CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

BACKUPS AND CYBERSECURITY CHEAT SHEET

① 3-2-1 Backups

Having good, well tested backups can save your business from the majority of ransomware and hardware failures. 3-2-1- is the best strategy to use

You must:

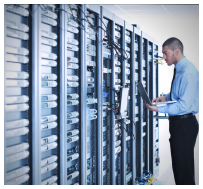
- Have at least three independent copies of your data.
- Store the copies on two different types of of media.
- Keep one backup copy offsite.

② Critical Need for Backups

It is the foundation for disaster recovery and business continuity. Technologies that were created decades ago to store data are simply not enough. Antiquated methods, like tape backup, aren't going to ensure data retention and recovery during business critical time windows.

Ensure you have a disk-based backup to allow for quick restores.

③ Choosing Backup Solution



The best backup software not only ensures that data is backed up, but provides replication and recovery and creates efficient backup processes.

- Establish goals
- Determine budget - Affordability
- Comprehensiveness
- Ease of use
- Performance and Reliability
- Scalability
- Recoverability
- Ensure usability for business continuity
- Vendor support
- End to End Protection
- Take a Test Drive

Do Your Backups Actually Work ④

Have you actually completed a full restore from your backup? We come across situations where the backup is not working correctly or not working at all, and the business manager and owner had NO IDEA this was happening..

- Low disk space
- Backup software issues
- User error
- Incorrect configurations
- Bad disks or backup tapes
- Everything stored onsite
- Inattentiveness

Are You Getting Regular Backups ⑤

Are backup logs being reviewed, with particular attention to all success/failure messages?

In many cases, notifications are sent only when a backup fails. If logs are not being closely monitored, I.T. might assume everything is backing up as it should and remain blissfully unaware that your company has NO backup system in place.

- Test backups regularly
- Restore data to ensure files are usable
- Make sure notification messages don't get sent to SPAM folders

© 2019 Craig Peterson. All Rights Reserved.

Continue reading on next page >

BACKUPS AND CYBERSECURITY CHEAT SHEET

CRAIG PETERSØN.COM

(CONTINUED)

⑥ Are You backing up Everything

When did you last evaluate your backup system? Have you added new sources of data that are currently excluded from your backup? Are you backing up any shared drives where the company saves data? Have your data assets changed priority? Any data retention compliance issues?

Consider:

- Tablets
- Smart phones
- Individual laptops
- Cloud storage
- Memory sticks
- Email inboxes and sent items
- Company contacts
- Calendars
- Files and Documents

⑦ Offsite Data Storage

It's a risky decision to store your backup data in your office. In the event of a fire or natural disaster, your data would be lost forever. It's almost mandatory to store data off-site. Remote or offsite backups allow you to store a secure copy of your data in a location other than your office. While it's good practice to use a remote backup solution, be sure you are using a good provider so you don't end up paying a lot of money only to find you can't recover your data within the amount of time you expect.

© 2019 Craig Peterson. All Rights Reserved.

How Often Are You Backing Up Data ⑧

Today's backup technologies allow for backup snapshots to be taken periodically throughout the day. If your business relies on up-to-date data, but your backups are scheduled to run once a day or even once per week, even daily backups are not sufficient for your business.

Does Your Backup Have a Backup? ⑨

Small businesses should keep an image of their entire server. This ensures you can recover from a complete system failure/ransom quickly.

And... Backups can and do fail (often)! So this simple precaution is a good idea, particularly if your data is critical to your business operations..

How Soon Can You Get Your Systems Up? ⑩

If you have a proper disaster recovery solution in place, you can recover your data in minutes. However, many business owners and managers are still unclear on how much time it will actually take to recover their system. Recovery time is based on the volume of data to be restored and the backup system you have in place.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We are not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, we make no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. We make no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH