Disaster Recovery as a Service for Business Continuity

WHITE PAPER

Abstract

Disaster can strike at any time. None is more vulnerable than today's technologically dependent businesses. Technology has created a boon for business. It has also created a weakness. Companies compensate for this weakness by creating disaster recovery plans that outline how the business is to react during a disaster. This includes technical and non-technical aspects of the business. The main intent of the plan is to make sure the business is at least functional at a basic level from which it can fully recover.

Disaster Recovery-As-A-Service is a way for businesses to recover at a cost much less than previously. This service relies on cloud resources to get the business functioning again. However, cloud resources are dependent on the Internet, making it susceptible to cyber breaches. Yet, for many small to mid-sized businesses Disaster Recovery-As-A-Service is a compelling option.

Disaster Recovery as a Service for Continuity

Disaster Recovery-As-A-Service (DRAAS) is a compelling idea, at least in theory. It's especially compelling for small to medium sized businesses. These businesses usually do not have the resources for an in-house disaster recovery plan and implementation. DRAAS allows companies to have replication or hosting of virtual or physical servers to another location in the event of a disaster. It is usually paid on a contract or pay-per-use basis, thus reducing costs.

The downside is that the company must trust that the DRAAS provider will be able to provide the backup when needed. Another downside that is often neglected relates to security. Since DRAAS relies on cloud for the backup, internet security is a major concern. Cloud services are inherently susceptible to breaches. Thus the provider must be equipped to handle such attacks. (Timmons et. al, 2014)

Another downside relates to data privacy. The provider must be trustworthy in how it secures the privacy of companies.

If a provider is deemed trustworthy for privacy and security according to the company, it may be a viable recommendation for disaster recovery. For larger organizations with sensitive data, such as health care

organizations and Government agencies, this service is not recommended due to security and privacy issues. Additionally, regulations may prevent the offsite storing of PII that is not under the organization's control.

The real intent of DRAAS is to ensure business continuity. A disaster or even small interruption in business operations can cause havoc on a business. Client files as well a product delivery could be compromised leaving a company's reputation and future in jeopardy.

If a disaster does occur, it's best to get ahead of it to reassure and inform clients of the compromise before they hear about it elsewhere. This is where a good Crisis Management plan can be effective. Ideally, there would be a designated command center with viable communications for the crisis team to meet and coordinate. This plan could potentially buy the company time to get basic operations up and going so that basic functionality is achieved. A good crisis management plan could retain clients and foster confidence in the company's stability in spite of the incident. (Virgona, 2011)

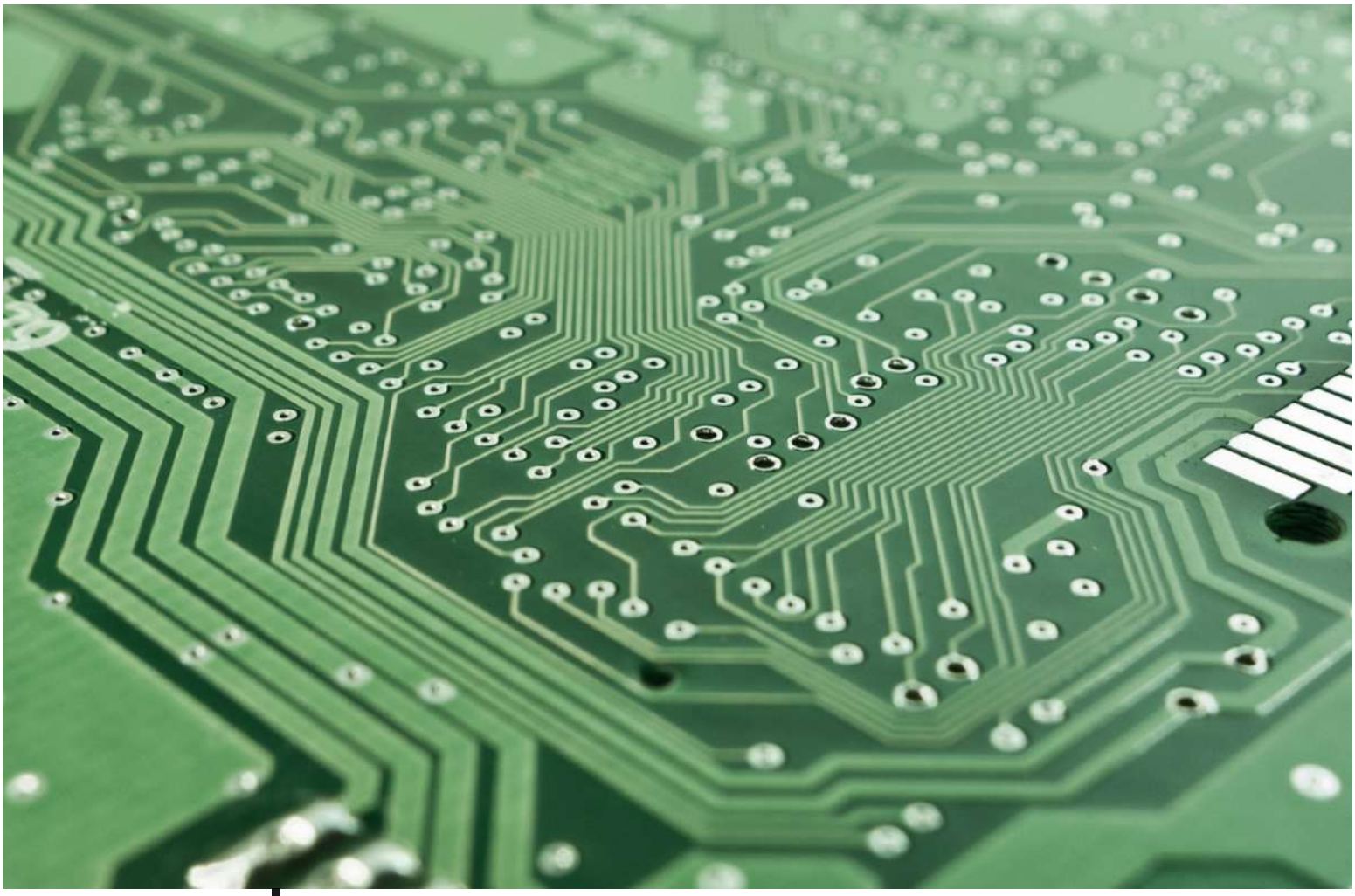
In order to implement a disaster recovery plan, training is essential for those employees who will be involved in the recovery. In addition, as part of the

disaster recovery plan, the business must define what constitutes a disaster and who is to invoke the plan.

When devising a disaster recovery plan, a business impact analysis should be completed. A BIA will gauge the criticality of having a particular system down. The higher the impact the more critical the system is to business operations. This is a part of the risk assessment.

There are several potential risks to a business: technical, financial and legal, non-technical, human, reputational, dependency, natural, and political. (Thejendra, 2014)

Technical Risks



Technical risks can refer to the data used in business operations, software and hardware the business relies on, servers, or telecommunications systems. Power failures and malware are common risks related to technical infrastructure.

Financial and Legal Risks

Bankruptcy, fraud, and regulations are examples of financial and legal risks to the business.

Non-technical Risks

Non-technical risks include fire, theft, and unauthorized access. Non-technical risks can be just as or more devastating to a business.

Human Risks

Industrial espionage, loss of employees to competitors, resignations, illness, or death are examples of human risks.

Reputational Risks

Reputational risks are all matters that can affect the image of a company including allegations of harassment to employees, wrongdoing, legal turmoil, and other bad publicity.

Dependency Risks

> *Dependency risks refer to dependency on third parties such as contractors and vendors to complete production.*

Natural Risks

Natural risks are the most well-known risks such as natural disasters including earthquakes, floods, fires, and hurricanes.

Political Risks

Political risks are more prevalent in certain geographic areas. They include civil disturbances, terrorism, and changes in government and policies.

In a business impact analysis these risks are classified according to their probability of occurrence. Given the risks associated with a disaster, the recovery plan must not impose additional risks such

as those associated with the vendor used for the recovery process.

Therefore, it is important that the cloud resources vendor is well vetted and secure. DRAAS is indeed an excellent idea if all goes well. The hesitancy is in regards to the vendor whose job is to protect the resources placed in their care. The company utilizing DRAAS must weigh the risks with the cost savings. If the data is not sensitive, DRAAS is a well suited recommendation.

References

Timmins, M. L., Bone, E. A., & Hiller, M. (2014). Healthcare system resiliency: The case for taking disaster plans further -- Part 1.Journal Of Business Continuity & Emergency Planning, 8(3), 216-237.

Virgona, Thomas. September 11, 2001: A Historical Study of the Human Aspects of Disaster Recovery.

Proceedings of the Northeast Business & Economics Association. 2011, p585-592. 8p.

Kadlec, Christopher; Shropshire, Jordan. Best Practices in IT Disaster Recovery Planning Among US

Banks.

Journal of Internet Banking & Commerce. Apr2010, Vol. 15 Issue 1, p1-11. 11p.

Thejendra, B. (2014). Disaster Recovery and Business Continuity : A Quick Guide for Organisations and Business Managers. Ely, Cambridgeshire, U.K.: IT Governance Publishing.

CREATED BY
Shayn DeMur