Technical Business Continuity

Bottom Line:

We help manufacturers avoid business disruption and financial losses from downtime and data threats caused by misallocation and criminal enterprises.

Background:

Manufacturers have realized an increasing need for business continuity. This use case focuses on adjustments associated with continuity of critical business systems.

To start a friendly dialogue, visit our website or call (614) 408-0900.

Common Problems

- **Data loss and system failure have an immediate impact on your business.** Protecting data within your facilities is hard enough. Now, work from home systems are creating data loss problems.

- **Uptime and availability are expectations within IT.** Downtime events can impact revenue, the business reputation, and restful sleep at night.

- **ERP, reporting services, document imaging, file shares, and email contain critical information for day to day operations.** Data loss through deletion, corruption, and/or ransomware can cause significant service outages, anxiety, productivity loss, and angry executives.

How We Solve Common Problems

- Independent data backup with automated verification **alerts to success and failure status so you can manage the exceptions.**

- **Backup + Disaster Recovery equals business continuity.** Recover one or all of your systems in a geo-dispersed cloud within hours instead of weeks or months. Employees can connect via VPN to your systems, anywhere in the world.

- **Human factors and hardware failures can cause downtime.** Spin up a failed server in minutes to drastically reduce disruption, and restore with bare metal recovery.

Results:

Manufacturers are experiencing an increased frequency of business disruption. Many businesses realize that they are not prepared, they are anxious, and they do not know where to start. Due to false claims and lack of trust, uncertainty is having a big effect on managing the business. Too many smart people assume their data is protected and later regret not verifying. **We can help you get started with your business continuity needs.**

Sample Mapping Diagram:
The following roles were identified within this business, their data backup responsibilities were noted, and their backup, recovery, and continuity concerns were documented.

Analyst

CEO

CFO

IT Dir/Mgr

Systems Admin

Auditor

Data Backup:
Protect data with block level, independent, image-based backup.

Verification:
Screen shot verification of backup image, provides automated status of success or failure.

Local File Restore:
File and folder restores from any prior image, which can also be mounted as a share.

Bare Metal Restore:
Restore your server backup image to dissimilar hardware.

Ransomware Detection:
Detecting patterns of change in specific file types, alert to suspected ransomware infection.

System Disaster Recovery:
Activate a virtual instance or your server in minutes and reduce downtime.

Three Copies of Your Local Data:
Your facility, one Tier 3 data center EST, and one Tier 3 data center MST.

Retention:
How often should we backup?
How long do we keep the backup files?

Site Disaster Recovery:
Spin up all of your servers in the cloud.
Users will have access to the systems from the Internet, anywhere in the world.

Business Continuity:
Backup + Disaster Recovery to reduce business disruption.
Meet demanding Recovery Time Objectives (RTO).
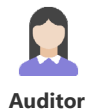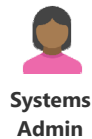Meet demanding Recovery Point Objectives (RPO).

Protection for Office 365:
Microsoft is not liable for any disruption or loss.
Granularly recover from ransomware in the cloud.
Protect and restore loss or corrupt cloud data from Outlook, OneDrive, and SharePoint.

If you need assistance, feel free to contact us at (614) 408-0900 or visit us at www.certitudesecurity.com. We can help you develop a plan and move forward with confidence.

Data Backup + Disaster Recover = Business Continuity

Blank Mapping Diagram:
Map the key roles with your business, data backup responsibilities, and backup, recovery, and continuity concerns.

Analyst

CEO

IT Dir/Mgr

CFO

Systems Admin

Auditor

Data Backup:
Protect data with block level, independent, image-based backup.

Verification:
Screen shot verification of backup image, provides automated status of success or failure.

Local File Restore:
File and folder restores from any prior image, which can also be mounted as a share.

Bare Metal Restore:
Restore your server backup image to dissimilar hardware.

Ransomware Detection:
Detecting patterns of change in specific file types, alert to suspected ransomware infection.

System Disaster Recovery:
Activate a virtual instance or your server in minutes and reduce downtime.

Three Copies of Your Local Data:
Your facility, one Tier 3 data center EST, and one Tier 3 data center MST.

Retention:
How often should we backup?
How long do we keep the backup files?

Site Disaster Recovery:
Spin up all of your servers in the cloud.
Users will have access to the systems from the Internet, anywhere in the world.

Business Continuity:
Backup + Disaster Recovery to reduce business disruption.
Meet demanding Recovery Time Objectives (RTO).
Meet demanding Recovery Point Objectives (RPO).

After you've completed the mapping exercise, contact us for assistance to review your mapping and develop a plan. Call us at (614) 408-0900 or visit us at www.certitudesecurity.com.

Protection for Office 365:
Microsoft is not liable for any disruption or loss.
Granularly recover from ransomware in the cloud.
Protect and restore loss or corrupt cloud data from Outlook, OneDrive, and SharePoint.

Data Backup + Disaster Recover = Business Continuity

Reducing the Financial Impact of Business Disruption

	Cloud Protection	Continuity	Remote Worker Continuity
Local data, application, system backup		x	
Offsite Replication		x	
Cloud based backup	x		x
Retension for years	x	x	x
Verification of backups		x	
Local file restores		x	
Cloud file restores	x	x	x
Microsoft 365 backup	x		
Ransomware detection		x	
Bare metal restore		x	x
Server Disaster Recovery locally		x	
Server Disaster Recovery in the Cloud		x	
Business Continuity		x	
Protect executive's W10 home systems			x
Protect remote workers' W10 laptops			x
Restore data to a new device		x	x
Granular file and folder restores	x	x	x
Restore applications and settings		x	x
Local applicance required		x	
Image based restore of device configuration		x	x

Inquires? Call is us (614) 408-0900 or visit www.certitudesecurity.com