IT Recovery:
Practical Approach from the Eye of Disaster

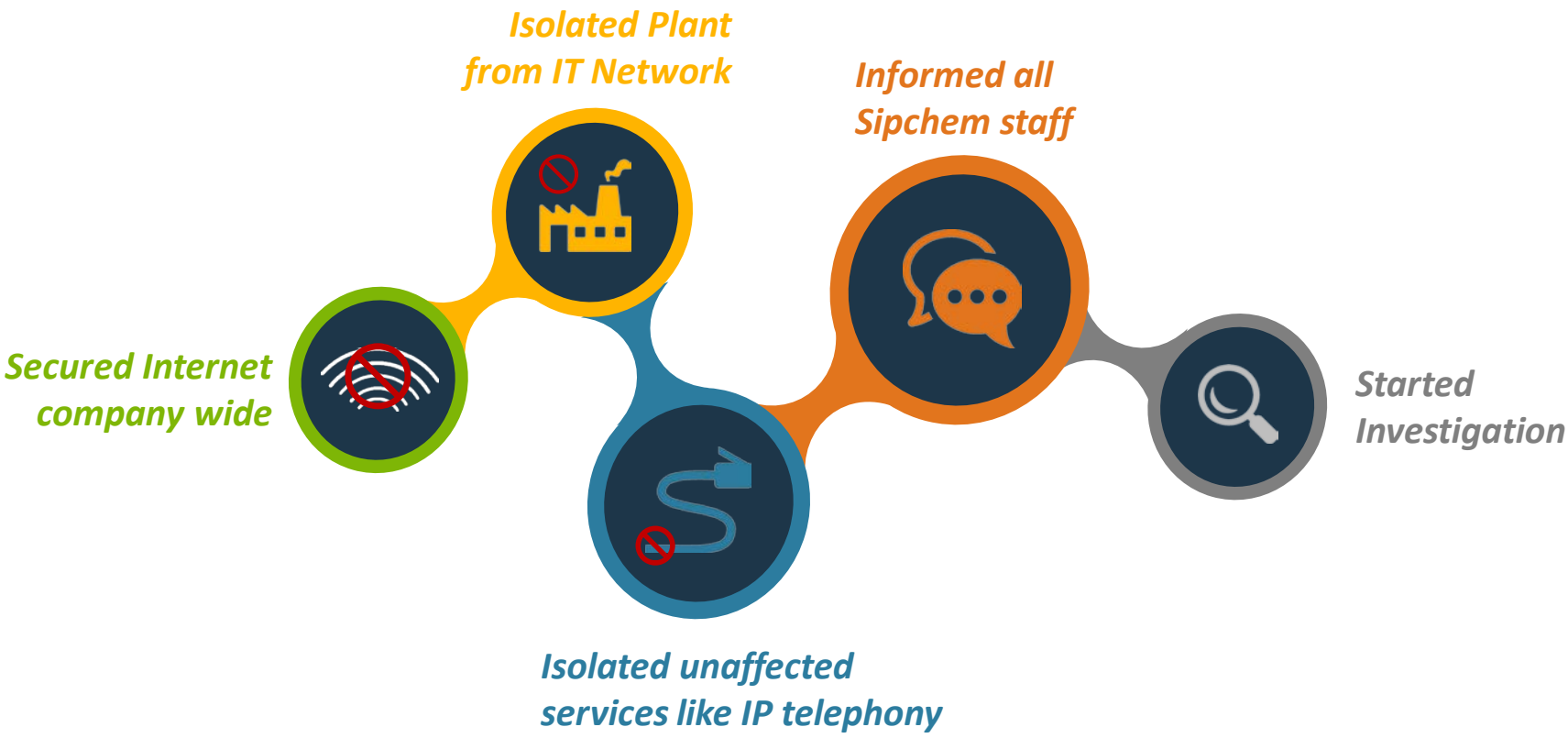
Khalid AlAmri
IT Infrastructure Section Head
Sipchem

سبكيم
Sipchem
EXCELLENCE everywhere

Saudi International Petrochemical Company

The beginning of the story

Immediate Mitigation Actions



Moral of the Story

It is comparatively

EASY

to recover systems but

VERY DIFFICULT

to recover

TEAMS MOTIVATION

Key Takeaway

Do not touch the defective storage

- Always do the recovery in different storage, drive, LUN and etc.

Key Takeaway

Replace the HDD for the user immediately and keep the user recovery for later stage

- User recovery is time consuming especially with huge numbers of attacked computers.
- Get the user with fresh OS image and let him do his work while you conduct the recovery at later stage.

Key Takeaway

While preparing the image for server or desktop, keep the data on any drive other than OS drive

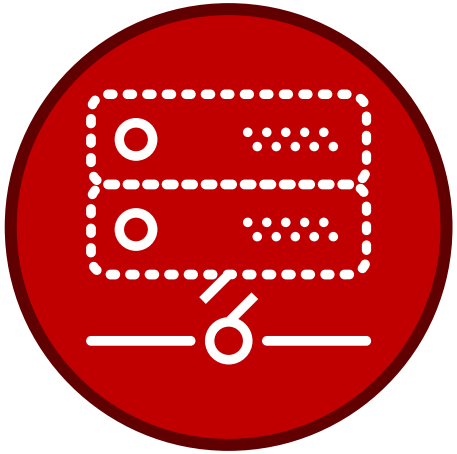
- While conducting the recovery, we found it very easy to recover data in any drive other than the OS drive (Usually C Drive).
- So keep the application data and user profiles in non-OS drive.

Key Takeaway

Backing up and recovering virtual servers are much easier than physical ones

- Try to virtualize your server workload as much as possible.

Key Takeaway



Have asynchronous replication of your backup/storage system

- If you are planning to replicate your storage or backup to another place, make the replication asynchronies with time lag of 12Hrs more.
- This will give you a change to recovery your data from that replication site if attacker gain access to your online systems and delete them manually.
- Of course, make sure the admin credentials for the replication site is different than the main site.

Key Takeaway

Do not trust HW vendor to do the recovery for you and get the system recovered by specialized recovery agent

- HW vendors can do great job in fixing their HW but not recovering data within the HW itself.

Key Takeaway

Do not rely on your backup system only for recovery

- Use storage volume/LUN regular snapshots.
- Make use of virtual server regular snapshots.
- Plan to use “store/write once” kind of storage. This storage is very handy during the disaster because any data written to it cannot be altered of changed.

Key Takeaway

Have the recovery tools ready prior to the disaster

- Download and test multiple recovery tools proactively and make sure they are reliable enough to be used during the real recovery.
- Have them copied with required license in external storage to have easy access to them during disaster.
- Make sure you know how to use them thoroughly because there is no room for trial and error during the recovery stage.

Key Takeaway

Have your secured systems credentials, system inventory and vendor support phone number in offline storage

- If such critical information is stored in your online storage, filers and etc, chances that you will not be able to access them if the online storage is attacked.

Key Takeaway

Assume the breach anytime and plan for solid recovery

- You should always assume that you will be attacked or breached at any time and you need to invest more time and resources for sold recovery plan.
- You may need to make a controlled drill attack to assess the feasibility of your recovery plan.

Key Takeaway

Protect the access to your environment, storage and backup systems with one time password and multiple factors authentication solutions

- This must go for all your systems including storage and back systems.
- These systems are the last resort for recovery and if you lose them your recovery plan will be affected severely.

Key Takeaway

Your IT disaster recovery plan must account for Cyberattack not only natural disasters

- Revise thoroughly your IT DR plan and make sure that it covers Cyberattack.
- In your plan, always assume that you have a psycho administrator who has full access to your systems and can destroy them at any time.
- This will lead you to plan the privilege access provisioning process and to avoid granting full access to a single account.

Key Takeaway

Do not rely on one software for recovery try others

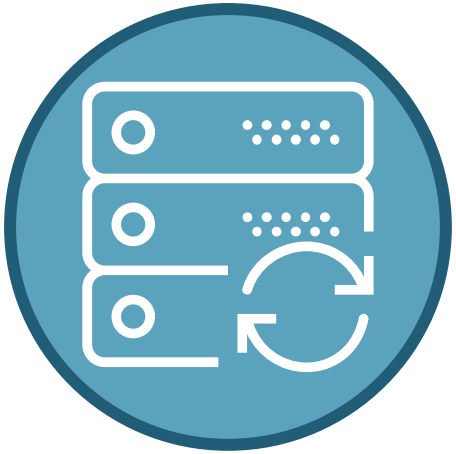
- Multiple recovery software yields different results so do not stick with one only.
- Try reputable recovery software and avoid the free ones.
- Always start the recovery with gradual pace.
- Go for “quick scan” and if there is no feasible result then step up to “deep scan”.

Key Takeaway

Place the required OS and applications images, ISOs, CD/DVD copies in external or offline storage

- During the disaster, you may not have the time or even the bandwidth to download huge files such OS and application CD/DVDs.
- So download them ahead of time and keep them in external and offline storage.
- Make a process to update the content of this storage regularly based on the OS or application version changes.

Key Takeaway



Rebuild your system OS and application whenever possible and recover/restore only the data

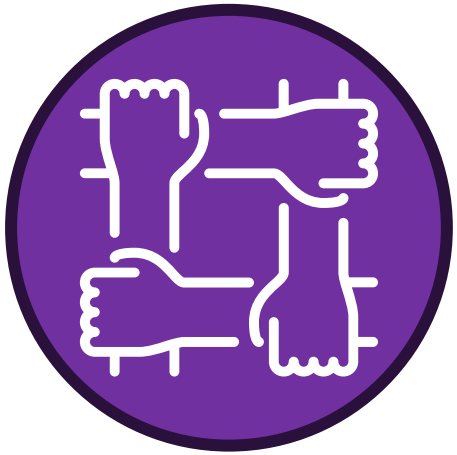
- During the recovery, you may have limited knowledge about the type of attack or the malware itself especially on the first days. It will be wise then to build the OS and application from scratch and restore only the data for the application because it is less likely to be infected.

Key Takeaway

HDD duplicator can be very handy during the disaster

- Invest in reliable HDD duplicator as it will save you a lot of time while copying new image to user desktop computers.
- You need to have a fresh image of your OS and applications stored in offline HDD to be used during the disaster.
- You may also setup a physically isolated imaging environment with one desktop machine acting as the image server and connected to isolated switch along with desktop/laptop computers to be re-imaged.

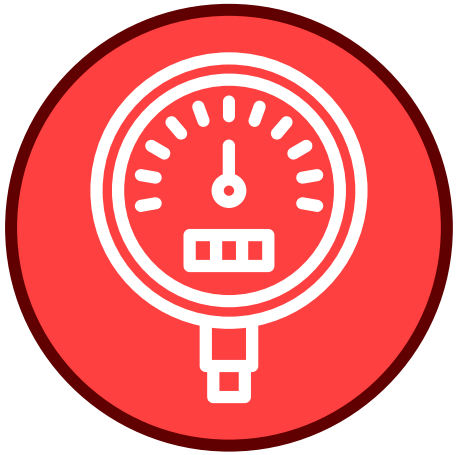
Key Takeaway



Recovery is time consuming so work in parallel

- Setup a dedicated team for recovery and with coordinate recovery efforts.
- Recovery process should be clear to the team and everyone needs to know exactly what he will be recovering to avoid recovery duplication and waste of time.

Key Takeaway



Make sure you have plenty of extra storage capacity for recovery

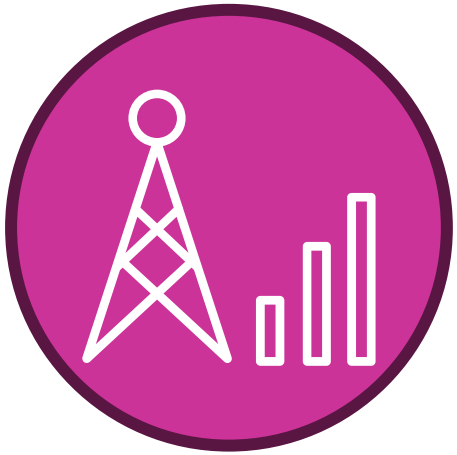
- Since the attacked systems with the recovery ones will coexist for some time, you need to have sufficient space to accommodate them all.
- 40% of your existing storage dedicated to recovery is a good start.

Key Takeaway

Assign only skilled engineers for recovery

- There no room for trial and error during the recovery because any small mistake can render your data useless.
- Recovering your systems in a timely manner is very crucial and you need caliber peoples who know what they are doing.

Key Takeaway



Make sure you plan for adequate Internet bandwidth during the disaster to be used for downloading missing patches or etc

- xDSL could be an option if the usage of the main Internet access is restricted during the recovery.
- 4G/3G modems are not reliable and do not provide stable bandwidth all the times so avoid them when possible.

Thank You

سبكيم
Sipchem
EXCELLENCE everywhere

Saudi International Petrochemical Company