Client Audit Report:

Business Continuity Scorecard

www.entechUS.com

Our Challenge

Though often confused, Business Continuity and Disaster Recovery (BCDR) and backup are not the same. While BCDR does in fact include backup, it adds two key elements: replication of your on-premise IT environment and virtualization of your business applications and services, both in the cloud.

The need for business continuity is driven by the cost of downtime caused by everything from cybersecurity threats to natural disasters. Can your business afford being down for 1-hour, 4-hours, 8-hours? If the answer is no, like most organizations, we need to work with you to define a Distaster Recovery, or better yet Business Continiuty Plan

Our Solution+

Data protection and business continuity should not be out of reach for any organization, and Entech's mission is to keep your business running; enabling you to do what matters.

Critical capabilities of include:

- Recovery Point Objective (RPO) of 15-minutes & Recovery Time Objective (RTO) of less than 1-hour
- Our AirGap technology protects your data against attackers and ransomware
- We AutoVerify checks for data corruption before backing up to limit your risk
- Unlimited storage and retention

Frequently Asked Questions+

Question: What is a BDR appliance and why is it an important part of DRBC?
Answer: A Backup & Disaster Recovery (BDR) appliance is a piece of computing hardware that's installed in your companies' network. This device becomes a target for data backups to be stored on and then this intelligent device security replicates your data to the cloud.

Question: RTO / RPO, the difference between the two and the need to define as part of a plan?
Answer: Recovery Time Objective (RTO) is how fast an environment can be recovered and fully operational, whereas Recovery Point Objective (RPO) is at what point we want to recover from. Each of these items must be defined (and not assumed) in a true BCDR plan.

Question: Isn't Office 365 backed up by Microsoft.
Answer: You would think/hope, but unfortunately, no. Despite what most people assume, your data is not backed up in the Office365 without a third-party solution.

Your Custom Assessment Profile+

As of today (September 3, 2020) the IT infrastructure at King Brands includes the following servers, data storage usage, data storage cloud target location and recovery path, in the event of a recovery incident.

Server Census

Server Name	Data Size	Target	Recovery Path	Status
KB-DC01	852/gb	Cloud & On-Prem	Disaster Recovery	✓
KB-HV01	789/gb	Cloud & On-Prem	Disaster Recovery	✓
KB-IQMS-V	1.20/tb	Cloud Only	Best Effort	⊘
KB-TS01	256/gb	On-Prem Only	None (Critical)	⊗

Office 365 Census

Server Name	22
Total Data Size:	487/gb

Your Data Protection & Recovery Path & Plan+

Whether you realize it or not, your organization IS at risk and taking proactive steps to ensure you have done your part to keep yourself secure, recoverable and compliant is critical.

Below is a general overview and budget the best upgrade path for your Business Continuity and Disaster Recovery platform.

Remediation Item	Qty	Monthly Budget
Managed Business Continuity Servers	4	$ 450.00
Managed Office365 User Backup	22	$ 88.00
Less Current Spend		-$ 125.00
Total Net-Monthly Investment		**$ 413.00**
One-Time Migration Project Investment		$ 798.00

The takeaway

Protecting your valuable data becomes even more important as business innovation increases your competitive advantage. Ever-eager cybercriminals are ready to exploit any new opportunities, including those resulting from your gains. To help defend your successes, Entech recommends a strategic mix of innovative technologies and proven basic processes.

Appropriate Hardware & Software defensive layer:

Creating a defensive IT security perimeter at the hardware and software level is table-stakes. As would-be hackers become more sophisticated, keeping your hardware and software current and under support is a minimum must have.

Threat analytics:

Advanced threat analytics systems flag behavioral changes in devices, services, and users accessing systems or applications on the network.

User Awareness Training:

Your people will ultimately be your greatest defensive weapon, or your great breech liability. Which one is deeply rooted in the organizations wiliness to train & test each staff member on how to detect and navigate and avoid the perils of the ever change threat landscape. This is a critical offensive defensive measure.

entech

6338 Presidential Ct, Ste 201
Fort Myers, FL 33919

615 67th St. Cir. East, Ste 101
Bradenton, FL 34208

3606 Enterprise Ave., Ste 206
Naples, FL 34104