TRUADVANTAGE POWER-HOUR

WEBINARS & WORKSHOPS

Disaster Recovery Readiness

Powered by Barracuda

Today's Presenter

Kyle Marsan

Senior Systems Engineer,
Barracuda MSP

About truadvantage

award-winning • IT & Cybersecurity

TruAdvantage is a Bay Area based, award-winning IT firm that specializes in managed IT, managed Cybersecurity, cloud solutions and strategic IT planning. Our passion is to bring enterprise-level productivity, simplicity, scalability, and security to over 100 small to medium businesses who have chosen us as their IT partner.

What Sets Our Managed IT (totalCARE) Apart & Impacts Our Clients' Success?

- **MSP501** Ranked #1 in Bay Area, #9 in California
- **Google** 200 Plus Reviews
- **CRN** MSP500 Award
- **Expertise**.com Top IT Bay Area
- **MSSP** Top Security Award
- **Clutch** Top IT & Cybersecurity California
- **UpCity** Excellence Award San Jose
- **CloudTango** Top MSP Bay Area
- **Great Place to Work** Certified

truadvantage
award-winning • IT & Cybersecurity

Free to our Audience:

- Currently, we are offering a completely Free Security Audit and Penetration Test. Take advantage of it here: https://www.truadvantage.com/cyberaudit/
- Please send your questions to Kayvan@truadvantage.com
- To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: www.truAdvantage.com/QuickChat
- Join our future Power-Hour Webinars and Workshops: TruAdvantage.com/power-hour

truadvantage
award-winning • IT & Cybersecurity

You Have More Data to Protect Than Ever

- [x] Financial Data
- [x] Payroll Info
- [x] Email Systems
- [x] Software Programs
- [x] Business Applications
- [x] Customer Data
- [x] Employee Information
- [x] And More!

The Data Loss Threat

The Cost of Downtime

Financial Impact

A report by Statista estimated the average cost of downtime is between $8,220 and $25,620 per hour.

Brand Reputation

A single downtime event can put your organization's reliability and reputation at risk.

Loss of Data

60% of small businesses that are victims of a cyber attack go out of business within six months.

Source: https://www.ibm.com/downloads/cas/A856LOWK
Source: https://www.fundera.com/resources/small-business-cyber-security-statistics

High Risk Industries

Downtime for these industries comes at a much higher price tag...up to $5 million per hour according to ITIC research.

Finance

Healthcare

Government

Manufacturing

Communications

https://www.ibm.com/downloads/cas/A856LOWK


POLL ALERT!
Do you have an incident response plan in case of a breach?
Let us know using the poll launched on your screen
for a chance to win some Barracuda MSP Swag!

You Have More Data to Protect Than Ever

You can't predict a disaster,
but you can prepare for it.

1. Prevent unnecessary risk

2. Prepare for what you can't control

What will you do to reduce your vulnerability?

1. Preventing Unnecessary Risk

5 Things You Can Do to Reduce Unnecessary Risk

Encrypt Data to Hide It From Prying Eyes

Educate Users on Virus and Malware Prevention Best Practices

Create BYOD Security Policies and Protect Mobile Devices

Implement Strong User Access Control

Use Off-Site Cloud Backup For Business Recovery

Encrypt Your Data

AT REST, IN USE, AND IN TRANSIT

Types of Encryption:

- Application Encryption
- Database Encryption
- E-mail Encryption
- File and Folder Encryption
- Full Disk Encryption
- Network Encryption
- Cloud Application Encryption (Sophos)
- Removeable Media Encryption

Educate Your Team on Virus and Malware Prevention Best Practices

For Example

Resist the temptation to download attachments or click links in emails from unfamiliar senders.
Refuse to surrender passwords or

sensitive info via internet.

BYOD Security Policies to Protect Mobile Devices

Your BYOD strategy should outline:

- Which mobile devices to support
- Relevant compliance requirements by industry or jurisdiction
- How to parse personal information to prevent easy capture
- Data plan management, payment, and tracking
- Options for automated and/or self-service configuration

Implement Strong User Access Controls

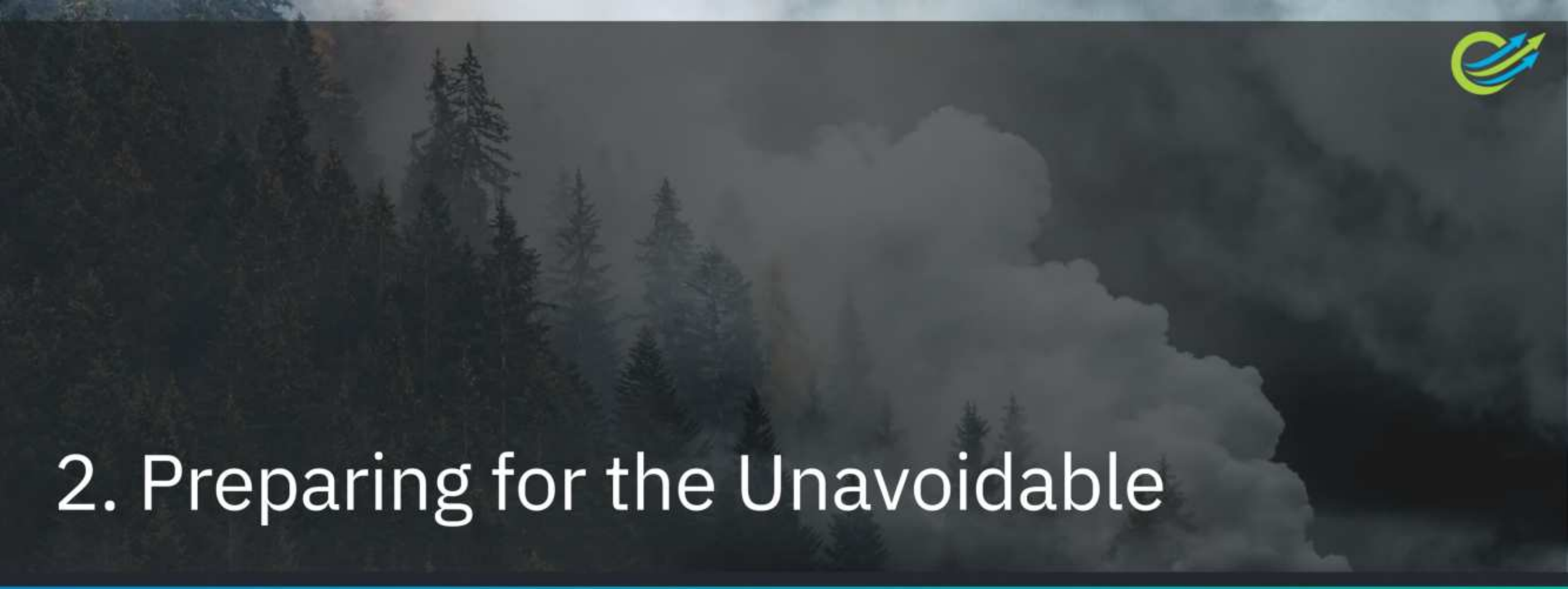
User education and BYOD policies are most effective when complemented by a strong user access control framework.

- Minimize unrestricted and unnecessary access
- Helps protect against less sophisticated types of malware

Use Off-Site Cloud Backup for Business Recovery

- Minimize the risk of data loss
- Scalable, and can’t be lost, stolen, or damaged
- Data can be restored anytime, anywhere
- Military-grade encryption maximizes security
- Quick resumption of operations

Important step in disaster preparedness

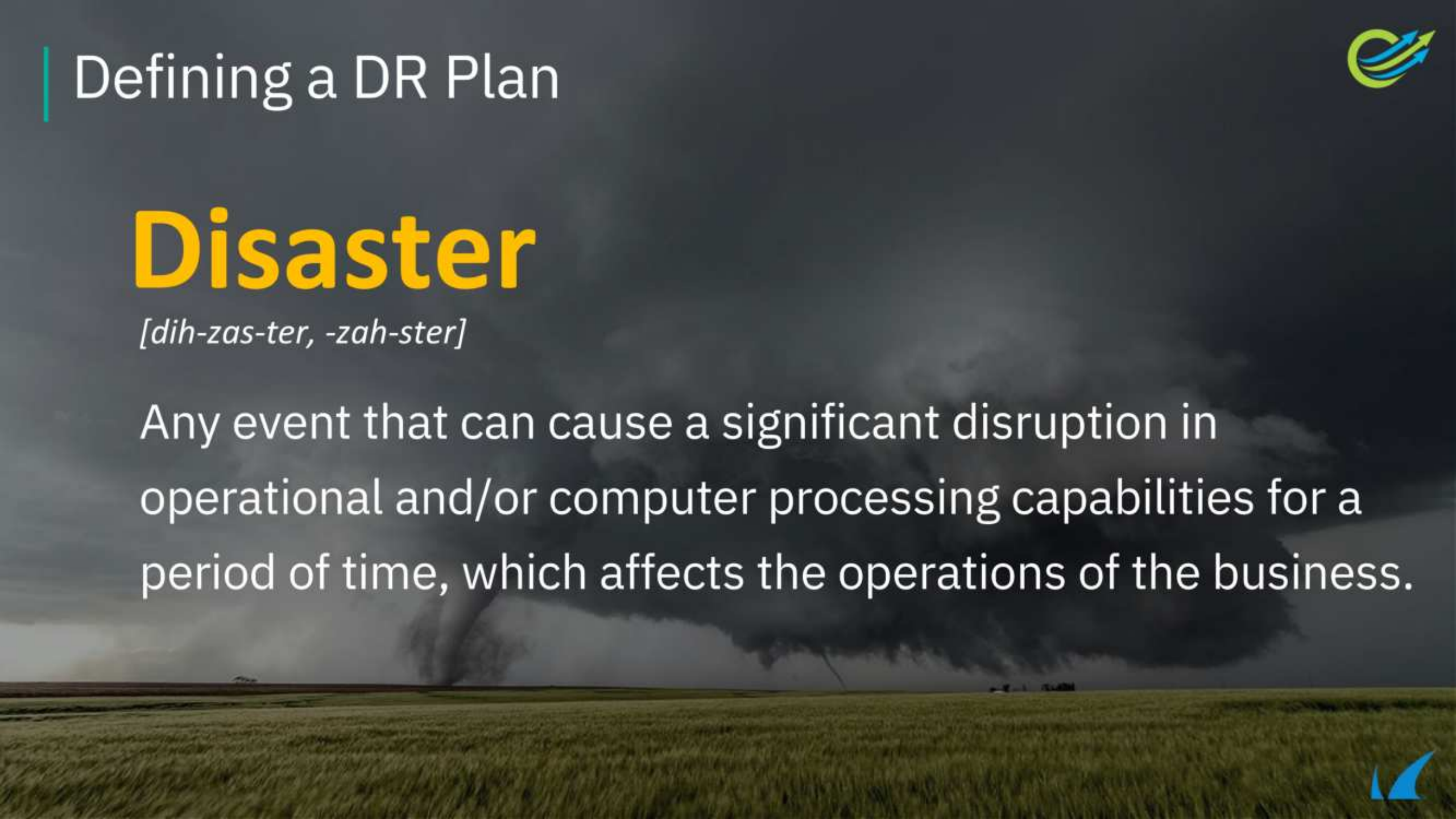


2. Preparing for the Unavoidable


POLL ALERT!
How confident are you in your organization’s ability to recover from a cyber attack?
Let us know using the poll launched on your screen
for a chance to win some Barracuda MSP Swag!

1 “Barracuda Networks Survey,” 2017

Defining a DR Plan



Disaster

[dih-zas-ter, -zah-ster]

Any event that can cause a significant disruption in operational and/or computer processing capabilities for a period of time, which affects the operations of the business.

Key Elements at Risk in a Disaster

PEOPLE

FACILITIES

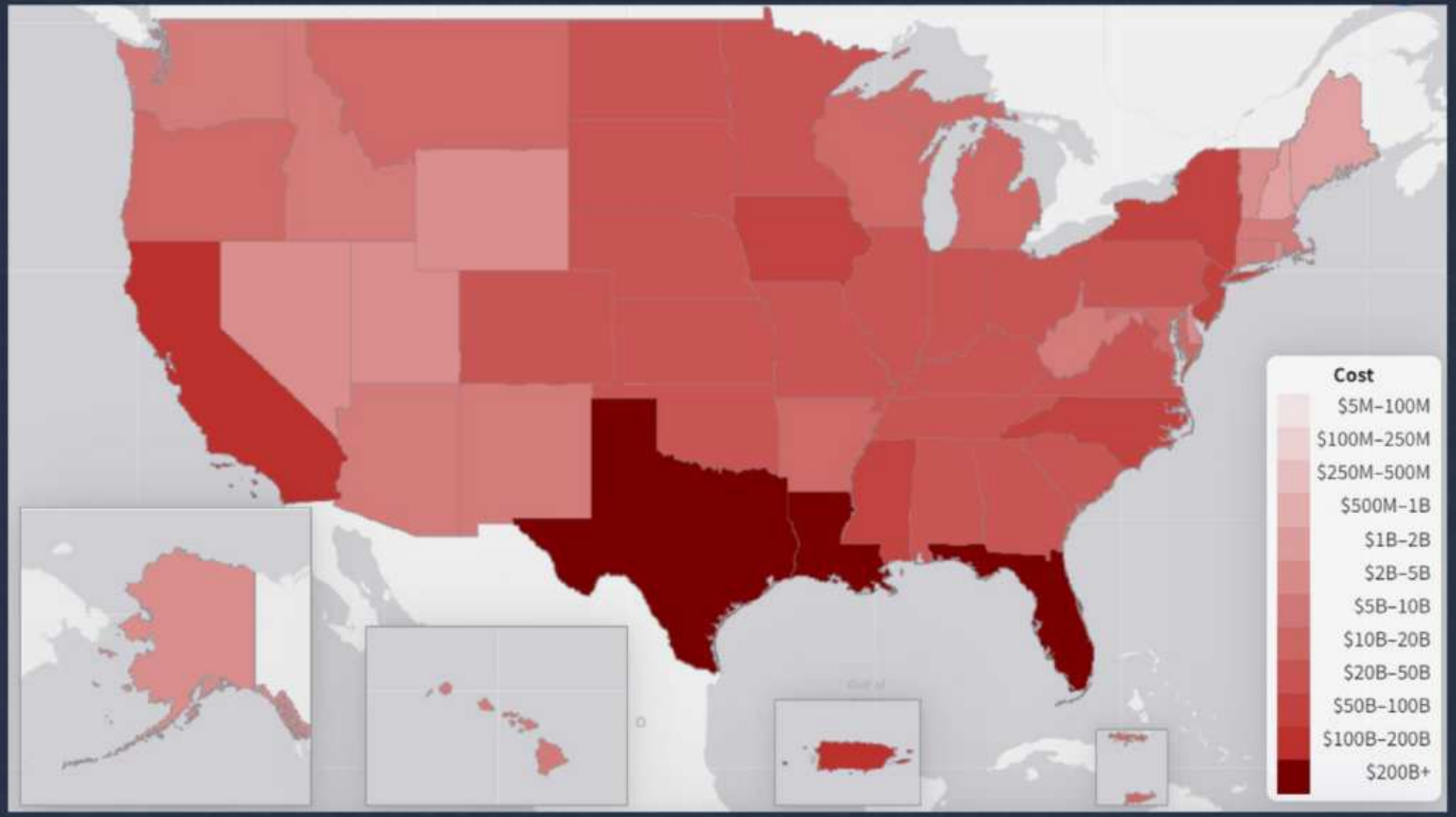
EQUIPMENT

DATA

In 2022, the U.S. experiences 18 separate weather and climate disasters costing at least 1 billion, with a total price tag of over $165 billion dollars.

Source: https://www.climate.gov/news-features/blogs/2022-us-billion-dollar-weather-and-climate-disasters-historical-context

1980-2022 Billion Dollar Natural Disasters in the U.S.



Source: https://www.climate.gov/news-features/blogs/2022-us-billion-dollar-weather-and-climate-disasters-historical-context

EVERY ORGANIZATION NEEDS A PLAN

Key Steps in Creating a Disaster Recovery Plan

1 Establishing a Planning Group

Include representatives from each role in the organization, along with their responsibilities

2 Risk Assessment

Assess the impact to each role in the organization:

- Personal Impact
- Customer Impact
- Lost Revenue
- Lost Data
- Lost Productivity

3

Application Prioritization

CLASSIFICATION		DESCRIPTION
1	**Mission Critical** • Order Processing or Email System	• Mission Critical to accomplishing the mission of the organization Can be performed only by computers No alternative manual processing capability exists Must be restored within 36 hours • Critical in accomplishing the work of the organization
2	**Critical** • Payroll Processing	• Primarily performed by computers • Can be performed manually for a limited time period • Must be restored starting at 36 hours and within 5 day • Essential in completing the work of the organization
3	**Essential** • Human Resources File Server or Marketing Data	• Performed by computers • Can be performed manually for an extended time period • Can be restored as early as 5 days, however it can take longer • Non-Critical to accomplishing the mission of the organization
4	**Non-Critical** • Access to Historical Data	• Can be delayed until damaged site is restored and/or a new computer system is purchased • Can be performed manually


POLL ALERT!
What is the biggest challenge your organization faces in implementing an effective disaster recovery plan?
Let us know using the poll launched on your screen
for a chance to win some Barracuda MSP Swag!

4 Recovery Strategies

How will you recover?:

- Where will you resume operation?
- What are the critical business processes?
- Who are your critical resources?
  - Are they available?

5

Inventory and Documentation

What do you have available and what do you need replaced?

- Equipment
  - Computers
  - Servers
  - Networks
  - Phones
- Facilities
- People
- Vendors
- Documentation

6 How Do You Know Your Plan Works?

Are all key elements in place?

Have you performed a “Disaster Drill?”

Does it meet your expectations?

7 Implementation

Verify everyone understands their role

Ensure the plan includes anything learned from the drill

Review the drills and ensure they meet the expected results

Best Practices Put to the Test

- Three-alarm fire just before the busy season
- Servers back up and running under one day
- Business met its next payroll without skipping a beat

When the fire struck, we were entering our busiest season of the year. Had all of our data been lost, it would have been very difficult to get our business back up and running.

~ JEFF WARGO, GENERAL MANAGER,
EASTERN YACHT CLUB


POLL ALERT!
Which aspect of disaster recovery is a priority for your organization?
Let us know using the poll launched on your screen
for a chance to win some Barracuda MSP Swag!

Key Takeaways

Back It Up

Incorporate the Cloud

Choose the Right Technology Partners

Prepare, Prepare, Prepare

Create a DR Plan & Test

TOP 10 ITEMS SMBs NEED TO BACK UP

1. Line of Business (LOB) Application
2. Emails
3. Client Records
4. Virtual Machines
5. Point of Sale Systems
6. Financial and Accounting Applications
7. Customer Relationship Management (CRM) Software
8. Electronic Medical Record Systems
9. Servers and Workstations
10. Files and Folders

Next steps

Contact your MSP to:

- Assess where your organization's vulnerabilities exist and develop or tweak your disaster recovery plan.
- Create an ideal schedule for ongoing testing of your disaster recovery plan in case of a breach.

Resources

Calculating the Hidden Costs of Data Loss

Find out how much data loss could really cost your business – especially if you're not prepared.

The Cost of a Data Breach

The average cost of a data breach is $4 million dollars[1]—and the average cost per record is $1581. Depending on your vertical, the cost per record can be more or less.

Average: $158
Healthcare: $355
Retail: $172
Transportation: $129

How many records do you have? _____

_____	X	_____	=	$ _____
Number of Records		**Cost Per Record for Your Industry**		**Cost of a Data Breach**

The Cost of Downtime

The average cost of downtime is $8,662 per minute[2].

How quickly do you respond to an outage or identify when it happens? _____

How long does your average downtime last? _____

Sources:

1.) https://www-03.ibm.com/security/infographics/data-breach

2.) https://italerting.com/state-of-incident-management%20

The Disaster Recovery Checklist

Prepare for Disasters When They Strike

Disasters can happen at any time. Whether preventing man-made disasters, such as a malicious attack, or protecting your business from natural disasters like a hurricane, you want to be prepared to ensure your business stays up and running with as little downtime as possible. Here's a checklist to help you build your disaster recovery plan.

Business Disaster Recovery Checklist

- ☐ Assess, prioritize, and determine
  - ☐ Assess which assets are necessary for recovery
  - ☐ Prioritize the assets that needs to recover
  - ☐ Determine steps to recover assets based on priority
- ☐ Make a list of responsibilities
  - ☐ List the associated tasks
  - ☐ Determine who is involved during the recovery process
  - ☐ Assign responsibilities from the DR checklist
- ☐ Test the recovery plan
  - ☐ Validate if the recovery plan is feasible
  - ☐ Run training drills
  - ☐ Test your backups
- ☐ Review and evaluate
  - ☐ Review and evaluate often to ensure that all aspects of your plan is current to your business needs
- ☐ Establish recovery goals
  - ☐ Identify critical systems
  - ☐ Prioritize recovery order
  - ☐ Determine the recovery location
  - ☐ Establish Recovery Time Objectives (RTO)
- ☐ Identify recovery methods
  - ☐ Recovery methods can vary depending on the critical systems. Apply the right backup methods, such as bare metal, full system, file-based, virtual, localized, or cloud-based to ensure desired recovery methods for each critical system.
- ☐ Test the backups
  - ☐ Frequently test backups to identify potential issues
  - ☐ Validate the recovery to restore to designated location and methodology
- ☐ Review and document
  - ☐ Provide a postnotum review to both tests and post disaster and look for room to improve
  - ☐ Document any changes to the recovery plan

Free to our Audience:

- Currently, we are offering a completely Free Security Audit and Penetration Test. Take advantage of it here: https://www.truadvantage.com/cyberaudit/
- Please send your questions to Kayvan@truadvantage.com
- To have a quick chat regarding this webinar, our IT services, or our free IT Audit please schedule a quick chat here: www.truAdvantage.com/QuickChat
- Join our future Power-Hour Webinars and Workshops: TruAdvantage.com/power-hour

truadvantage
award-winning • IT & Cybersecurity


Thank You