ISSUE
01
September
2019

MONTHLY
TECH TIPS

TechTalk

this issue

Hurricane Dorian P.1

Preparing for a Hurricane P.2

The 3-2-1 Rule of Backups P.3

The Benefits of a Clean Desk Policy.

A clean desk policy can be an important tool to ensure that all sensitive/confidential materials are removed from an end user workspace and locked away when an employee leaves their workstation.

It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace.

Such a policy can also increase employee's awareness about protecting sensitive information.

A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

How Hurricane Dorian Benefited IT Departments

Hurricane Dorian kept us on the edge of our seats for quite a long time. We were fortunate that the storm did not cause significant damage to Florida and can take away a few lessons.

The primary lesson to be taught is that a data recovery plan must be put into place and tested prior to the formation of a storm. As Dorian approached, some organizations scrambled to get systems backed up onto cloud-based solutions. The issue with this procedure is that it takes days to upload some file servers due to the massive amount of data. If the initial backup has not been started a week prior to a storm affecting services, power disruptions can cause the backup to fail.

We kept close tabs on the storm for our clients using ventusky.com and were fortunate to not have to interrupt services!

Setup Alerts for Backup Jobs
One of the most heartbreaking moments is when someone goes to restore their files and finds that the backup jobs have been failing for months. Setup automated alerts to notify multiple staff members if a backup fails.

Test Restore of Files Monthly
An equally heartbreaking moments is when someone goes to restore their data and finds that the data is corrupt or that the backup solution has been falsely reporting successful backups. It is for this reason that backups **MUST** be tested regularly.

Last Step - Unplug Everything
Ensure backups are offsite before the storm and that all servers, routers, firewalls, switches, and workstations that are critical to your organization are unplugged from power and external network connections.

Advanced Systems Solutions Inc.

Office 365 and Google Drive are Not Backup Solution!

Many people think that their use of Microsoft OneDrive in their Office 365 account is a backup of their data. Google users feel the same way. The issue is that it is merely a copy of your data and are susceptible to infection or deletion.

WE SUGGEST VEEAM

When it comes to a proven cloud-based backup solution, we suggest Veeam.

Veeam is not only a solid solution for backing up your onsite data, their ability to backup cloud solutions makes them a great choice to ensure your data is protected.

Should you accidentally delete files or experience a data infection, Veeam can easily restore your data from the most recent backup whereas Microsoft or Google take much longer.

We have had clients that have had to restore from backup using Microsoft and Google. The request must be escalated and takes days before the data is restored.

How to Prepare Your Computers for a Hurricane.

Unless your business has a safe room, you may want to take some extra precautions for your computers when preparing for a Hurricane.

Most importantly, protection for humans and pets should always take priority over computer equipment and software when preparing for a storm. Once personal safety is ensured before the storm is arrives, efforts should be made to protect computer equipment and software information.

Here are some guidelines that we believe you will find useful:

1. Back up your data and keep a copy in a safe place. Follow the 3-2-1 Rule!

2. Shut down your computer and turn off your monitor. You should also turn off any peripherals, such as printers and external drives.

3.. Unplugging everything from the wall will help ensure the devices will be protected. Storms can cause power fluctuations can have extremely serious consequences for any equipment left plugged in or turned on.

4. Unplug the network cable going to your router and computer, as well as your printer for networked printers. Lightning can send voltage through these lines, damaging the network cards. Again, even if there is grounding protection in place, it is still a good protective measure to take.

"PLAN FOR THE WORST, AND HOPE FOR THE BEST"

5. Cover your computer with a garbage bag in case water comes in*.
*NOTE: Be sure to unplug the power from the devices before doing so. This will ensure that the computer does not overheat when power is restored.

6. The major cause of damage to computer hardware and software will be from water. Broken doors and windows would bring rain and debris. Select a protected location and try to determine what would occur if a window broke. By moving computer equipment (i.e. monitors, CPUs, printers, keyboards) to protected locations and wrapping them with plastic, the chances of damage will be greatly reduced. Double wrap equipment in plastic garbage bags to reduce rain/water damage. Keep in mind that a collapsing ceiling or roof can damage your equipment so place equipment under a sturdy desk or piece of furniture that could possibly withstand the effects of falling debris. If equipment is to be located directly on the floor, take into consideration the possible effects of flooding. Placing equipment on or in water resistant objects such as totes or garbage cans may be helpful.

7. Collect your manuals and original disks. After Hurricane Andrew, there were stories of software vendors who were reluctant or refused to replace software without the original disk, manuals, or some other form of ownership being presented.

The 3-2-1 Rule of Data Backups

There are two groups of people in this world: those who have already had a storage failure and those who will have one in the future. In other words, the 3-2-1 backup rule means that you should:

Have at least three copies of your data.

Store the copies on two different media.

Keep one backup copy offsite.

Let's consider these statements one by one in more detail.

Have at least three copies of data:

In addition to your primary data, you should also have at least two more backups.

Store the copies on different media:

Keep copies of your data on at least two different storage types, e.g. hard disk drives AND removable media.

Keep one backup copy offsite:

You never know when disaster will strike, so physical separation between copies is important.

Storing your backups to the cloud might also be an option. Companies of all sizes still use the practice of an off-site tape storage rotation schedule.

This Month's Q&A Technology Tips

Q: Dale from Daytona asks, "How long should I expect a Hard Drive to last?"

A: Unless they are sitting powered off on a shelf, hard drives fail 100% of the time. That's right, traditional hard drives fail 100% of the time. The question is when will yours fail; will it be one year? Three years? Hopefully 8-10 years?

Backblaze, a pioneer in cloud storage, records the reliability of different hard drives from different suppliers.
This is important to them because they own over 30,000 drives so it matters which ones last longer. Backblaze reports that you're pretty safe the first year, with only a 5.1% failure rate, but cut to three years later and you will find that a whopping 20% of drives have failed. Only 50% will make it to year six.

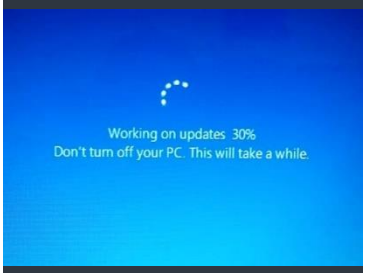
SSD Hard Drives have no moving parts and a much lower failure rate but are more expensive.

EYE ON IT

Current Industry Trends

The most recent tread that we are seeing that has us concerned is the proliferation of Ransomware as a Service. This subscription-based model enables even the most novice cybercriminal to launch ransomware attacks without much difficulty.

Cybercriminals write ransomware code and sell/rent it under an affiliate program to other cybercriminals who have the intent to launch an attack. They provide technical know-how and step-by-step information on how to launch a ransomware attack using the service, a platform which may even display the status of the attack using a real-time dashboard. Once the attack is successful, the ransom money is divided between the service provider, coder and attacker.



September Patching

We're not hearing of any pains after two days so now is the time to apply your Windows updates. 80 security holes are addresses in yesterday's update.

A “critical” rating has been assigned to almost a quarter of the vulnerabilities, meaning they could be used to hijack vulnerable systems with little or no interaction on the part of the user.

Upcoming Events

- **The Orlando Power Lunch**

  Advanced Systems Solutions is proud to sponsor the Orlando Power Lunch. This luncheon is composed of professionals that are looking to expand their network with other professionals in the Orlando area. https://orlandopowerlunch.com/

- **The T^2 Tech Talk Podcast**

  You won’t want to miss a single episode of the T2 Tech Talk Podcast! We know tech and marketing can be daunting, but we break it down into bite sized chunks. https://www.t2techtalkpodcast.com/

- **Enterprise Connect**

  Registration is now open for Enterprise Connect. This Orlando event is March 30th - April 2nd at Gaylord Palms. Come join us to see what the best options are for upgrading your communication solutions. https://www.enterpriseconnect.com/orlando/onsite

- **Microsoft Ignite**

  Registration is sold out for Microsoft Ignite November 4th - 8th at the Orange County Convention Center. Let us know if you are attending and we look forward to seeing you there! https://www.microsoft.com/en-us/ignite

Advanced Systems Solutions Inc.

1051 Winderly Place #307
Maitland, FL 32751
407-414-6626 ph
www.advancedsystemssolutions.com