FOUR STEPS

FOR CYBER RECOVERY READINESS

11:11 SYSTEMS

Being able to recover from a cyber intrusion has become imperative. Statistics tell the story: it isn't a matter of **if** your organization will become the target of cyber criminals, but **when**.

236M+

RANSOMWARE ATTACKS IN 2022

Source: 2023 Veeam Data Protection Trends Report

85%

OF ORGANIZATIONS SUFFERED AT LEAST ONE CYBERATTACK IN THE PAST YEAR

Source: 2023 Veeam Ransomware Trends Report

50%

OF ORGANIZATIONS THAT ARE ATTACKED BECOME VICTIMS

Source: 2023 Fortinet Global Ransomware Report

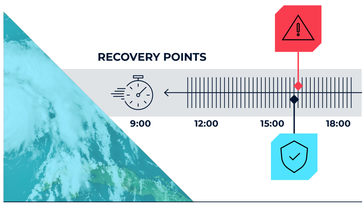
All this is evidence that you need to get your cyber recovery plan in place in order to survive when you are compromised.

If you have a disaster recovery (DR) solution, this is only part of the picture.

BECAUSE CYBER RECOVERY IS DIFFERENT THAN TRADITIONAL DISASTER RECOVERY.

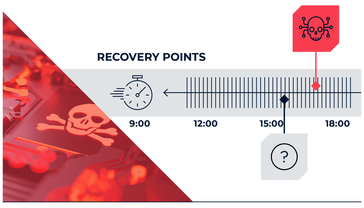
WITH DISASTER RECOVERY...

When an outage happens, you find the latest point-in-time from your DR solution and fail over in the cloud.



WITH CYBER RECOVERY...

When cyber criminals strike, you have no idea when your data was first compromised. Your latest point in time replica of your data is most likely infected with ransomware.



1

Follow the 3-2-1-1-0 rule of data protection.

Three copies of data...
On **two** different types of media...
With **one** copy offsite...
One copy should be offline and immutable...
And you should verify that your backup has **zero** errors.

2

Identify vital data assets (VDAs).

Most organizations can't afford to follow the 3-2-1-1-0 rule for all of the data in the IT environment. So you need to figure out what assets are absolutely vital.

This includes data that could threaten business viability if the information becomes:

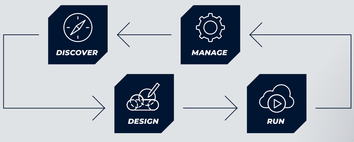
- Exposed
- Compromised
- Unavailable

SENSITIVE OR REGULATED INFORMATION | ***ANYTHING THAT GENERATES REVENUE*** | ***DATA RELATED TO YOUR ORGANIZATION'S MISSION***

3

Create VDA-specific recovery plans that address cyber incidents.

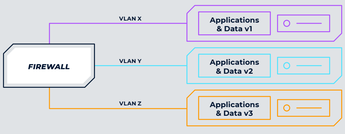
- Map out recovery plans for all vital assets
- Keep up-to-date lifecycle information, including passwords, as infrastructure and environment evolves
- Regularly test and ensure that VDAs can be recovered
- Adapt your plan as threats and technologies change



4

Set aside recovery resources needed to recover from a cyber intrusion:

- Environment to recover multiple replicas of your environment simultaneously
- Multiple point-in-time snapshots of your VDAs to ensure data isn't compromised
- Clean room to test data viability



BEING CYBER RECOVERY READY REQUIRES AN ONGOING PROGRAM, AND 11:11 SYSTEMS HAS THE EXPERTS AND THE TECHNOLOGY TO HELP.

We bring together more than 40 years of history providing tactical expertise and customer success in disaster recovery and cyber recovery. We will work with you to build a cyber readiness program that will ensure that your team is ready when cyber criminals strike.

11:11 SYSTEMS

CLOUD | CONNECTIVITY | SECURITY

RETHINK CONNECTED

1111systems.com

11:11 Systems, the 11:11 Systems logo, and all other 11:11 Systems product or service names are registered trademarks or trademarks of 11:11 Systems, Inc. All other registered trademarks or trademarks belong to their respective owners. ©2023 11:11 Systems. All rights reserved.