TECHNOLOGY RISKS IN MUNICIPAL GOVERNMENT

Bloustein Local Government Research Center/NJ Municipal Excess Liability Joint Insurance Fund

TECH IS HARD

Introducing new technologies into a government environment that includes:

- *Many competing issues*
- *Cost/tax/fee pressures*
- *Citizen expectations*

Political dynamics that work against long-term planning

- *"We can defer that purchase for another year, can't we?"*
- *It's not broken, why do we need to spend more money?*

Software and services pricing moving to per user subscription from capital cost model while local governments face levy caps.

Why Understanding Digital Technology Risk is Important

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.

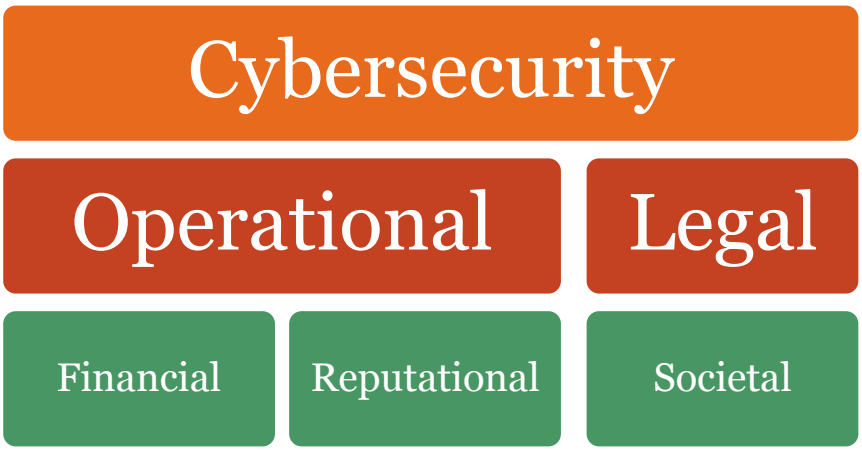
KEY TECHNOLOGY OPPORTUNITIES

Determining what we need, want, can afford; when and how we get it, how to manage it.

Understanding that technology is more than **information** (data) technology, but also includes **operational** (sensors, video) and **communications** (phone, radio, video) technologies; and they all have risks to manage.

Recognizing risks; that technology risks go beyond cyber-security; that it includes the other risks that need to be reckoned with.

THE SIX TECHNOLOGY RISKS



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

Legal: 3rd 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, and change from capital to operating expenses.

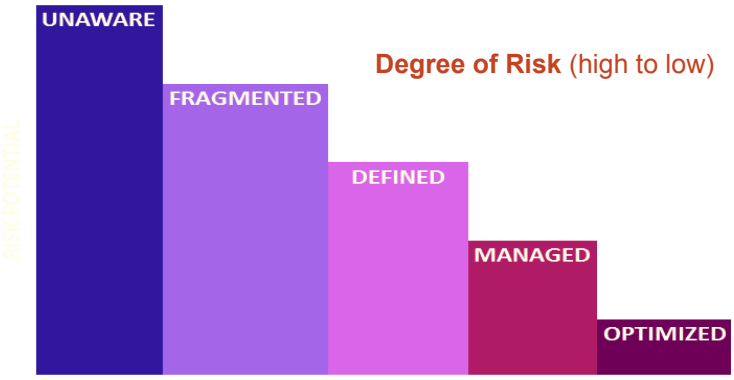
Reputational: loss of public trust, media risk, social media, political responses, bond rating agency evaluation.

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

Full details at http://blousteinlocal.rutgers.edu/managing-technology-risk

TECHNOLOGICAL MATURITY AND RISKS OF ORGANIZATIONS

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



Check your organization's risk using the Risk Maturity Survey Form at http://blousteinlocal.rutgers.edu/managing-technology-risk

CYBERTHREATS FACING MUNICIPALITIES TODAY

Targeted Attacks

Local government agencies are not usually specifically targeted, but you might be targeted by someone disgruntled or if something goes wrong.

Mass Attacks

This stems from successful email phishing and its cousins, as well as social engineering attacks.

Your Humans:

Staff that click on the wrong link/open the wrong file.

Bottom Line: bad people try to manipulate people into divulging personal or business information or tricking them into schemes to defraud!

About this Report

The full report, **"Managing Technology Risk through Technological Proficiency,"** provides the background and additional information on the material in this summary. The Report and a detailed Supplement are online at: http://blousteinlocal.rutgers.edu/managing-technology-risk

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

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

…With *Technological Proficiency* *

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 needed to provide technology competently
   This will cost time, attention, and money!

…With *Cyber Security* *

Have your technology staff/contractor do these!

1. Inventory authorized and unauthorized *devices*
2. Inventory authorized and unauthorized *software*
3. Create secure configurations for hardware and software on mobile devices, laptops, workstations and servers
4. Conduct continuous vulnerability assessment and remediation activities
5. Control use of administrative privileges

***See the Supplemental Report at http://blousteinlocal.rutgers.edu/managing-technology-risk for support in implementing of these activities.**