Policy recommendations

Secure and reliable cloud services

The opportunity

As cloud computing gives rise to powerful new capabilities, it offers the potential to increase productivity, reduce costs, and drive new levels of innovation, security, and resiliency. But it also creates new risks—both by providing fresh avenues of attack for malicious actors and by introducing new complexities that will require a reassessment of current practices and policies.

The challenge

To address the risks and threats of the cloud computing era, governments will need to adapt existing security programs and policies, and enhance current approaches to ensuring the security and resilience of their systems. To achieve this, new frameworks that incorporate active risk-based decision-making and leverage public-private partnerships will be required. Given the global nature of security threats, cross-border partnerships and harmonized legal approaches will also be important.

Policy recommendations

Governments recognize that cloud services offer enormous value and can help the public and private sectors offer new and better services to citizens and customers. As a result, governments are moving beyond questions about whether to implement cloud computing approaches and infrastructure and are now focused on creating regulatory frameworks to ensure that secure and reliable services are used, particularly for workloads involving sensitive data.

To achieve this, we recommend the following:

Establish risk management processes. Cloud policies should prioritize the assessment, management, and mitigation of risk in the delivery of cloud services for government. Governments should implement risk management processes across their IT environments that enable them to improve their risk profile, whether on-premises or in the cloud. They should also strive to distinguish between risks that are common across governments or departments (such as logical access controls) and unique risks (such as those associated with access to personal health information). Distinguishing common and unique risks will help determine how to manage certain risks and when to use international standards.

Structure a cloud assurance program designed to achieve balanced goals. Establishing a cloud assurance program enables governments to adopt secure cloud solutions for delivering and extending services. Such programs should be structured to balance security goals with performance and innovation goals. The framework should take into account the roles that relevant stakeholders play including governments (as both regulator and customer), service providers, and third parties. It should also establish processes for performing an initial analysis of security practices against required baselines and conducting ongoing assessments of a smaller set of practices and controls.

Establish baseline security measures aligned with or based on proven best practices. How governments approach the development and implementation of security baselines will have profound effects on both security and economic development. Fragmented, inconsistent approaches will redirect limited resources from security to compliance. Instead, governments should utilize and adapt existing best practices such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework to advance security and drive economic opportunities.

Scope requirements based on the cloud service delivery model. Cloud service delivery models vary significantly in their architecture, function, and usage. Therefore, it is important that security is managed in proportion to the risks that arise in different environments. For example, because the security of software applications depends heavily on the security controls of the underlying infrastructure on which they are built, security requirements should target the infrastructure system directly rather than solely focus on the application.

Preserve and support voluntary information exchange. Many governments are focused on increasing visibility into cyberthreats to their technology environments and to critical infrastructure services operating in their country. Some have developed mandatory incident notification frameworks that require industry to inform regulators in case of severe incidents. Governments should preserve and support existing information exchange communities that operate based on mutual trust. Because information exchange is most effective when it is two-way, governments should also share information developed through strategic analysis of incident information disclosure to help private-sector firms tackle new threats.

Implement a data classification system for the cloud. Data classification is the process of dividing data into distinct categories based on sensitivity levels and risk profiles, and then articulating the security controls needed for each level to manage risks appropriately. Having a cloud-specific data classification system will help enterprises and government agencies identify both their most sensitive and least sensitive materials and evaluate the costs and benefits of storing varying levels of sensitive materials in the cloud. To the extent possible, governments may adapt existing data classification schemes to data stored in the cloud.

Leverage global standards. Because governments everywhere have many risks in common and cloud computing utilizes aggregation and scale to drive down costs and improve performance, by leveraging global standards as the basis of their cloud security certifications, governments can improve efficiency, lower costs, and improve market competition. The baselines should be comprehensive enough to minimize the need for organizations to add their own controls but not so broad that they encompass one-off controls that are not widely used.

Develop a common security compliance model for ICT. Because every sector of the economy depends on digital technology, there is a high degree of commonality of the risks and controls across sectors, yet there are also some risks that are unique to each. For common risks, governments should develop a security compliance model that sets minimum security goals and standards for regulated sectors, but that also allows those sectors to establish a smaller subset of additional requirements appropriate for their unique operating environments.

Evidence and further reading:

National Institute of Standards and Technology: "National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity"

Microsoft White Paper: "Transforming Government: Cloud Policy Framework for Innovation, Security and Resilience"

Microsoft White Paper: "Transforming Government: A Cloud Assurance Program Guide"

For links to these and other resources, please visit:
http://www.microsoft.com/cloudforgood