Published on *MTAS* (http://www.mtas.tennessee.edu) July 05, 2020

Online Data Backup

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Online Data Backup

Reference Number: MTAS-1775

As we have come to rely on electronic files being ever present on our computers, backing up these files is more important than ever. The target audience for this tip is cities that have a small number of computers, and do not use a central server system for file storage. For cities with a central file storage system, I would encourage you to discuss the current backup plan with your IT department or vendor. Everyone else should keep reading!

Having a backup plan in place is important because the majority of data is stored in a single location, which is generally on the hard drive of a single computer. Hard drive capacity and reliability have steadily increased over the years, but the hard drive is still the most likely piece of hardware in your computer to fail (one to four percent average failure, based on various sources). Other causes of lost data could include a PC being lost, stolen or compromised, software or file corruption, a Ransomware/ Encryption virus or natural disaster, etc. Any of these scenarios could cause you to lose access to your data. If you have data that you cannot replace, is critical to your operation, or would be very time intensive to rebuild, then keeping that data in one place could be catastrophic.

Think about the above data and or documents that you are responsible for and that are necessary for you to complete your job or tasks. This could be data related to a million dollar federal grant, and you must keep this data in order to report on how the grant money is being used or you risk losing the grant. It could be the minutes from a controversial city council meeting pertaining to purchasing contracts for a vendor that will most likely be challenged by the bidders that didn't win the bid. Whatever the data, it only resides on a single few bits within your hard drive.

Imagine the following scenario.

> You come in one day and you receive and email PDF invoice from someone you recognize. You open this email to learn that it is the invoice is for another company. You reply to the email to let them know they sent you someone else's invoice. You open a file before you leave for the day, but the file will not open. It is the end of the day and you decide to lock your computer and head home. The following day you come in, turn on your computer, realizing you are not able to open any of your electronic files. When you open a file it only shows you electronic gibberish. Next, you open your email to find an email from someone you do not recognize but the subject line says that it is important. As you read this email you realize the email is from a hacker. This hacker has encrypted all your electronic data and is holding the encryption keys and the data hostage for a ransom payment of $50,000.

You were the keeper of this data and the burden for its loss is on your shoulders. You have no possible way to recreate this data. Some of the data may exist in hard copy form, or it might be possible to hire a company that specializes in data repair or recovery, but this could be very expensive and or time intensive. The rasomware scenario the only way to retrieve the data is to get the encryption keys. Sometimes if the hacker is paid you will get the keys but sometimes you will not. The most practical way to protect your data is with a backup.

I recommend keeping your data in a minimum of two places, but in some cases using three might be desired.

- Local computer hard drive
- Local alternate media (external hard drive or USB flash memory) - optional
- Cloud storage or Cloud based backup solution

The first location is your hard drive, which is the most convenient and fastest place to access your data. Because the hard drive is usually the default storage location for the computer, it is the most popular. Continuing to use the hard drive as your primary data storage location is acceptable, but just be aware of the potential risk.

The second location can be a USB thumb drive or external hard drive. This location can be your quick go-to for recovery, as well as a portable option. This location is optional and does have some benefits over the third location such as portability, quick access, availability without Internet access, etc. However, if you also add the third location then keeping up with your files in all three locations could

become cumbersome, and add unneeded or unjustified complexity to the process. If you have a slow or unreliable Internet connection, this optional location may be necessary. However, if you prefer to use only two locations, then eliminate this one and use option three as the secondary location.

The third location is a cloud-based backup or storage solution. Some cloud-based services could be your primary data storage location, depending on the speed and reliability of your Internet connection and the types of data you are storing. If you are storing Personally Identifiable Data for citizens or customers, you will need to be more cautious with the system that you choose (encryption, security, etc.). Your options for this service vary in features, design, ease of use, and cost. The selection and use of one of these services is outside the scope of this article, but I have included a brief overview and a list of some options. The two overall categories are: 1) backup systems whose primary design and purpose are for data backup; and 2) cloud document systems that were designed for cloud storage of your files (an online hard drive). Some of the cloud services overlap and share some of the same features.

The first category is an online/offsite backup service. If your primary goal is an automated system to back up your files from your hard drive to the cloud (set it and forget it solution) then you should consider the online backup category. Some backup services offer complete backup and restoration of the protected system. Some examples in this category include services such as Acronis [1], Carbonite [2], Crashplan for Small Business [3], Elephant Drive [4], IDrive [5], justcloud [6], myPCBackup [7], and SOS Online Backup [8]. Most of these products offer protection and automatic updating of local files to the cloud storage. Features to consider are: the restore process, cost, security/privacy, encryption, and whether you can get physical media for the restore.

The second category is an online document system of services. These services are primarily designed as an online hard drive. Some of these options include G Suite by Google Cloud for government [9], personal Google Drive accounts, Microsoft Office 365 for governments [10], Microsoft OneDrive [11], Dropbox [12], SugarSync [13], CertainSafe Digital Safety Deposit Box [14] and box [15] that offer both personal and business versions. These services are primarily designed to store your working files, such as Word, Excel, and Powerpoint. Some services store limited file types, while others allow any type of file. A few offer encryption of your data both in transit and while at rest on the cloud storage. This is a very desirable characteristic if you plan to store all your files in the cloud. Some of these services offer a client that you install to make using the service and accessing the files quicker and easier. Various services keep a copy both locally, and in the cloud and keep those files synchronized in all the locations where you use the client. Other services offer a client for smartphones and tablets, as well, so you can access your files from many locations.

In closing, you need to choose a plan that works best for your city. Remember, if your data exists in only a single location and something happens to that data, or if you are not able to access that location, then your data is vulnerable to loss. Take time now to do something about it!

Links:
[1] https://www.acronis.com/en-us/business/backup/
[2] http://www.carbonite.com/
[3] https://www.crashplan.com/en-us/business/resources/
[4] http://home.elephantdrive.com/
[5] https://www.idrive.com/small-business
[6] http://www.justcloud.com/
[7] http://www.mypcbackup.com/
[8] https://www.sosonlinebackup.com/
[9] https://www.google.com/enterprise/apps/government/
[10] https://enterprise.microsoft.com/en-us/industries/government/state-and-local/
[11] https://onedrive.live.com/about/en-us/
[12] https://www.dropbox.com/
[13] https://www.sugarsync.com/
[14] https://certainsafe.com/digital-safety-deposit-box/
[15] https://www.box.com/