Cheatography

Cybersecurity PSaaS Roles & Responsibilities Cheat Sheet

by [deleted] via cheatography.com/2754/cs/13187/

Introduction: Complex Deployments

Cybersecurity responsibilities for more complex PSaaS deployments are simply extended across the vendors and cloud infrastructure providers involved. It is possible, for example, to have two or three PSaaS vendors — for example, one each for access control, video management, video analytics and visitor management.

Each PSaaS vendor may have a different cloud infrastructure provider. There may be both cloud-level integrations and on-premises integrations between the various PSaaS offerings. All of the cybersecurity issues must be identified and the responsibilities accounted for to ensure that there are no gaps in cybersecurity protection. This should be reflected in the documentation of the various product and service offerings.

Assurance of continuous conformance to cybersecurity requirements should be provided by the chain of Service Level Agreements from cloud infrastructure provider, to PSaaS vendor, to security systems integrator, to cloud service customer.

Whether the picture is simple or complex, it is important to ensure the cybersecurity of a PSaaS offering by determining, fully agreeing on, documenting, and verifying who is responsible for what, and how those responsibilities will be lived up to.

Credit: Ray Bernard, PSP, CHS-III

http://www.securityinfowatch.com/article/12270050/cloud-security-roles

PSaaS Security Roles

Role	Description	Security Responsibilities
Cloud Service Customer	Utilizes the PSaaS offering for security operations and investigations, and uses the business-related video analytics data for business planning and decision-making.	■Identifying and/or specifying cybersecurity requirements of data that will reside in the cloud. That includes the classification of the data (confidential, private, etc.) as well as any regulatory requirements such as country residency (data must be stored within that country). Classification and residency requirements determine the encryption requirements and backup data location options ■Approving the cybersecurity profile of the cloud service, including its on-premises equipment ■Stringent management of user logons credentials to the SaaS application and on-premises security systems equipment, unless integrator provides user logon credential management as a service ■Regularly reviewing/auditing system and device access records and user access privilege assignments, and for timely performing or initiating termination of access privileges when appropriate ■Network security for the on-premises equipment, if the on-premises equipment resides or connects to the Internet via on the corporate network

PSaaS Security Roles (cont)

Security Systems Integrator	Installs & maintains the PSaaS on-premises equipment.	■Verifying the status of cybersecurity controls for the PSaaS offering and any cloud-based integrations involved ■Accurately informing the customer of the cybersecurity profile of the cloud service ■Cyber-secure configuration of the on-premises equipment ■Stringent management of service technician logon credentials for accessing on-premises equipment and the cloud service
PSaaS Vendor	Provides the SaaS Application and provides or specifies the on-premises equipment that the Security Systems Integrator resells.	■The cybersecurity of the SaaS application and any cloud-based integrations to it ■Cyber secure configuration capabilities for any on-premises equipment provided or specified ■System hardening guidance ■Vulnerability policy and method for integrators and their customers to report cyber vulnerabilities
Cloud Infrastructure Provider	Provides the Platform as a Service (PaaS) infrastructure on which a SaaS application runs (such a Microsoft Azure or Amazon AWS)	■Computer and network security of the cloud infrastructure provided ■No responsibility for SaaS application security ■No responsibility for on-premises equipment