (if there are addresses), or by using a posting agency web site.

- Mandatory notification to credit agencies, if more than 1,000 individuals are affected.

Preventing data breaches and meeting compliance standards are key outcomes of technical competency within an organization, and are essential steps toward the reaching goal of technological proficiency.

The Best Practice Guides recommend that agencies adopt a data breach policy. While this policy can be composed of various elements, there are several common features that all policies should have contingent on the risks confronting the agency:

- **When confronted with a breach:** The plan must require that senior management, legal advisors and insurers be advised, and that the organization must act in compliance with the state's data breach law. When a breach is discovered, staff members need be clearly aware of their reporting responsibilities, and those along the chain need to understand the organization's legal responsibilities. The policy should include the names and contact information of all participants.

- **A single point of public contact:** A specific single point of contact should be established. Designating a spokesperson is critical in order to ensure that all information disseminated to the public is consistent with law and agency responsibilities.

- **Post Breach Remediation and Protection:** A plan should be in place to protect those whose data has been compromised ; most often this plan provides identity protection/credit monitoring for an appropriate length of time.

Many agencies (including the Municipal Excess Liability Joint Insurance Fund) purchase cyber insurance. This commercial insurance policy (data breaches are normally excluded from general liability coverage) provides services designed to protect agencies from the costs of a data breach. These policies usually provide guidance on damage assessment, respond to legal challenges, notification of concerned parties, and provide first-hand experience in managing compromised data systems. Cyber insurance is an important part of a technology risk management plan, but should not be thought of as a substitute for maintaining high levels of technological proficiency; the thoroughness of an agency's preparedness is the first line of defense against breaches.

3. Cyber Hygiene

The bulk of successful attacks on computer systems happen because an employee clicked on an email or web page link that they shouldn't have, or was otherwise "engineered" into doing something careless like[13]:

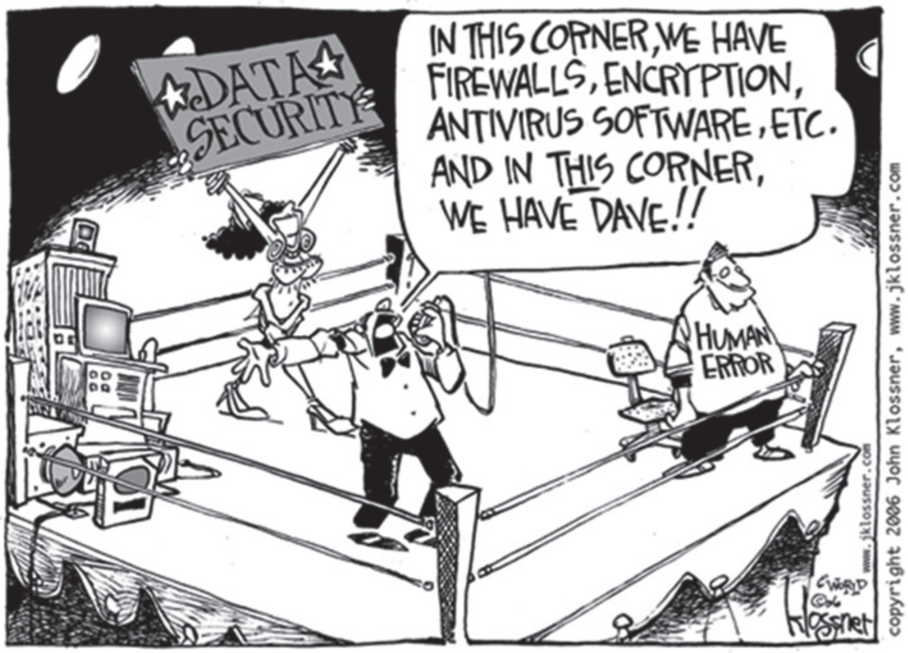
- Taking "phishing" bait
- Falling for phony phone calls that expose information or network access
- Not applying patches issued by developers (in standalone systems)
- Using weak passwords
- Using unprotected public Wi-Fi with mobile devices
- Posting too much information on social media
- Using non-sanctioned resources (i.e., using "found" USB sticks)

Employees do not automatically "know" a bad email from a good email. Hackers (remember those one million additional new viruses per day?) are organized, getting smarter, and use tools that are easy and inexpensive to obtain. Non-technology management employees are the single largest point of technology security failure. Thus, part of being technologically proficient, is that employees practice good cyber hygiene.

Agencies must train their staff, and training cannot stop after one in-service workshop, as the threats keep changing.[14] Employers must require initial and ongoing training. There are many video training portals and information resources of varying sophistication (SANS, MS-ISAC, the U.S. Department of Homeland Security's StopThinkConnect program, Security Mentor, KnowBe4) that can be part of an agency's technology plan (see also the Best Practice and Resource Guide).

In addition, to further secure technology resources, agencies can consider intrusion or penetration testing services. Outside organizations that offer these services can be hired to try to infiltrate systems or convince employees to click on a compromised email or otherwise divulge sensitive information.

Finally, organizations need informed employee guidelines to deal with individuals who violate policies that result in damage. Penalties need to take into account whether employees who create a breach, "should have known better" (because they were trained) or if they were reasonably fooled by a sophisticated hack. Employees can also be recognized or rewarded if they discover a new effort to break into an agency's systems.


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 John Klossner, www.jklossner.com
www.jklossner.com
Klossner

[13] www.darkreading.com/endpoint/7-deadly-sins-that-get-users-hacked /d/d-id/1320003

[14] See the "National Campaign for Cyber Hygiene sponsored by the Center for Internet Security at www.cisecurity.org/about/CyberCampaign2014.cfm

4. Technical Competence

Competency is the ability to do something successfully or efficiently. Here the term applies to an approved technology plan that is implemented with technical competency. To start, this means that all technical aspects of maintaining networks, servers, desktops, laptops, tablets, handheld devices, dedicated appliances, operational technology and process-related equipment are installed and maintained securely in accordance with sound practices.

It also ensures that goods and services are purchased efficiently and effectively, budgetary needs are met, staffing is sufficient, employees have appropriate certifications and keep their skills up-to-date. It also means that open source resources are considered, managed services are used as relevant, and new software needs are met through careful consideration and review. In addition, all application development must use contemporary standards and be expertly managed (i.e., the developers use agile development practices), desktop and user support needs are met, service contracts are managed, and specialized needs are addressed.

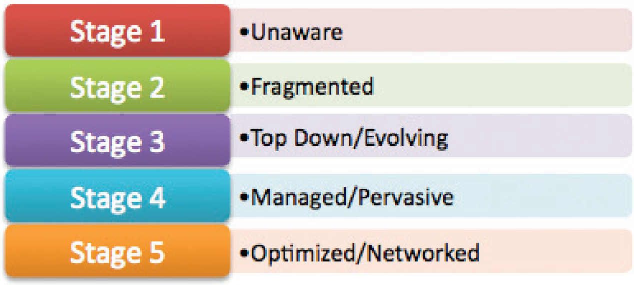
Technical competency also means that:

- Governance is kept up-to-date on activities to prevent surprises.
- Governance-approved policies are applied and enforced (e.g., password strength, employee access controls, job changes, turnovers, access rights).
- Contractors are secure and protecting you as well as themselves, and that their practices are periodically audited, e.g., reviewed and monitored/tested by a third party[15] or the agency itself.
- Staff remains up-to-date on changing security circumstances; escalates and shares issues with professional groups and peers as appropriate.
- Staff keeps abreast of technologies that could affect plans and governance; shares information and resources with peers and agency managers.
- Competency is applied consistently; reductions in vigilance are minimized.

ON ACHIEVING TECHNICAL PROFICIENCY

Every organization has a different mix of risks stemming from the scope, maturity, and technology processes. This risk matrix further varies by the different ways they manage, plan, and govern technology, or by their failure to do any of these things. This creates challenges for organizations that strive for credible levels of technological proficiency. Two concepts can help meet those challenges: **technology risk maturity** and techn**ology profiles.**

Figure 4 – Stages of Technological Risk Maturity



Stage 1	•Unaware
Stage 2	•Fragmented
Stage 3	•Top Down/Evolving
Stage 4	•Managed/Pervasive
Stage 5	•Optimized/Networked

Technology Risk Maturity Model

A technology risk maturity model focuses on the way an organization manages its technology and its risks. It addresses the degree of formality and sophistication of an organization's processes, from ad hoc practices, to formally defined steps, the metrics used to quantify results, and the degree to which it actively seeks optimization of its processes. Maturity models exist for specific industries and business practices (project management, software development and quality management). Other models focus on maximizing the use of technology.[16]

The maturity model on technology risks described below (and as Figure 4) is intentionally general and high level. The model has five levels of increasing sophistication. Its use here is to help organizations spot where they are and provide guidance on the conditions they need to create in order to improve their capacity to manage technology risks. Knowing where you are helps define where you need to go to reduce risks.

[15] The concept of using third party auditors is an evolving process and is potentially a useful process.

[16] Organizations that want to explore this deeper can refer to: i) IT Capability Maturity Framework; http://ivi.nuim.ie/it-cmf and ii) DelCor IT Maturity Model for Associations and Nonprofits www.delcor.com

Stage 1: Unaware: The organization sees technology management as largely irrelevant, and it does not form part of the organization's management process. The organization is not aware of its level of interconnectedness and its risks. They are doing nothing or are consciously ignoring the risks.

Stage 2: Fragmented: Management recognizes technology issues as a potential source of risk, and has limited insight into its technology management practices. The organization has a silo approach to technology and its management, with fragmented and incidental reporting.

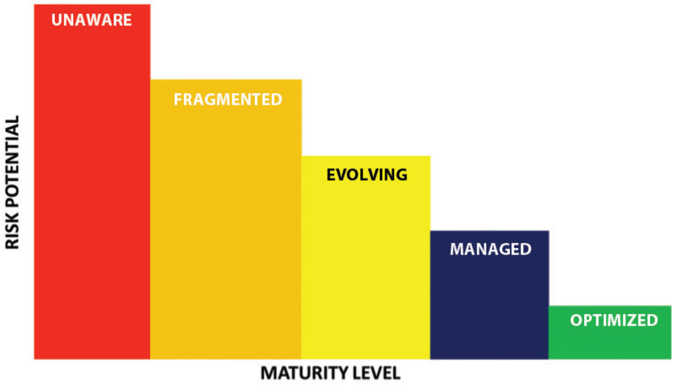
Stage 3: Top Down/Evolving: Management acknowledges the need for technology proficiency, has initiated policies, and understands its risks. The organization has begun to manage technology resources, has initiated planning, and started implementing government-wide technological coordination.

Stage 4: Managed/Pervasive: The organization's leadership takes full ownership of technology risk management, has developed policies and plans, and has defined responsibilities and oversight mechanisms. It makes calculated, informed decisions on technological needs. It understands the organization's vulnerabilities, controls and interdependencies with third parties.

Stage 5: Optimized/Networked: The organization is highly connected to its community, peers and partners. It shares information, meets citizen and client expectations, and coordinates technology risk mitigation as part of its day-to-day operations. Its people show exceptional technological acumen and cyber-awareness, and the organization is a leader in technology management.

A visualization of these stages (**Figure 5**) underscores their relationship to risk. Here risk is shown as shrinking as organizations move from being Unaware to becoming Optimized.

Figure 5 – Relationship of Technological Maturity to Risk



Technology Profiles

While technological proficiency and maturity affect how an organization manages its technology risks, each organization has a unique **technology profile**. Determining factors may include the range and depth of the operational processes supported by an organization's technological assets, the services it provides, and the organization's needs. Thus, each of the four proficiency practices must be adapted to the organization's profile.

Technological profiles can be incredibly varied based on an organization's networks, its use of contractors and service providers, its email model (server, cloud, or ISP based), and the range of services it provides to the public; they all have different permutations and options. At the risk of oversimplifying this infinite and complicated continuum, four profiles are suggested to assist local governments in fitting their risk management practices to their technology profile.

This research effort has also produced a "Best Practice and Resource Guide" [17] for each of these four profiles that helps match the best techniques for dealing with technology risk to an organization's profile. Ideally, the governance activity should be knowledgeable of the agency's profile so that the planning process can be shaped by these practices so the organization can

[17] The four Guides are in the Supplement to this report, which can be found online at blousteinlocal.rutgers.edu/managing-technology-risks

improve its proficiency.

The four profiles are:

Basic: Stand-alone desktops with no internal network; internet access and cloud-based email managed via direct connection through an ISP, few if any third party service providers.

Core: Has a small internal network with cloud-based email or may use Microsoft Exchange managed by a third party contractor, through a shared service agreement with another government agency, or managed by a part-time or full time employee (who may be a police officer assigned to manage that function). Other applications are purchased through third party providers (i.e., finance systems, police records or online services) with hardware and licensed software supported by a third party. In this profile, the police department may run its own technology separate from the rest of the organization. It is likely that some departments manage standalone systems with their own staff.

Managed: Has a fully wired internal network and possibly a wifi network with a small staff or contractors to manage them. This organization probably uses local servers to host third party software and is connected to cloud-based services; police services may be mixed in or supported by the managed system. Specialized department applications run on the main system and supported by a combination of dedicated employees, application developers, and contractors. Technology management decisions are made centrally and separately managed applications are minimized.

Sophisticated: Operates in a fully networked environment, often combining wired and wireless services. This organization uses a mix of applications that are either developed internally or licensed and are hosted on-site or in the cloud. It supports specialized servers and has robust technical management that employs well-trained staff and competent service providers.

Figure 6 – Technology Profiles

THE TAKEAWAY

A) It is clear that technology is found everywhere.
B) Its use will only increase over time.
C) Local governments face risks from technology. In order to manage these risks, organizations need to develop technological proficiency.

Achieving technological proficiency is an ongoing process; it is not something that is simply started, achieved, and stopped. It starts by putting technology proficiency on an organization's agenda so that it can start the process and set goals to improve its technology risk management and proficiency. That happens by creating a governance structure, integrated withfollowed by a planning process. The next step is to deploy resources (suggestions are in the Guides) to improve employee cyber hygiene. Finally, the agency needs to work with the people who manage its technology to provide resources that are needed to achieve competency. Underlying all of this is the way government spends its three most valuable resources: time, attention and money, and the need to do so prudently.

So…start.

Research Methodology

The project consisted of several research elements:

1. A comprehensive literature search of academic journals and publications covering terms such as technology risk, cyber risk, cyber threats, and specialized terms related to various fields of local government administration (e.g., public safety, water and waste water, etc.). Allan Zaretsky, a graduate student at the Bloustein School of Planning and Public Policy assisted the author in conducting the literature search.
2. An ongoing search and discovery of online resources from government institutions (both U.S. and international) as well as commercial vendors with an interest in selling goods and services related to technology risk. Of particular note is the work of the National Institute of Standards and Technology, the Center for Internet Security (and its subsidiary, MS-ISAC), the SANS Institute, various units of the U.S. Department of Homeland Security, and the National Association of Corporate Directors.
3. Focus Groups and Surveys: Two focus groups and a survey were conducted to obtain data on current New Jersey local government technology practices.

   The goal of the focus groups was to identify potential preliminary profiles and risk management practices. The first included selected members of the New Jersey chapter of GMIS International, the association of local government technology managers. A second event was conducted with members of the Tri-County Joint Insurance Fund (a member fund of the MEL with members in Cumberland, Gloucester, and Salem counties) consisting of mostly smaller, rural municipalities. An online survey of MEL members was conducted to further develop the technology profiles and to provide other useful information about current New Jersey local government technology use and administration. Separate surveys were planned for municipal, environmental and housing authorities, and fire district members. The municipal survey provided background for developing the profiles, however, it had limitations due to the widely varying technological knowledge of the individuals completing the survey (especially in smaller organizations). Interviews and the use of other resources helped fill in the gaps in developing the profiles.

   Useful results of the survey are found in Appendix A. The limitations of the municipal survey, combined with limited development input from authority and fire district members resulted in the elimination of those surveys. That noted, the results are generally applicable to those entities as well. Supplemental analysis and resources for environmental authorities and fire districts are in the sidebar, "The Special Risks of Water and Fire."

   The Bloustein Center for Survey Research administered the focus group and survey under the direction of Dr. Marc D. Weiner, Esq., and Orin Puniello managed the effort. Neha Mehta, a recent graduate of the Bloustein School, analyzed the survey data. Consultation with members of the New Jersey chapter of GMIS, several of whose members hold the designation of Certified Government Chief Information Officer, helped bring practical viewpoints to the work.
4. The author's personal experience, gathered over 40 years of New Jersey local and state government technology management and administration informed the study. That experience helped synthesize and adapt the material and guidance gleaned from the research. The results were the categorization of technology risks, the concept of technology proficiency and its four elements, the adaptation of common cybersecurity maturity models to reflect technology generally, and delineation of the technology profiles.
5. Dr. Shark evaluated and contributed to the concepts and their applicability to local governments generally. Dr. Caprio provided invaluable assistance and guidance in reviewing the report. [18]

[18] See Project Notes and Acknowledgements for information on these individuals.

Appendix A – New Jersey Local Government Technology Survey

A web-based (Qualtrics) survey was developed and administered through the summer and early fall of 2014. The sample population was drawn from the 380 Municipal Excess Liability Insurance Fund (MEL) member municipal governments. Email survey invitations were sent to the member risk manager and fund commissioner, with the instruction that the questionnaire was designed to be completed by the person within their organization most responsible for technology management. Following standard survey research protocol, several follow-up contacts were made to enhance the number of responding agencies. Overall, the effort resulted in 186 responding municipalities, constituting a 48.9% response rate.

The high response rate notwithstanding, incomplete and/or inadequate item responses limited the utility of the survey response set. Most notably, 30 percent of the individual respondents indicated little understanding of their agency's technology. Further, while a small sample of NJ-GMIS members pre-tested the survey, post-data-collection analyses demonstrated that the diversity in how technology is delivered (or at least the knowledge of it by the individual respondents) was not adequately reflected in the survey's outcomes. While this complicated analyses, it made clear the range of practices and knowledge levels of local agencies, as well as the importance of embracing an awareness of risk.

It is important to recognize the speed at which new technologies and practices are adopted; hence the survey is a snapshot of practices in mid-2014. The survey results were critical, as they informed the development of the profiles and helped identify risks while also highlighting the challenges of managing technology in today's dynamic environment.

The responding agencies were fairly well distributed across the state's municipal population categories and reflective of the MEL's membership. Breaking down the state's 565 municipalities into quintile population groups, the number of mostly useful responses (174) in each group was generally in concordance with the statewide percentage. This, however, excludes the largest municipalities, which were underrepresented:

Population Size	Percent of Respondents	Percent of State Total
0 to 4,440	31.0%	30%
4,401 - 8,200	20.1%	20%
8,201 - 14,750	19.5%	20%
14,751 - 39,000	23.6%	20%
39,001 - largest	5.7%	10%

Survey questions probed the following:

- Whether the respondent municipality had its own police department, followed by questions about its use of the Criminal Justice Information System (CJIS), a law enforcement data base system overseen by the FBI and the N.J. State Police;
- Numbers of CJIS and non-CJIS technology users;
- Ways in which municipalities provide email, internet, website, IT infrastructure, and social media technologies;
- Use of various software and management technologies, the type of product (commercial or home-grown) and hosting methods (local or cloud);
- Whether the municipality had an environmental utility, followed by questions concerning its use of operational technologies; and

- Levels of employee training, security practices, maintenance of personally identifiable information and experiences with security breaches.

Despite the above-noted limitations on the survey results, the following observations are sustainable:

- Contractors and police officers (for CJIS and non-CJIS systems) were the predominant custodians of their organization's networks in municipalities with a population below 23,000; in populations greater than 23,000, there is a predominant, but not-exclusive shift to full and part-time IT staff;
- Of the 110 respondents identified as CJIS users, 58 percent of the systems were maintained by police personnel, 17 percent by a municipal employee, and 24 percent by a combination of sources that were not clearly identified;
- Of the 130 responses to a question about who maintained their local network (some agencies had several answers): 59 percent were maintained by a contractor, 21 percent by a police department employee, 19 percent by a full-time IT staffer, 17 percent by a full time employee who had other non-technical duties, and 7 percent through a shared service agreement with another government agency;
- At the time of the survey, 91 percent of 167 respondents maintained their office productivity applications (e.g., Microsoft Office) on local servers, while 9 percent used a cloud-based service;
- 77 percent of 133 respondents had specific policies prohibiting personal use of office email;
- 75 percent of 143 respondents had their website maintained offsite by a contractor, the remaining websites were either managed locally (19 percent) or locally hosted/contractor managed (21 percent);
- Regarding content management, 52 percent managed their content through a content management system administered by a staff member, 25 percent were managed by a contractor, 16 percent had their sites (non-CMS) updated by an employee, and 6 percent were staff-supported blog sites;
- Of the 174 municipalities, 102 used web-based emergency notification services, 86 had Facebook pages, 48 had Twitter feeds, and 27 did not use any social media tools;
- Regarding employee IT and security training, of 174 responses, 30 percent of agencies provided no training, 21 percent provided initial training on hiring, 26 percent provided annual training of some kind, and 24 percent did not respond;
- 58 percent of 144 respondents properly back up their data by maintaining on- and off-site backup recover systems;
- Of approximately 125 respondents, 45 percent performed IT strategic planning, 24 percent had a third party IT audit conducted at some time, and 24 percent had conducted intrusion testing.
- Over half the respondents manage some type of personally identifiable information, with most of it stored on worksheets or in databases. If not encrypted, this information is at risk if stored on a network drive that is compromised by an intrusion;
- Only nine agencies had a data breach policy; and,
- Of the 174 municipalities, 122 provide battery backup to their servers, 100 used generators, 28 had power filtering.

Researchers with compelling interest in the data can contact the author to discuss it further.

Primary Reference Sources

In addition to a literature search that included a review of dozens of academic and professional journal articles, the following resources were instrumental in the study and developing its concepts. Several of them are specifically referenced in the Report and the Best Practice and Resource Guides.

Cebula, James; & Young, Lisa. A Taxonomy of Operational Cyber Security Risks (CMU/SEI-2010-TN-028). Software Engineering Institute, Carnegie Mellon University, 2010. *http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9395*

Center for Internet Security, *https://www.cisecurity.org/about/CyberCampaign2014.cfm*

CIO Leadership for Cities and Counties: Emerging Trends and Practices, Alan Shark, BookSurge Publishing, 2009. *www.amazon.com/CIO-Leadership-Cities-Counties-Practices/dp/1439240787*

Council on Cyber Security, *http://www.counciloncybersecurity.org/critical-controls/*

Domo, "Data Never Sleeps 2.0" *https://web-assets.domo.com/blog/wp-content/uploads/2014/04/DataNeverSleeps_2.0_v2.jpg* and *http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/*

Executive Companion -10 Steps To Cyber Security, Crown Copyright, 2012: *www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility*

Fiberlink Corporation: *http://content.maas360.com/www/content/wp/wp_maas360_mdm_tenCommandments.pdf*

Fusion Liaison Officer Cybersecurity Toolkit, April 2015, US Department of Homeland Security

GovLoop, Achiving Security with NIST Cybersecurity Framework, *www.govloop.com/resources/achieving-security-with-the-nist-cybersecurity-framework/*

GovLoop, Your Cybersecurity Crash Course, *www.govloop.com/resources/cybersecurity-crash-course/*

GovTech Magazine and website, general information *www.govtech.com*

Implementing Information Technology Governance: Models, Practices, and Cases, edited by Wim Van Grembergen and Steven DeHaes © 2008, IGI Global, Chapter V, IT Governance Implementation Guide

Information Week, 2014 Strategic Security Survey, *http://reports.informationweek.com/abstract/21/12509/Security/Research:-2014-Strategic-Security-Survey.html*

Infrastructure System Overview – Water System, *http://brilliancesecuritymagazine.com/wp-content/uploads/2015/02/ocia_water_systems.pdf* (US Dept. of Homeland Security)

ISACA, COBIT 5, A Business Framework for the Governance and Management of Enterprise IT, *www.isaca.org/cobit/pages/default.aspx*

IT Capability Maturity Framework, *www.ivi.nuim.ie*

IT Capability Maturity Framework; *http://ivi.nuim.ie/it-cmf* and DelCor IT Maturity Model for Associations and Nonprofits *www.delcor.com*

McGraw-Hill basic security training, concepts, definitions, two-minute drill and a self-test. *www.mhprofessional.com/downloads/products/0072254238/0072254238_ch01.pdf*

Metasploit penetration testing tools *http://en.wikipedia.org/wiki/Metasploit_Project*

National Association of Counties, cyber_for_counties {guidebook} v1.0 *http://naco.cyberguidebook.com/Vizion5/viewer.aspx?id=1&pageId=1*

National Institute of Standards and Technology, generally, Computer Security publications *http://csrc.nist.gov/publications/PubsSPs.html*

NIST Computer Security Incident Handling Guide *http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf*

NIST Guide for Conducting Risk Assessments, *http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf*

NIST Risk Assessments Guide *www.nist.gov/customcf/get_pdf.cfm?pub_id=912091*

NIST Small Business Information Security, The Fundamentals *http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf*

NIST Special Publication 8000-150 (Draft) Guide to Cyber Threat Information Sharing (Draft), 2014, NIST at: *http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf com*

Ponemon Institute, 2015 U.S. Cost of Data Breach Study, *http://www.ponemon.org/news-2/23*

Public Risk Management Association, *www.primacentral.org*

SANS Institute *www.sans.org/critical-security-controls*

The Open Web Application Security Project live CD: testing tools for website security *www.owasp.org/index.php/Main_Page*

Trustwave perimeter scanning for vulnerability and PCI compliance *www.trustwave.com/*

Verizon, 2015 Data Breach Investigations Report – Public Sector, *www.verizonenterprise.com/resources/reports/rp_dbir-public-sector-2015_en_xg.pdf*

Wikipedia, various IT reference pages

World Economic Forum, 2012, Partnering for Cyber Resilience, C-Suite Executive Checklist, *www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf*

www.americanbanker.com/issues/179_210/there-will-be-battles-some-will-be-lost-1070963-1.html

www.consumerfraudforum.com/why-hackers-now-prefer-your-medical-records-to-credit-card-information/

www.darkreading.com/endpoint/7-deadly-sins-that-get-users-hacked /d/d-id/1320003

www.genpact.com/insight/five-elements-most-companies-miss-when-trying-to-build-a-target-operating-model

www.governing.com/columns/smart-mgmt/col-cybersecurity-organizational-culture-risk-management.html

https://en.wikipedia.org/wiki/Corporate_governance_of_information_technology

www.govtech.com Searchable articles on “procurement” and “problem” or “innovation” for many articles on this challenge. Also *www.codeforamerica.org/blog/2013/09/27/the-state-of-local-government-procurement/*

www.infosecurity-magazine.com/news/cybersecurity-maturity-lacking/

www.routefifty.com/2015/05/cybersecurity-issues-state-local-governments/112081/

Project Notes and Acknowledgements

The Municipal Excess Liability Joint Insurance Fund (MEL), an organization composed of almost 600 New Jersey local government agencies (municipalities, counties, local authorities and fire districts), sponsored the Technology Risk Management Research Project. Its purpose is to educate local government officials on the technical, managerial, legal, and other related risks of digital technology used by government agencies. This report is an initial professional development resource that may be supplemented with educational materials, such as printed collateral information, online webinars and videos, and in-person seminar presentations. This may also include detailed guidance to local governments, particularly smaller ones, on technology risks, technology governance models, technology plans, and the development of adaptable policy templates that provide options for local use.

The project underscores the MEL's position that educating local government officials on the risks facing their organization and the actions they can take to mitigate and manage such risks are inherent elements of sound government risk management practices.

The Bloustein Local Government Research Center, a unit of the Bloustein School of Planning and Public Policy at Rutgers University conducted the research. The Principal Investigator was Marc Pfeiffer, MPA, and Assistant Director of the Bloustein Local Government Research Center.

The author is greatly indebted to two reviewers who provided invaluable comments and thoughtful guidance on the effort: Bloustein Local Government Research Center Director and University Professor Raphael J. Caprio, PhD, and Alan Shark, DPA, Director of the Center for Technology Leadership at the Rutgers School of Public Affairs and Administration and Executive Director of the Public Technology Institute. Also acknowledged are Debra Meltzer who edited the material, and Karyn Olsen of the Bloustein School who designed and formatted the report.

Over the course of the project, the lack of academic research, information, and publications that assessed the "big picture" of technology risk became clear; work that went beyond the not-to-be-underestimated cybersecurity and data breach risks was relatively rare. As a result, the classification of the six risk categories and the concept of "Technological Proficiency" with its four practices might be considered "original." They do reflect, however, an extension and adaptation of the existing literature, and in some cases "mash-ups" of individual elements that came before it. Appendix B lists significant resources that were relied upon for the project.

Finally, while the project was focused on New Jersey local governments, the conclusions and recommendations resulting from it are likely to have applicability to other government entities as well as other organizations that rely on technology.

The author welcomes comments and evaluations of the work *(marc.pfeiffer@rutgers.edu)*.

RUTGERS
Edward J. Bloustein School
of Planning and Public Policy

Bloustein Local Government Research Center
Rutgers, The State University of New Jersey
33 Livingston Avenue
New Brunswick, N.J. 08901

p. 848-932-5475 blousteinlocal.rutgers.edu