Why strengthening information security is essential for every successful cloud service provider

Migration to the cloud has accelerated in recent times, to help organizations continue to operate remotely in response to Covid-19. It has proven to be a powerful and useful set of technologies with significant benefits, even for the smallest of enterprises. However, whilst adopting a cloud first strategy brings vast opportunities, being aware of the security, data privacy and compliance challenges that it can pose, is essential to offering an effective service to cloud users.

The key watchouts

5,255 data breaches were reported in APAC alone in the last year, 85% of which involved human error, as stated in the Verizon 2021 Data Breach Investigations Report1[i].

Phishing was present in 36% of the reported data breaches, an increase of 25% from the year prior. A lack of awareness and visibility to security vulnerabilities can lead to an organization failing to identify potential risks, while a lack of transparency can make it difficult to rationally evaluate whether information is continuously being stored and processed securely, or in accordance with ever changing data privacy regulations.

Cloud providers need to be aware of what the threats are and have best practice information security measures in place to minimize risk, enhance visibility and provide reassurance to users.

Addressing information security challenges

In the last year 'social engineering', a psychological manipulation method used to trick users into making security errors and giving away confidential information, caused the highest number of breaches. Cloud Service Providers need to reassure users that they are aware of such risk and have measures in place to successfully manage these threats to help ensure information resilience.

Addressing challenges effectively means combining both data protection and compliance and operational considerations, for instance:

- Striking a balance between operational agility, data protection and compliance
- Deploying consistent security policies
- Recognizing the roles and responsibilities of your team and how they contribute to information security success
- Embedding education and training programmes to help your team to be aware of any potential threats
- Actively engaging with the behaviours and habits outlined by an information security framework.

ISO/IEC 27001 Information Security - your pathway to success

Successful cloud adoption requires investing in regular employee training so that information security becomes a priority and part of the company's culture. Internationally recognized, ISO/IEC 27001 Information Security Management, is an excellent framework which helps organizations manage and protect their information assets so that they remain as safe and secure as possible.

It helps you to continually review and refine the way you do this, not only for today, but also for the future.

The benefits of implementing ISO/IEC 27001 include:

- Reduced operational risk
- Improved internal business confidence
- Improved customer satisfaction.

Through increased visibility into potential information security risks, ISO/IEC 27001 helps to protect your business, your reputation and adds value.

Organizations should take the necessary steps to implement a secure and resilient cloud-first strategy to sustain business success. BSI provides an expansive range of solutions to help organizations address challenges in information management and privacy, security awareness and compliance so your cloud services continue to be successful and resilient

[i] https://www.verizon.com/business/en-au/resources/reports/dbir/

Contact us

Australia
Call: 1300 730 134
Email: info.aus@bsigroup.com

New Zealand
Call: 0800 583 965
Email: info.nz@bsigroup.com