WHAT GOVERNMENT LEADERS THINK ABOUT:

- Why am I constantly being asked to spend more money on IT?
- Is our system secure from hacking?
- Who would try to hack us anyway? We are a small government.
- How can I be expected to make decisions on complicated technology?
- How should we be managing our Facebook account?
- Why don’t my IT guys take care of the risks?”
- How can technology screw up my re-election?

TECHNOLOGY IS EVERYWHERE!

THAT MEANS SOMETHING

1. It’s constantly evolving
   - Creates uncertainty - managing uncertainty is harder.

2. Integrating new technologies into a government environment
   - Competition for time and attention of leaders concerned with a lot of other issues

3. Dynamics that work against long-term planning
   - “We can defer that purchase for another year, can’t we?”

Marc Pfeiffer
Assistant Director
Bloustein Local Government Research Center
Rutgers University

© 2019 Bloustein Local Government Research Center, Rutgers University
Technology Management Challenges

Prioritizing
Determining what we need, want, can afford

Identifying
Understanding that there are more risks than cybersecurity

Accepting
Knowing that managing technology and their risks is a not race with a finish line; it’s a journey

Defining
Understanding that “technology” is more than “information technology

Technology Risks are Human Based

External
- Hackers (into network)
- Criminals (compromised data)

Internal
- Malicious (stolen data)
- Inept (malware infections)

Leadership
- Limited management
- No planning

Competence
- Poor training
- Inadequate facilities

Technology is Risky Business

What’s it to you?

Technology Risks are Human Based

Categories of Technology Risk

Operational
- Societal

Cybersecurity
- Financial

Reputational
- Legal

RESOURCES
- Time
- Attention
- Money

© 2019 Bloustein Local Government Research Center, Rutgers University
WHAT ARE CYBER SECURITY RISKS?

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>Criminals use every tool available to get information they can monetize: passwords, PII, email addresses</td>
</tr>
<tr>
<td>Network Access</td>
<td>They infect with ransomware, use your system to attack others (botnet)</td>
</tr>
<tr>
<td>Everyone</td>
<td>No target is too big or too small; targeted and random</td>
</tr>
<tr>
<td>Limit access</td>
<td>They disrupt operations, compromise the agency – ransomware!</td>
</tr>
<tr>
<td>Financial</td>
<td>Harvesting logons and passwords leads to identity theft, financial compromises</td>
</tr>
</tbody>
</table>

AND COMPLICATED BY...

- Limitations On Resources of
  - Time
  - Attention
  - Money

- Endless barrage of news and marketing, that...
- Promotes fear, uncertainty, and doubt...
- And creates confusion

THIS MEANS THAT TECHNOLOGY...

- Is Constantly Changing
- Has Risks to manage
- Costs Time, Attention & Money
- Requires Expertise
- Needs a decision-making process

SO HOW DO WE GO ABOUT MANAGING THIS?
BY BECOMING A TECHNOLOGICALLY PROFICIENT ORGANIZATION

Which is an organization that:

- …understands its technology needs
- …is assured that the technology will work when it needs to, including routine and emergency situations
- …is protected against tech-generated risks, including protecting and responding to cyber threats

MINIMUM TECHNOLOGY STANDARDS FOR TECHNOLOGICAL PROFICIENCY

Do you meet them? If not, start moving!

BUT FIRST,

Do you meet the rock-bottom, basic things you should not be without?

YOU MUST HAVE...

- System and data backups and assurance that they will work when you need them to; and,
- Someone you trust to give you advice on your technology.

- If you don’t have both of these, you need to fix that first.
- Then you can start meeting (and exceeding) the minimum standards.
WHAT YOU DO IS DRIVEN BY YOUR TECHNOLOGY PROFILE

- Sophisticated
- Managed
- Core

LEADERSHIP RESPONSIBILITIES

- How does your agency manage its technology?
  - Is there a tech planning process?
  - Is it tied to your budget process?
  - Who makes decisions and are they accountable for them?
  - Are they appropriately placed in the organization, with access to senior management?
  - Can you get an answer to: what’s our response plan if we have a ransomware bite, network attack, or data breach?

ELEMENTS OF TECHNOLOGICAL PROFICIENCY

- Leadership
- Planning
- Decision-making
- Budgeting
- Technical Competency
- Cyber Hygiene

To the extent one is weaker than the others, they are all weaker.

TECH LEADERS GO BY MANY NAMES

- Director of Management Information Services
- Director of Information Technology
- Director of Technology Services
- Network Manager or System Administrator
- Manager of Information Services
- Chief Information Officer
- Chief Technology Officer
- Chief Innovation Officer

- Can be an employee or a contractor
- Be properly placed on the organization chart
- Be responsible for making an executing decisions
- Meet the needs of the organization

© 2019 Bloustein Local Government Research Center, Rutgers University
WHAT IS IT THAT TECHNOLOGY LEADERS DO?

• Provide technology guidance concerning needs and risks to the organization (aka, planning).
• Plan, implement and manage applications to serve the organization’s needs.
• Supervise information systems and communications network.
• Manage technology resources: human, physical, and fiscal
• Meet user support/training needs
• And more, depending your profile

IMPORTANCE OF PLANNING

• Process has to be led and have buy-in from senior management
• Plan over 1-3 years
• Set up a team

THIS IS NOT A PLAN
**WHAT SHOULD BE IN A PLAN?**

- Tech plans need an...
- **Inventory**: Know what you do and have
- **Evaluation**: apply what you learn to identify needs
  - Meet internal needs and those driven by citizens
- **Risk Assessment**: Are there poorly managed or unmitigated risks to manage?

**FILL THE GAPS**

- **Conduct** a gap analysis
- **Identify** gap-filling options,
- **Establish** plan review cycle
- **How’s** your resiliency?

**MAKE DECISIONS AND FUND THEM!**

- **Setup** a process to balance needs, wants, and capacity
- **Meet** Minimum Technology Standards
- **Make** decisions

- **Link** planning and decision-making to budget cycle
- **Think** 1-3 year plan
- **Consider** operating vs. capital spending challenges

**THERE’S MORE: THE OTHER MINIMUM STANDARDS**
CYBER HYGIENE BASICS:

- Train (and retrain) employees in safe cyber hygiene
- Adopt policies to make sure
  - Sensitive information is protected
  - Appropriate password use
- Network with experts
  - Join MS-ISAC, the NJ-CCIC and GMIS!

ENABLE TECHNICAL COMPETENCE

- Sound backup regimen
- Servers and devices are patched
- Defensive software installed
- Access to servers is controlled
- Least privilege policies in place
- Support is available
- An incident response plan that works
- Infrastructure capacity exceeds needs

THEN IT ALL COMES TOGETHER: TECHNOLOGICAL PROFICIENCY

- Leadership
- Planning
- Decision-making
- Budgeting
- Technical Competency
- Cyber Hygiene

And there’s much more that sophisticated or higher risk places can do. This doesn’t end; it just evolves!

DO YOU MEET THE MINIMUM?

- Great...now you can do more and reduce risks even more:
  - Do risk assessments of your third-party providers who have access to your network
  - Conduct a full inventory of your devices and software; and refresh it at least annually
  - Secure internet usage with filters and white listing of applications
  - Limit social media access to those who need it
  - Implement wifi controls over segmented networks
  - Ramp up technical training of tech staff and cyber hygiene training of everyone else
  - Formalize all critical policies
  - Apply the balance of the CIS Top 20 and implement a framework (larger places)
QUICK PERSONAL CYBER HYGIENE DON’TS

- Don’t click on links in email that is offering you something, or making you worried or concerned about an account you have; Do: Go to the website of the company separately and check your account.

- Don’t open attachments from people you don’t know, or were not expecting from people you do know; Do: If you know the sender, check separately with the sender to see if they sent it.

- Don’t open zip files from anyone you don’t know - just delete it

- Don’t open zip files from someone you know, unless you separately positively confirm with them they sent it.

- Don’t click on pop-ups; be careful on clicking on links on cluttered screens

- Don’t click on text message links from people you don’t know; or reply to people you don’t know

QUICK CYBER HYGIENES ALWAYS’S...

- Use lock screen on all devices, use a separate password manager, and use biometric sand 2-factor authentication whenever possible

- Use separate passwords for email and banking; work and personal

- Keep operating systems and apps up-to-date and set systems for automatic updates

- Be suspicious of any email that’s not “normal.” You probably don’t need whatever it wants

- Run antivirus on all desk and laptops as a minimum and don’t download apps from 3rd parties unless you know they are safe

- Make sure you have some kind of backup plan, and test it periodically to make sure it works
### SOME PERSONAL TECH RESOURCES

- **www.Malwarebytes.com**
  - Excellent “freemium” software to keep your machine clean

- **www.StopThinkConnect.org**
  - US DHS site with security resources for all ages and groups

- **https://HavelBeenPwned.com**
  - Can tell if your email related password has been stolen

- **https://go.rutgers.edu/o230c0an**
  - Crash Course (YouTube) video series on “Navigating Digital Information”

### AND FOR YOUR ORGANIZATION...

- **www.gmis.org**
  - Professional association of public sector IT managers

- **www.cyber.nj.gov**
  - US Cyber Communications and Integration Cell and MS-ISAC, the free federal/state/local IT security support group

- **OUCH Newsletter** (search for it)
  - SANS Institute free monthly employee cybersecurity newsletter and Security Awareness Tip of the Day

### BEST TECH PRODUCT RESOURCE/REVIEW SITES: WWW.

- pcmag.com
- thewirecutter.com
- tomguide.com
- theverge.com/reviews
- cnet.com/reviews/

### AT-HOME BACKUP CHALLENGE

- Cloud backup backs up files constantly, and can do system back-ups
- Local storage needs an external hard drive and good software
- Phones and tablets: sync to a home computer, or enable online/cloud backups (may have small cost)
SAMPLE ONLINE BACKUP SERVICES

- Acronis
- Backblaze
- iDrive
- Carbonite
- Mozy
- For data files/images only: Microsoft Live and Google Drive

FOR FURTHER DISCUSSION & COMMENTS

More Information
- Technology Risk Management Papers
- Find them online with a web search for “Bloustein Technology Risk”

Marc Pfeiffer
Assistant Director
Bloustein Local Government Research Center
Rutgers University
Marc.Pfeiffer@rutgers.edu

Marc.Pfeiffer@rutgers.edu

© 2019 Bloustein Local Government Research Center, Rutgers University