You don't have to be in security to be insecure

Many organisations struggle with keeping their information secure. Whilst IT departments are very experienced in on premise or private data centre security controls, moving to the cloud has significantly shifted the mindset, skillset and risk of data security and controls. Further new data privacy concerns and governance required from around the world require an uplift in knowledge to understand current regulations. Further, the criticality of a data breach extends to cross company reputational damage and hefty regulatory penalties and costly and difficult notification obligations.

A misunderstanding of cloud security methods can lead to developers who are used to operating in isolated environments finding themselves unwittingly in the situation that their decisions can dramatically increase company risk when they are given too much access and too little governance. The ease in which alterations to security configurations can be altered when not controlled and governed is often not considered or fully understood.

Perimeters and layers of security controls are more important than ever, along with the understanding that a lot of these layers are now virtual rather than physical. Always asking the question of what security layers exist to protect against one layer failing (think of a backup parachute or spare tyre) is essential.

The tools to keep your information secure in the cloud are significant and when well-managed, logging and traceability has never been better. This has however, created a veritable raging river of security information that needs to be digested, interpreted and acted upon. Keeping a handle on the amount of security information has become a skill in itself. Using machine learning techniques can identify changes in user behaviour and irregular system changes that can otherwise be missed or acted on way too late to be effective. Understanding where there is a breach, or risk of a breach needs to be highlighted as soon as possible and lock down automatically to.

It is highly recommended that organisations begin to take data and information security very seriously. Organisations should be considering uplifting their existing security teams in understanding of cloud operations. Sufficient resource should be given to the security teams to monitor and handle potential security holes or attacks. Human eyes over security logging should be

supplemented with the latest machine learning and artificial intelligence tools. Developers and architects should be following principles of least privilege and security by design. Multiple layers of security should be in place from the very beginning and encryption of all data at rest and in flight should be mandatory. Independent security and architectural reviews on a regular basis is highly recommended for all cloud operations.

If these are all put in place as an organisation matures into true cloud operations, risks can be mitigated as you move to take advantage of the power and capabilities you can unleash with your information.

To find out more, please contact a Fujitsu Data & AI specialist now.

Contact
Fujitsu Data & AI
+61 3 9924 3000