4 Essential Steps to Cloud Computing Security

Tips for cloud computing security from Greg Smith

Congratulations! Your organization made the leap to the cloud. Employees from multiple offices are collaborating with ease. Your data is safe from fires and floods. And with reduced need to maintain costly data centers, you have adjusted your IT budget to explore new areas of innovation. But before you celebrate, be sure you have addressed cloud computing security.

The collaborative benefits of the cloud also bring significant risks. Without specific controls, sensitive business and customer data may make its way into unauthorized hands, risking both intellectual assets and organizational image.

Make cloud computing security a priority before a data breach occurs. Clearly identify the risks involved and create appropriate policies. Understand the security tools and features you have acquired with the cloud. And finally, conduct regular security audits.

1. Know the Risks

Before the cloud, options for sharing data were relatively limited. Employees could accidentally or willfully attach a file to an email or misplace a thumb drive with sensitive files. Now, with so much business conducted in the cloud, employees have dozens of ways to share information outside the organization.

To protect sensitive information, you must first identify data security vulnerabilities. Know what information you have and where it resides, including data shared with business partners. Know what cloud applications and services employees use. Understand applicable industry regulations.

Finding all the points of data ingress and egress can prove a daunting task. A knowledgeable IT Consultant can help you develop a comprehensive outline of security and operational risks.

2. Power in Policies

Once you have identified your information assets and the risks associated with them, it is time to create electronic document policies to protect those assets and limit the organization's liability. To ensure that policies are comprehensive and enforceable, include all stakeholders in the process, from human resources to legal, financial and IT.

Policies should cover data access, regulatory compliance, encryption, naming conventions, passwords, data retention and other actions that affect how data is created, stored and shared. Evaluate the requirements of different departments and individuals in relation to data. For instance, project managers may need more access to share certain files externally.

3. Understand Cloud Computing Security Tools

Most cloud applications and services include features to help you manage cloud computing security. Microsoft Office 365, for instance, includes message encryption and auditing tools and allows organizations to define data access based on user or role.

Take time to thoroughly understand the security features available to you. For example, Office 365 includes the ability to define data loss prevention (DLP) policies that can block attempts to send certain types of data outside the organization. If set up correctly, the tool can prove an effective method of monitoring compliance.

4. Security Audits are a Must

Plan for ongoing security audits to assess the safety of data within the organization. The auditing process reviews actions taken with data, such as sharing files or changing access rights. Actions that look questionable are flagged for review. The audit should also check all data policies and any exposure to the internet.

The frequency of security audits depends on the type of data you are trying to protect, how sensitive the system is and the fear rating for the organization. For example, an organization with significant turnover or disgruntled employees will need more frequent audits. For most organizations, monthly or bi-monthly audits should be sufficient.

Strategic Partnerships

The right partners help you leverage the benefits of the cloud. With deep experience in cloud computing, Messaging Architects can guide you through understanding the risks involved and then defining and enforcing effective policies for information governance. They can also conduct regular audits to keep security up-to-date and help you safely embrace the power of the cloud.

Greg Smith, Vice President of Services Delivery, heads a team of experienced engineers at Messaging Architects. Drawing on a wealth of experience, the Services Delivery team deploys top notch solutions, from large-scale email migrations to security audits and information governance assessments. Smith aims to minimize headaches and cost for his clients, while ensuring business continuity throughout the project.