IT NATION™ SECURE

hosted by CONNECTWISE®

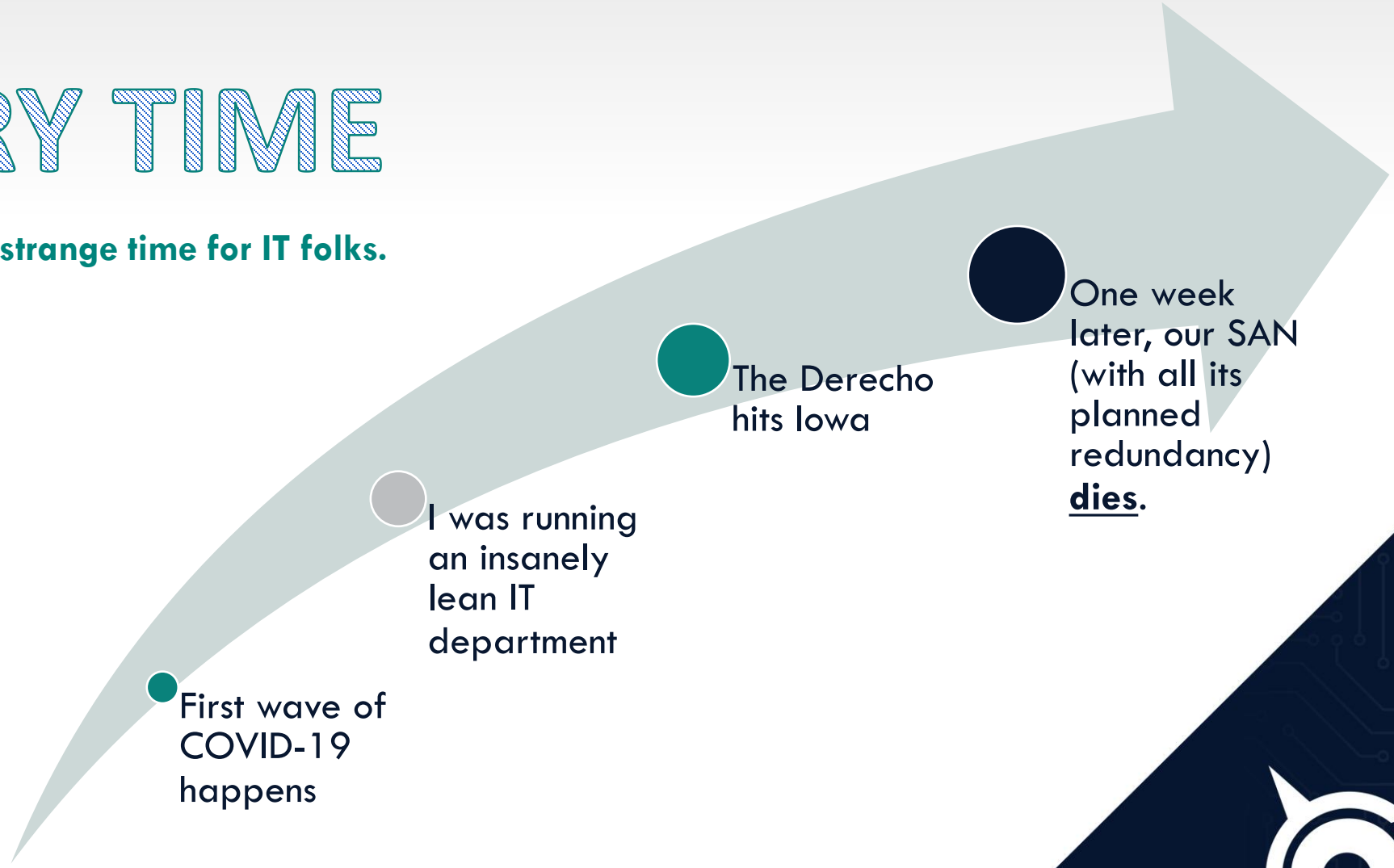
MANAGEABLE **MAYHEM**

Presented by Drew Dunkel, Director of Technology Solutions, ACS

IT NATION™ SECURE

STORY TIME

August 2020. A strange time for IT folks.



HOW DO YOU PLAN FOR THE UNPREDICTABLE ?

THE PROBLEM WITH DISASTER RECOVERY TESTING

We've all had that incredibly resistant client who is unwilling to commit to the final phase of a complex business continuity project. **Let's call him Bob.**

MEET **BOB**

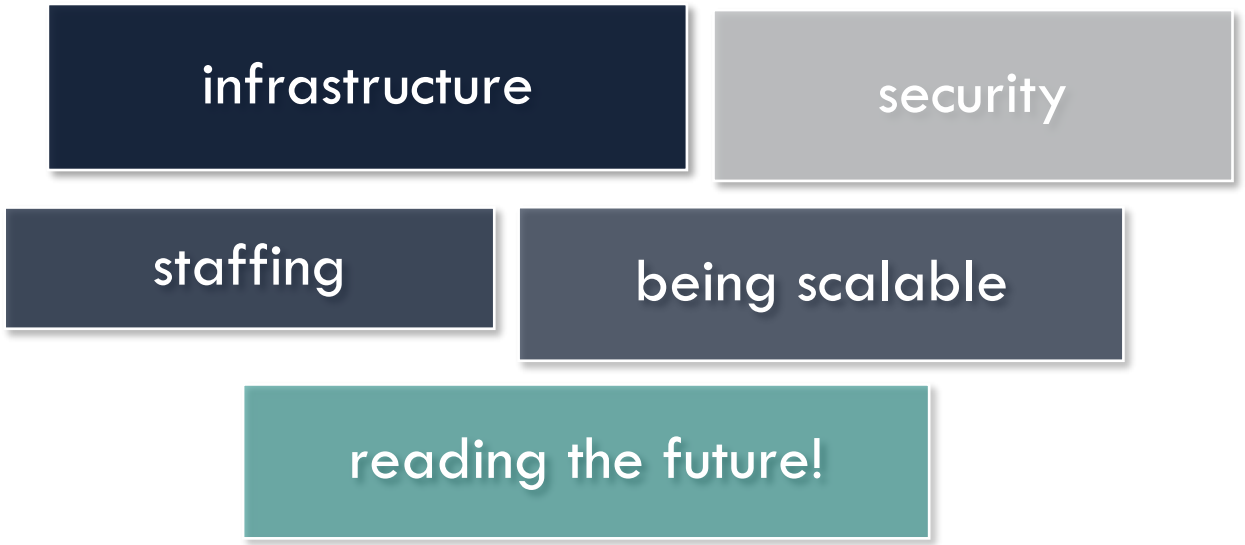
You've gone the distance for Bob:

- Built out a solid disaster recovery strategy
- Tools and systems are in place
- Backing everything up
- RTO and RPO are set

… But you're missing the crucial final component: Putting that hard work to the test to prove you can put Humpty Dumpty back together.

WHY IS BOB NOT BUYING INTO THIS?

Bob must balance:



… all within a pre-approved budget which is a triage of paperwork and approvals filed *just* the right way to get an exception.

When hit with this realization, his only choice is to mitigate risk as much as possible.

THE RISKS OF BOB

1

ENVIRONMENTAL

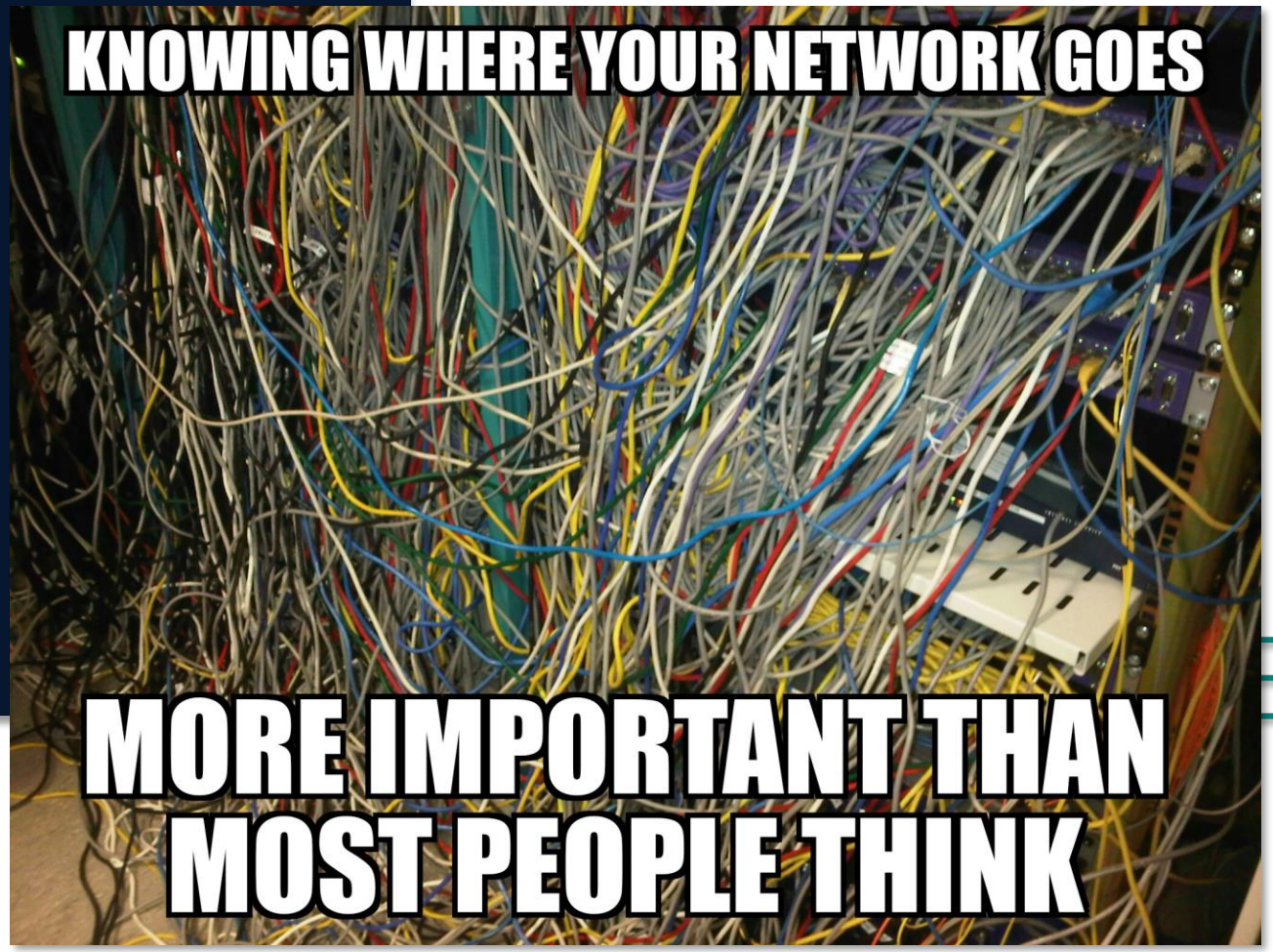
ENVIRONMENTAL

Consider what mother nature can throw at you:

- Hurricane
- Tornado
- Earthquake
- Flooding

2

NETWORK


KNOWING WHERE YOUR NETWORK GOES
MORE IMPORTANT THAN
MOST PEOPLE THINK

NETWORK

Consider what your hardware can do to you.

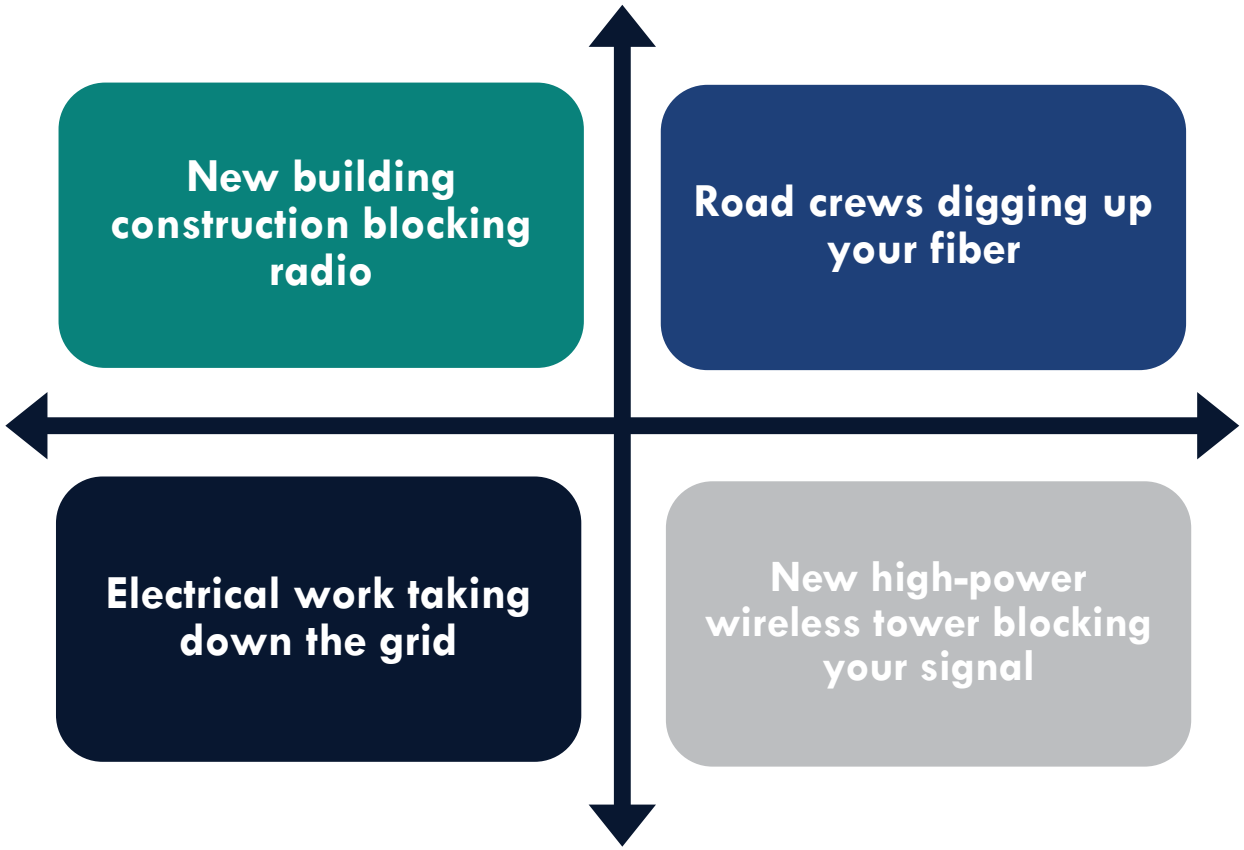
- Where are you in your network lifecycle?
- Have you prepared for redundancy?
- How do you react when your network fails?

3

EXTERNAL

EXTERNAL: PHYSICAL

What are your neighbors really doing out there?



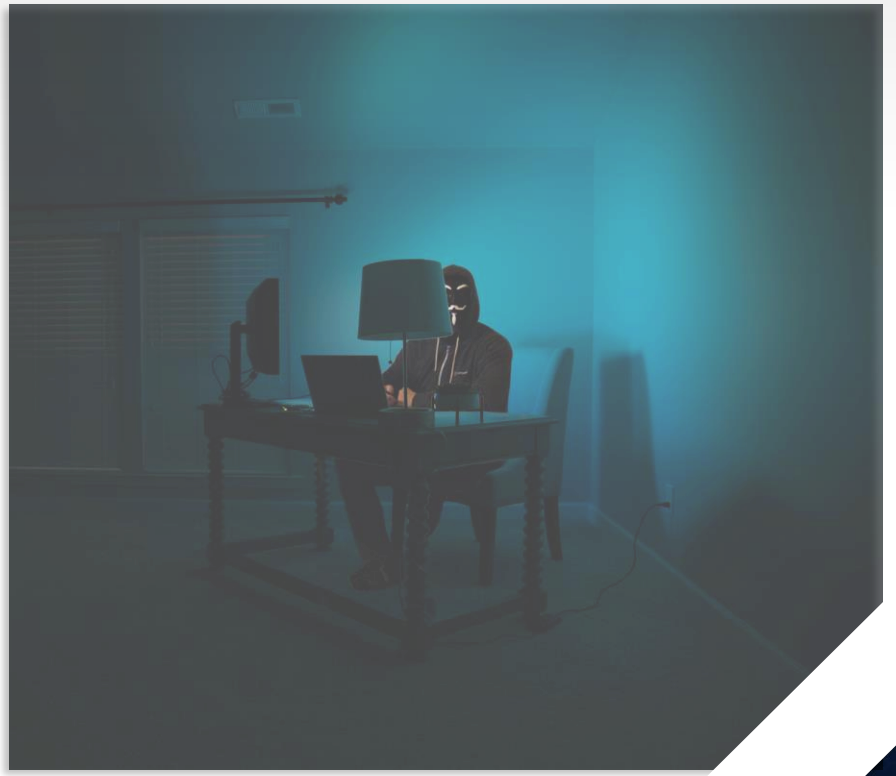
… And where are your backups really located?

4

CYBER


klossner
" MAYBE WE SHOULD TRY A DIFFERENT SECURITY APPROACH THIS YEAR. "

CYBER

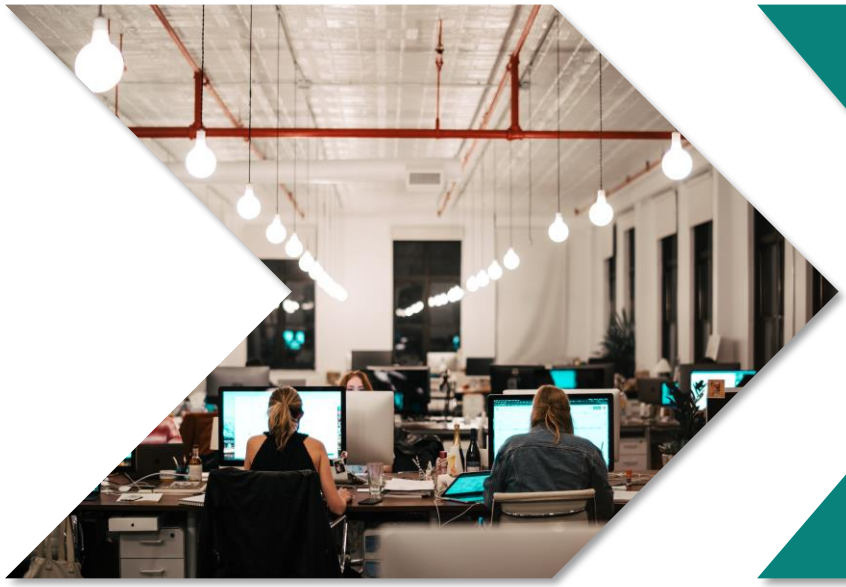


Threat actors waiting to exploit
your systems – or finding ways to do it right now.


BUY AN IPHONE 5, THEY SAID
COMES WITH A MAP, THEY SAID.

BUSINESS SYSTEMS

Why are these systems so behind the times?!



6

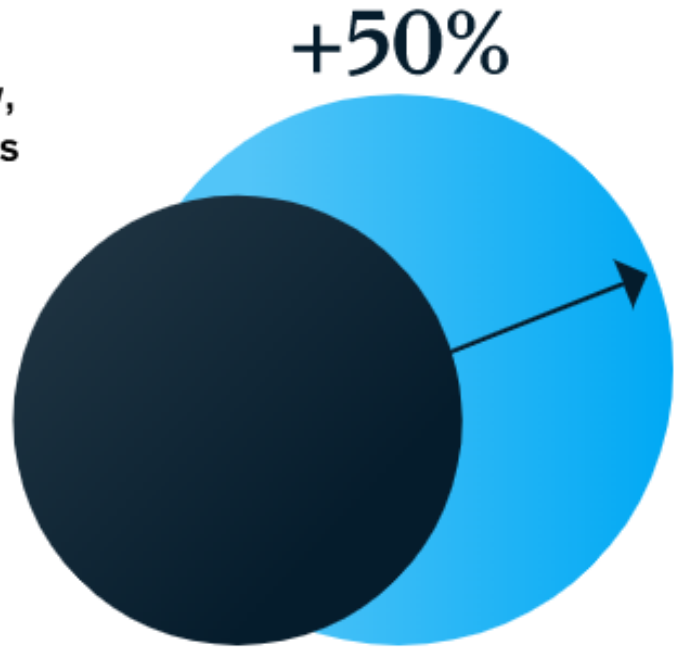
MAYBE EVERYTHING IS PERFECT BUT THAT ONE MISSED ELEMENT.

EVERYTHING ELSE

Yes, we all know it's primarily users causing issues.

INCREASING SPEED & RESILIENCE

In the 2020–21 economic recovery, resilient companies generated TSR 50% higher than their less resilient peers'

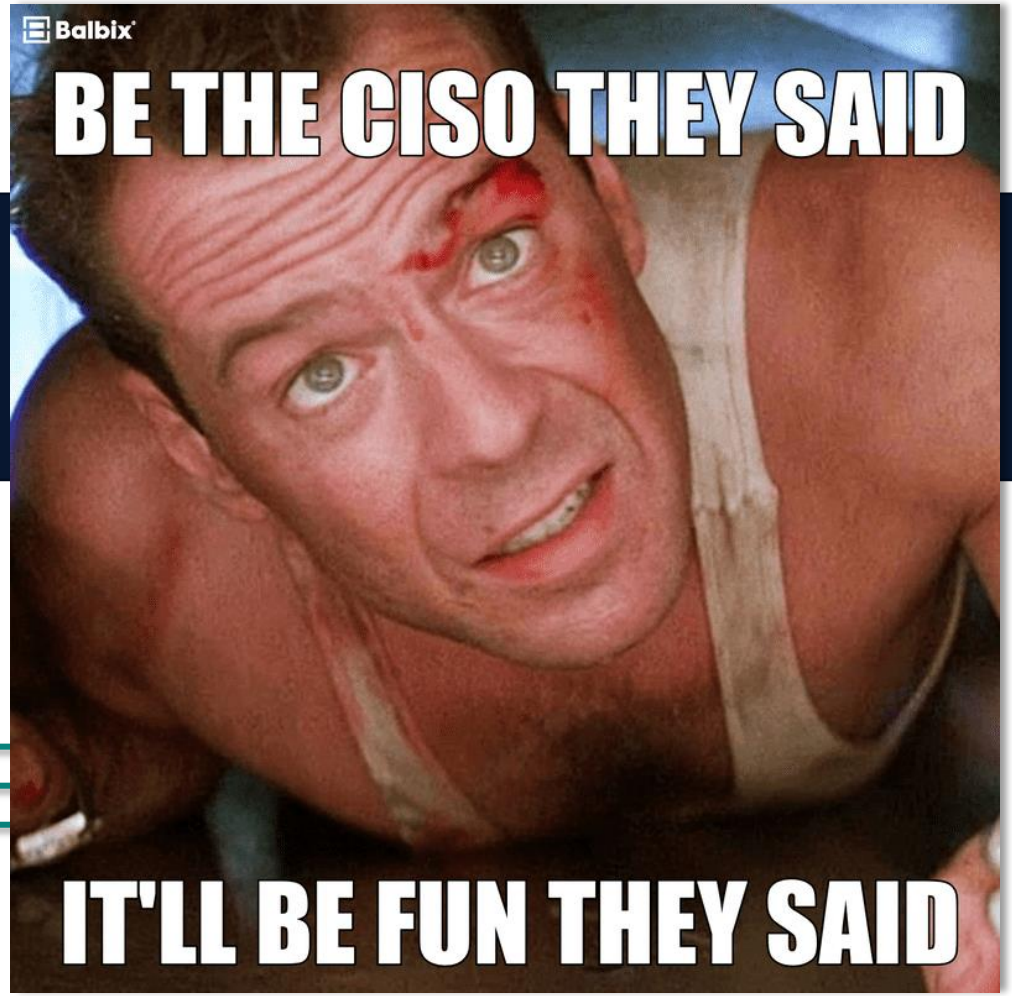


McKinsey & Company

According to a survey by McKinsey, half the respondents said their organization is unprepared to react to future shocks.

THE SOLUTION!

SMALL SCALE, **MANAGEABLE MAYHEM**



SO, HOW DOES IT WORK?

Create safe scenarios for the team to practice different events:

1. Make sure someone from the **business** is involved to conduct their own testing. Business buy-in is key.
2. Make it **random**: Random and weird is the life of the IT pro. The unexpected always happens.
3. Use previous **examples**
4. **Document** everything: This is a training exercise so when the real event happens, everyone knows what to do.
5. MAKE IT **FUN**!!!

1

KNOW THE ASSETS

- For this to be successful, you need to have a documented list of **ALL assets.**
- Understand what assets are **critical**
  - You may not realize a specific component is critical to keeping the business alive. Think how that piece of production machinery is connecting to the network.
- With the business, review the **risk tolerance** for critical assets.
  - This will be important when simulating so you can prove it back to the business.

2

UNDERSTAND THE ELEMENTS

Review your environmental risks. Is the office at risk for a flood, tornado, hurricane, etc.?

Understand where the physical lines come into the buildings.

Compare this to the critical assets to line up your risk potential.

What options are available in the event the office is inaccessible due to environmental reasons?

3

BE AWARE OF THE NETWORK

How is it configured?

How do the lines traverse the locations (physical and wireless)?

- Is there copper and fiber?
- How many locations does the company have and how many ways are they interconnected?

How is operating technology connected?

Make sure you have wiring diagrams and network maps so you can put it back together again!

4

LEARN THE BUSINESS

What business systems are in use?

- Are these on-prem or hosted?
- Are there known exploits to these?
- How is the vendor response time?

What machinery connects to the network and how does it go outside your network?

- Is the data on-prem or hosted?
- What does the vendor do to support these systems?
- Are they on a segmented network?

Are there cloud systems in place?

What processes must happen every day to stay in business?

5

DOCUMENT WHAT IS CRITICAL

Hold a business meeting with key stakeholders (Not just the IT department)		
Review the list and make sure everyone agrees what is critical.	Rate the list from most to least important.	Discuss RTO and RPO and what the steps are to guarantee those metrics.
Consider how you would test each critical component one at a time versus a full-scale Disaster Recovery simulation.	Make sure you develop core documentation.	

6

MAKE IT PART OF YOUR DAY-TO-DAY

Recovery is not something you do only when needed. It needs to become a lifestyle.

Make sure every layer of the business is asking themselves: What would I do if this was not available today?

Ensure the technology department is challenging themselves to have a defense-minded strategy when making changes to the network.

7

CREATE SOME MAYHEM – AND MAKE IT FUN!

With the previous items in place, you have built a solid foundation to create some safe scenarios to SHOW why Disaster Recovery testing is important.

- You have documented what is **critical**
- The business agreed to a **recovery objective**
- You have **documentation** on how to put the environment back together

Time to create scenarios to test for various incidents.

- In the next section, we'll outline some scenarios. These may not work for every client, but they'll help you put some thought into small-scale testing.

SCENARIO 1: BOB BLEW UP THE FILE SERVER

Bob is attempting to upgrade the file server. He creates his new Windows Server VM, joins the domain, and starts the copy process.

Upon inspection, Bob realizes he put all the capacity to the C drive and did not break out disks. Bob decided to start over and delete the VM… except he accidentally deleted the production file server!

SCENARIO 1: BOB BLEW UP THE FILE SERVER

HOW TO SIMULATE

- Simple scenario that tests your RPO and RTO.
- Clone a VM (Your file server is fine if it is renamed and does not affect production, and you have the capacity to do so).
- Practice how to restore a VM and verify the files are there.
- Extra points: make a file from the previous day to store on that server and make the tester find it.

It's critical that each member of the IT team who has security to do this practices in a save environment.

SCENARIO 2: CONSTRUCTION COMPANY CUT THE FIBER

1. The CEO of Bob's Company INC is introducing a revolutionary expansion.
2. Bob is responsible for making sure there are ZERO tech disruptions.
3. The construction company snags an odd cable and decides it's useless. They pull on it to "clean it up."

SCENARIO 2: CONSTRUCTION COMPANY CUT THE FIBER

HOW TO SIMULATE

You do not need to go outside and tear the fiber out!

- Simulate what the environment would be like with a longer internet outage.
- **MUST** be done after hours if it will affect production.

1. Unplug any wired internet connections.
2. See how the network responds.
3. What systems break?
4. Is there latency?
5. Does your redundancy work?

SCENARIO 3: SERVERS ARE DOWN

Bob just hired Super Clean janitorial services. The receptionist is helping them navigate the office as they are doing their first cleaning job.

When attempting to plug in the vacuum, they realize there are zero outlets available. In a flash of insight, the receptionist mentions there is a strange closet with tons of outlets.

They enter the closet, and while there are still no outlets available, they decide it would be fine to unplug a few things to plug in the vacuum.

Bob is met with an unexplainable barrage of phone calls that the sky is falling and profits are tanking due to the network being out of commission.

SCENARIO 3: SERVERS ARE DOWN

HOW TO SIMULATE

- No matter what: **ensure** you have redundant power to critical devices.
- In a safe scenario that does not affect production, you can test the load on your batteries and document what is connected to each outlet to ensure you're covered. Most UPS have a function just to test for X number of seconds.
- The other method is to remove primary power if you can do safely.
    - Example I had an environment with a generator that could be toggled on/off where I could test toggling it on and cutting primary power.

SCENARIO 4: I AM UNDER ATTACK

Timmy wants to be a hacker. He has his new Alienware laptop and a fresh copy of "How to Hack For Dummies."

Timmy dabbles in the dark web and finds a reputable company selling Ransomware as a Service software.

Timmy crafts an elaborate email applying for an internship at Bob's company with a spoofed link to his resume.

The HR department opens the attachment, downloading the ransomware application.

SCENARIO 4: I AM UNDER ATTACK

HOW TO SIMULATE

1

If you are okay with PowerShell, create your own image or macro-embedded file with a PowerShell script. It really doesn't matter what it does, the goal is to test your prevention software to:

- A: Detect abnormal behavior
- B: Track what the rogue application did

2

Purchase a ransomware simulator like KnowBe4's Ransomware Simulator or something like PSRansom that tests various attack vectors.

MAKE THIS YOUR OWN

- Differs based on the client's appetite.
- At ACS: monthly agreement product with a random event each month to help coach and add value.

+

MAKE THIS PART OF THE BUSINESS

- Repetition creates preparedness!
- Makes real-life events less scary.
- Helps know what to budget for to shore up weaknesses.

QUESTIONS?

THANK YOU

515.223.0078

/in/drewdunkel/

/company/acs_5

acsltd.com

Don't forget to fill out your

SESSION SURVEY