Lock It Up

By encouraging everyone in your organization to be "technologically proficient," you can lower your risk of a cyber attack or data breach

By Marc Pfeiffer, Assistant Director, Bloustein Local Government Research Center; Senior Advisor, NJ-GMIS

All government organizations face technology risks; some more than others. Generally speaking, risks are problems that individuals cause either by taking, or not taking action in a given situation. They can come from people inside or outside of your organization. The actions can be inadvertent (usually by insiders) or deliberate (by insiders or outsiders); they can also be caused by inaction (generally by insiders).

Technology risks are also caused by elements beyond an individual's actions (though their actions can contribute). These include system and technology failures, failed internal processes and external events.

More specifically, these risks break down into several categories: cybersecurity (threats to your networked computer systems), legal (litigation and claims when your technology fails or is misused), operational (inability to deliver services because your technology isn't working), financial (costs of responding to failures), reputational (loss of public confidence and trust), and societal (failure to keep up with public expectations of your technology). The challenge is to develop procedures and policies that manage those risks.

An ongoing challenge The biggest of these risks is cybersecurity. Knowing where your data is and who has access to it is the biggest challenge in today's networked world. Keep in mind

that cybersecurity is an ongoing challenge, that will require your ongoing attention.

Simply because your organization uses the internet, you and your users are targeted and threatened by people who want to get into any system to see how they can exploit or use your system as a way to hack into other ones. The good news is that a specific local government is not usually targeted for attack. That said, a disgruntled citizen or hacker could target your systems or you personally if something goes wrong. For example, local officials in Ferguson, Missouri had their personal information disclosed online following the shooting last year.

The bottom line when it comes to computer security is this: bad guys are constantly trying to manipulate people into divulging personal or business information; they trick users in order to defraud them. When data is divulged, it is known as a data breach.

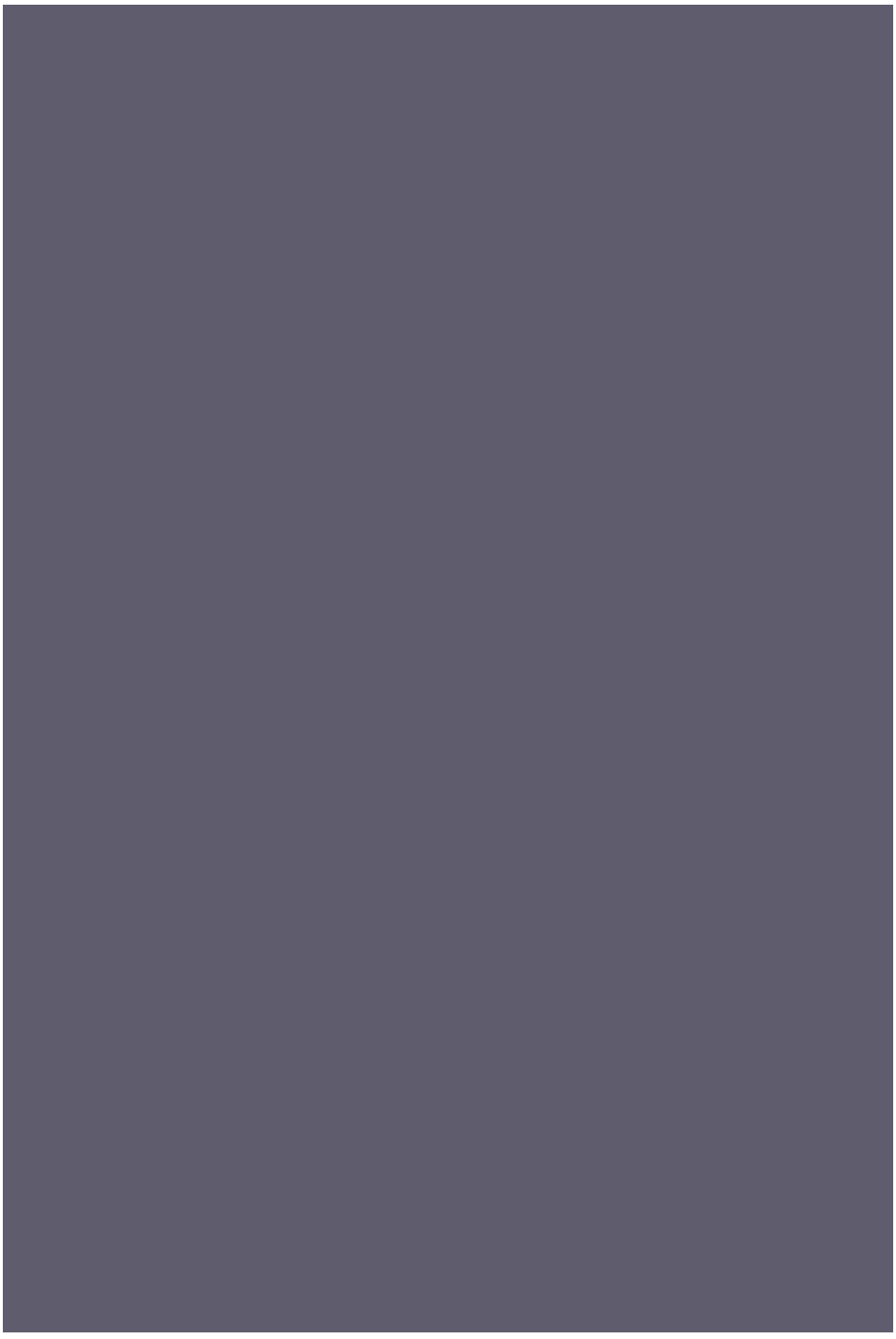
In the world of cyber security the maxim is: "it's not a matter of if you will have a breach; it's a matter of when."

Knowing where your data is and who has access to it is the biggest challenge in today's networked world.

Types of data breaches Keeping that in mind, there are four types of data breaches. The first are those that are deflected by your protection technologies (that's good). The second are those that get through your technologies, but are picked up by actively managing your network activities (which needs to be done). The third are the ones that are successful. They result in a data breach or compromised activities that may then hit the media; these are the ones you read about almost every week. Fourth, are those that get through, but you don't catch them. These active breaches either currently compromise your systems or will at some future point; these are the most dangerous.

The ongoing nature of these threats makes cybersecurity a never-ending battle against changing adversaries with evolving techniques. However, there are steps you can take. Agencies can adopt policies and practices that improve their security. You can protect your data by effectively using cybersecurity information and developing greater expertise in protection and resilience.

Research-based lists Technologists like lists. Accompanying this article are two lists that almost every organization can use. The first lists the responsibilities of "humans;" what people need know to be cyber-safe at work and personally.



The second is a list of standards that should be implemented by the technology specialists in your organization. They are responsible for keeping your systems and humans safe. Organizations have to do both, and do them in a way that is consistent with the technology the organization uses. Municipal leaders should review these lists and implement their recommendations.

These lists are based on research done by the Bloustein Local Government Research Center and underwritten by the Municipal Excess Liability Joint Insurance Fund. The project was commissioned to study how government organizations can minimize their technology risks. A full report on this research will be published soon.

The study concludes that these risks can be managed by being "technologically proficient." This involves implementing technology governance practices, having a technology planning process tied to the budget, and making sure all computer users act securely and competently. Bloustein Local Government Research Center and the MEL will make the report available to all government agencies.

Join NJ-GMIS One way in which government agencies can help manage their technology is to make sure that their technology specialists are up-to-date in their field. They can support them by joining NJ-GMIS, the state's association of local government technology leaders. NJ-GMIS is also the League's technology resource organization. Information on joining the association and registering for TEC events is online at www.njgmis.org.

Basic Practices of Secure Humans

- Only use business-related websites
- Check with the sender if they are not expecting an attachment to an email
- Cooperate with IT's instructions regarding security patches
- Never open suspicious attachments or unexpected emails
- Never install hardware or software without IT's approval
- Never download any programs without IT's approval
- Never use a USB drive from an uncertain source
- Understand and apply your organization's technology policies
- Use strong passwords. Such passwords:
  - use a phrase relevant to the user;
  - contain at least eight characters and a minimum of two numbers;
  - are never written down or divulged; and,
  - are changed every 30 to 90 days.

Minimum Technical Actions for Secure IT Systems

- Run and maintain anti-virus, firewalls, anti-spam, anti-malware software on all desktops and laptops.
- Backup! Store data on and off site as appropriate.
- Restrict user installation of applications Use only approved "whitelist" applications.
- Ensure that operating systems and applications are patched with current updates.
- Restrict administrative privileges and regularly review them.
- Protect online financial transactions: dedicate a computer to make financial transactions that prohibits email and general web browsing.
- Require a strong password/phrase, and force periodic changes.
- Join MS-ISAC, the free cybersecurity clearinghouse for local government agencies (www.msisac.org). There is no reason not to join MS-ISAC; they are an invaluable resource.