Disaster Recovery Checklist & Best Practices for Municipalities

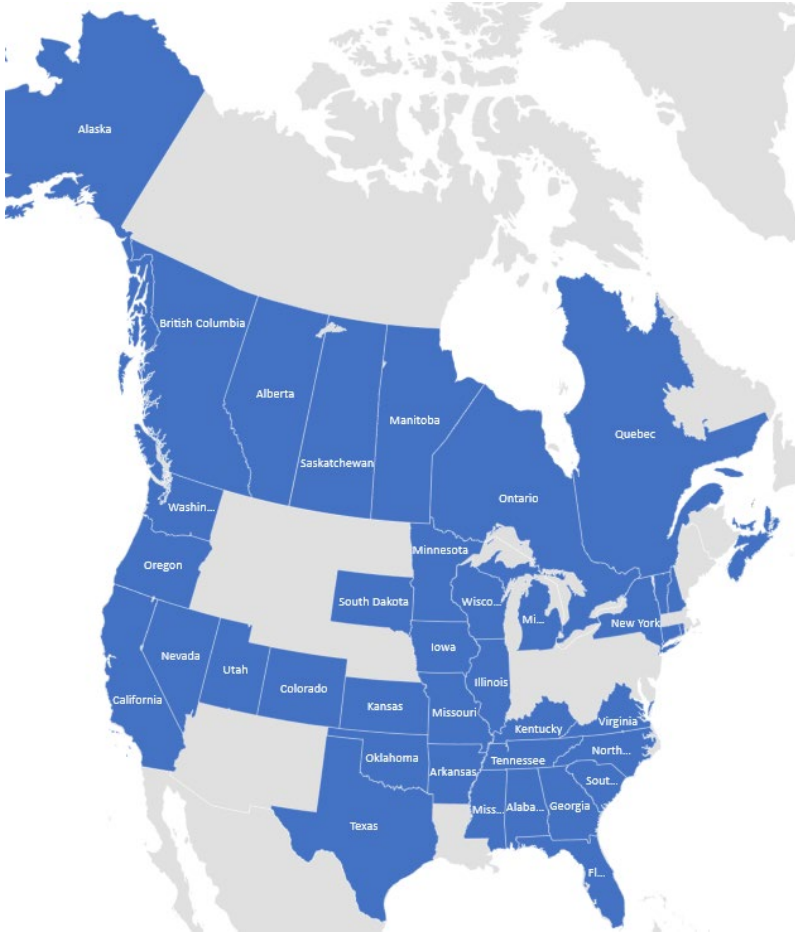
PRESENTED BY

COREY KAUFMAN, DIRECTOR OF CLIENT STRATEGY & SOLUTIONS

WELCOME

Corey Kaufman
Director, Client Strategy and Solutions

- Corey Kaufman, Director, Client Strategy and Solutions at VC3 & Registered Practitioner for the Cybersecurity Maturity Model Certification Accreditation Body
- Serving Municipalities, Special Districts, and small to medium sized businesses since 2001
- Serving more than 1100 cities and towns and over 900 small to medium sized businesses across 32 states and 8 Provinces



WELCOME

- Current threat landscape & why this is important
- Identifying critical versus non-critical data
- Assessing your current data backup situation
- Understanding the recovery ability of your solution
- Verifying your offsite data includes isolation
- Getting the plan in writing
- Practice, Practice, Practice

Current threat landscape

$5M The average data breach cost in 2023 is **$5M.**

#1 **Public sector** is the most attacked and compromised vertical.

314 **314 days:** Average time from breach to containment.

- 7 months to identify
- 4 months to identify

95% **95%** of successful cyberattacks start in email.

333 **333.2 billion emails** were sent daily in 2022, about 1/3 being spam.

300K **300,000 new pieces of malware** are created daily.

$3.8M 2022 **2022:** The average cost of a data breach was **$3.80 million.**

$6T 2023 **2023:** The entire cost of cyberattacks is **$6 trillion.**

$10.5T 2025 **2025:** Cybercrime will cost the world **$10.5 trillion** yearly.

24k An average of around **24,000 malicious mobile apps** are blocked daily on the internet.

50% More than 1/2 the organizations with IoT devices have **no security measures in place.**

Current Threat Landscape

IT WON'T HAPPEN TO ME, RIGHT?

- **January 3, 2023:** "Cities and Governments are the Latest Target in a New 'Leakware' Attack"
- **February 10, 2023:** "One Pricy Hospital Bill: Ransomware Attack Costs Hospital $1 Million"
- **February 15, 2023:** "US Cities Remain at Risk of Cyber Attacks"
- **March 23, 2023: "**Phishing Scam with Fraudulent Invoice Costs City of Fresno Over $600,000"
- **May 9, 2023: "**Dallas Police Department is latest Victim of a Ransomware Attack"
- **February 25, 2024**: "Hamilton refuses to pay hackers 'huge' ransom in wake of cyberattack"
- **July 18, 2024**: "City of Columbus Says Data Compromised in Ransomware Attack"
- **August 14, 2024**: "Flint's network outage caused by criminal ransomware attack"
- **August 18, 2024**: "What happened? Questions to city go unanswered on Killeen cyberattack that spewed ransomware on city's IT systems"

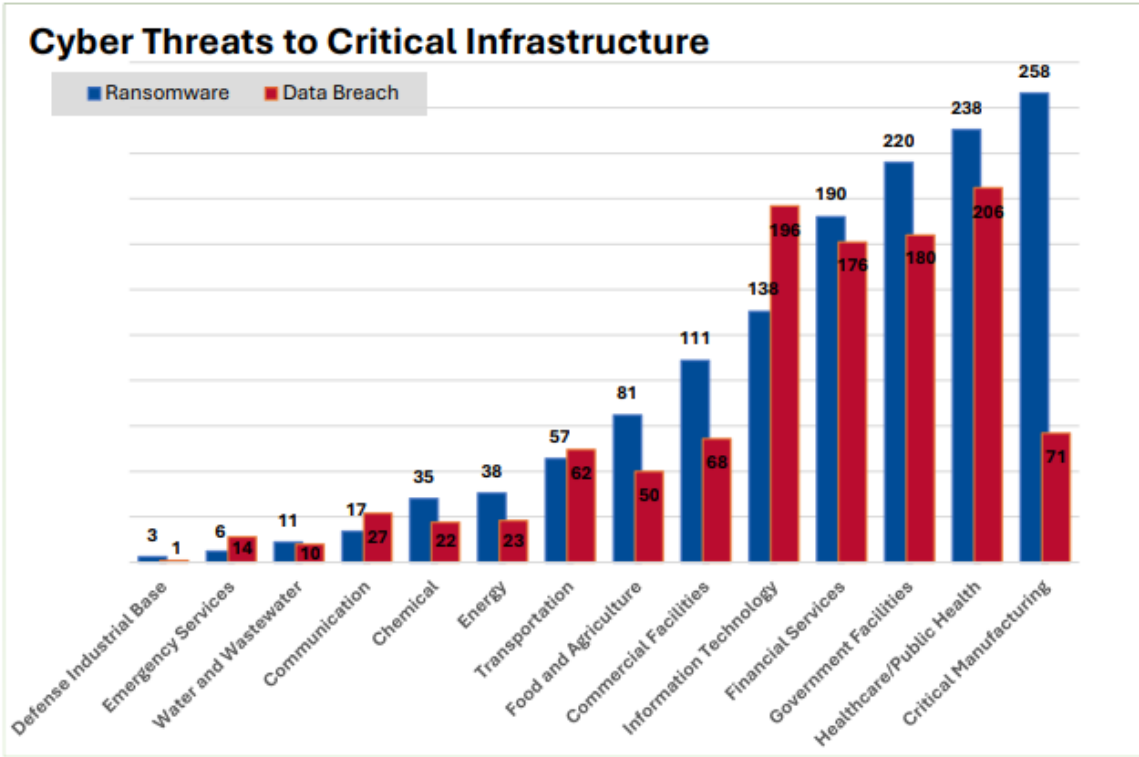


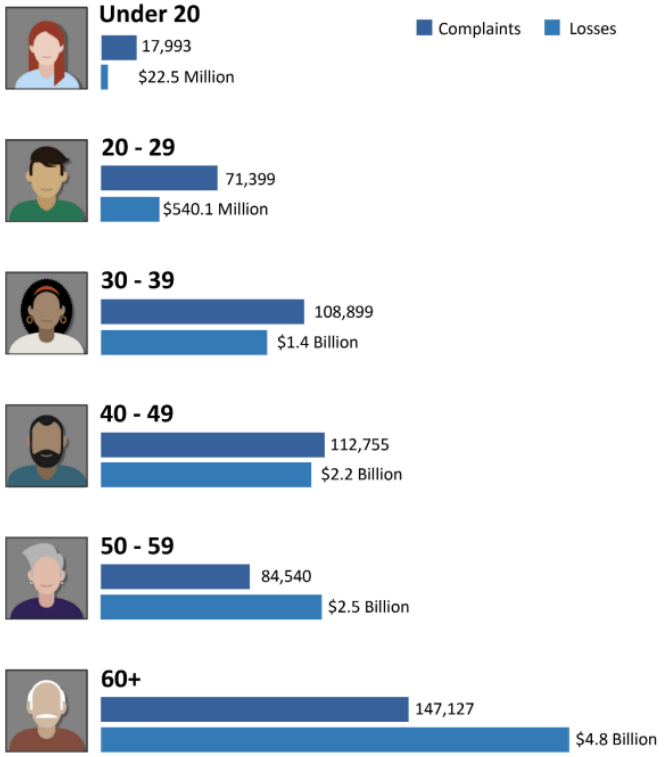
How much do you enjoy the following conversation at a council meeting?

“BECAUSE OF IT ISSUES WE HAVE TO SPEND A LOT OF UNPLANNED MONEY.”

The Cost and The Targets

ACCORDING TO THE DEPARTMENT OF JUSTICE'S 2024 INTERNET CRIME REPORT:





859,532 Total Complaints in 2024

$16.6 Billion Losses in 2024

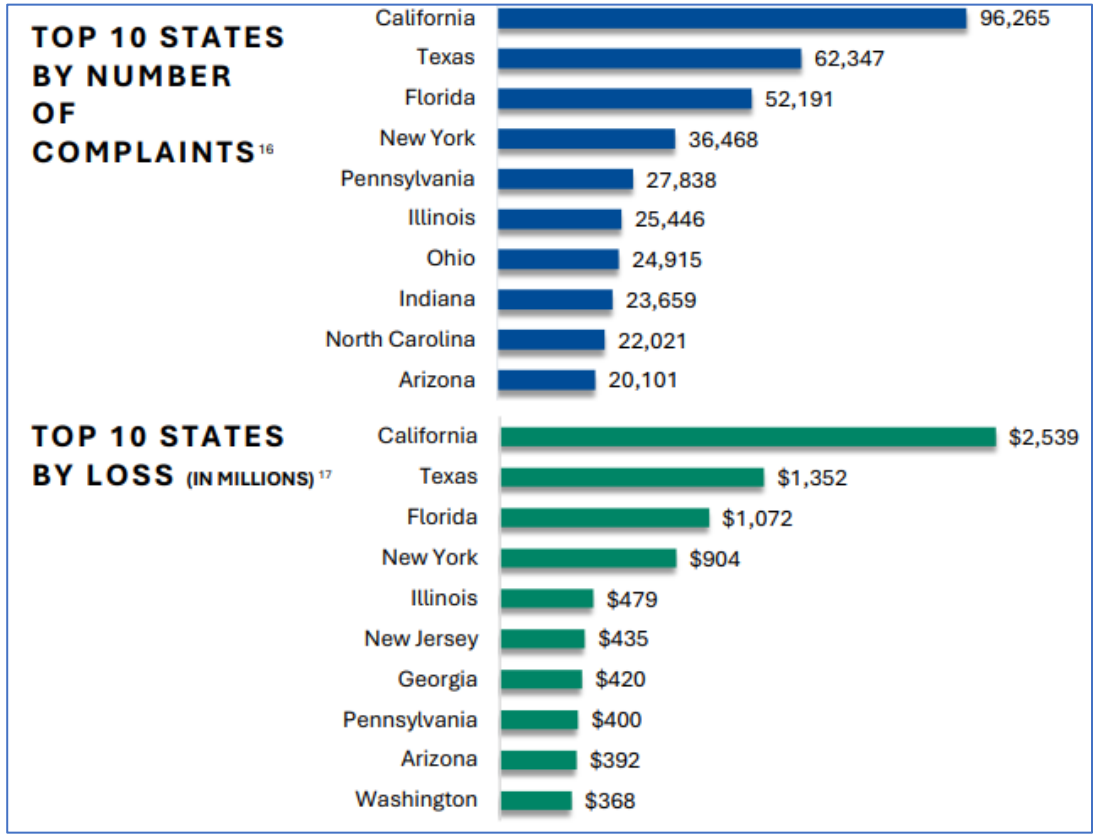
33% Increase in Losses from 2023

256,256 Complaints with Actual Loss

$19,372 Average Loss

The Cost and The Targets

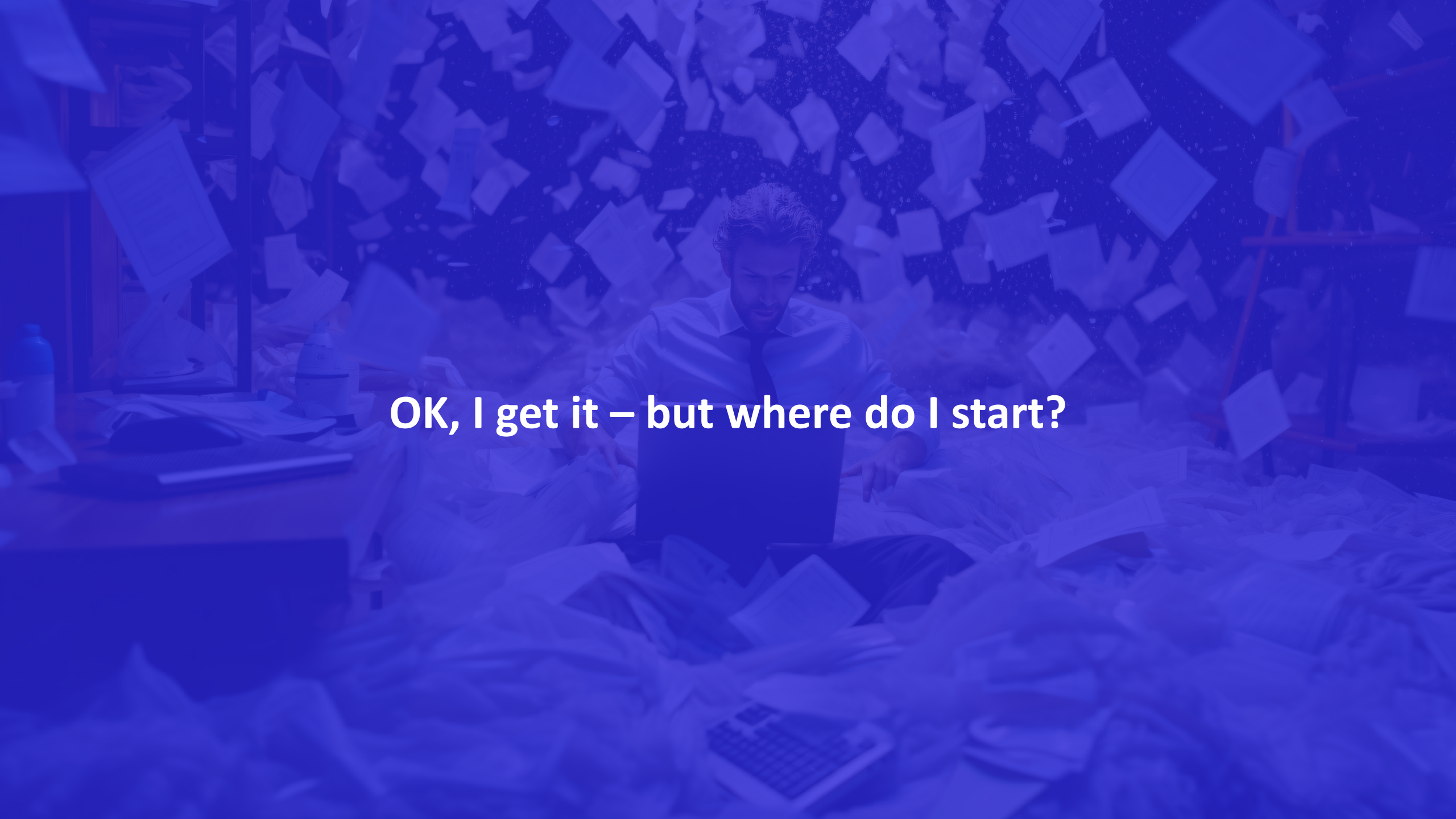
ACCORDING TO THE DEPARTMENT OF JUSTICE'S 2024 INTERNET CRIME REPORT:



2024 CRIME TYPES

BY COMPLAINT COUNT

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	193,407	Harassment/Stalking	11,672
Extortion	86,415	Real Estate	9,359
Personal Data Breach	64,882	Advanced Fee	7,097
Non-Payment/ Non-Delivery	49,572	Crimes Against Children	4,472
Investment	47,919	Lottery/Sweepstakes/ Inheritance	3,690
Tech Support	36,002	Data Breach	3,204
Business Email Compromise	21,442	Ransomware	3,156
Identity Theft	21,403	Overpayment	2,705
Employment	20,044	IPR*/Copyright and Counterfeit	1,583
Confidence/Romance	17,910	Threats of Violence	1,360
Government Impersonation	17,367	SIM Swap	982
Credit Card/Check Fraud	12,876	Botnet	587
Other	12,318	Malware	441
*Descriptor***			
Cryptocurrency	149,686		


OK, I get it – but where do I start?

“Where do I begin with data backup strategy?”

It’s one of the most common questions we get from municipalities & special districts.

To answer this question, we’ve created a step-by-step processes that special districts can use to create an action plan to address their data backup strategy.

Gov/Muni/State entities **struggle** with the same **backup challenges**

DATA LIVES IN MORE PLACES THAN EVER BEFORE

BACKUP IS TIME CONSUMING TO MANAGE

BACKUP IS COMPLEX AND PRONE TO COSTLY MANUAL ERRORS

BACKUP IS EXPENSIVE AND INFLEXIBLE

What challenges are you trying to solve?

- Upgrade to modern backup & disaster recovery
- Gain confidence in quick ransomware recovery
- Consolidate backup solutions required
- Meet compliance requirements
- Spend less time managing backup solutions
- Complete my security portfolio
- Just seeing what's out there?

Let’s Talk About You

Strategy

Which **backup solution(s)** are you using today?

Are backup copies sent **offsite** for DR?

How often do you **test** your backups?

In the event of **ransomware**, what would recovery look like for you today?

Are there **compliance standards** or business requirements you and your clients need to hit?

Environment

Which **data and applications** do you need to protect?

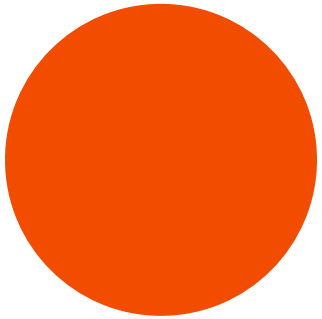
How many **locations** do you manage?

Key employees with **roaming laptops**?

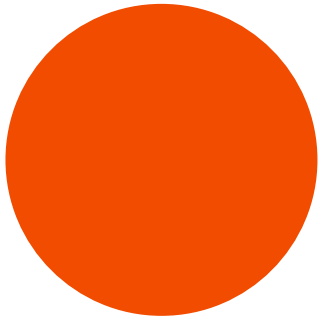
Are you using or planning to migrate to **public cloud** like Azure, or AWS?

Tell me about your **purchase process** for a solution like this one?

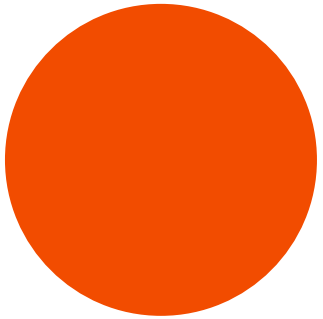
What Actually Causes Downtime?



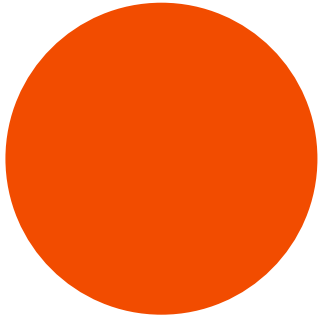
Ransomware / Malware
Bad Actors



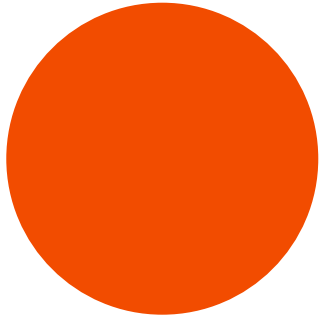
Angry Employee



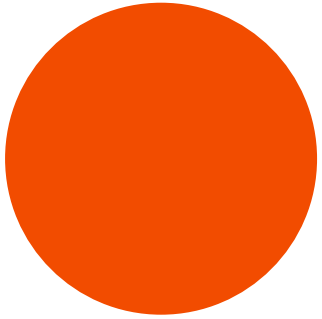
Accidental Deletion



Malicious User



Hardware Failure



Software Provider
Failure

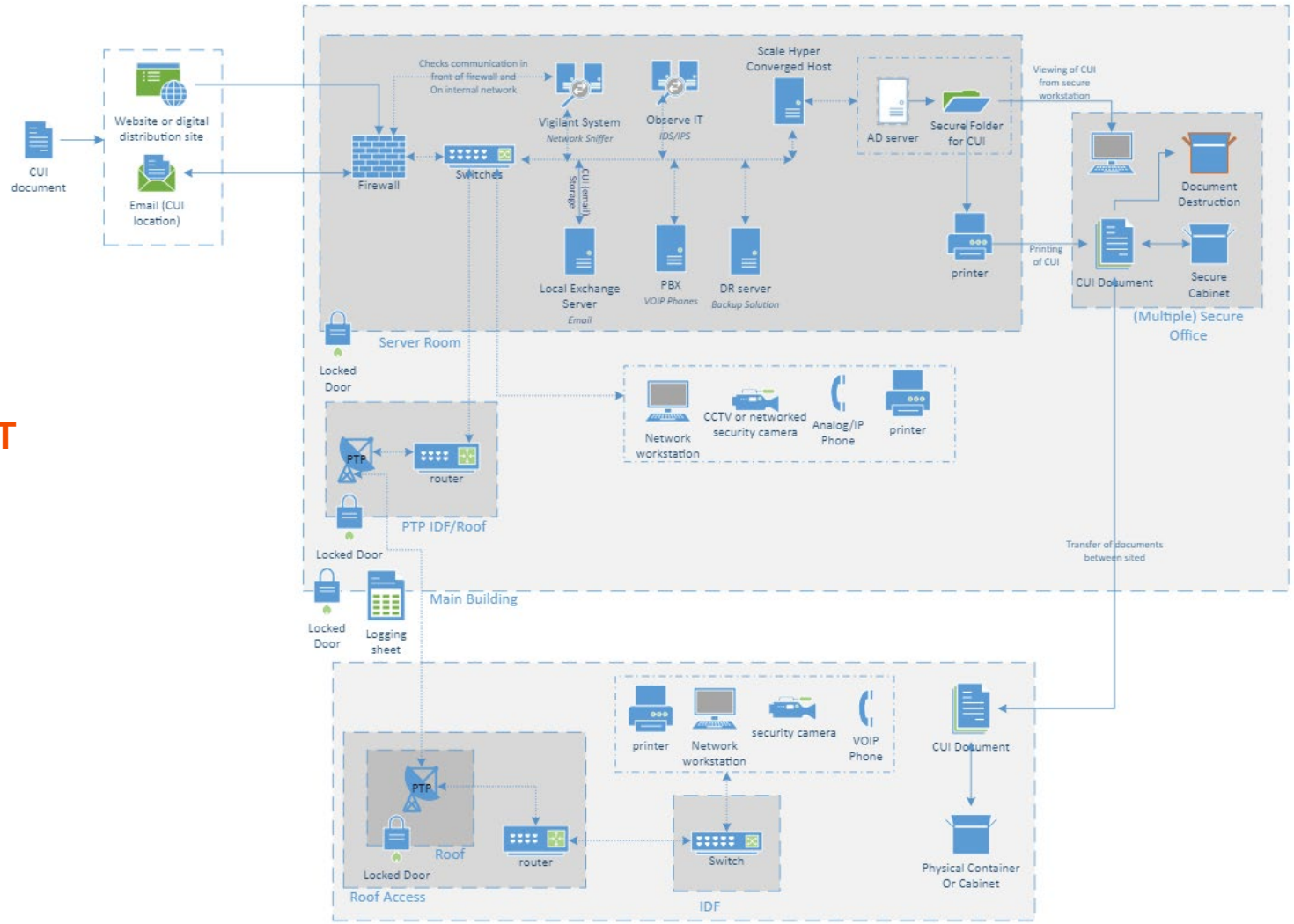
Identifying critical versus non-critical data

SOME QUESTIONS TO ASK REGARDING OUR DATA

- **What is my most critical data?**
  - Take the time to identify all critical records, documents, databases, payroll, accounting, financial databases, public safety data, court data, utility billing, 911, and any other mission critical systems.
- **Where does that data live?**
  - Where is that data actually housed? Is it on local servers in your office? Is it stored on individual computers? Is it stored on thumb drives or external hard drives? Or is it accessed over the internet?
- **Who has access to it?**
  - Is the data stored on centralized servers? Is the access controlled by active directory? Does the data live on someone's individual computer or in a cloud storage application?

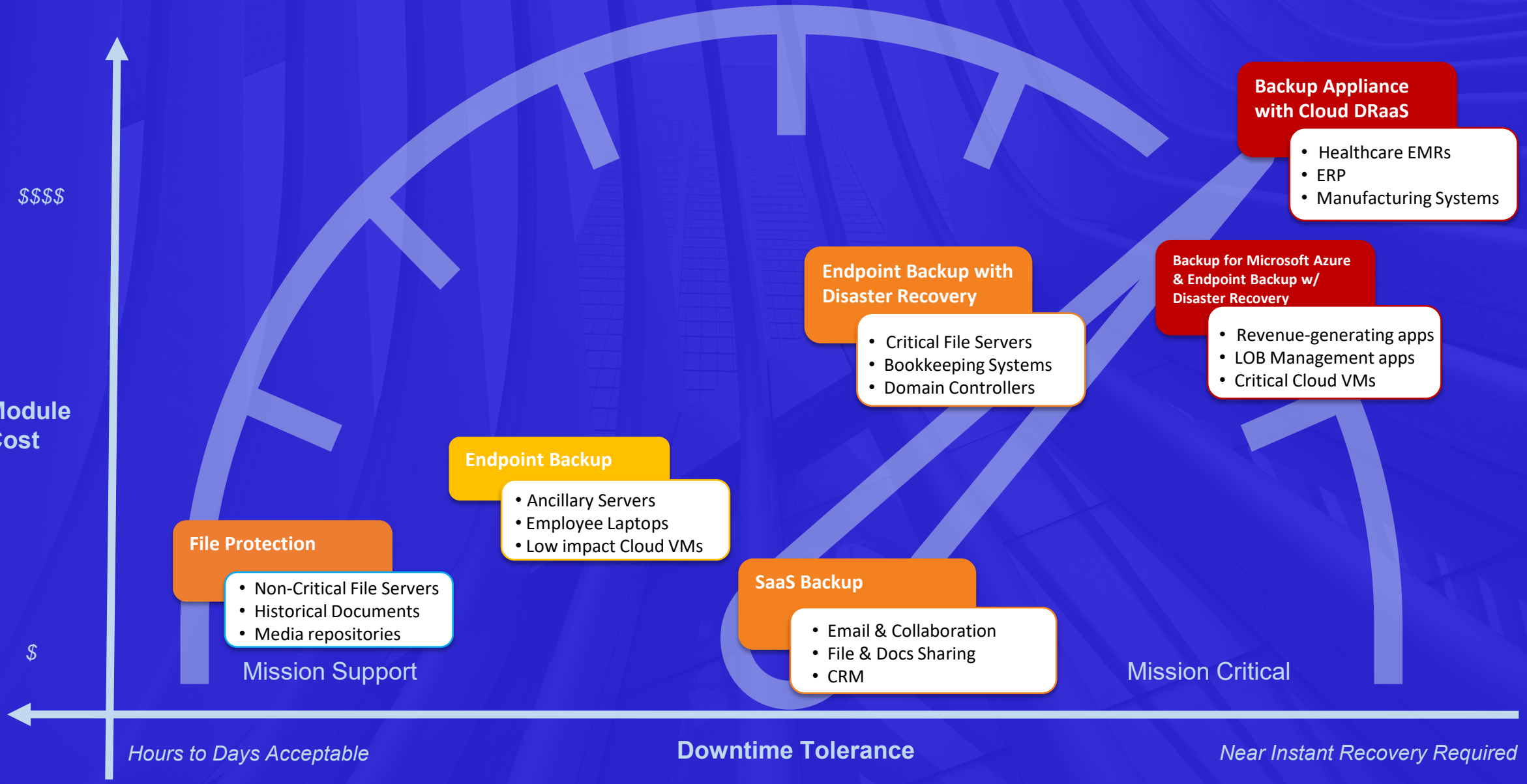
Identifying critical versus non-critical data

MAPPING OUT WHO & WHAT ACCESSES YOUR CRITICAL DATA NEEDS TO BE PROTECTED:

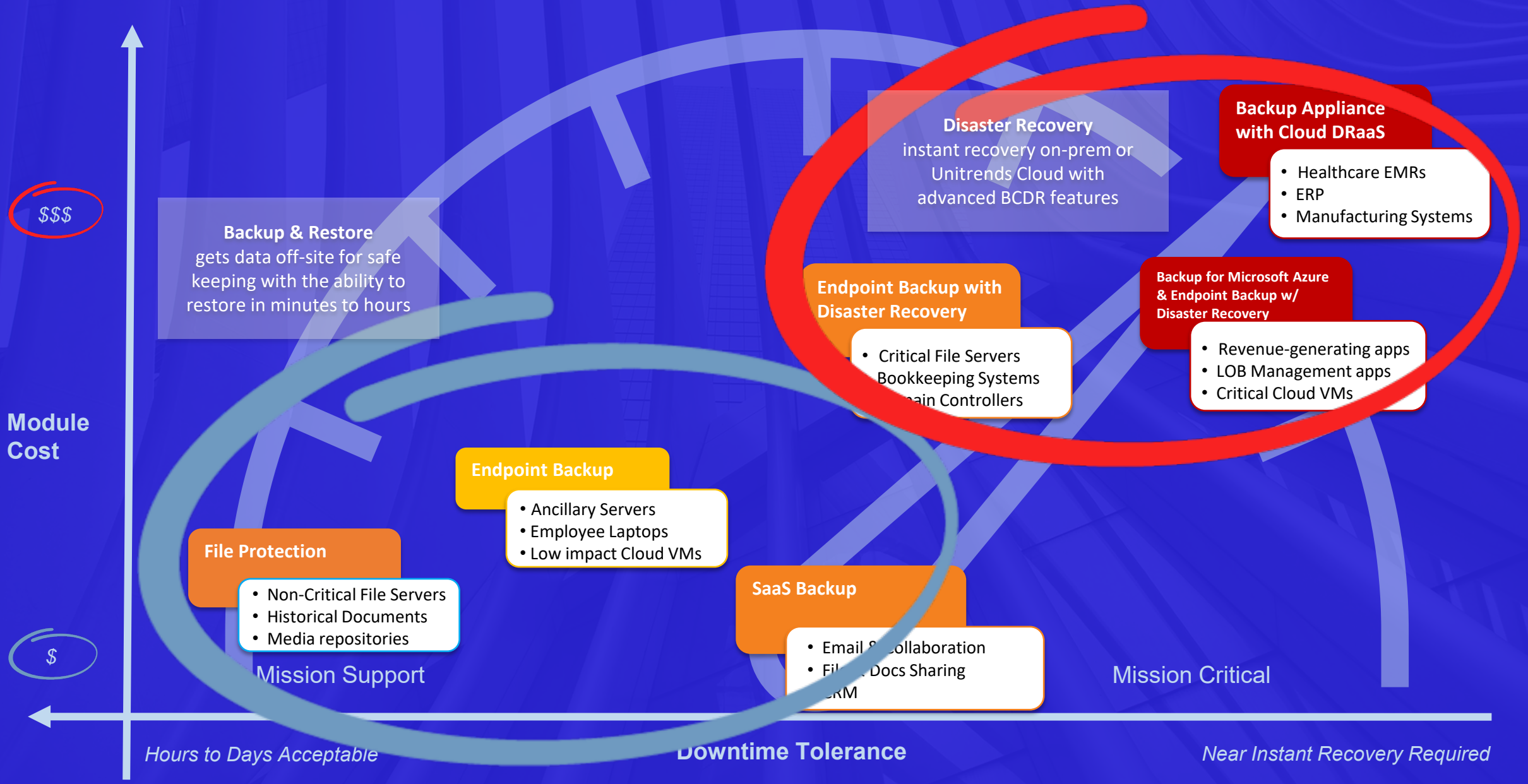


Data Protection for Every Use Case

Data Protection for Every Use Case



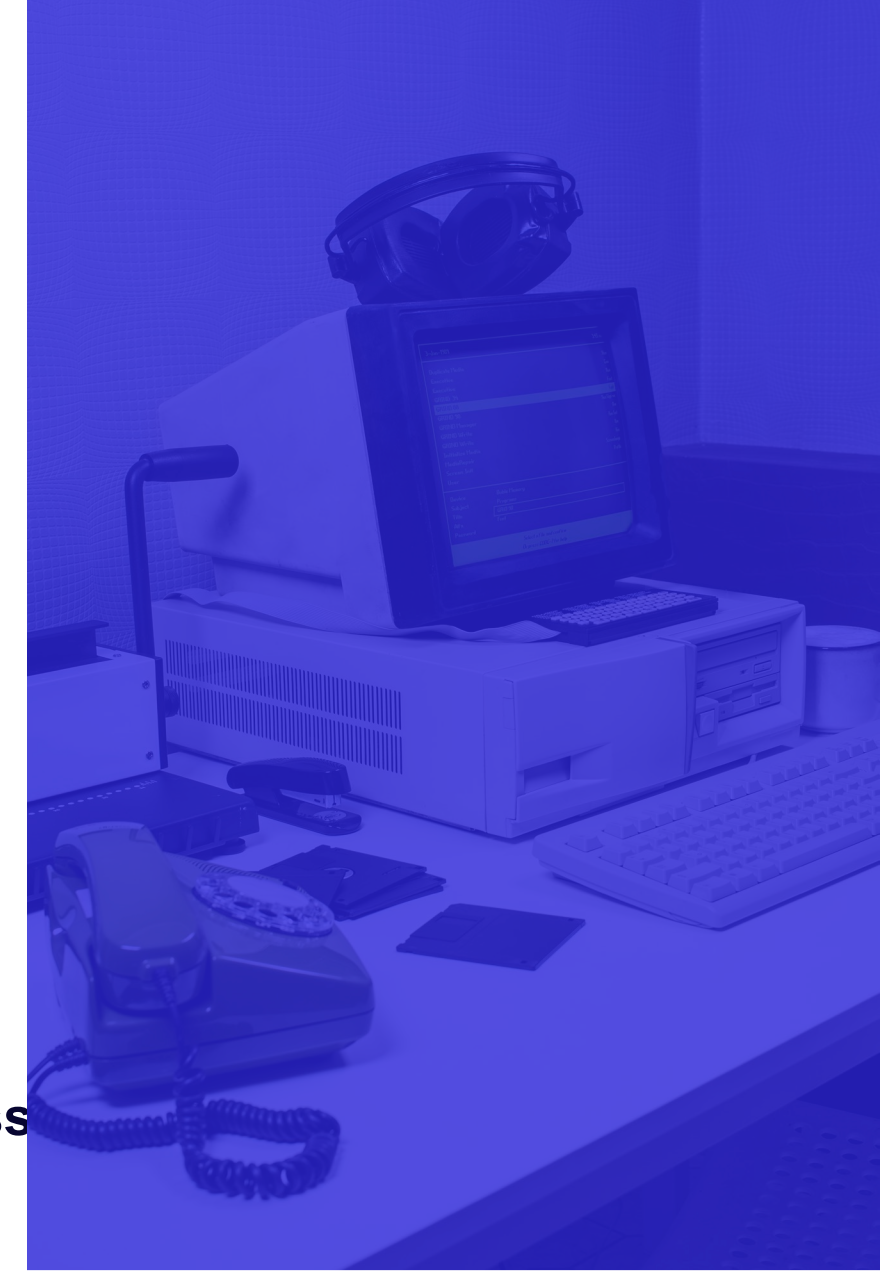
Data Protection for Every Use Case



Assessing your current data backup situation

HOW AM I CURRENTLY BACKING UP MY DATA? WHAT METHOD AM I USING:

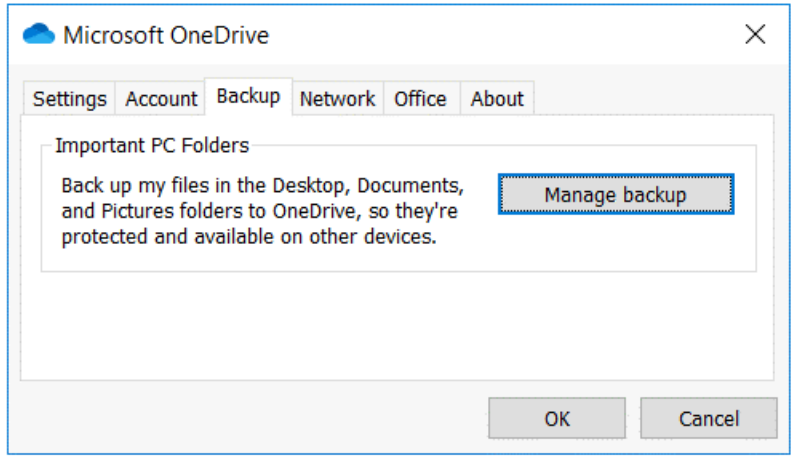
- **Backup Methods**
  - Tape Backups
  - External Hard Drives / Thumb Drives
  - Alternate Server Replication
  - Cloud Data Backup Solution Only
  - Backup Appliance with a Backend Cloud Storage
  - Software & Application Backups
  - OneDrive or Google Drive Syncing – Is this really a backup?
- **The method you choose will affect the quality, thoroughness and certainty of your data backup**



Assessing your current data backup situation

I HAVE ONEDRIVE OR GOOGLE DRIVE SETUP – THAT SHOULD BE ENOUGH RIGHT?:

- **Synchronization vs Backup Methods**
  - Files sync'd to the cloud within seconds
  - If your local hard drive is damaged this can be very helpful and accessible
  - Is versioning enabled – This is necessary
  - Retention periods & Version history
- **What happens if there is a ransomware event and I am using OneDrive or Google Drive?**
  - Potential for encrypted data to be synchronized to the cloud and overwrite good data
  - If ransomware changes extension and not file name you might be ok. (Ex. Doc1.doc to Doc1.doc.ransom)
  - If file names are changed (Ex. Doc1. doc to sdf6548dsd.ransom) then you are in trouble – There is no bulk restore function
  - Extremely time confusing and extremely lucky if you can restore in the case of ransomware
    - No chance if versioning is not enabled



Assessing your current data backup situation

HOW OFTEN IS MY DATA BACKED UP?

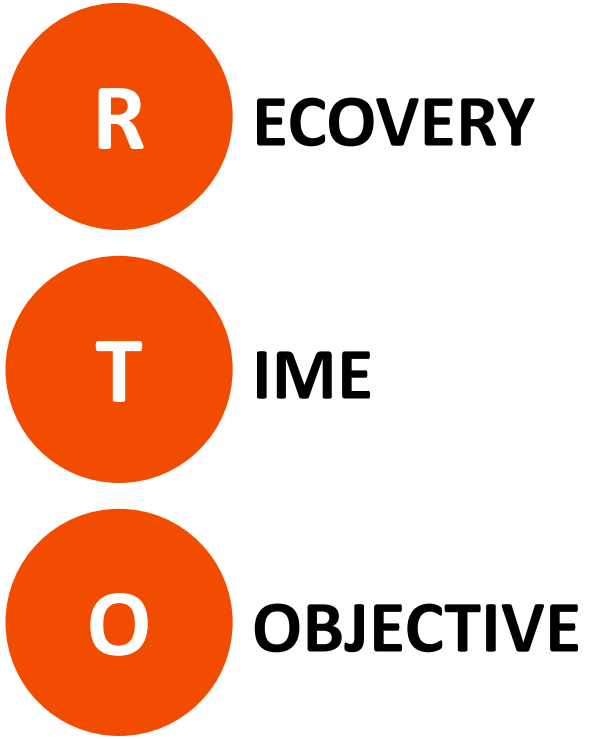
- Continuously? Hourly?
- Daily? Weekly?
- Monthly? Irregularly?

- The frequency (or lack of frequency) will affect how much data you back up and if you will be able to recover critical data after an incident or disaster.

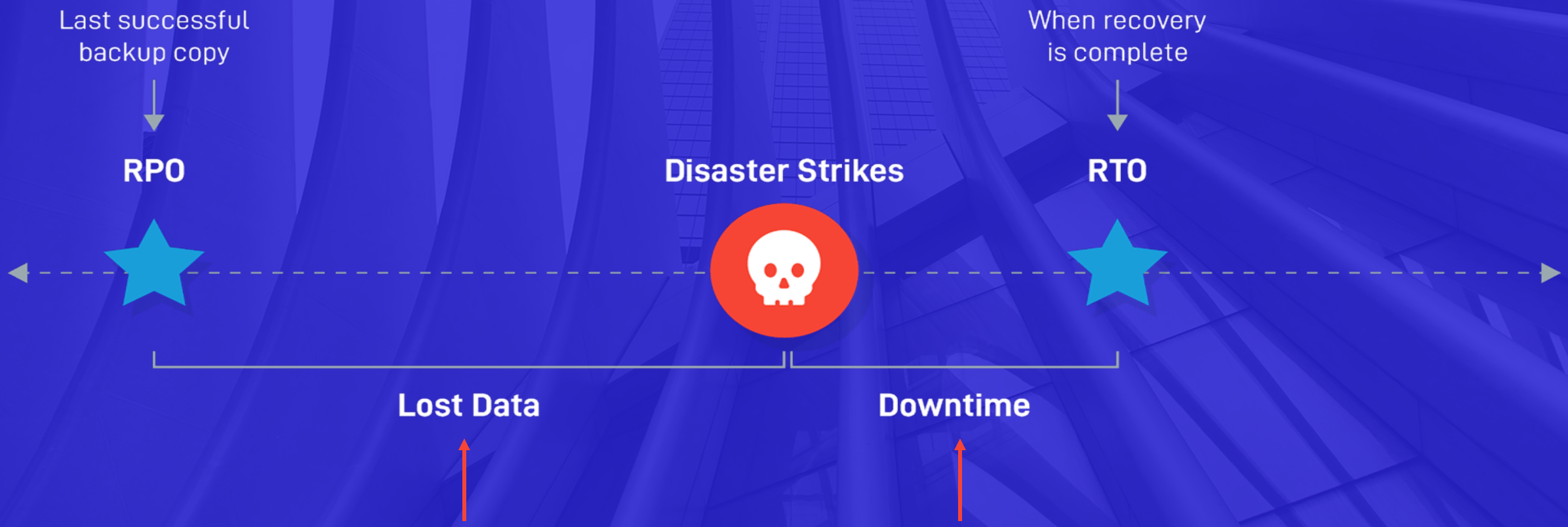
Assessing your current data backup situation

HOW FAST CAN YOU RECOVER?

- **What is our RTO (Recovery Time Objective)?**
- **Different methods will lend themselves to different recovery speeds**
  - Think about how long you can be without access to your data – If it took two months to recover your data, would that be acceptable?
  - Restoration times are not the same as backup times
    - Backups can take a few minutes to complete, but hours or days to restore
- **Think about the critical functions and what services need to be up first – Creating a list of priority services is critical to share with your IT team**



The Fundamentals of Business Continuity



Assessing your current data backup situation

HOW MUCH DATA CAN I AFFORD TO LOSE?

- **What is our RPO (Recovery Point Objective)?**

RPO

Recovery Point Objective

- **If an incident occurs, at what point can you pick up as if nothing happened?**
  - Would yesterday be acceptable?
  - A week or two ago?
  - Three Months Ago

- Knowing your recovery point is very important as it can impact the amount of data you permanently lose in a disaster.
- Think also about how long a malicious actor may have access to your environment – Does your recovery point objective cover the dwell time?

Quick Response is Key

The average time an attacker has to "dwell" in an environment before detection is somewhere between 11 and 24 days

Can you recover your onsite data backups quickly?

LOCAL ONSITE DATA IS CRITICAL:

- **Recover your data within minutes:**
  - If you have data backup servers (appliances) onsite that replicate data from your primary servers, then they should be able to take over quickly if a server fails. Conversely, more manual data backup solutions such as an external hard drive or tape may take much longer to restore.
- **Works continuously and automatically:**
  - An onsite data backup server should back up your data throughout the day without you having to do anything. Again, manual solutions such as an external hard drive often require human intervention. If someone gets busy or forgets to plug it in, then you are not prepared for an incident.
- **Does not require internet access:**
  - If you rely only on an online data back up solution, the you will not be able to access critical data if there is an internet outage. While offline, you can still restore and access data onsite such as your payroll application.

Make sure your offsite data backup allows quick recovery

WHAT DOES YOUR OFFSITE DATA BACKUP LOOK LIKE:

- **Do I have an offsite data backup component?**
  - If not, you need to address this component as soon as possible. Otherwise, you don't have a way to recover from a disaster – Whether it's a natural disaster, ransomware, or a water emergency.

- **What does it mean to have my data offsite?**
  - Offsite does not mean in the trunk of the car – Offsite means that the data lives far, far away. The data needs to the be regionally separated from where the local data lives.

- **How long would it take to me to recover my data?**
  - If your offsite component leaves you with uncertainty about the amount of time it will take to recover, or if the recovery time is weeks or months, then you need a new solution. With internet access, you should be able to access your data within hours after a disaster.

Offsite backup necessities

DOES YOUR OFFSITE DATA BACKUP INCLUDE OFFSITE LOG RETENTION:

Used for evidence related to cyber incidents.

Without this data, you will be unable to analyze the full nature of a cyberattack, deduce the source of the attack, and remediate effectively.

- Can we see how our data has been impacted?
- Has our critical data been exfiltrated?

What Does Offsite Mean when I am using OneDrive or Google Drive?

WHY DO I NEED A BACKUP OF MY CLOUD STORAGE?:

- **Both OneDrive and Google Drive have limitations that need to be addressed**
  - Bulk restore capability – Both Google and M365 are limited in their restore capability
  - Incremental backups – The ability to restore from point in time
  - Infinite retention periods – Both systems have limited time retentions
  - Infinite storage capacity – Both systems are limited to 1TB
  - Immutable options – Backups cannot be touched or alerted
  - Backup everything – SharePoint, Mailboxes, OneDrive, Etc.
- **Not having a backup of your data stored in the cloud could lead to potential loss of data and will lead to extended restore times if there is a ransomware event**

Don’t forget about your other cloud apps too!

Testing your data backup solution

WHAT DOES OUR DATA BACKUP TESTING PROCESS LOOK LIKE:

- If you test your data backup solution, then you know if you can recover, how fast you can recover, and if any critical data is missing when you recover.

- If you don't test, you may experience a horrible "surprise" after an incident or disaster when your data recovery is incomplete or doesn't work at all.

    - **What about my employees working at home? Is the data they are working on backed up?**

Incident Response Planning

WHAT DO WE DO IF WE HAVE TO RESPOND TO A BREACH OR DATA LOSS?:

Developing a plan detailing how you respond to a cyberattack will help you react to an incident with "muscle memory"— like a fire drill.

Covers:

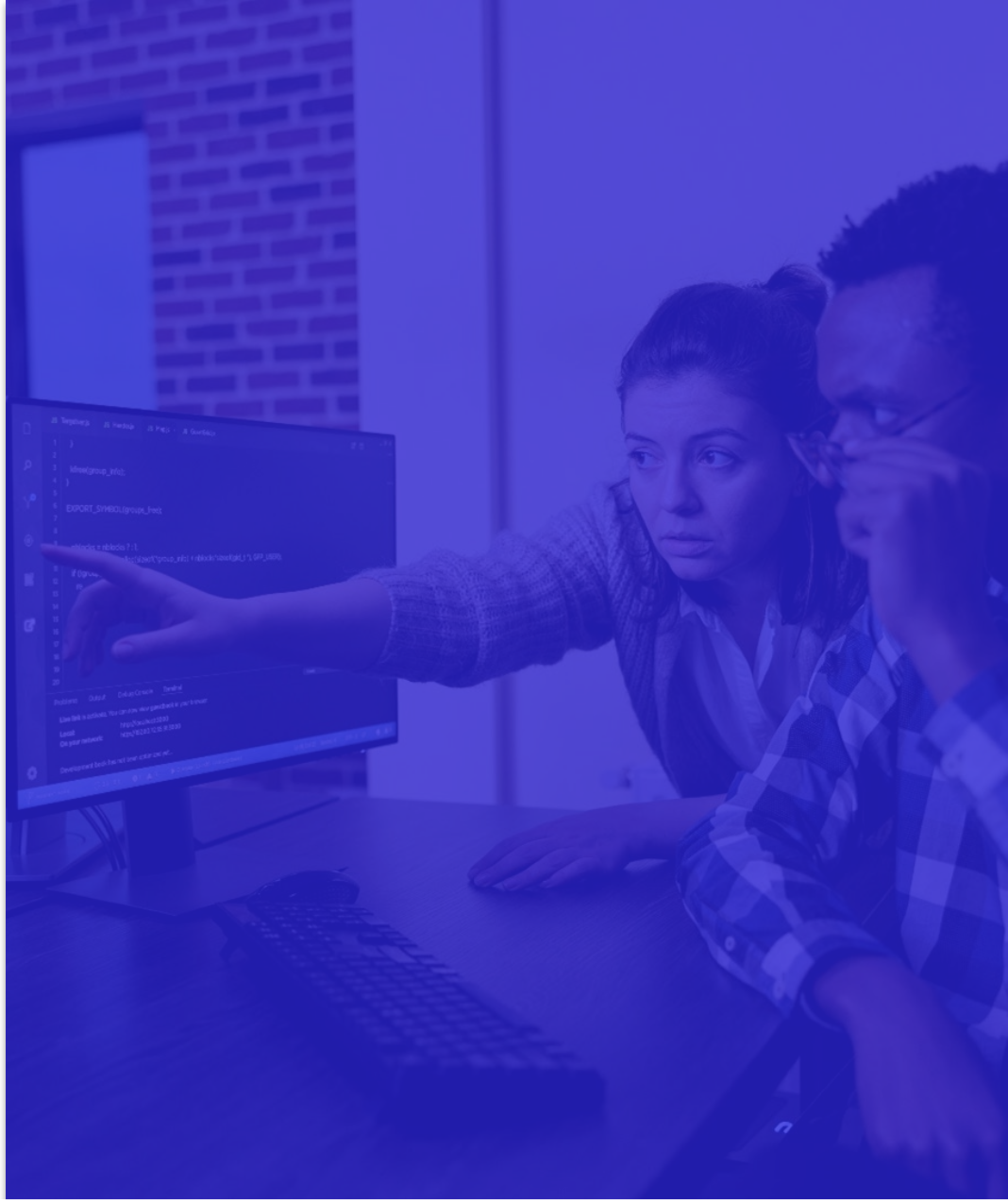
- How you will respond to a cyber incident
- Who will respond
- Planning and testing the plan long before an incident happens

Make Time to Plan

PLANNING IS CRITICAL TO THE SUCCESS OR FAILURE OF A CYBER EMERGENCY:

- Work with your IT team to identify critical systems, data, & process
- Not all data and systems have the same value to your organization – understand the priority
- ***Your incident response plan MUST be written down***
- Ask your team to identify who will do what and how long it might take in an emergency scenario
- The “who” might not always be in your organization – you may need to reach out to your cyber insurance or authorities to start the process

How will I ensure my team is ready? Did we think of everything?



Is My Team Ready?

ONLY WAY TO KNOW IS TO TEST YOUR PLAN:

- Do tabletop exercises with your team – you come up with the scenario and have your team run through it
- Document your results so you can update the plan as needed
- Don’t just talk through it – do it! Test monitoring and restore capabilities. Ask for evidence so you can verify the effectiveness and timing
- Review the results with the team – Let them know that any failures represent an opportunity to improve and reduce stress in the case of a live emergency

Is My Team Ready?

WHAT ABOUT MY CLOUD APPS?:

- Your vendors should be asked to test their backup and disaster procedures as well
- Treat them the same way you would your internal teams and ask for their testing results
- Review the results with the team – Let them know that any failures represent an opportunity to improve and reduce stress in the case of a live emergency

Ask them for security documentation as well

Data Backup Essentials

Identify

- ❑ What do we need to backup
- ❑ Who has access to it
- ❑ What devices have access to it
- ❑ Where does that data live

Assess

- ❑ What would it cost if we lost it
- ❑ How much can we lose
- ❑ How long can we be without the data
- ❑ How are we backing it up now
- ❑ Where are we backing it up now

Test / Validate

- ❑ Does our backup work
- ❑ Did the restore capability meet our expectations
- ❑ Do we have backups of all of our data (Apps too)
- ❑ Does our team know how to respond in case of emergency
- ❑ Is that process written down

Some Closing Thoughts

- Implementing all of the steps in the plan will not make your backup and disaster recovery efforts bullet proof, but if you follow the checklist it will set you up for the best chance to succeed when the emergency strikes
- Start by reviewing your current data backup plans and procedures as soon as possible
- Make the time to plan – Write that plan down (A lot of times this is the hardest part)
- Don’t put everything on the IT team – this is an organization/agency wide endeavor
- Test the plan once it is in place (Ask your vendors for their test results as well)
- Lastly, we all have similar challenges – Ask your peers about their plans and experiences