# The Hybrid Cloud Security Professional

**Adam Gordon**
New Horizons Computer Learning Centers

**AS CLOUD COMPUTING CONTINUES TO EVOLVE, THE ROLE OF THE HYBRID CLOUD SECURITY PROFESSIONAL PROVIDES AN INTERESTING STUDY IN ENTERPRISE OPERATIONS AND INDIVIDUAL EDUCATION REQUIREMENTS.** Cloud computing is a product of both inherited and learned characteristics. It blends conventional definitions of resources with innovative usage patterns and solutions to facilitate user access to ever more powerful hybrid systems and introspective data. Cloud computing characteristics, service models, and deployment models are well documented, and hopefully well understood. Less apparent are the key trends shaping hybrid cloud computing: where they come from, what they're driven by, how they interact, whom they impact, and why they're important to understand.

The current rates of cloud deployment model adoption and cloud workload placement provide an example that helps to frame the discussion around key trends. According to the RightScale *2015 State of the Cloud Survey*[1]:

- Hybrid cloud remains the preferred model for most enterprise adoption, rising to 82 percent from 74 percent in 2014.
- Public cloud usage continues to be higher than private cloud usage overall, with 88 percent of enterprises using a public cloud and 63 percent using private clouds.
- Private clouds lead in workload placement, with 13 percent of enterprises running more than 1,000 virtual machines (VMs) in public clouds, and 22 percent running more than 1,000 VMs in private clouds.
- Workload placement overall shows that 68 percent of enterprises currently run less than a fifth of their application portfolios in the cloud, while at the same time, 55 percent report that a significant portion of their application portfolios are being built with cloud-friendly architectures.

These facts illustrate the general direction cloud deployment is trending toward in the enterprise, but they do not tell the entire story. What about the security concerns and implications of continued placement of cloud workloads across one or more cloud models? According to Eurostat's *Cloud Computing—Statistics on the Use by Enterprises* report[2]:

- Nineteen percent of EU enterprises used cloud computing in 2014, mostly to host their email systems and store files.
- Forty-six percent of those firms used advanced cloud services related to financial and accounting software applications and customer relationship management applications.
- Four out of 10 enterprises (39 percent) using the cloud reported the risk of a security breach as the main limiting factor in the use of cloud computing services.
- A similar proportion (42 percent) of those not using the cloud reported insufficient knowledge of cloud computing as the main factor preventing their use.

These additional facts bring to light the dichotomy between enterprises' need/desire to migrate high-value data into cloud workloads to realize the promise of increased productivity and operational efficiency, while at the same time fearing the

 2325-6095/16/$33.00 © 2016 IEEE

risks associated with operation of the cloud models used to host this data. In addition, a general lack of knowledge and understanding of cloud computing is keeping many organizations from adopting and using cloud platforms and services overall.

One way to examine this trend is to think about the role of a cloud security professional in a hybrid cloud environment. The National Institute of Standards and Technology (NIST) defines a hybrid cloud environment as a "composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability."[3] According to the Gartner IT Glossary, hybrid cloud computing "refers to policy-based and coordinated service provisioning, use and management across a mixture of internal and external cloud services" (www.gartner.com/it-glossary/hybrid-cloud-computing).

## Information Security and Risk Management in the Enterprise

All of this serves to focus us on the primary cloud computing concern for the enterprise, which can be framed in terms of information security and risk management. The need to provide comprehensive confidentiality, integrity, and availability protections for data hosted in the cloud continues to grow in lock step with cloud computing adoption across the enterprise, as does the need to understand how to integrate the data hosted in the cloud into the enterprise's risk management practices (for example, audit/compliance and business continuity/disaster recovery).

Although risk is a broad topic, and must be understood within the context of the enterprise's operational environment, we can establish a working definition of risk using the guidance provided by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in the *Enterprise Risk Management—Integrated Framework*: "Risk is the possibility that an event will occur and adversely affect the achievement of objectives."[4]

What's interesting, and often misunderstood, is that the types of risks that must be faced in the cloud are identical to those encountered outside of the cloud (for example, confidentiality, integrity, and availability). In other words, risk categories do not change just because we add the word "cloud" to our enterprise provisioning and service vocabulary. However, the more things stay the same, the more they change. Specifically, the level of risk encountered and the organization's overall risk profile change. The key factor driving this change is the fluctuation in likelihood and impact with respect to risk events, due to the cloud service provider's (CSP) ability to manage risk across its service organization. Common risks associated with cloud environments include:

- Multitenancy hosting
- Lack of transparency
- Reliability and performance concerns
- Vendor lock-in
- Compliance
- Data leakage
- Cloud service provider viability

Although there's no "magic bullet" that will solve all of the risks and security concerns associated with cloud computing, there is something almost as powerful and effective—something that's always within our grasp if we're just willing and able to recognize it for what it is: training.

## Importance of Training

Today many organizations recognize the importance of training, and the value it can provide in furthering the organization's objectives. The biggest challenges that organizations face vis-à-vis training are

- clearly articulating the objectives that a training program is designed to address,
- clearly defining the metrics associated with the training program's success and failure, and
- clearly communicating the objectives and metrics broadly and widely across the organization.

A catalyst, something that when added to a system will facilitate a desired reaction's occurrence, is often necessary to ensure successful outcomes. The key to overcoming these challenges is to understand that although most organizations could address one or more of these concerns internally, usually with an acceptable level of success, they are often unable to address all of these challenges across their entire organization consistently without some additional help

and guidance. Thus, a catalyst in the form of a strategic partnership with acknowledged experts can become a success enabler for the organization. The US Government's approach to building the Information Assurance Support Environment (IASE) Information Assurance baseline certifications matrix for the Information Assurance Workforce under US Department of Defense Directive 8570.1 is one example of this use of a strategic partnership as a catalyst to overcome the challenges associated with training (see www.isc2.org/dodmandate/default.aspx). This directive, signed in August 2004, requires every full- and part-time military service member, defense contractor, civilian, and foreign employee with "privileged access" to a DoD system, regardless of job series or occupational specialty, to obtain a commercial certification credential that has been accredited by the American National Standards Institute (ANSI).

By identifying training and certification organizations that are leaders in the information assurance and cybersecurity areas, and partnering with them to associate their training and corresponding certification to job roles, the DoD has been able to craft a training and certification program that jointly addresses the identified information assurance concerns by role, while leveraging tested methods and programs to achieve their desired outcomes while simultaneously overcoming the challenges associated with training.

As we focus the training and certification discussion on cloud computing, several things become clear. First, many options for vendor-specific training by platform and solution offering are available in the marketplace today. Examples include products from Microsoft, VMware, Cisco, SalesForce, EMC, Oracle, and Citrix. Although these offerings are valuable and necessary, they're vendor specific, and are applicable only in cases where a customer is deploying the specific technology solutions that the training and certification program is designed to address. Other training and certification offerings (such as CompTIA's Cloud Essentials or Cloud+ curriculums) offer an entry-level baseline of knowledge with regard to cloud computing. Finally, some vendor-neutral and agnostic training and certification programs with a security focus (such as offerings from $(ISC)^2$ and the Cloud Security Alliance) are designed specifically to address cloud-security-related concerns and needs.

## Certification for Cloud Computing Professionals

Although all three areas offer valuable knowledge and skills for the cloud computing professional, the third area offers the biggest advantages with regard to risk and security challenges as they pertain to cloud computing. An overview of the Certified Cloud Security Professional (CCSP, www.isc2.org/ccsp) will help illustrate the type of skills and knowledge a cloud computing professional pursuing training and certification will acquire.

The CCSP curriculum is designed to recognize the need to identify and validate information security professionals' competency in securing cloud computing services by presenting an international cloud security credential that reflects the most current and comprehensive best practices for securing and optimizing cloud computing environments. The six domains of the CCSP common body of knowledge are

- architectural concepts and design requirements,
- cloud data security,
- cloud platform and infrastructure security,
- cloud application security,
- operations, and
- legal and compliance.

According to $(ISC)^2$, the CCSP credential is designed for experienced information security professionals with at least five years of full-time IT experience, including three years of information security and at least one year of cloud security experience. The CCSP is most appropriate for those whose day-to-day responsibilities involve procuring, securing, and managing cloud environments or purchased cloud services. Many CCSPs will be responsible for cloud security architecture, design, operations, and/or service orchestration. Job functions that a CCSP candidate might hold in an organization include, but aren't limited to, enterprise architect, security administrator, systems engineer, security architect, security consultant, security engineer, security manager, and systems architect.

A full ecosystem of training offerings has been

built to support a candidate looking to access the CCSP materials and certify, including

- a traditional instructor-led training class delivered in person using official curriculum and training materials;
- a traditional instructor-led training class delivered online live as a synchronous solution using official curriculum and training materials;
- an asynchronous, self-paced version of the instructor-led training class using the official curriculum and training materials; and
- a self-study review and reference guidebook, *The Official (ISC)$^2$ Guide to the CCSP CBK*.

Regardless of the mechanism chosen for training, a CCSP candidate will acquire detailed knowledge spanning multiple key areas, including:

- cloud computing concepts, reference architectures, and design principles for secure cloud computing;
- the cloud data life cycle, design and implementation of cloud data storage architectures, design and application of data security strategies, design and implementation of data discovery and classification technologies, and design and implementation of relevant jurisdictional data protections for personally identifiable information (PII);
- analysis of risks associated with cloud infrastructure, design and implementation of security controls, and disaster recovery and business continuity management activities for the cloud;
- cloud software assurance and validation, the cloud software development life cycle (SDLC) process, the use of a secure SDLC for cloud software development, and identity and access management (IAM) solutions for the cloud;
- implementing, running, and managing a cloud's physical and logical infrastructure;
- collection, acquisition, and preservation of digital evidence; and
- audit processes, methodologies, and required adaptions for cloud environments.

These areas comprehensively cover the risks and security concerns associated with cloud computing.

## Areas of Focus

With this background, we can now ask ourselves, "What would the responsibilities of a security professional be in a hybrid cloud environment?" I identify four major areas.

The first is regulatory compliance. We need security due diligence across the enterprise to ensure continued regulatory compliance. Various government regulations limit or restrict where sensitive data can be stored. Often the restrictions are linked to geographic borders. Even though cloud computing is theoretically borderless, data still resides on physical hardware subject to local government jurisdictions. Because of the uneven nature of intellectual property protections, companies might need to use cloud providers that guarantee appropriate regional presence.

The second area is intercloud data transfer. Secure data transfer between CSPs can be a complex undertaking. To do this properly, the enterprise might need to negotiate additional contractual agreements or leverage the expertise of a cloud service broker. Using the open Internet for transport can introduce additional security concerns.[5]

A third area of focus is federated identity access management and single sign-on. Online operations increasingly require the use of common credentials to access multiple systems and services, such as the use of Google, Microsoft, or Facebook credentials to log into various websites. Federated identity access management and single sign-on technologies provide this ability. Often, a group of organizations will share identity attributes based on security frameworks, trust, standards, and policies.

Finally, security professionals will need expertise in intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). Hybrid cloud environments also require the deployment of hybrid IDS/IPS systems. This could require the provisioning and integration of disparate security event and incident management technologies as well.

**NO SOLUTION OFFERS 100 PERCENT COVERAGE OF ALL AREAS AND CONCERNS.** However, an organization that's looking to address the risks and security concerns associated with cloud computing, and that's willing to entertain

the idea that training and certification will provide a reliable and measureable path through a strategic partnership, can benefit from the pursuit of one or more training classes and certifications as part of a coordinated effort to identify and manage the risks and security concerns associated with hybrid cloud computing across the enterprise.

## References


1. K. Weins, "Cloud Computing Trends: 2015 State of the Cloud Survey," blog, 18 Feb. 2015; www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2015-state-cloud-survey.
2. K. Giannakouris and M. Smihily, *Cloud Computing—Statistics on the Use by Enterprises*, Eurostat, Nov. 2014; http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises.
3. P. Mell and T. Grance, *The NIST Definition of Cloud Computing*, NIST Special Publication 800-145, Nat'l Inst. of Standards and Technology, 2011, p. 3; http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
4. *Enterprise Risk Management—Integrated Framework*, Committee of Sponsoring Organizations of the Treadway Commission (COSO), Sept. 2004, p. 16; www.coso.org/erm-integratedframework.htm.
5. R.R. Chalse et al., "Inter-cloud Data Transfer Security," *Proc. 4th Int'l Conf. Comm. Systems and Network Technologies* (CSNT), 2014, pp. 654–657.


**ADAM GORDON** *is a chief information security officer/chief technology officer at New Horizons Computer Learning Centers. His research interests include security, cloud, and GRC in the enterprise. Gordon has a master's degree in international political affairs from Florida International University. Contact him at agordon@nhflorida.com.*