Principles for Government Cloud Security Laws and Policies

BSA urges governments around the world to support laws and policies that enable both governments and industry to use state-of-the art solutions like those currently offered and being continuously improved through cloud services. Such laws and policies will be risk-based, outcome focused, flexible, technology-neutral, and will make concrete improvements to cybersecurity risk management.

Governments and industry continue their digital transformation by leveraging the benefits of cloud services. This digital transformation allows organizations to better serve citizens and customers, as well as more effectively manage their cybersecurity risks. Cloud services—infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS)—enable governments and industry to operate advanced computing environments that would not be as cost-effective if operated on premises. These services provide flexibility, increase productivity, enable efficiencies, and improve security.

Cloud service providers can provide unique benefits to governments and industry by leveraging economies of scale to minimize costs to customers while repeatedly updating and enhancing security practices well beyond the security capability of on-site data storage. These cloud data centers are designed to meet the requirements of multiple customers; their security practices function at a higher level than those typically used by any single organization. For example, these data centers often restrict access to only personnel with completed background checks, require biometrics to gain physical access, and apply a least privilege policy. Likewise, large client pools provide key security insights and allow cloud service providers to examine security intelligence across their entire environment, having access to more information than a typical corporation or government's traditional on-premises infrastructure and allowing big data security-intelligence systems to discover and combat malware and network intrusion attempts quickly. In a highly competitive global cloud services market, cloud service providers use security to differentiate themselves from competitors, hiring the best talent in this space and dedicating significant resources to its development. Indeed, compared to on-premises security, cloud security frequently delivers significant distinct advantages. Cloud services accomplish all these security improvements while also enabling improved functionality for customers.

Still, governments' and industries' ability to capitalize on improved security and efficiency through cloud services is supported (or thwarted) by governments adopting applicable laws and policies that either enable innovative, adaptable, resilient solutions or that limit choice, stifle competition, and increase costs without producing material security improvements.

The log4j vulnerability illustrated the advantages of cloud services. In response to log4j, cloud service providers were able to more efficiently implement patches on cloud-based software compared to on-premises software and were able to do so without interrupting their customers' workflow.

Despite the advantages that cloud services can offer to enterprises and governments, some governments have expressed concern that global cloud services could outcompete local industry and disadvantage their local cloud services ecosystems. In response to these concerns, some governments are considering or enacting protectionist laws and policies that institute significant barriers to cloud service procurement and operations. These protectionist laws and policies may insulate local cloud service provider ecosystems in the short-term, but ultimately stifle local innovation by creating a captured domestic marketplace that disincentivizes international competitiveness and isolates local cloud provider enterprises from the global market. Furthermore, these laws and policies limit the access of other local enterprises and governments to the most innovative, secure, and cost-effective solutions available globally. Conversely, when laws and policies embrace globally integrated and competitive cloud services, governments and industry can gain greater access to global supply chains, advanced security technologies and practices, and a greater ability to innovate on platforms—enabling economic growth, global connectivity, and public trust.

The starting point for laws and policies that support innovation while also improving security is recognizing that cloud security is not categorically different than cybersecurity in general. Both begin with a foundation of effective risk management. Although cloud services pose unique technical challenges, those challenges are still best confronted from a risk management, outcomes-based posture focused on establishing and implementing best practices.

For example, cloud security laws and policies should recognize that security is not inherently linked to data location but rather to the security controls that a cloud service provider or user applies to data, such as identity and credential access management. When governments restrict a company's ability to move data, they may create unnecessary obstacles to data security. Locally hosted data is not free from cybersecurity risk but is actually subject to many of the same cyberattacks as cloud services; they, however, must combat these attacks without ready access to cloud providers' multinational resources and security measures, which are a major focus for those providers. Indeed, cross-border data transfers are an important cybersecurity tool for several reasons, including the ability to protect against physical access, as well as to create redundancy, increase resiliency, and reduce latency. In addition, cross-border data transfers allow for cybersecurity tools to monitor traffic patterns, identify anomalies, and divert potential threats in ways that depend on global access to real-time data. When governments mandate localization or restrict the ability to transfer and analyze data in real-time, they may create unintended vulnerabilities, or deny themselves access to the latest global threat information.

Policies like data localization may be justifiable in narrow and specific circumstances, for example, highly classified national security information, but these circumstances can be address through specific, tailored decisions and not by imposing broad limits on the use of cloud services.

BSA urges governments to support laws and policies that enable organizations to use state-of-the art solutions, like those currently offered and being improved through cloud services. Such laws and policies will be risk-based, outcome focused, flexible, technology-neutral, and will make concrete improvements to cybersecurity risk management.

BSA RECOMMENDS GOVERNMENTS' APPROACH TO CLOUD SECURITY LAWS AND POLICIES BE BASED ON THE FOLLOWING PRINCIPLES:

1. Promote the Development and Use of Internationally Recognized Standards
2. Recognize Existing Certifications
3. Support Role-Based Security Responsibilities
4. Adopt Modern Approaches to Cybersecurity
5. Combine Good Cloud Security Laws and Policies with Other Best Practices

1 Promote the Development and Use of Internationally Recognized Standards

Governments should base cloud security laws and policies on internationally recognized standards, which are developed in open, transparent, consensus-based processes, and are widely adopted in the international marketplace. Internationally recognized standards leverage global security expertise from governments, industry, and academia. For example, ISO 27001, "specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of an organization," while ISO 27017 provides "guidelines for information security controls applicable to the provision and use of cloud services."

Regional, national, or local standards fragment this landscape and increase the costs to customers (including government customers) and decrease both the ability to provide innovative solutions and the number of cloud service providers competing for customers. Unfortunately, in some instances, the decrease in the number of cloud service providers competing in a market due to a requirement to meet regional, national, or local standards is the law or policy's intended consequence—this harms the entire cybersecurity ecosystem.

In contrast to regional, national, and local standards, laws and policies based on internationally recognized standards enable international interoperability, allowing governments and industry to better communicate at the technical level. They have a track record of being developed and updated more efficiently than laws, increase competitiveness, incentivize innovation, and account for how technology is evolving. Ultimately, internationally recognized standards result in services that are more effective, efficient, and innovative, while also being less expensive. By participating in the standards development process, governments can raise and address their concerns without passing costs to customers, hampering innovation, or limiting competition.

2 Recognize Existing Certifications

Governments should recognize certifications of cloud services carried out by external accredited assessors and based on internationally recognized standards. Requiring additional and duplicative local verification of existing certifications is wasteful and slows cloud adoption with virtually no security benefits. Government certification processes should recognize equivalent international audits and certifications where possible.

If local attestation is required, cloud service providers should be able to provide evidence prepared from previous audits by qualified auditors against internationally recognized standards, rather than having to repeat audit services against the same controls for different customers. This evidence should be accepted in digital form.

Another advantage of recognizing existing certifications is it elevates security considerations over political considerations, which helps build a stronger digital transformation ecosystem in which all parties are working toward the same shared goal: a more secure and prosperous future.

3 Support Role-Based Security Responsibilities

Laws and policies should support the cloud services shared responsibility security model, which clarifies that the responsibility of security in the cloud depends on the services procured by the customer and the extent the customer has migrated its data to the cloud.[1] Effective security programs assign appropriate responsibilities to providers and customers relative to their role in, and level of control over, the cloud environment. This model of shared responsibility can be tailored to best benefit customers and providers needs and has been successfully implemented in the financial services and other sectors.

Laws and policies that do not recognize this fundamental separation of security responsibilities increase the risks to customers by forcing the removal

[1] A shared responsibility security model is explained and supported in multiple valuable documents. See for example, *Cloud Computing: Shared Responsibility Security Models*, National Cyber Security Centre, July 2019.

of vital security controls, reducing customers' ability to control the security of their cloud environment, and increasing the likelihood of missing important security signals. For instance, two parties to a cloud service arrangement may assume that the security of a particular piece of infrastructure is the other's responsibility, creating a blind spot that can become a vulnerability. Instead, each party needs to be aware of and ensure it fulfills its responsibilities.

4 Adopt Modern Approaches to Cybersecurity

Laws and policies should recognize and enable modern approaches to cybersecurity, as well as promote innovation by investing in research and development to create the next generation of security assurance tools. For example, traditional auditing and certification processes measure security at a point in time. Such approaches do not adapt well to the scale and continuous evolution of cloud services. Laws and policies should support the use of new software-enabled approaches to auditing and compliance that automate compliance monitoring, providing flexibility and real-time visibility of the cloud environment's security posture. Evidence to support audits and certifications should be accepted in digital form to support governments, industry, and auditors shifting to receiving and processing machine-readable evidence, which in turn will support applying additional resources to other priority challenges.

Similarly, effective, modern approaches to identity, credential, and access management (ICAM) grow in importance as governments and industry continue their digital transformation and cloud migration, and as the Internet of Things grows and more devices connect. Effective ICAM, including zero trust architecture, single sign-on, and phishing-resistant multi-factor authentication, are cost-effective approaches to improving cybersecurity risk management in the cloud.

5 Combine Good Cloud Security Laws and Policies with Other Best Practices

As governments develop and implement laws and policies that apply to cloud services, governments should understand these solutions within the broader technology products and services landscape. Approaching cybersecurity regulations horizontally enhances the security of all products and services, not just cloud services, as well as promotes greater cross-ecosystem consistency, and fosters risk-based approaches that not only evolve with changing technology but encourage its continued improvement.

Taking advantage of readily available commercial solutions expedites digital transformation. Readily available commercial solutions also are regularly updated with both security and functionality improvements, thereby ensuring that organizations that take advantage of commercial cloud solutions are not relegated to old, less secure, and less functional products and services.

Governments should proactively improve cybersecurity broadly and participate in global efforts to improve best practices, which will create positive spillover effects and strengthen the security of the entire ecosystem. This effort should include harmonizing the types of entities and cyber incidents that governments require to report, and the time frame for reporting.

To improve the effectiveness of cloud security laws and policies, governments and industry should support laws and policies that strengthen cybersecurity, software security, and IoT security, including The BSA Framework for Secure Software and BSA Policy Principles for Building a Secure and Trustworthy Internet of Things. A robust and harmonious cybersecurity environment, cultivated across governments, technologies, industries, and products, will strengthen the security of cloud infrastructure and benefit governments and their citizens as well as companies and their customers.