Tech Watch

April 2019

Municipal Joint Insurance Fund
South Jersey Communities Securing Their Future

Partnering with the public sector to minimize their cyber liabilities

Passwords, Passwords, Passwords

We all preach about the strength, complexity of a password and changing it often, so what's wrong with that? Nothing, except that we tend to reuse a variation of the same passwords, i.e. Spring 2018, Spring 2019 and that's when we get in trouble. Not to mention that we use the same password for our banking, eBay, Amazon, Facebook, Twitter, Phone, Cable and so on.

According to Verizon's 2018 Data Breach Investigation Report, 81% of hacking-related data breaches involved either a stolen or a weak password. According to a separate analysis of 10 million stolen password by WordPress, the crack time for the average password – including professionals at Google, DropBox, and other tech companies – was just 22 seconds.

A solid password should be long (minimum 15 characters), the longer the better. So how am I supposed to remember a long password? Think of a phrase related to something you can remember, or a verse of your favorite tune.

Use a password manager, huh???

Think of a password manager as a book of all your passwords kept in a safe that only you know the combination.

Password managers store and help you generate and save strong, unique passwords which are typically encrypted. Whenever you go to a website or app, you can pull up your password manager, copy your password, paste it into the login box, and you're in. Password managers often come with browser extensions that automatically fill in your password for you.

For more information, below is a link to PC Magazine's Best Password Managers for 2019:

https://www.pcmag.com/roundup/300318/the-best-password-managers

Content

Lou Romero is the Technology Risk Services Director and Managing Partner of Secure Data Consulting Services and works with numerous Joint Insurance Funds (JIFs) and local government to help them implement a cyber loss control program and improve their overall cyber security posture.

Lou Romero
Lromero@SecureDataCS.com
(732) 690-4057

Disaster Recovery & Business Continuity

Out of about 215 municipalities I have visited over the last two years, very few have a well-documented DR/BC plan.

What's the difference between Disaster Recovery & Business Continuity?

Disaster Recovery and Business Continuity are closely related but have different scopes and objectives.

Disaster Recovery is the process of getting all important operations up and running following an outage, major crisis or cyber-attack, while ***Business Continuity*** focuses on getting the entire business back to full functionality after a crisis.

Because we rely so much on technology and computers, IT is typically at the center of most operations and is regarded mission critical.

You should be asking yourself, are all supporting hardware, software, and relevant equipment in place to resume normal operation and provide government services?

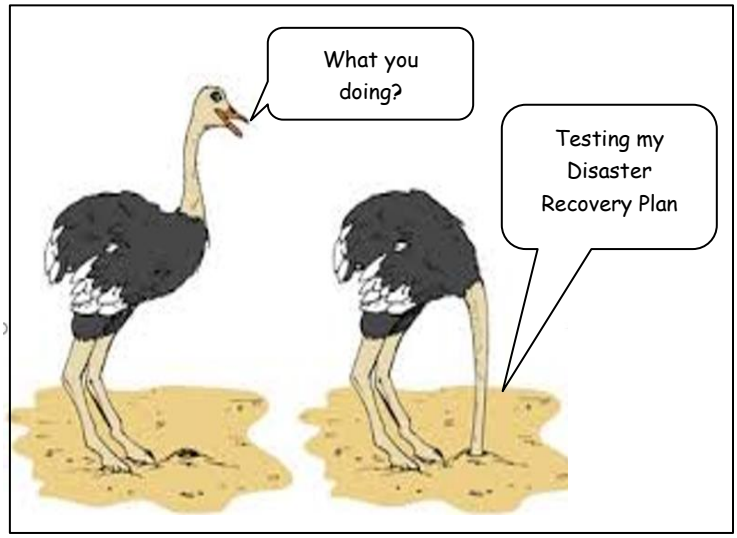
A Business Impact Analysis or BIA is key to a successful DR/BC plan.

Business Impact Analysis is an information gathering process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, emergency or cyber-attack. It identifies potential vulnerabilities and operations that directly or indirectly affect other operations and their dependencies that may cause a cascading effect.

Disaster Recovery and Business Continuity plans need to be documented and tested at least every six months.

Why so often? – because threats and vulnerabilities constantly change.

- ✓ **Who do we call?**
- ✓ **Have backups been tested?**
- ✓ **How long will it take to restore?**
- ✓ **Do we need new equipment?**
- ✓ **Where are we getting it from?**
- ✓ **How long will it take to order?**
- ✓ **How much will it cost?**
- ✓ **Where do we operate from in the mean time?**
- ✓ **Is there network capability in the temporary facility?**
- ✓ **How do we restore government services?**
- ✓ **Do we have a documented plan?**



Disaster Recovery is serious business – don't bury you head in the sand thinking it's never going to happen to you!

BACKUP

It's your life saver

With cyber-attacks on the rise, backups are your life savers and should take highest level of priority. Selecting the right backup solution is crucial and requires careful consideration. It is also important to identify the data to backup, which is where data classification and the information gathered during a Business Impact Analysis come into play.

When planning a backup solution, don't just think of the cyber-attack, but think of hardware failure, and weather or fire related disruptions.

Common Backup Options

- ***Disk to disk*** backups are not the perfect solution, simply because if your backup disk drive fails you now lost your backup data, unless you have an element of redundancy in place.
- ***Tape backup*** is relatively safe, but you need to keep in mind that tapes have a life span and will need to be replaced at some point. Also tape cartridges are typically made of plastic which can be affected by heat. If you store your tapes in a fireproof metal cabinet, make sure to check the fire rating of the cabinet. In the best scenario, tapes should be kept off-site.
- ***Cloud backup*** is becoming more popular due to its scalability and reliability. Many cloud service providers offer data encryption and 24/7 monitoring. Due to its scalability, you don't have to worry about running out of space, purchasing additional tapes or hard drives. In addition, there is no need to store your media at an offsite facility.

  When selecting a cloud service provider, make sure to do your homework.

  Some food for thought….

  - Where is the data stored? US, China ???????
  - What uptime Service Level Agreements (SLAs) are in place?
  - What are the upload & download cost?

What are your mission-critical applications and data sets?

In The News

New Jersey Cybersecurity & Communications Integration Cell

The NJCCIC has detected an increase in phishing attempts using Microsoft OneDrive and SharePoint. Attackers attempt to steal a victim's account credentials using a legitimate OneDrive login page, allowing it to bypass security protocols. A new social engineering tactic observed is that the threat actor, masquerading as a Microsoft employee, may call the victim while they are retrieving their multi-factor authentication (MFA), ask to verify the authentication code. It is important to note that Microsoft will never call to verify this code. MFA is still a highly effective protective measure and should still be utilized. The only limiting factor is the person being influenced by social engineering. The threat actor then has control over the victim's Office 365 account with the ability to view or manipulate files and send emails, continuing the phishing attack life cycle.