9 KEY DIFFERENCES BETWEEN CYBER RECOVERY AND DISASTER RECOVERY

As businesses increasingly rely on technology, the risk of cyberattacks grows exponentially. Cybersecurity incidents are no longer a question of if but rather when, and organizations must prepare for the worst.

While Disaster Recovery (DR) and Cyber Recovery (CR) share similar goals of minimizing downtime and restoring data, there are nevertheless some important differences between the two.

1. IMMUTABLE BACKUPS

Immutable backups are optional for one, essential for the other, best practice for both.

Among the key differences between CR and DR is the importance attached to immutable backups. These are backups that cannot be modified or deleted, even by administrators. Immutable backups should be a critical component of your CR plans as they help ensure that backup data is tamper-proof and can be restored to its original state, minimizing the risk of data loss in the event of a cyberattack.

By contrast, DR is typically more focused on creating backups that can be restored quickly and efficiently in the event of a disaster. So, while backups are equally important to your DR strategy, it's not critical that they be immutable.

2. DETERMINING THE DATE OF RECOVERY

DR and CR differ dramatically when it comes to the ease with which you can determine the best date to recover from, aka the date of recovery or the last known good point.

In DR, the date of recovery is an obvious point in time. For example, if an earthquake takes out your data center, it's a safe bet that you'll know the exact date and time at which that happened. Cyber attacks on the other hand may have lain dormant in your environment for days, weeks, or even months, making it substantially more difficult, though not impossible, to determine the last known good point from which to restore a clean copy of your data in the CR process.

3. OFF-PREMISES OR ON-PREMISES BACKUPS – WHICH NEEDS WHAT?

Best practice DR requires a second site or some other off-site backup of your data, in case an earthquake really does put an end to your data center. With the right CR plan, however, on-premises backups can be used to speed up the restoration process. This means you can quickly restore your production site.

4. DIFFERENT PRIORITIES IN THE EVENT OF AN EMERGENCY

DR's primary concern is with recovery time objectives (RTOs) and recovery point objectives (RPOs). RTO is the maximum amount of time it takes to restore your data, while RPO is the maximum amount of data loss and downtime you can tolerate.

CR on the other hand is primarily focused on the integrity and cleanliness of the recovered data, to ensure you don't restore any ransomware packages or executables and reinfect your environment. After the health of the recovered data has been determined, that's when CR's emphasis shifts to RTOs and RPOs.

5. TESTING IS VITAL

Testing your recovery processes is vital for both DR and CR. For CR, however, it's also critical to test that you can restore from a week or even a month prior.

As far as the testing itself goes, for both DR and CR it's important to test the processes for recovering locally as well as from an off-site or cloud copy, and also to determine if you can mix and match restoration processes. By regularly and rigorously testing these processes, you can ensure that your data will be recovered efficiently and effectively.

6. 'CLEAN AND DIRTY' NETWORK PROCESS

Unlike DR which assumes the data being restored is clean, CR requires a 'clean and dirty' network process. This means having the ability to restore data into an error that is presumed bad, in order to verify cleanliness, and to run scanning and checking software before moving the data back to your production networks. This process prevents reinfection of your newly recovered environment.

7. THREAT HUNTING

Threat hunting is a critical component of CR that doesn't apply to DR. This is the process of actively searching through backups and restored systems to identify signs of a cyber attack, for example, infected servers from backup copies or restored servers. This is important because it helps you to identify the scope of the attack and to mitigate any further damage.

Most good CR plans will include proactive threat hunting to identify potential threats early on, allowing you to take steps to contain the damage and prevent further attacks. This involves proactively searching for signs of a cyber attack, even if there are no indicators of a breach. This may include searching for signs of unauthorized access, unusual network activity, and other indicators that suggest a breach may have occurred.

8. ALERTING AUTHORITIES

In CR, it's necessary to have a plan of action for alerting the authorities if certain data types have been exfiltrated as part of a cyber attack. Depending on the country and the type of data that has been compromised, you may be required by law to report data breaches to the authorities and industry governing bodies. In such instances, it's crucial to identify what data may have been stolen and then to execute on the plan that specifies to whom you need to report the breach to.

9. DIFFERENT BUT NOT DISPARATE

Finally, it's important to remember that despite the differences between CR and DR, and the many special requirements of CR, they are not standalone solutions. Instead, they should both be part of a comprehensive recovery plan that includes incident response, backups, and disaster recovery.

In conclusion, Cyber Recovery and Disaster Recovery are both critical components of any business continuity plan, but they are not interchangeable. By understanding the key differences between them, you can develop a comprehensive recovery plan that addresses your unique needs and ensures your business can recover rapidly from any event while minimizing data loss.