



Managing Technology Risks

Through Technological Proficiency

A Leadership Summary

**Research and Guidance for Local Governments to
Understand and Address the Risks Presented by
Contemporary Technology**

Prepared by:

*Bloustein Local Government Research Center
Bloustein School of Planning and Public Policy
Rutgers University*

for the

Municipal Excess Liability Joint Insurance Fund

Technology Has Risks



Digital technology permeates everything we do.

Its impact on local government is constantly increasing.

It goes beyond cyber security issues such as data breaches and network intrusions.

This summary identifies*¹ the risks that face local governments and steps they can take to manage and mitigate them.

¹ This summary is based on the full report, "Managing Technology Risks Through Technological Proficiency" and its Best Practice and Resource Guides, all found at www.blousteinlocal.rutgers.edu.

What is Digital Technology



Digital technology involves the use of microcomputers (computers on a chip) that run in devices that perform a wide variety of tasks.

They constitute the “brains” of computers, laptops, smart phones, tablets, and countless other devices. They are everywhere: in cars, traffic lights, medical devices, coffee makers, appliances, planes, and most everything wireless.

They can be broken down into three areas of application:

- Information technology – computers
- Communications technology –voice, video and data that move over wired and wireless networks
- Operational technology – digitally-driven devices such as video cameras, process controllers at water treatment plants, ice-detecting road sensors, meters, drones, including the so-called “internet of things.”

Impact of Digital Technology on Local Governments



Citizens are driving government to adopt new technology (web pages, social media, online services).

Local governments are challenged by:

- Cost/tax/fee pressures
- Varying and changing public expectations
- Political dynamics

The result is that citizens and businesses want their government to use more technology, but they don't want to pay more for it; this inhibits government from moving forward at the pace these constituents expect.

Thus, elected and appointed officials need to:

- Determine what is needed, wanted, can be afforded, and how to acquire and manage it
- Realize that technology is more than computers
- Understand that managing technology is an ongoing process; it is not a short-term project that is completed and ignored.

Managing Risks



Technology in all its forms present risks to local government.

The primary causes of technological risk are:

- **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. These activities are often classified as “cyber hygiene.”
- **Systems and Technology Failures:** the abnormal or unexpected functioning of technology. This can include hardware, software, and 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 generally (but not always) outside the organization’s control; disasters, infrastructure failure, legal issues, business issues, and service dependencies.

The effects of these risks are significant; they overlap and break down into six categories.

Six Categories of Risk

Cybersecurity: Data breach/theft and disclosure of personally identifiable information, data loss/corruption, network breach, cyber-extortion, website/social media attack.

Legal: Third party liability for denial of services, discrimination, litigation costs, OPRA liability, police system failures, employee misuse

Operational: loss of capacity to manage work, compromised physical security of technology, electrical system failures, contractor failures, failed backup systems

Financial: cost of cyber insurance, responses to breaches (time and money), procurement delays, change from capital to operating expenses

Reputational: loss of public trust, media risk, social media, political responses, bond rating agency evaluation

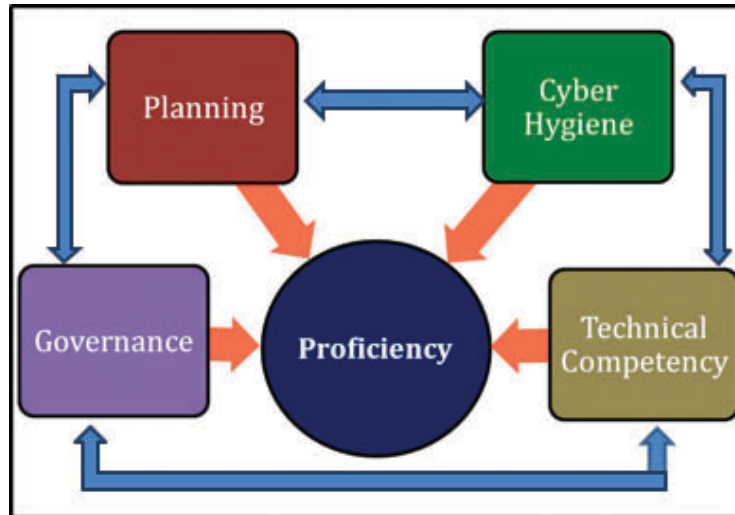
Societal: differing expectations of the next generation of workers, speed of change and the ability to manage it, increased expectations of government transparency that are rooted in technology



Technological Proficiency

Becoming technologically proficient enables governments to:

- Understand and manage their risks
- Be assured that technology will work when it needs to
- Protect themselves from compromise



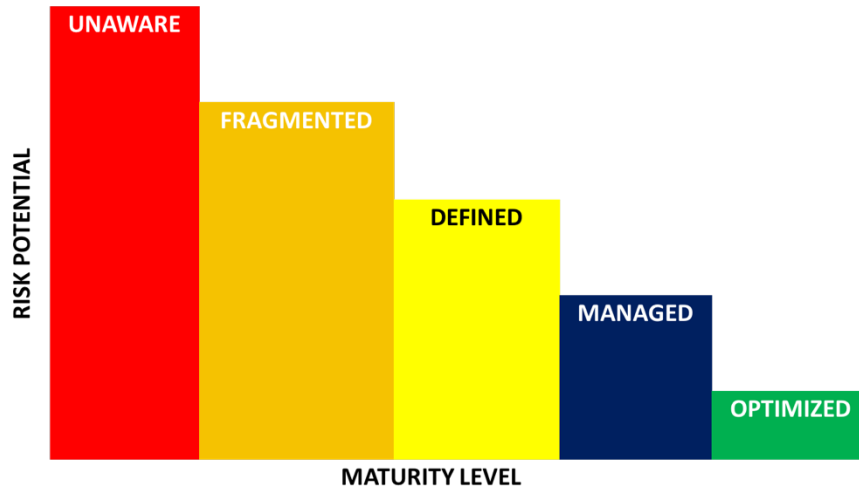
Technological proficiency has four interconnected practices:

1. **Governance:** governing body and executive management provide overall technology policy goals and guidance, evaluate risk, approve and fund plans, and monitor activities.
2. **Planning:** governance and technology managers combine to approve a technology plan that implements the long- and short-term goals and recommends risk management strategies.
3. **Secure Humans:** all employees understand and practice safe use of technology (cyber hygiene) and receive ongoing training to prevent technology compromise.
4. **Competence:** the staffing, management attention, and financial resources necessary for sound technology strategies are properly and adequately deployed to fulfill the plan.

Technology Risk Maturity Model

A risk maturity model relates to how an organization manages its technology and addresses its risks

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



Technology Profiles

Profiles address the wide variety of technology use in organizations:

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



Core: has a small internal network and may use Microsoft Exchange. Other services are purchased through third party providers. The police department and other agencies may run their own technology separate from the rest of the system.

Managed: fully wired internal network with small staff or contractor management; uses local servers for hosting third party software and is connected to cloud-based services; police services may be mixed in or supported by the managed system.

Sophisticated: fully networked in a wired or wireless environment with a mix of applications both owned and licensed, which may be hosted on-site and in the cloud; organizations with this profile support specialized servers and robust technical management using well-trained staff and service providers.

How to Get Started



1. Create a governance process appropriate to your agency
2. Start developing a technology plan
3. Implement employee cyber-hygiene training
4. Find out what's need to provide technology competently

This will cost time, attention, and money.

But, you have to do it.

Use the project's best practice and resource guides for help and support.

Technological proficiency safeguards a government organization's ability 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.

Project References and Resources

The study and reports were prepared for the Municipal Excess Liability Joint Insurance Fund by the Bloustein Local Government Research Center, Rutgers University. Marc Pfeiffer, MPA, was the Principal Investigator and author.

The full report, “**Managing Technology Risk through Technological Proficiency,**” provides the background and additional information on the material in this summary.

The accompanying material found in the “**Best Practice and Resource Guide for Achieving Technological Proficiency**” provide specific, profile-based actions local governments can take to move toward understanding and managing their technology risks. They are based on the four elements of technological proficiency presented in the report. The material is available online at www.blousteinlocal.rutgers.edu and www.njmel.com/.

Credits

Bloustein Local Government Research Center

Bloustein School of Planning and Public Policy
Rutgers University
33 Livingston Avenue, New Brunswick, New Jersey 08901
www.blousteinlocal.rutgers.edu
marc.pfeiffer@rutgers.edu

Municipal Excess Liability Joint Insurance Fund

9 Campus Drive, Suite 16,
Parsippany, New Jersey 07054
www.njmel.org
mel@permainc.com

All material © 2014-2015, Municipal Excess Liability Joint Insurance Fund and Rutgers, the State University.

RUTGERS

Edward J. Bloustein School
of Planning and Public Policy

NEW JERSEY MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND - CAMDEN

NEW JERSEY
MUNICIPAL
EXCESS LIABILITY
INSURANCE FUND
- CAMDEN



NEW JERSEY
MUNICIPAL EXCESS LIABILITY
JOINT INSURANCE FUND - CAMDEN