SaaS Cloud Service Providers - what you need to know.

WHO is responsible for security threats in a SaaS environment? Here's what you need to know.

a. **If you are using a Public cloud hosting provider:** they are responsible for ONLY the storage space infrastructure as a service (IaaS) for your data and application needs. They will not be responsible in any way to solve a Ransomware issue, you will. Security is NOT their concern, providing the storage is the only concern infrastructure is their only responsibility.

b. **If you are using a Managed Service Provider (MSP):** it is their responsibility to solve the Ransomware issue. They manage not only your infrastructure but also your data and security. So they must provide a solution for any data/security issues.

c. **If you have In-house hosting:** if you aren't prepared, it could take as much as 3 weeks to get back online.

**Imagine this -
a major security threat - Ransomware
has interrupted all business operations.**

**WHAT'S NEXT?
If your team isn't prepared, it may take
longer than preferred to get back online.**

A major financial services company experienced this exact scenario and through this incident learned a very valuable lesson around security threats in the cloud. They then began re-thinking their 3rd party managed service provider. Soon after, they moved to LTi Cloud Hosting, with peace of mind.

As demonstrated above; not understanding the potential pitfalls of responsibility when it comes to security threats in the cloud when using a 3rd party services provider could bring some critical business interruptions.

We do things differently - our cloud was built for OUR products, and not generic - that makes all the difference.

(cont.)

1. Our cloud is specifically tailor-made for use with ASPIRE and our products – it is NOT a general purpose cloud

2. The speed we manage issues due to the fact we get information and data quickly, with the special team we have in place that are experts in monitoring our hosting

3. We have control over ALL aspects and have teams dedicated to each aspect of cloud hosting

4. We take the burden off a business' IT department – becoming your IT department managing the environment

What are you getting with LTi's Cloud Hosting Environment?

1. **Security and Compliance** concerns are managed for businesses working with financial institutions which typically have very specific compliance needs, our team is well versed for this type of conversation and will get the financial institution comfortable quickly.
2. **Monitoring 24/7/365 -** we have monitoring in place that troubleshoots issues before our customers experience any performance issues. We monitor closely and clean it up before it affects your business.
3. **We fully manage our products internally**…anything that could be catastrophic, is addressed immediately, internally and customers do not ever see the issue affecting them.
4. **Remove burdens from the IT department** of any business...we become part of your IT department, manage your environment, we ARE your team.
5. **Speed of response** are done within hours not days, as most public cloud hosting companies. Our team is dedicated to our customers only…not to a regional area…just you and your business's needs…we can move quickly to resolve any issue/concern that might arise.

The LTi Cloud is part of the SaaS offering from LTi Technology Solutions utilized to host your critical software applications. The LTi Cloud offers a proven solution, utilized by 100+ current customers.