TECHNOLOGY LEADERSHIP BASICS

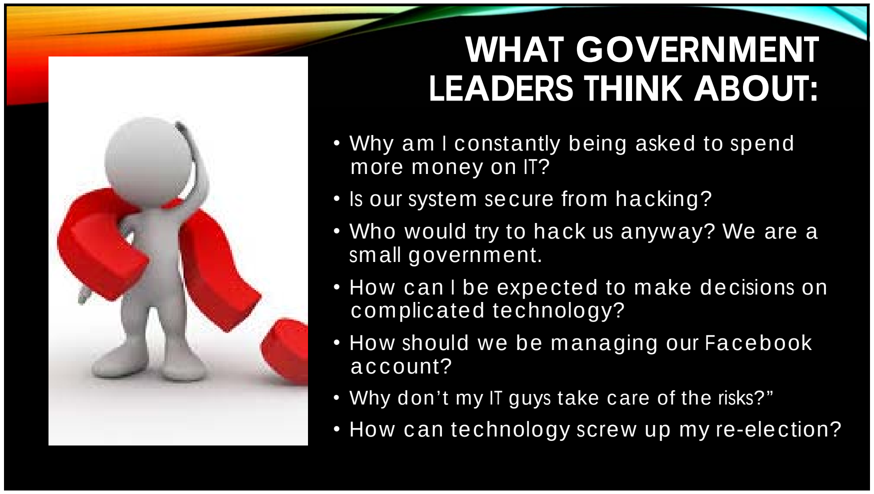
for
Government Policy Makers and Managers

Marc Pfeiffer
Assistant Director

Bloustein Local Government Research Center

Rutgers University

1



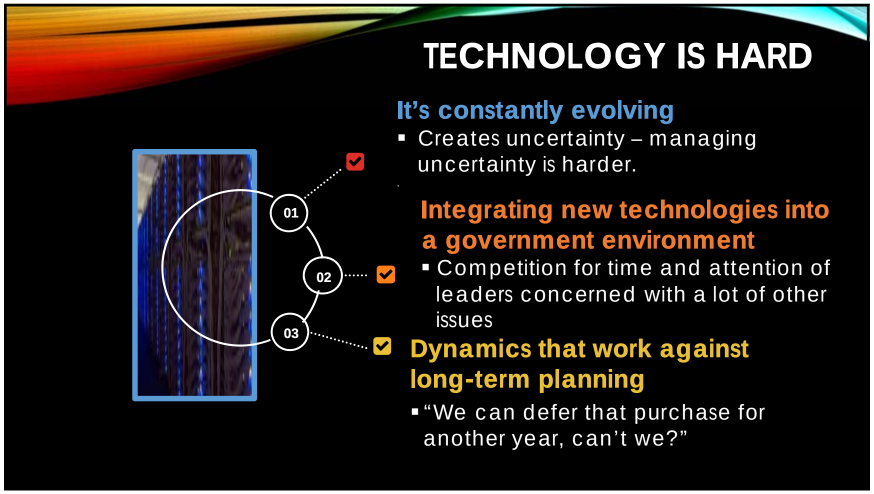
WHAT GOVERNMENT LEADERS THINK ABOUT:

- 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?

2

PART 1: TECHNOLOGY IS EVERYWHERE! THAT MEANS SOMETHING

3



TECHNOLOGY IS HARD

It's constantly evolving

- Creates uncertainty – managing uncertainty is harder.

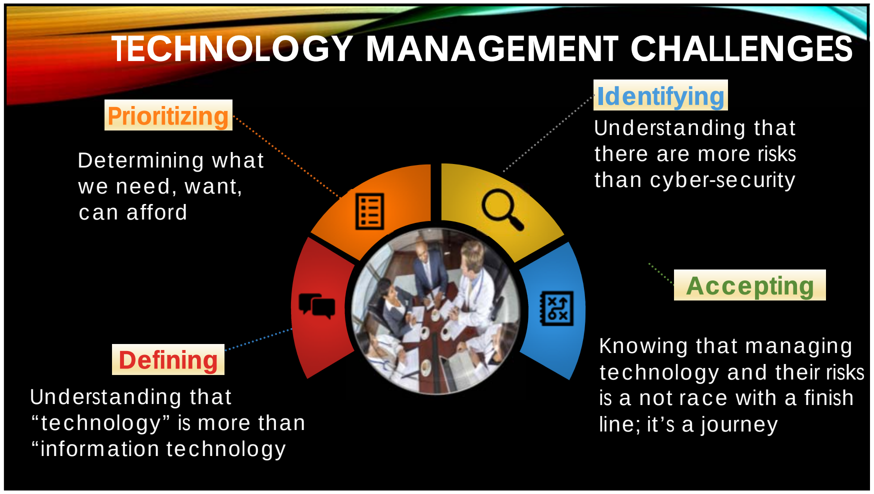
Integrating new technologies into a government environment

- Competition for time and attention of leaders concerned with a lot of other issues

Dynamics that work against long-term planning

- "We can defer that purchase for another year, can't we?"

4



TECHNOLOGY MANAGEMENT CHALLENGES

Prioritizing

Determining what we need, want, can afford

Identifying

Understanding that there are more risks than cyber-security

Accepting

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

Defining

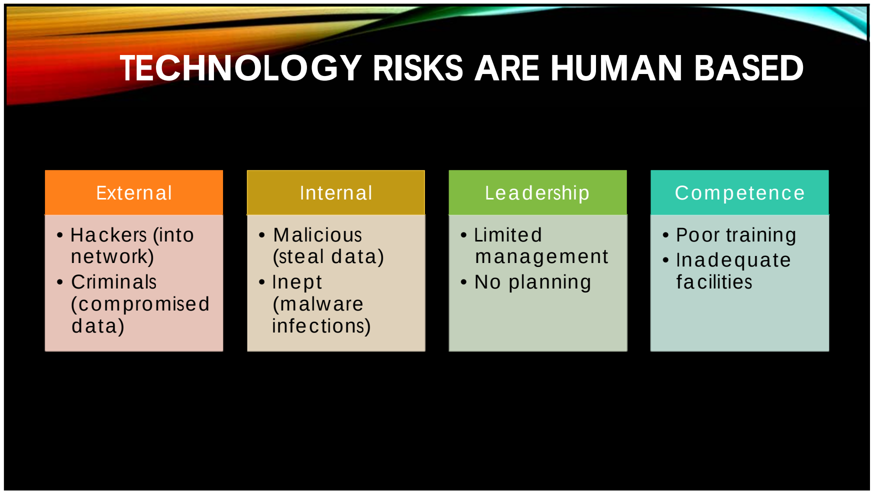
Understanding that "technology" is more than "information technology

5

TECHNOLOGY IS RISKY BUSINESS

What's it to you?

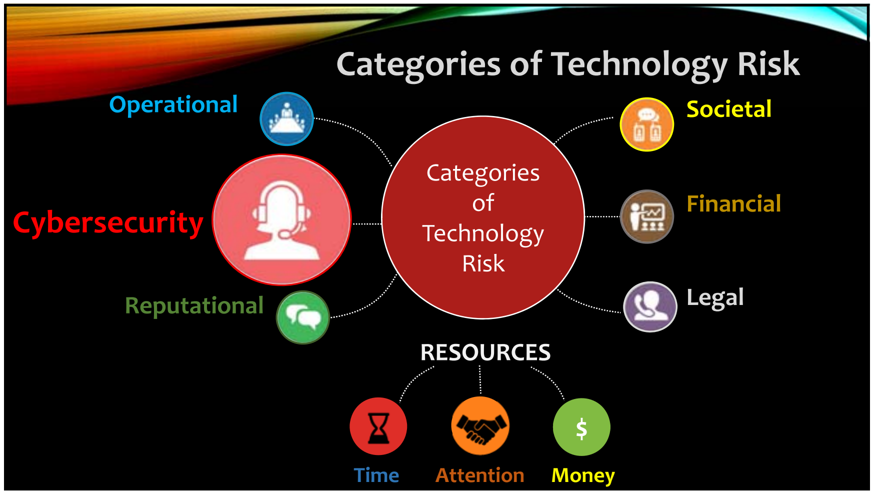
6



TECHNOLOGY RISKS ARE HUMAN BASED

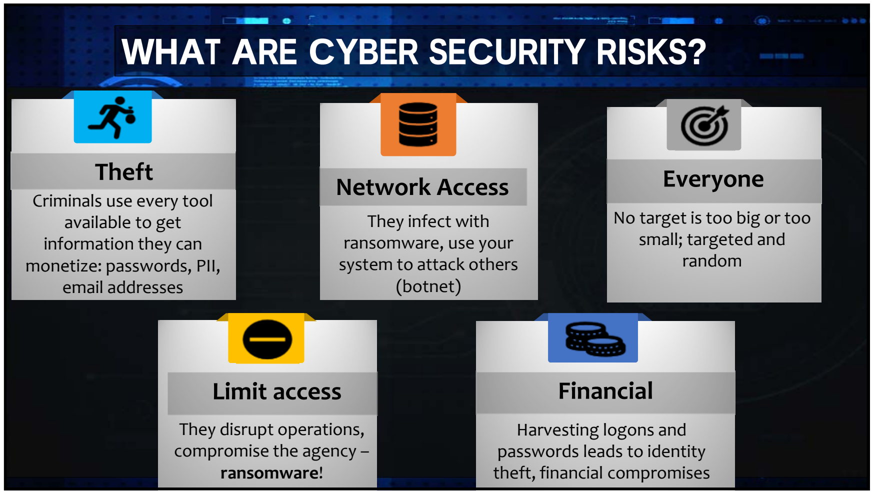
External	Internal	Leadership	Competence
• Hackers (into network) • Criminals (compromised data)	• Malicious (steal data) • Inept (malware infections)	• Limited management • No planning	• Poor training • Inadequate facilities

7



Categories of Technology Risk

8



WHAT ARE CYBER SECURITY RISKS?

Theft

Criminals use every tool available to get information they can monetize: passwords, PII, email addresses

Network Access

They infect with ransomware, use your system to attack others (botnet)

Everyone

No target is too big or too small; targeted and random

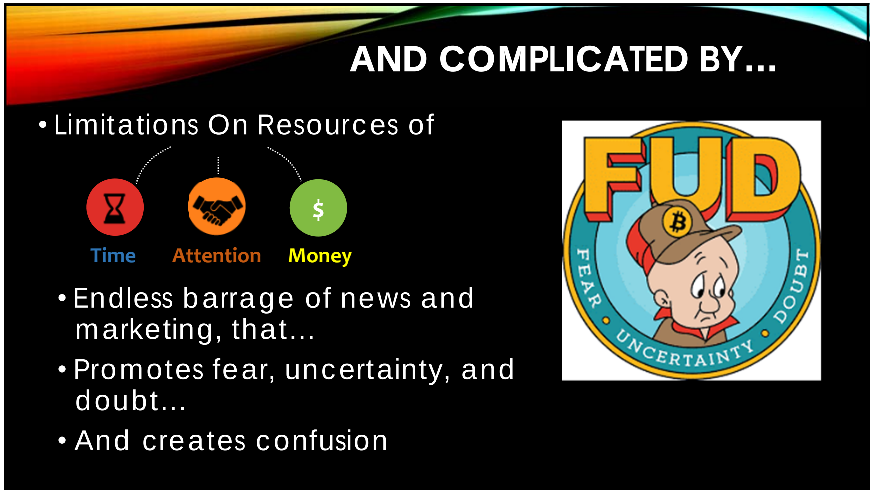
Limit access

They disrupt operations, compromise the agency – **ransomware!**

Financial

Harvesting logons and passwords leads to identity theft, financial compromises

9



AND COMPLICATED BY…

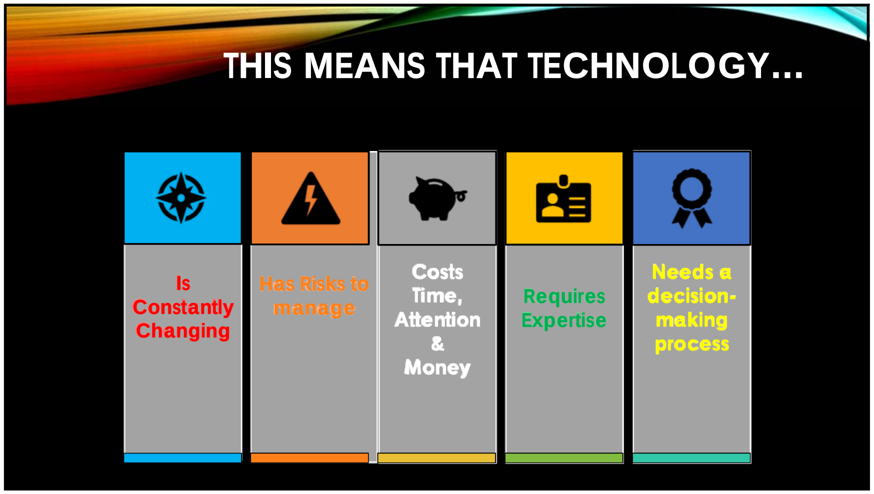
- Limitations On Resources of

Time Attention Money

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

FUD
FEAR
UNCERTAINTY
DOUBT

10



THIS MEANS THAT TECHNOLOGY…

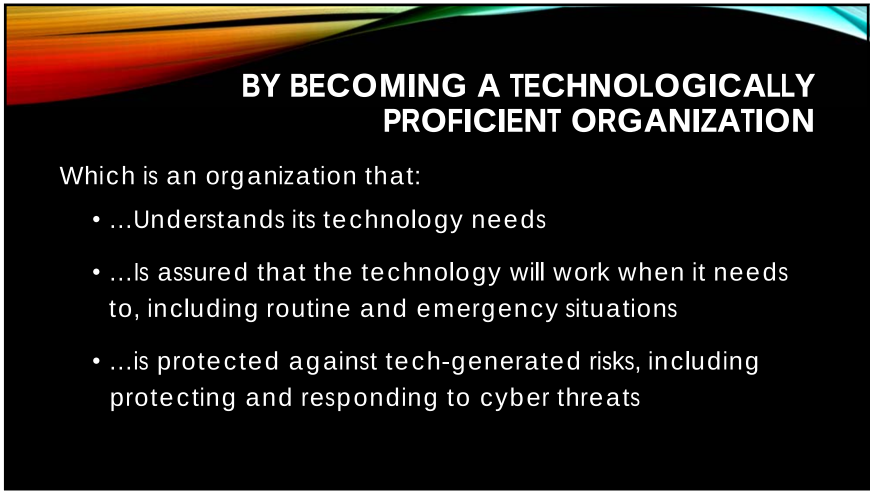
Is Constantly Changing	Has Risks to manage	Costs Time, Attention & Money	Requires Expertise	Needs a decision-making process

11

PART 2

SO HOW DO WE GO ABOUT MANAGING THIS?

12

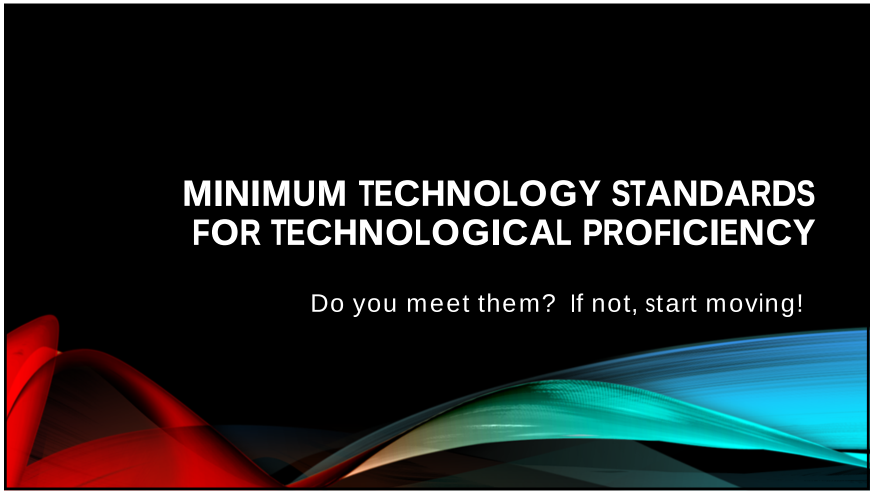


BY BECOMING A TECHNOLOGICALLY PROFICIENT ORGANIZATION

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

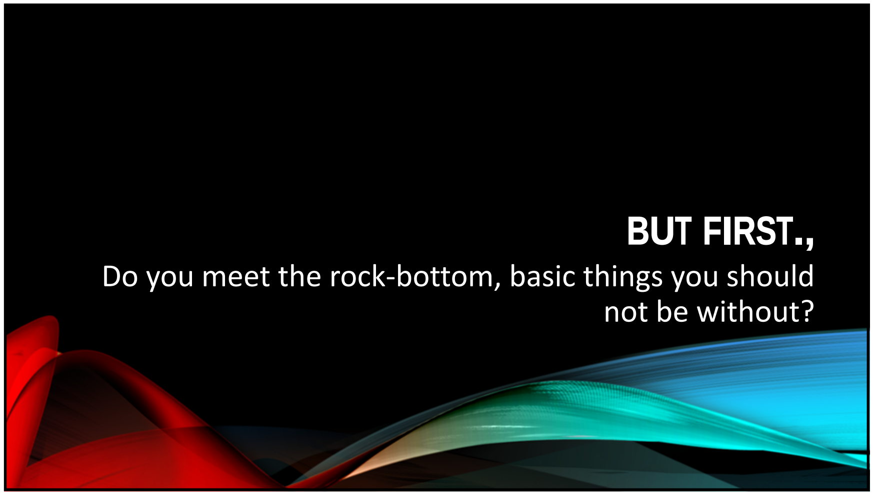
13



MINIMUM TECHNOLOGY STANDARDS FOR TECHNOLOGICAL PROFICIENCY

Do you meet them? If not, start moving!

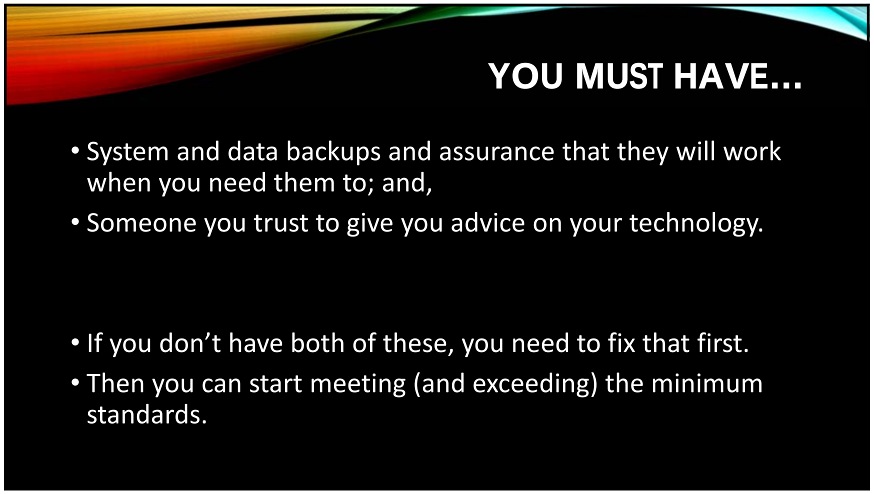
14



BUT FIRST.,

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

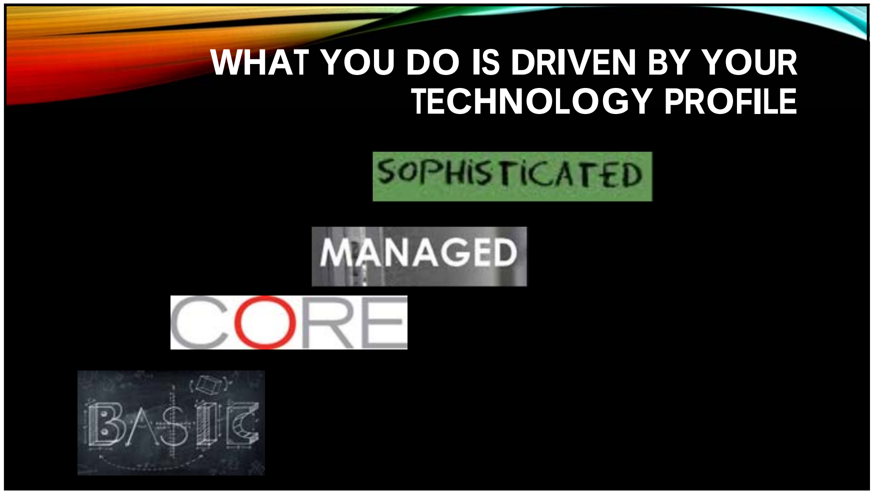
15



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.

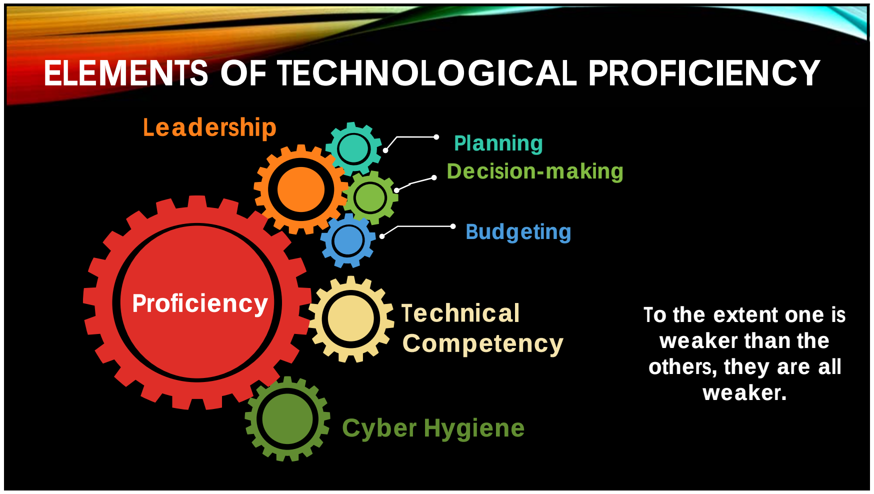
16



WHAT YOU DO IS DRIVEN BY YOUR TECHNOLOGY PROFILE

SOPHISTICATED
MANAGED
CORE
BASIC

17



ELEMENTS OF TECHNOLOGICAL PROFICIENCY

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

18

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?

19

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***

20

WHAT IS IT THAT TECHNOLOGY LEADERS DO?

What I Think I Do

What My Mom Thinks I Do

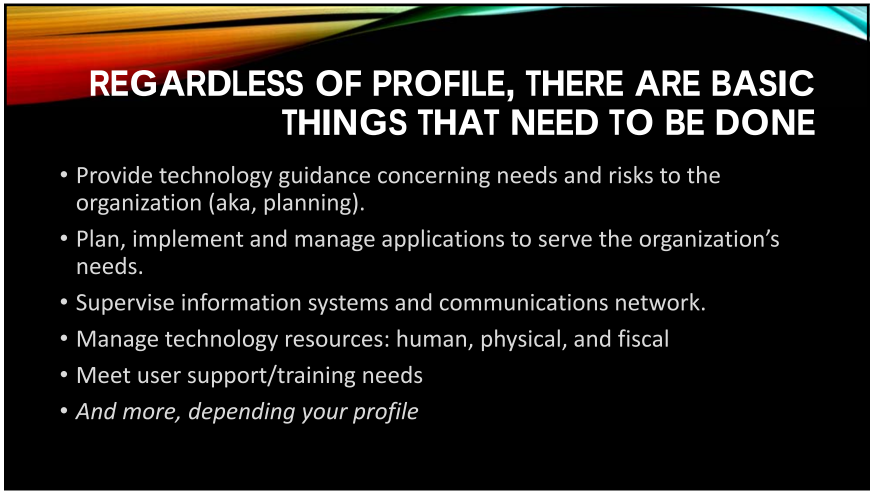
What Finance Thinks I Do

What Business Users Think I Do

What Business Users Want Me To Do

What I'm Actually Doing

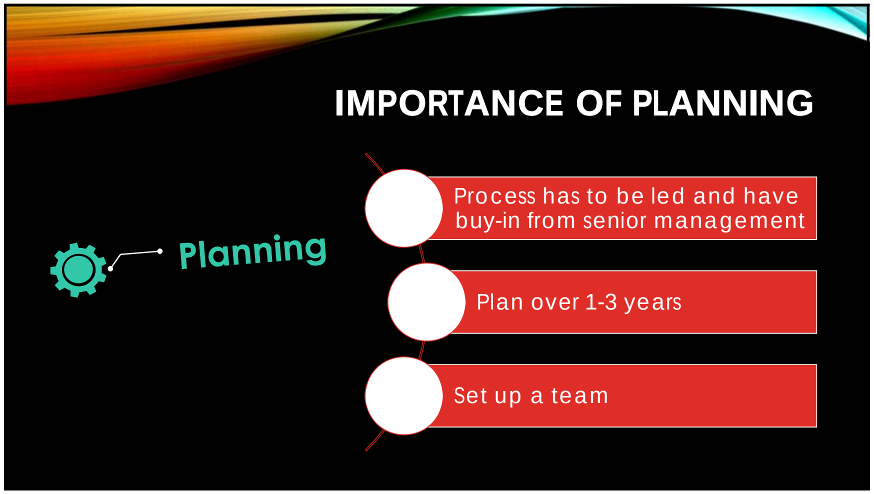
21



REGARDLESS OF PROFILE, THERE ARE BASIC THINGS THAT NEED TO BE DONE

- 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*

22



IMPORTANCE OF PLANNING

Planning

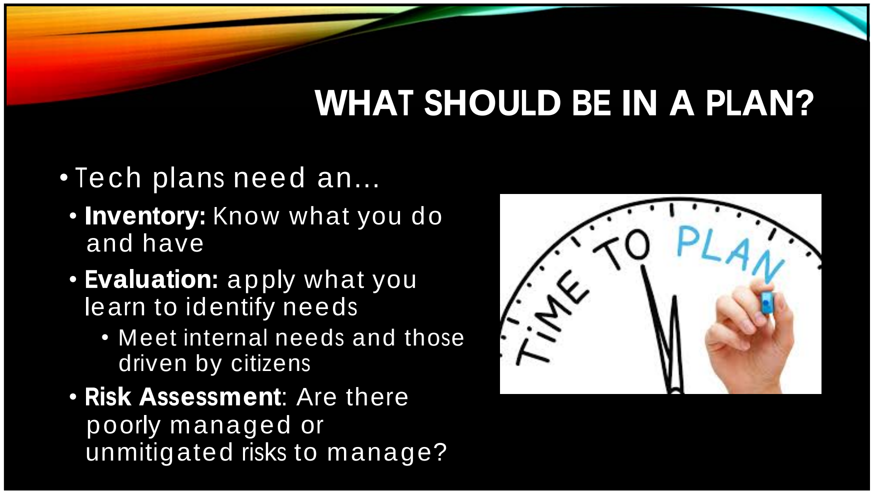
- Process has to be led and have buy-in from senior management
- Plan over 1-3 years
- Set up a team

23

THIS IS NOT A PLAN

Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!
DILBERT
By Scott Adams

24

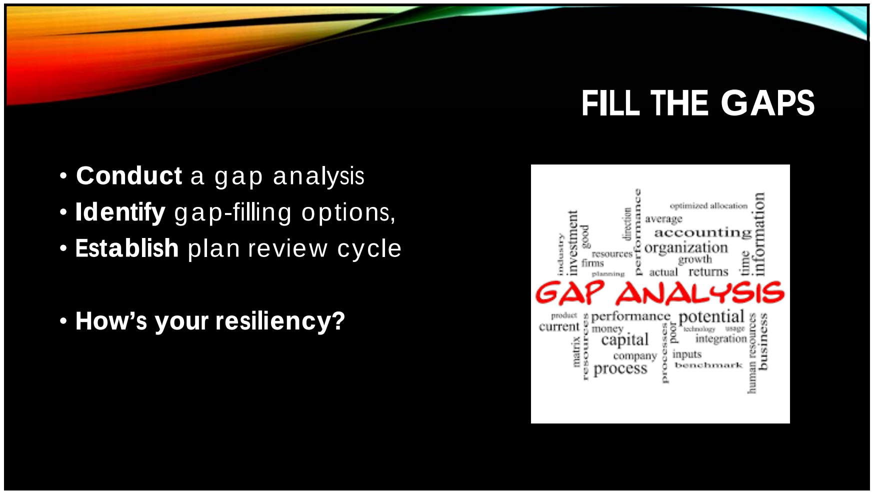


WHAT SHOULD BE IN A PLAN?

- 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?

TIME TO PLAN

25



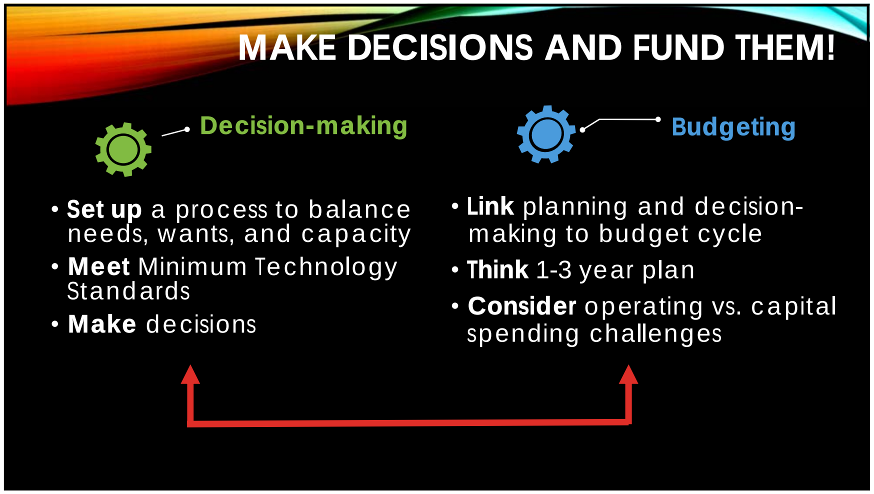
FILL THE GAPS

- **Conduct** a gap analysis
- **Identify** gap-filling options,
- **Establish** plan review cycle

- **How's your resiliency?**

GAP ANALYSIS
performance
potential
capital
process
accounting
organization
investment
information

26



MAKE DECISIONS AND FUND THEM!

Decision-making

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

Budgeting

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

27

THERE'S MORE: THE OTHER MINIMUM STANDARDS

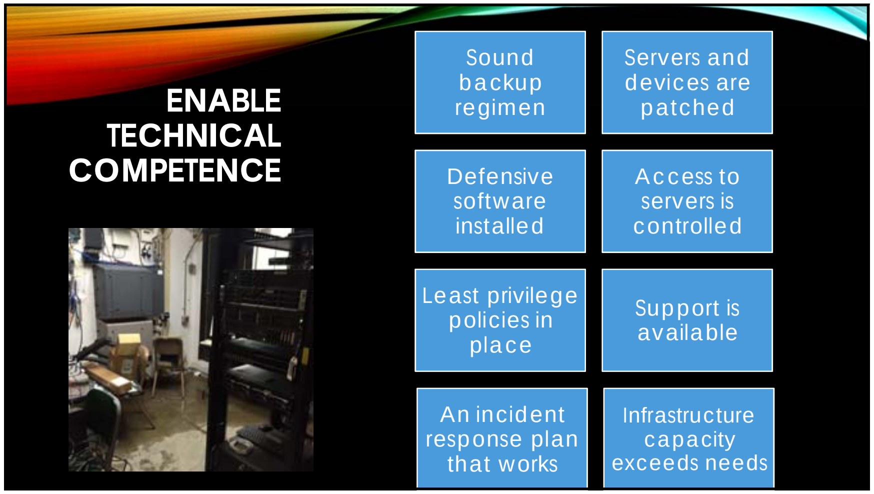
28

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!

CYBERSECURITY
starts with good
CYBER HYGIENE

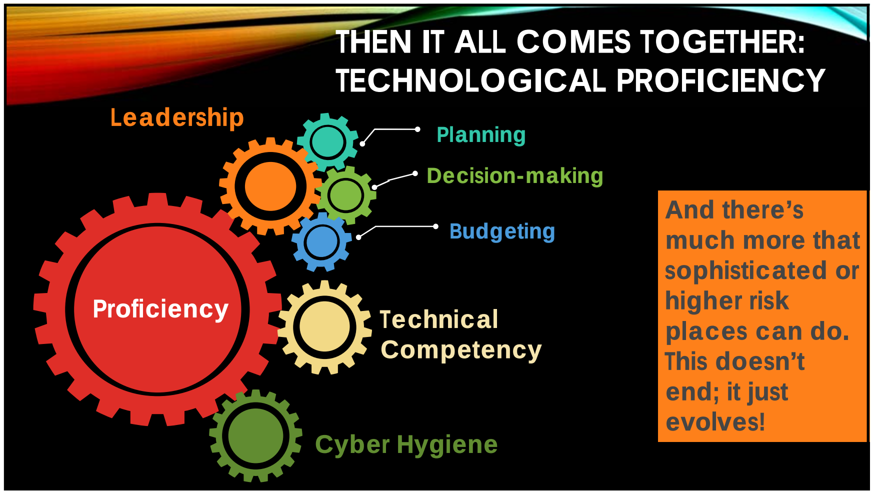
29



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

30



THEN IT ALL COMES TOGETHER: TECHNOLOGICAL PROFICIENCY

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

31

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)

32

Bloustein Local Government Research Center Products

MANAGING TECHNOLOGY RISKS THROUGH TECHNOLOGICAL PROFICIENCY

Guidance for Local Governments

SUPPLEMENT TO: MANAGING TECHNOLOGY RISKS THROUGH TECHNOLOGICAL PROFICIENCY

Guidance for Local Governments

BEST PRACTICES AND RESOURCE GUIDES

Managing Technology Risks Through Technological Proficiency: *A Leadership Summary*

Research and Guidance for Local Governments to Assess and Manage the Risks Presented by Digital Technology

Prepared by:
Bloustein Local Government Research Center
Bloustein School of Planning and Public Policy
Rutgers University
for the
New Jersey Municipal Excess Liability Joint Insurance Fund

RUTGERS
Edward J. Bloustein School of Planning and Public Policy

TECHNOLOGY RISKS IN MUNICIPAL GOVERNMENT

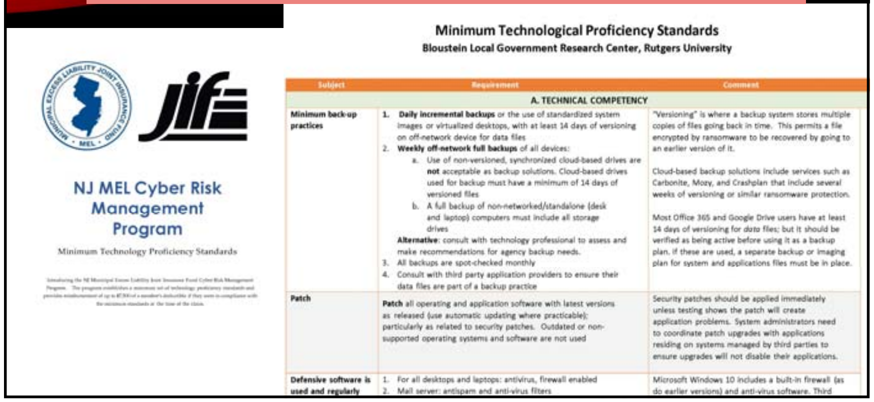
TECH CHALLENGE

KEY TECHNOLOGY OPPORTUNITIES

THE SIX TECHNOLOGY RISKS

33

N.J. Municipal Excess Liability Fund (njmel.org): Cyber Risk Management Plan



NJ MEL Cyber Risk Management Program

Minimum Technology Proficiency Standards

Minimum Technological Proficiency Standards

Bloustein Local Government Research Center, Rutgers University

Subject	Requirement	Comment
	A. TECHNICAL COMPETENCY	
Minimum back-up practices	1. **Daily incremental backups** or the use of standardized system images or virtualized desktops, with at least 14 days of versioning on off-network device for data files 2. **Weekly off-network full backups** of all devices: a. Use of non-versioned, synchronized cloud-based drives are **not** acceptable as backup solutions. Cloud-based drives used for backup must have a minimum of 14 days of versioned files b. A full backup of non-networked/standalone (desk and laptop) computers must include all storage drives **Alternative**: consult with technology professional to assess and make recommendations for agency backup needs. 3. All backups are spot-checked monthly 4. Consult with third party application providers to ensure their data files are part of a backup practice	"Versioning" is where a backup system stores multiple copies of files going back in time. This permits a file encrypted by ransomware to be recovered by going to an earlier version of it. Cloud-based backup solutions include services such as Carbonite, Mozy, and Crashplan that include several weeks of versioning or similar ransomware protection. Most Office 365 and Google Drive users have at least 14 days of versioning for *data files*; but it should be verified as being active before using it as a backup plan. If these are used, a separate backup or imaging plan for system and applications files must be in place.
Patch	**Patch** all operating and application software with latest versions as released (use automatic updating where practicable); particularly as related to security patches. Outdated or non-supported operating systems and software are not used	Security patches should be applied immediately unless testing shows the patch will create application problems. System administrators need to coordinate patch upgrades with applications residing on systems managed by third parties to ensure upgrades will not disable their applications.
Defensive software is used and regularly	1. For all desktops and laptops: antivirus, firewall enabled 2. Mail server: antispam and anti-virus filters	Microsoft Windows 10 includes a built-in firewall (as do earlier versions) and anti-virus software. Third

34

QUICK PERSONAL CYBER HYGIENE DON'TS

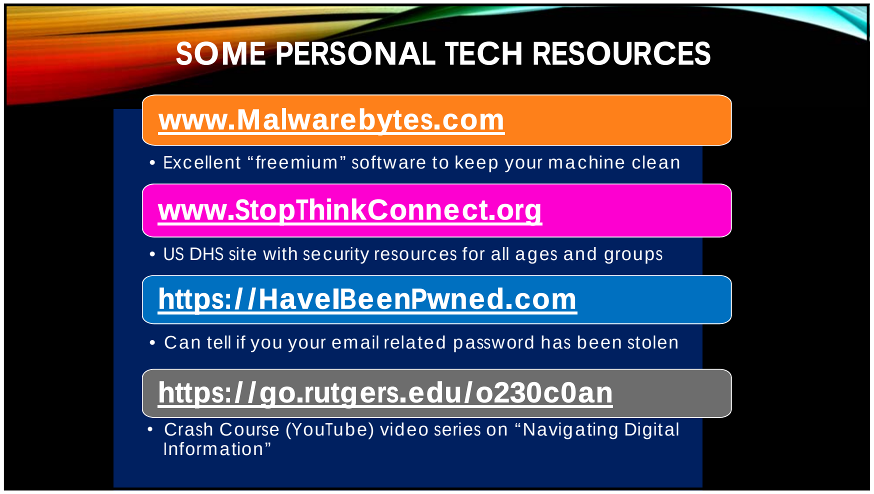
- **Don't** click on links in email that is offering you something, or making you worried or concerned about an account you have; **Do:** Go to the website of the company separately and check your account.
- **Don't** open attachments from people you don't know, or were not expecting from people you 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

35

QUICK CYBER HYGIENES ALWAYS'S…

- …Use lock screen on all devices, use a separate password manager, and use biometrics and 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

36



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

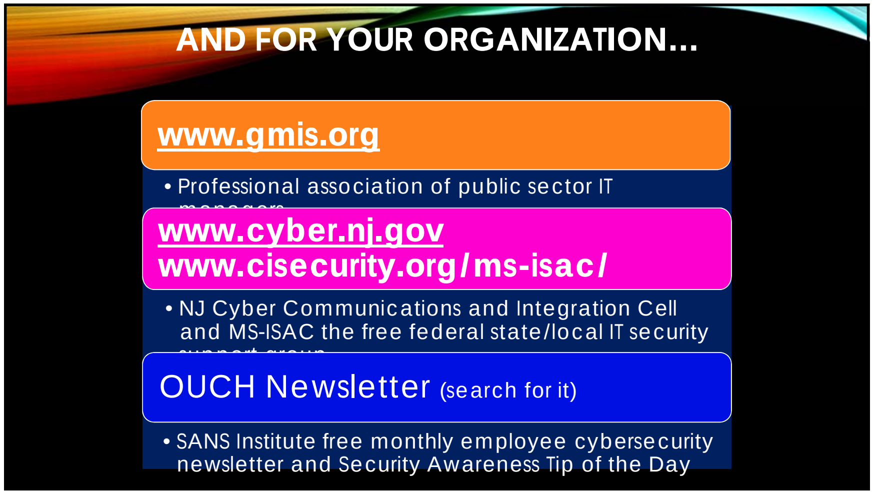
https://HaveIBeenPwned.com

- Can tell if you your email related password has been stolen

https://go.rutgers.edu/o230c0an

- Crash Course (YouTube) video series on “Navigating Digital Information”

37



AND FOR YOUR ORGANIZATION…

www.gmis.org

- Professional association of public sector IT managers

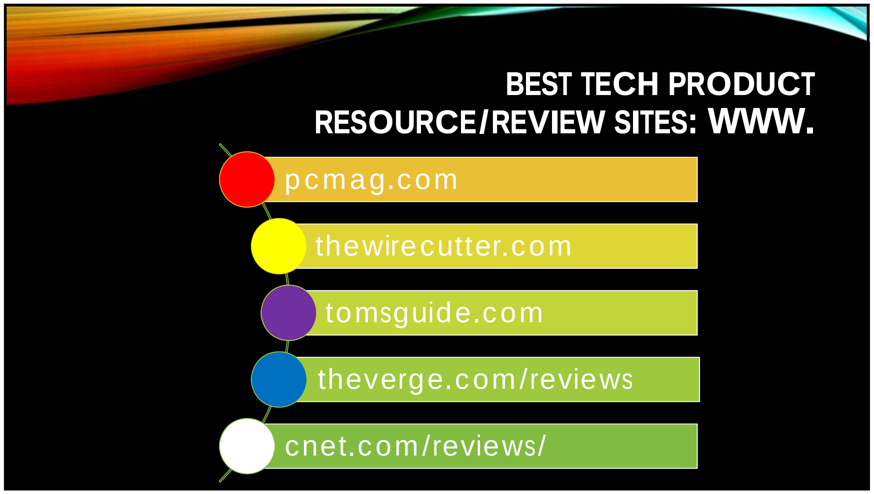
www.cyber.nj.gov
www.cisecurity.org/ms-isac/

- NJ 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

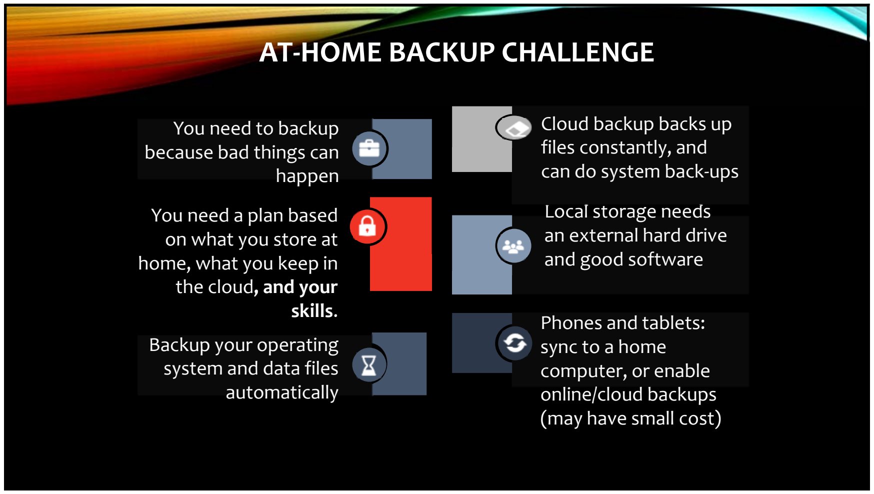
38



BEST TECH PRODUCT RESOURCE/REVIEW SITES: WWW.

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

39



AT-HOME BACKUP CHALLENGE

You need to backup because bad things can happen

You need a plan based on what you store at home, what you keep in the cloud, **and your skills.**

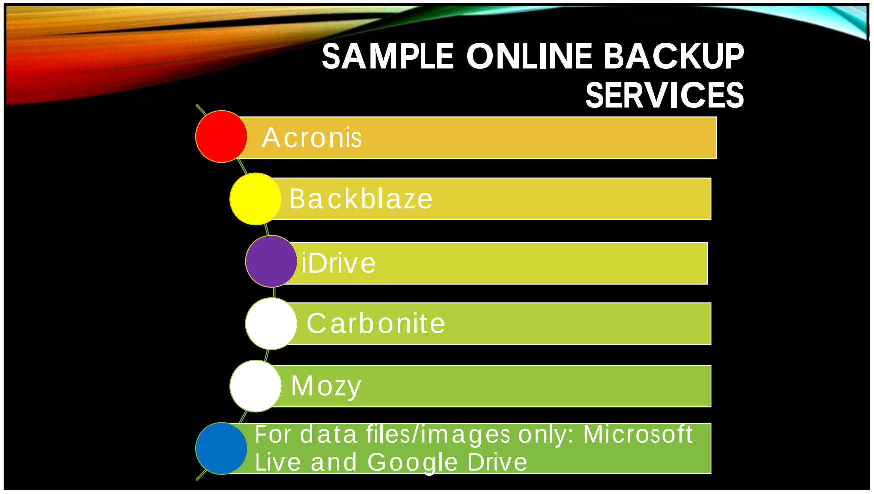
Backup your operating system and data files automatically

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)

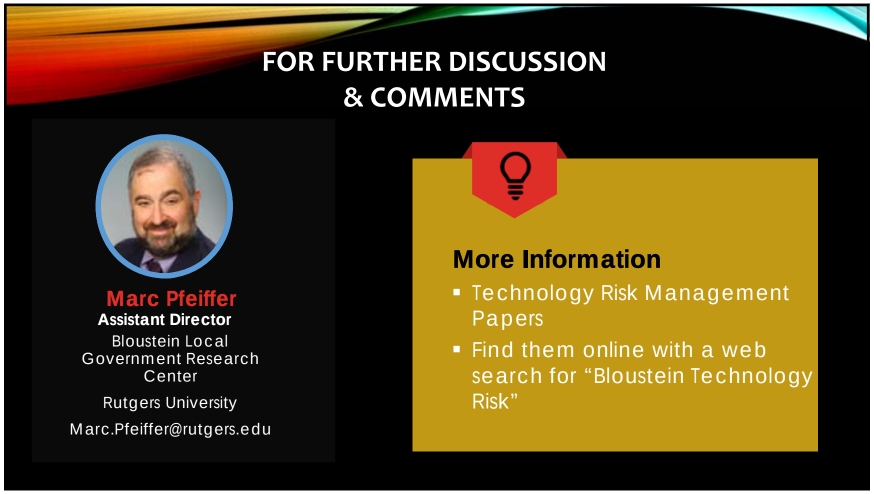
40



SAMPLE ONLINE BACKUP SERVICES

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

41



FOR FURTHER DISCUSSION & COMMENTS

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

More Information

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

42