DISASTER RECOVERY – HOW TO SURVIVE WHEN RANSOMWARE STRIKES

1 IN 3 ORGANIZATIONS WERE HIT BY A MALWARE ATTACK IN THE LAST 5 YEARS

High-profile malware and ransomware attacks are becoming hard to ignore, while getting more sophisticated and difficult to detect. Even IT professionals can click on an infected link.

Example:

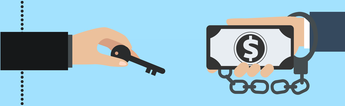
An employee opens an email that looks like it's coming from a customer. The subject line is a request to review an invoice. Most employees respond to important looking emails – just before the IT department realizes it might be malicious.

IS SOFTWARE AND TRAINING ENOUGH?

Companies try to stop ransomware by investing in security products and employee training. The problem is that it only takes one user and one mistake to invite the ransomware in. Once the ransomware starts to spread, your only steps away from a catastrophe.

HAVE A BACKUP PLAN

If your organization is hit – there is often no way to get back on your feet except restoring from backups (which takes time) or switching over to your Cloud-Replicated standby backup systems (to instantly get back online).



ELIMINATING THE ATTACK RISK

Do all that you can to prevent ransomware within your organization. These efforts do help, but they don't eliminate the risk. In addition to proper training and other security measures, you should also have a solid Disaster Recovery Plan, where paying the criminals is not an option.

BACKUPS: YOUR LAST RESORT

The good news:

Your IT department has a separate data backup that can't be affected by malware.

The bad news:

You got hit by ransomware.

Restoring data backups is a common solution for ransomware

Having these in place is an absolute must. However, this approach may not prevent financial losses - restoring backups takes time and can require downtime which will affect your customers and your profits.

Many companies only run nightly backups. When ransomware attacks, they will lose all the work created after the last backup – Even worse, they may not be aware they have been victimized for days, requiring them to restore significantly older backups.

If a ransomware attack goes undiscovered for more than a day, you could lose a lot of data. Plus it's almost certain that executives will have lost a file of utmost importance. With this loss, you need a process that instantly gets you back online and also mitigates the loss of data.

DISASTER RECOVERY AS A SERVICE

To avoid expensive data loss and downtime from the inevitable ransomware attack, you need a process that:

- Preserves all your data.
- Gets you back online immediately.

Disaster Recovery as a Service or DRaaS, can recover your files in minutes. You can move you IT infrastructure to the cloud, giving you time and space to repair the infection. All this without affecting your business and customers.

DRaaS gives you a point-in-time recovery. This saves you from having to go back to last week's backup, meaning the loss of all the data collected in the meantime.

Having a DRaaS solution in place makes ransomware powerless against your business and quickly recovers the data you need when attacked with no need to pay the ransom.

DON'T GAMBLE - Be prepared when IT disasters strike

Receive a FREE consultation of your company's Disaster Recover Plan visit www.TurnKeyInternet.net/myplan