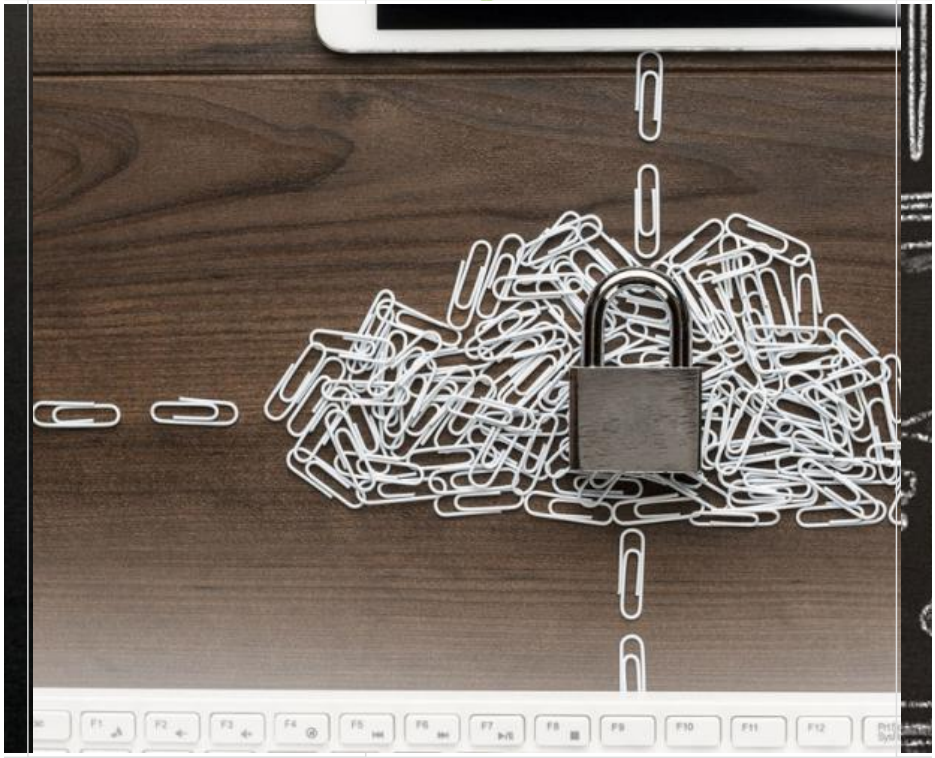
THE CYBER EDGE



Overspending on cyber tools and appliances placed in the wrong location or configured poorly can be equally bad if not worse than under-resourcing. 2,500 years before the advent of digital networking, military strategist Sun Tzu's advice is still applicable: You must know your enemy and know yourself to be victorious. Credit: Pexels/meo

Bef
prov
or o

Cloud-Based Systems Security Must Be Shared

THE CYBER EDGE

April 1, 2020

By Sarbari Gupta, Ph.D.

Protection responsibility belongs to every resident within the environment.

Security is among the single greatest concern government agencies have about moving their systems to the cloud. Although it offers significant benefits, cloud computing continues to raise questions about data and system protection. Regardless, the Office of Management and Budget via its Cloud Smart Strategy and the previous Cloud First policy mandates government agencies move to the cloud.

Confidence in the cloud approach has grown during the past several years. It offers many benefits, including hardware and software footprint reduction, scalability, elasticity, lower cost and improved

availability. However, despite acknowledging the opportunities cloud computing usage provides, 66 percent of **LogicMonitor** survey respondents stated reservations about the status of cloud security as their single greatest hesitation in using the cloud approach for computing and storage; the same survey found the single greatest concern about moving to the cloud is security. But LogicMonitor's survey still concluded that approximately 83 percent of enterprise workloads already reside in the cloud.

Many government agencies might inaccurately believe that a cloud service provider is totally responsible for all aspects of cloud security. Before jumping into the cloud, potential users must determine whether the cloud service provider or the cloud user is responsible for the various elements of cloud security. It is not an either-or option; instead, the answer lies somewhere between cloud service providers, such as Amazon, Microsoft and Google, and the system owner. Consequently, federal agencies are left with the challenging task of delineating the security boundary and assigning responsibility.

Three factors amplify the challenge. First, the complexity of the architecture of today's cloud-based systems makes it difficult to identify the exact boundaries of functional responsibility. Second, security terminology such as security control inheritance and common controls, which were established before cloud services became prevalent, can be confusing when used in the cloud-based systems context. And third, clear guidance about how to identify the system owner's security responsibility has not been established.

Collectively, these factors translate to cloud-based systems that could be at high risk if system owners underestimate or are not aware of their own security responsibility.

Depending on the solution architecture, the system owner's and cloud service provider's responsibilities can vary greatly. In the Infrastructure as a Service (IaaS) model, the system owner is responsible for more items than the cloud service provider; in the Platform as a Service (PaaS) and Software as a Service (SaaS) models, the cloud service provider assumes more responsibility. The bottom line is this: No matter what model an agency selects, the system owner will always hold some level of security responsibility.

Today, cloud-based information systems may leverage one or more cloud service providers, so an agency system may implement a high-level commercial SaaS solution built on an underlying IaaS from another cloud service provider. One example would be a SaaS provider putting software on top of an Amazon IaaS platform.

In addition, a cloud-based system may simultaneously leverage one or more organizational common control providers (CCPs). For instance, an agency may implement a general support system for its enterprise network that includes security controls common to the agency such as security policies and procedures, security training and acquisition. The cloud-based system may leverage some of the common controls implemented by the general support system while leveraging controls from one or more cloud service providers.

A more realistic model of security authorization boundaries today involves an agency system boundary that includes one or more cloud service providers and organizational common control providers. According to guidance from the National Institute of Standards and Technology (NIST), a system owner can designate a security control in one of three ways. The first is a common control, which is a security control central point inherited from one or more organizational information systems. The second is a system-specific control that has not been designated as a common security control or a portion of a hybrid control that would be implemented within an information system. The third is a hybrid control, which is a security control implemented in part as a common control and in part as a system-specific control.

However, because NIST's terminology predates cloud-based systems, describing cloud service provider controls as common is confusing when the provider is an external organization. Likewise, common controls within an organization include policies and procedures, staff training, acquisition and physical protection, so it's inappropriate to consider these common when referring to external organizations.

One solution would be to replace the traditional term "common control" with the term "fully inherited control" and define the latter as a security control that provides protection to one information system but is fully implemented by another. The system that implements a fully inherited control can be another organizational information system and an external system outside of the organization.

Along the same lines, replacing the traditional term “hybrid control” with the term “partially inherited control” adds clarity. It would be defined as a security control that is partially implemented by each of two different information systems.

Finally, redefining the traditional term system-specific control would clarify responsibilities. It should be described as a security control that has not been designated as a fully inherited security control or the portion of a partially inherited control that is to be implemented within an information system.

These changes simplify the description of when a control is inherited from an organizational information system versus from an external system such as a cloud service provider and helps delineate security responsibility more appropriately.

FedRAMP is a government program that approves and authorizes commercial cloud providers for government use. FedRAMP certification assures agencies that a cloud provider has been vetted and is a preapproved provider.

The FedRAMP authorization process employs a **Control Implementation Summary** (CIS) workbook that cloud service providers must complete to attain authorization. The **summary template** reflects 400 rows of controls. Cloud service providers must go through the template line-by-line and, for each applicable control, identify its implementation status and its origin as either cloud service provider or customer.

Controls marked as configured or provided by the customer are the customer’s full responsibility. Controls identified as a shared responsibility must be further designated as independent shared in which both parties must implement the control individually, or as dependent shared in which each party implements parts of control.

In accordance with NIST’s **Risk Management Framework** (RMF), a system owner must first select the security control baseline of low, moderate or high for a system’s level of perceived impact. **NIST SP 800-53** provides a comprehensive list of security controls for each baseline. The system owner must then tailor the security controls in the selected baseline to align with the specific conditions within the organization and the information system. The system owner also must allocate the controls, designating the responsible party for each.

The proposed methodology for identifying security responsibility for a cloud-based system would be to refine the control allocation process described in the RMF. First, it would be necessary to distinguish controls that can be inherited from common control providers available within the organization and also identify the controls that could be either fully or partially inherited from them in accordance with the proposed definitions above.

In addition, the system owner would review the CIS worksheet from the cloud service provider’s FedRAMP package to identify candidate controls that can be fully or partially inherited. CIS worksheet controls that are not marked as configured by, provided by, or shared responsibility with the cloud customer can be documented as fully inherited. CIS worksheet controls marked as shared responsibility would be considered partially inherited controls, and the portions to be implemented by the cloud customer should be documented.

The next step would be to identify system-specific controls. All controls not yet documented as fully or partially inherited would be the system-specific controls. System owners would determine the extent of their responsibility for partially inherited controls and these comprise the system owners’ retained security responsibility.

In situations where the cloud service provider has not undergone the FedRAMP process, the system owners could request that the cloud service provider complete the CIS worksheet. Without this worksheet, the proposed process is more challenging because the system owner must guess which controls can be fully or partially inherited from the cloud service provider.

Federal organizations’ cloud-based information systems are at risk when system owners’ retained security responsibility is underestimated. System owners can leverage the proposed terminology for fully inherited and partially inherited controls as well as the cloud service provider’s FedRAMP CIS worksheet to better delineate their retained security responsibility for a cloud-based system. A better delineation of security responsibility results in lower risk.

*Sarbari Gupta, Ph.D., CISSP, CISA, has been active in the information security industry for more than 25 years. She is the president and CEO of **Electrosoft Services Inc.**, a provider of technology-based services and solutions to the government with a special focus on cybersecurity.*

You may also like:

SIGNAL WEBINAR: **Instrumenting Cloud Security to Validate Critical Controls**

SIGNAL WEBINAR: **DoD Cloud Future: Mission Assurance Through Strategic Workload Modernization in Azure**

Government Experts Tell Congress FedRAMP Needs Some Work