Cloud Computing and Software as a Service (SaaS)

An Overview for Security Professionals

Presented by
the Information Technology Security Council (ITSC)
and Physical Security Council (PSC)

ASIS INTERNATIONAL
Advancing Security Worldwide®

Cloud Computing and Software as a Service (SaaS)

An Overview for Security Professionals

Table of Contents

ABOUT THIS PROJECT

This project was conceived during Q4 of 2009 and this paper is the result of a collaborative effort of two ASIS International Councils: the Information Technology Security Council (ITSC) and the Physical Security Council (PSC).

This paper was researched, drafted, and written with the specific intention of introducing Cloud Computing and Software as a Service, relevant to the security practitioner, particularly those who have an interest in, and responsibility for, physical and electronic security and the potential application of cloud computing in this environment. It does not address Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) or other variants of Cloud Computing; such white papers may be the result of further initiatives.

Although some of the concepts are technical, they are explained and expanded upon with the intention of providing an introduction to the concept, not the final word.

Enterprise Security Risk Management and Convergence have become more than emerging concepts, and a new platform of physical and electronic security products and services are emerging that realize the convergent nature of the security industry.

The rapid, worldwide adoption of cloud computing by organizations, both federal and commercial, has profound implications for business. With this adoption there are significant security considerations, and alternatives to the traditional model in which core security services are being delivered.

Cloud hosted services and their companion hardware products for physical security are also emerging; supporting such functions as hosted access control, alarm monitoring, and video surveillance. Given the reliance that is placed on these important security functions for the protection of life, property, and information, any implementation requires careful consideration.

This paper is a valuable resource for organizations considering a “cloud” solution, raising many questions to consider and discuss with potential providers.

Sincerely

Shayne P. Bates, CPP
Chairman
Cloud Computing Workgroup

Ronald Lander, CPP
Chairman ASIS ITSC

Benjamin M. Butchko, CPP
Chairman ASIS PSC

ACKNOWLEDGEMENTS

ASIS members are unpaid, expert volunteers, contributing their time and expertise to the continuing education of fellow security practitioners. In addition to the efforts and sponsorship from the two ASIS International Councils, the following individuals assisted in the research and compilation of this white paper. Their work is greatly appreciated.

Contributor	Company	Role
Shayne Bates, CPP, CHS-V	Brivo Systems, LLC.	Chair, Reviewer, Writer
Benjamin Butchko, CPP	Butchko Security Solutions	Vice Chair, Reviewer, Writer
Kelly Kuchta, CPP, CFE	Forensics Consulting Solutions, LLC.	Vice Chair, Reviewer, Writer
Working Group 1		
Ronald Martin, CPP	Department of Health and Human Services.	Reviewer WG1
Gary Klinefelter	Creative Innovation Strategies.	Writer WG1
Working Group 2		
Phillip Banks, CPP	The Banks Group.	Reviewer WG2
David Lam, CPP, CISSP	Stephen S. Wise Temple.	Writer WG2
Thomas McElroy, CPP, PCI	The Hospitality Security Consulting Group, LLC.	Writer WG2
Richard Withers, CPP	TRC Systems.	Writer WG2
Working Group 3		
Coleman Wolf, CPP, CISSP	Environmental Systems Design, Inc.	Reviewer WG3
David Morgan	Booz Allen Hamilton.	Reviewer
Thomas Ianuzzi, CPP, CISSP	Information Security Consultants, Inc.	Writer WG3
Steven Yanagimachi, CISSP	The Boeing Company, Inc.	Writer WG3

Disclaimer: The views and representations made within this document are those of the contributors and do not necessarily reflect the views of the organizations that they represent.

INTRODUCTION

The traditional electronic security industry, whose origins are rooted in the burglar alarm, is now moving very rapidly toward more complex networked systems and information management. Much discussion has occurred about the role of IT and physical security and the need to work closely together to manage and deliver efficient and risk appropriate security systems for the benefit of organizations. Much of this discussion has occurred around the developing framework for enterprise security risk management and convergence.

As the security and reliability of the Internet and the services offered over it matures, there is a movement toward shared services. Some of the shared services are manifested in technology offerings that have such characteristics as fast implementation, reduced operational expense, and a multi-tenant model sharing common computing resources. The common terminology for this is Cloud Computing, and it is explained in this paper.

Companies such as the $1.2B+ per annum Salesforce.com (NYSE:CRM), demonstrate how the delivery of Cloud Computing services are taking hold, as they participate in the delivery of an "on demand" service model for hosted business applications.

A discussion within the security domain is evolving around how Cloud Computing, which has a distinctly different technology and business model (than traditional physical security technologies), might be utilized to deliver security services and applications. The discussion includes such security topics as continuity, reliability, and compliance; and what the associated risk profile and business benefits are in considering such a proposition.

This paper touches on several of these issues and is best read in conjunction with other material available to the security professional about cloud computing. References for further research are included herein, in footnotes at the bottom of the relevant pages, which contain "click on" hyperlinks.

DEFINITION OF SOFTWARE AS A SERVICE AND CLOUD COMPUTING

The United States Government's National Institute of Standards and Technology, (NIST) defines cloud computing as:[1]

> *Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential* ***characteristics,*** *three* ***service models****, and four* ***deployment models****.*

Essential Characteristics

On-demand self-service*:* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access*:* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and Personal Digital Assistants (PDAs).

Resource pooling*:* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity*:* Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service*:* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Service Models:

Cloud Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are

[1] NIST Definition of Cloud Computing, see:http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

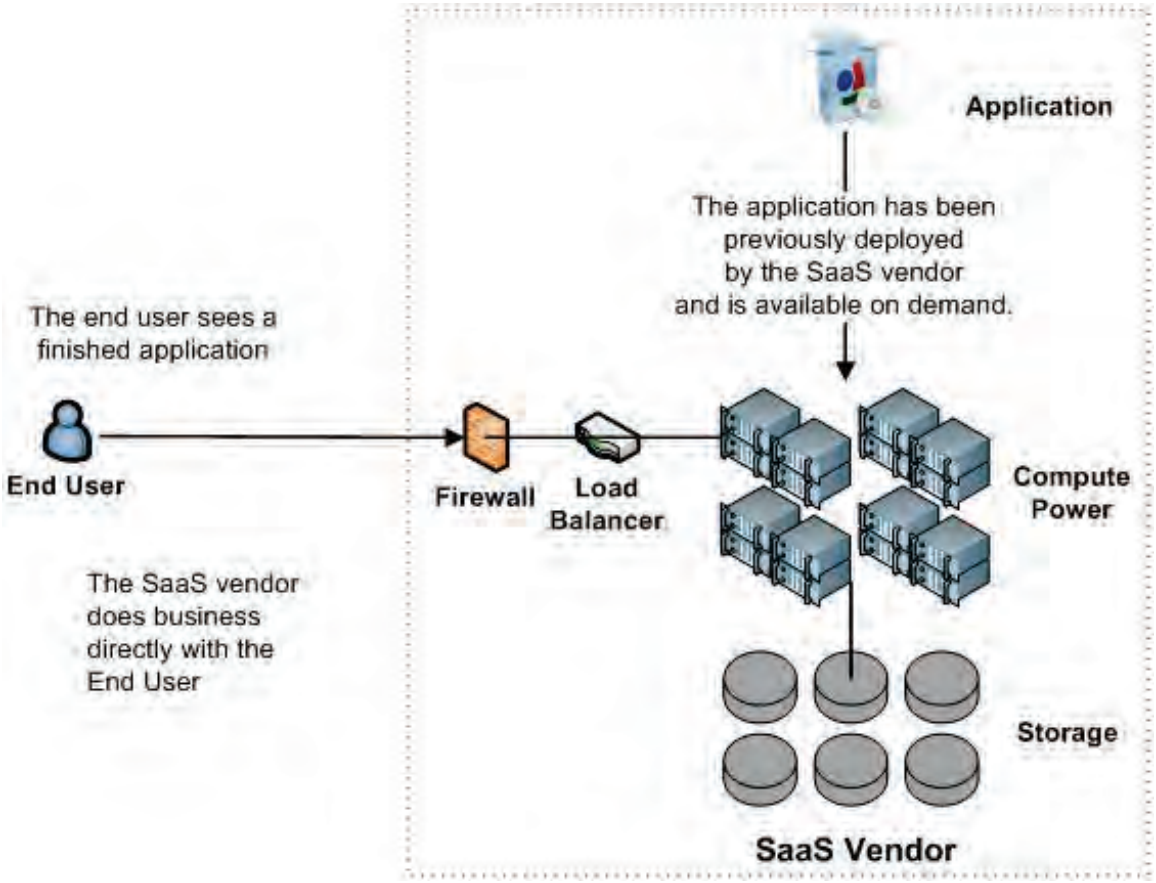

Figure 1 - Software as a Service (SaaS)

[2]

Cloud Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

[2] Understanding Public Clouds, see: http://www.keithpij.com

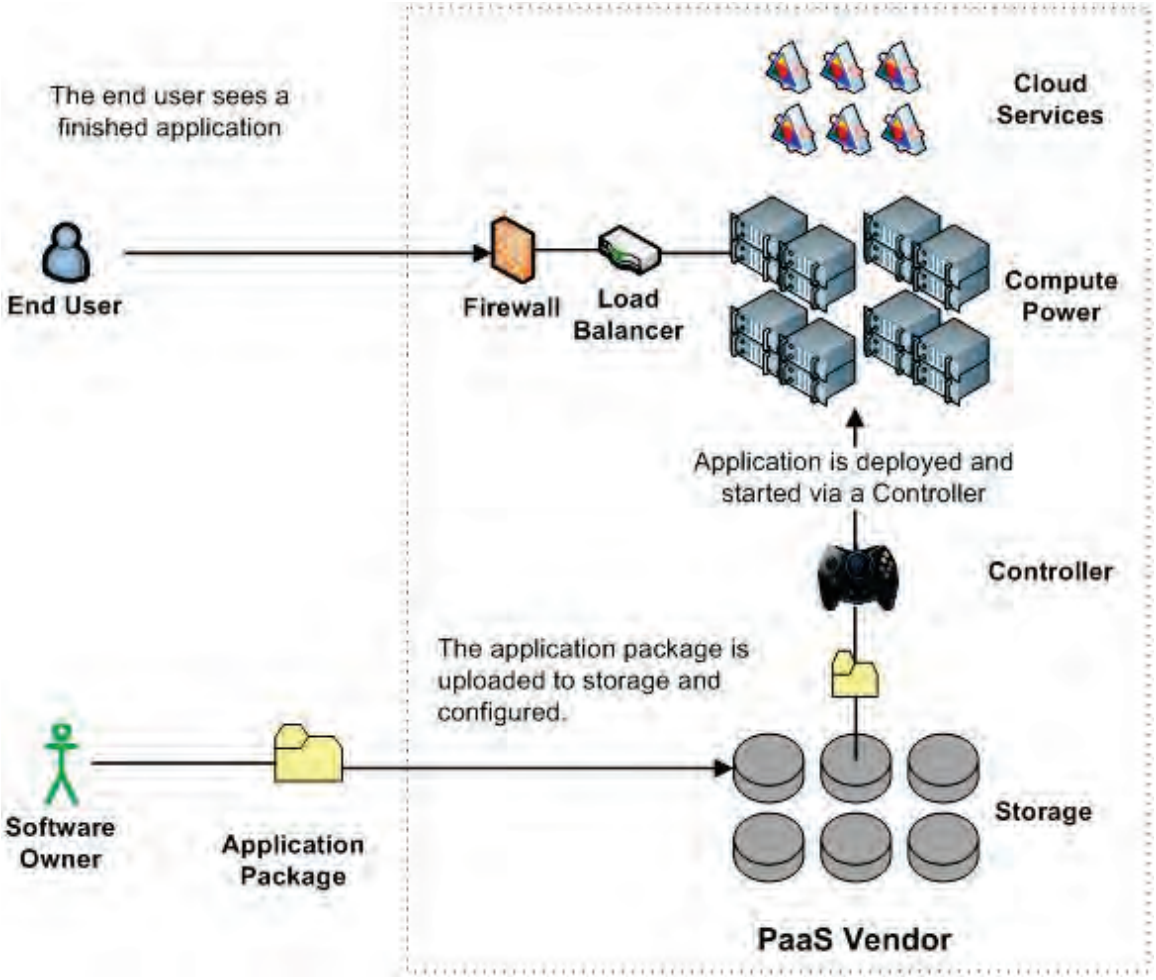

Figure 2 - Platform as a Service (PaaS)

[3]

Cloud Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[3] "Understanding Public Clouds" http://www.keithpij.com

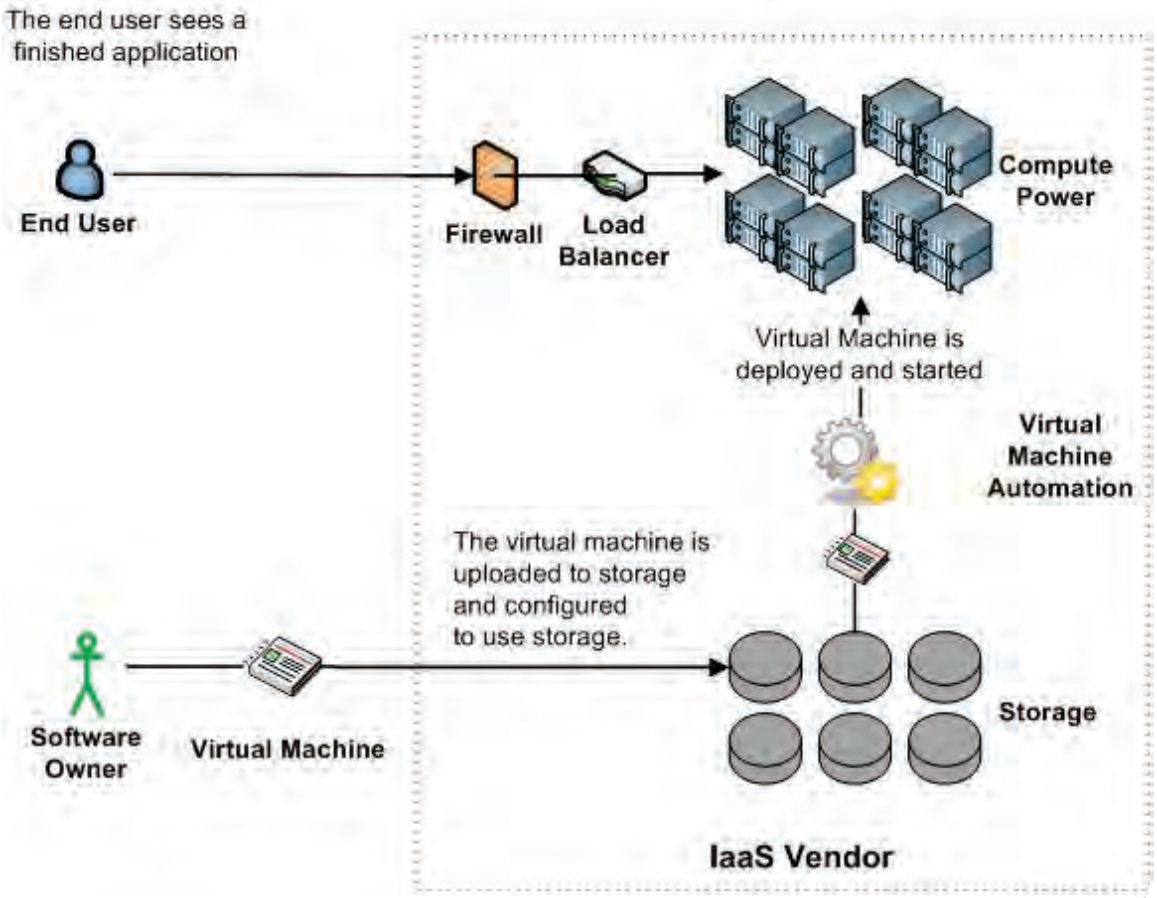

Figure 3 - Infrastructure as a Service (IaaS)[4]

Deployment Models

Private cloud. The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., "cloud-bursting" for load-balancing between clouds).

[4] "Understanding Public Clouds" http://www.keithpij.com

IT Deployment Examples[5]

- Google offers a vast array of software on demand using their enormous server power. There is no software to install on the user's computer—everything actually runs on Google's machines and is accessed via the user's web browser. There is nothing for the user to install and since the application runs on Google's servers, the processing prowess of the user's computer can be minimal, even a simple cellular phone web browser can write documents and presentations utilizing the processing power contained in the cloud.

- Salesforce.com offers clients the ability to independently use powerful servers with built-in database structures, mapping utilities, and other application interfaces. Whilst a generic SaaS model is supported through use of a web browser, an alternative to the SaaS approach is offered, allowing clients to use their own proprietary frontend software suite, which is more correctly defined as client-server.[6]

- Amazon's Elastic Compute Cloud (EC2) allows users to run their own software on an extremely powerful server farm.[7] Such use can drastically cut computation times for unique, complex databases and other types of software calculations.

CONTEXT AND STATISTICAL INFORMATION

The context of this paper is to examine Cloud Computing for physical security as a service offering (an SaaS model). While we could also explore platform and infrastructure offerings as a service, this is left for a future discussion. According to Gartner the SaaS market is expected to grow 22% per year with 25% of the software being delivered by software as a service by 2011.[8]

While physical security technology has traditionally lagged many IT trends, there are SaaS offerings in the security market today, offered by several companies which incorporate the latest advances in IT technology. A key differentiator of physical security SaaS offerings, from generally known SaaS offerings such as Salesforce.com, is the need for hardware security components on the customer's premises, to interact with the hosted applications in the cloud environment.

---

[5] Corporate and product examples in this section and throughout the document are provided for explanatory purposes. Inclusion does not denote endorsement by ASIS International.

[6] Client-Server, see: http://en.wikipedia.org/wiki/Client-server

[7] Server Farm, see: http://en.wikipedia.org/wiki/Server_farm

[8] Gartner - Market Trends: Software as a Service, Worldwide 2008-2013, see: http://www.gartner.com/DisplayDocument?ref=g_search&id=965313

These hardware security components (e.g., Access Control and Video Surveillance hardware) are also subject to regulatory and life safety code[9] requirements for compliance. The Code establishes minimum criteria for the design of egress facilities to allow prompt escape of occupants from buildings or, where desirable, into safe areas within buildings.

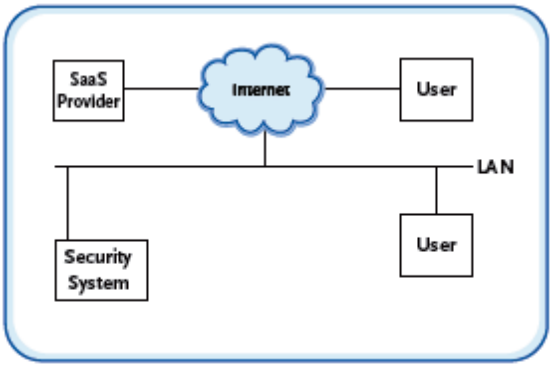

Figure 4 - SaaS Architecture

This adds an additional dimension of responsibility and security.

One advantage of physical security as a service is much like the traditional alarm companies in operation today—they can serve both small and large companies across a very wide geography.

Small companies that may not otherwise afford the purchase of the physical security infrastructure that they require may find it desirable to share services with other companies when delivered in a common "pay-as-you-go" model. Likewise, large companies may struggle to provide consistent security for multiple and remote sites. Thus, large companies may benefit from a service provider who already has the capability to deliver SaaS. Furthermore, the very nature of the shared service model extends consistent services across a large geography, and scales from a small number of users or devices (depending on the use and metric) to a large number.

Another reason to consider SaaS is scalability. In the case of the small organization, the services delivered may grow with requirements—expanding and adding services as needed either locally or across dispersed locations. For larger organizations, the ability to scale up and down as business needs change can be a benefit.

One of the most serious questions to ask about SaaS is that of security and compliance with regulations.

[9] NFPA 101 Life Safety Code, see: http://www.nfpa.org/aboutthecodes/list_of_codes_and_standards.asp

- Is data secured? How do I know it is secured?
- Is access controlled?
- What is the contractual agreement for responsibility?

This white paper addresses a number of the above concerns in the later part of this paper, and assists in framing some of the questions that should be addressed when considering a system.

COST OF OWNERSHIP

In a physical security system the cost of ownership will most likely include the services that you purchase, and people that you employ, to manage the technology that you purchase. In addition, the ongoing costs are significant to maintain infrastructure, including the network and data center, and when properly measured the overall costs are significant.

Any comparative example could include software as a service used for setting and monitoring physical security; employees that set security policies and modify system settings; as well as security components such as readers and cameras.

A comprehensive review of the *total cost of ownership* is required for a substantial comparison to any alternative model under consideration. Several vendor papers exist and identify the components of service, hardware, maintenance and IT cost associated.[10]

For example, a traditional implementation of an access control system factors in IT, software and server costs that are removed in the typical shared computing model that SaaS provides, and capital expenditure is replaced or augmented by an operational expenditure model. Consideration therefore, needs to be given to these differences, using business logic and financial analysis.

If there is already a physical security system in place, there may be an opportunity to utilize some of the existing equipment when converting to a SaaS model. Likely candidate items are door locking hardware, request to exit (REX) switches, alarm sensors, existing cabling, and Video Surveillance cameras. Cable reutilization requires evaluation of plans regarding structured cabling and Power over Ethernet (PoE) technology which are leveraged in SaaS deployments. Although many organizations are switching to digital camera technology, significant debate still continues with respect to Video Surveillance.

[10] How Web-hosted Software-as-a-Service (SaaS) Lowers the Total Cost of Ownership (TCO) for Electronic Access Control Systems, see: http://www.brivo.com/benefits/cost

Generally, the investment in locking, readers, door position switches, accessories, power supplies and cabling infrastructure may be retained as part of the existing in-place systems. Installation of network connected access control panels (hardware) replacing the direct-connected access control panel, and software application conversion from dedicated systems to SaaS solutions supporting reuse and conversion

Current physical security policies should be reviewed to establish which policies might require refinement or implementation when migrated to a SaaS system. For example, what is the service level available to the site administrator in the event that the Internet connection becomes unavailable? What is the role of IT in supporting connectivity to the system?

DEPLOYMENT CONSIDERATIONS

As a system is deployed for physical security SaaS, security concerns such as building intrusion need to be considered in conjunction with IT concerns like network availability and access. Service providers and corporate IT departments are a good source of knowledge on both subjects. Security integrators and consultants, with proven experience in deploying Cloud solutions will provide additional points of view.

Deployment of a service starts with a service level agreement relevant to the solution being implemented. This agreement needs to represent the service provider's and premise holder's needs alike. Clear responsibility for continuity, reliability, and security needs to be addressed. Responsibilities may be complicated by the internal components required for security access of doors or detecting events on security cameras. Company security policies may also dictate responsibilities that need to be outlined in a service agreement.

Evolving standards for security in organizations authored by ASIS International (ASIS) and the Security Industry Association (SIA) are worth reviewing with "security as a service" vendors. These standards can help to provide a common framework and the ability to use multiple vendors of the same security services. Additionally, at a technology level, various manufacturer driven industry alliances are emerging, which present several interoperability possibilities for vendors of security equipment technologies.

If an outside SaaS hosted security application provided as a service through the web browser, is going to access on-site security components, additional questions need to be addressed:

- Does this change the cost of providing on premise IT infrastructure and security?
- What new security considerations arise?
- Do external, or outbound ports at firewalls require opening, or does the service utilize standard ports?
- What are the security implications of opening up such access?

IT RESOURCING CONSIDERATIONS

In the case of small organizations, it is likely that one integrator may provide all services. For larger organizations, IT and physical security integrators may provide services which complement SaaS services and thus, need to be involved in the resourcing decisions.

Larger, centralized sites may stay with internal systems while a smaller site (or multiple smaller sites operating as one) may adopt the SaaS model for physical security.

In some cases, a hybrid of internal systems and external services may be an advantage.

A hybrid solution represents one way to migrate toward a more flexible SaaS model. The perceived norm today is to redeploy internal resources for common services while focusing IT on internal business needs. Although the reality is that in the case of a SaaS application for physical security, the application appears "online" instead of "inside" the organization. Administration is still achieved by the security administrator (unless outsourced), but several costs are reduced and eliminated.

INVESTMENT MODEL — CAPITAL AND OPERATIONAL EXPENDITURE CONSIDERATIONS

As capital and operational considerations are formulated into buying decisions, the differences in SaaS and traditional models need to be understood. The usual expenditures for components and maintenance need to be considered along with changes in policies and employee involvement. For instance, if SaaS for physical security changes the behavior for employee identification, how does the cost change? How do the internal versus external services play out over time when insurance, electricity and building costs are considered?[11]

A thorough financial analysis is a good companion for such considerations.

DISASTER RECOVERY CONSIDERATIONS

SaaS Provider Security Process

- Ensure cloud suppliers for critical systems are vetted to ensure that there is a clear understanding of what data is to be shared and what controls are to be

[11] How Web-hosted Software-as-a-Service (SaaS) Lowers the Total Cost of Ownership (TCO) for Electronic Access Control Systems, see: http://www.brivo.com/benefits/cost

utilized. The vetting process should determine whether the risk is acceptable to the business. The Introduction of a higher risk proposition in the cloud environment should trigger further reviews of the risks related to the vendor, platform or application.

- Ensure that the SaaS provider disaster recovery plans, capability for critical applications, and the impact on critical business systems are commensurate with business risk thresholds.

Crisis Communication

Clearly define what level of communication between the user and the SaaS provider is required during environmental or cyber related crisis, so that the user crisis communication program can be effective. Ensure a "back-out" or "roll-back" plan is available to re-start operations if the SaaS supplier is unable to recover. Ensure the supplier understands the requirements of customer's public relations polices to ensure that no statements are made during a crisis that will negatively impact the user.

Compliance

Ensure infrastructure, policies and procedures of the provider deliver the required regulatory and international standards compliance sought. Ensure the ability to evaluate, test and monitor the compliance requirements are clearly defined in contracts and policy. If third parties need access to verify compliance, ensure provisions are included in contracts.

APPLICATION TO PHYSICAL SECURITY MARKET

COMMON COMPUTING INFRASTRUCTURE CONSIDERATIONS

As mentioned previously, a service agreement between end users and service providers should define the responsibilities of each party. Several items to consider responsibility for remediation are:

- Power outages on-site or at the service provider;
- Internet outages on-site or at the service provider;
- Outages from natural disasters;
- Security breaches; who will assume the risk?
- Access to data and on-site security components;
- Redundancy of equipment and data;
- Rapid recovery from disaster situations;
- Ongoing compliance with an accepted standard (such as SAS-70 type I & II).

What is the interface between the security service software and the internal IT network? What kinds of internal equipment are connected to the service? For instance, internal security panels, and in particular on-site video recorders (network video recorders and digital video recorders), may reduce the need for external bandwidth, compared to connecting cameras directly to an external storage source.

This raises another important question: What is the *actual* requirement? In the case of surveillance video, what is the frame rate and resolution that is required? If a frame rate of 5-7 frames per second for a handful of cameras per site to provide general observation video is acceptable, then it is likely that hosted video is a useful candidate for consideration in meeting the requirement.

Is the video utilized in real time or stored for potential analysis later? How long is the storage requirement?

If high resolution, high frame rate video, with a large density of cameras on the site, then it is likely that local storage in some form will exist to support the enormous amount of traffic circulated.

Frame rate, resolution, movement, brightness and color are all items that affect required bandwidth and requirements should be carefully considered.

SCALE OF ECONOMY OVERVIEW

One clear advantage of a SaaS system is the ability for companies to share resources. This is generally going to be better value because the investment in infrastructure is avoided and access to a larger, well-maintained system is available—similar to an electric utility service. Knowing what this means to your organization's security system and the ability of a service provider to react to demand is important.

Service providers need to have capacity for growth, redundancy protection in place, and the ability to react to increased demand in the event of a disaster or temporary increase in need. Bandwidth can be a formidable hurdle. One way to mitigate bandwidth issues from becoming problematic is to implement locally installed security panels or video recorders in-house, while the software and computing resources are located in the cloud.

SYSTEM INVESTMENT MODELS

Although system investment models will vary depending on the vendor involved, there are some important differences between a more traditional system and a SaaS based system.

A traditional system involves the expenditure of upfront capital for the entire system, with an ongoing maintenance cost. SaaS services delivered through the cloud generally require the purchase of equipment at the site (e.g., an access control panel, video surveillance cameras) and any locally installed components that are required for the infrastructure such as network switches or interconnection equipment.

In a SaaS model delivered through the cloud, purchase of items such as servers, the associated system, and application software that delivers the security management capability, and all of the associated peripherals is avoided.

Given the avoidance of capital investment; the ongoing maintenance and upgrades, as well as the associated staffing resources and infrastructure to deliver service, is provided by the SaaS provider, in most cases for a monthly fee.

The calculation of the SaaS fee varies by vendor solution, but is based upon common elements:

- **Features/Modules Utilized** — The feature set employed (many vendors have alternative choices and modules).
- **Number of Devices** — The footprint and function of the hardware (e.g., number of doors controlled and number of video surveillance cameras).
- **Number of Identities** — In the case of interconnection between a Physical Access Control System (PACS) and an enterprise identity system (such as HR or payroll), there are usually associated costs with providing connectivity and synchronization services between system databases.

THE MULTI-TENANT SOFTWARE MODEL EXPLAINED

TECHNOLOGY DESCRIPTION

The diagram below shows all of the basic components of a physical security system using SaaS: the service provider, a user inside or outside the premises and the security system.

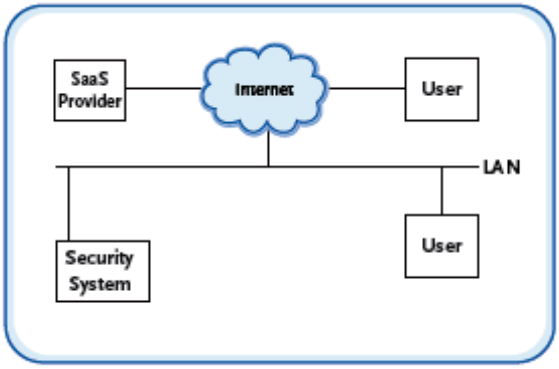

Figure 5 - SaaS Architecture

The security system could be any number of security components, either at one physical site, or across many different sites. With respect to electronic access control, a common way to manage door access is through a security panel that connects door readers and intrusion sensors together. In the case of network connected hardware devices (such as Power over Ethernet (PoE) access control devices), these devices generally have their own access control list individually loaded on a "per device" basis, instead of centrally through an access control panel.

Whether a PoE device (often referred to as an "edge" device), or a more traditional card reader and panel combination is used, both devices connect to security management software, which synchronizes data, including configuration and policy changes. In the case of a SaaS hosted system, the components of the security management system are located offsite at the data center of the SaaS provider. Configurations related to access are synchronized from the cloud, to local equipment in existence at the site, which performs the immediate access function. In the event that the network connection becomes unavailable, data is cached at the local device and synchronized with the host system when the connection is restored.

Network connected door readers that are available today (of which many are PoE devices) have the ability to simplify the security infrastructure and provide significant benefits including cost, speed of deployment, and use of existing cabling infrastructure. In the case of PoE, the computer network may also provide power to some or all of the components of the access control hardware, such as card readers, edge devices, and

locking hardware. This allows the PoE system to conform to the standard for which it was designed[12].

In the event that PoE power requirements are exceeded (such as a large capacity magnetic lock), power may be provided locally as is customary with a traditional system. Additionally, because they are networked devices, they may be managed and controlled using existing IT infrastructure (e.g., SNMP[13] alerts if the device becomes unavailable). This is very useful for devices such as PoE powered IP Cameras. For example, one scenario may be that power to the camera is cycled (off-on) in the event that the network loses visibility to the camera. This has several advantages including the potential, almost immediate restoration of the surveillance function, recording of the error for further investigation, and an immediate response to non-functioning security assets.

Similarly, if surveillance functionality is the SaaS service being provided, a number of "inside the premises" options exist. The camera may include intelligent processing or an on-site video recorder may be intelligent. The software may have all of the intelligence. The main goal is to detect and notify events with a camera so that humans either don't have to monitor them real time, or that the real time monitoring may be focused on responding to events that have been notified by the system itself.

With respect to surveillance technologies, the configuration of the system and the bandwidth available will influence SaaS options, and local infrastructure, and cost-benefit analyses. High resolution and high frame rate video commonly requires some form of local storage and playback (such as a Digital Video Recorder (DVR) or Network Video Recorder (NVR)). Lower data rate solutions with non-megapixel resolution and image rates of 7 images per second or less are readily available with SaaS hosted video solutions. Wider deployment of advanced compression technologies and continued improvements in compression, intelligent processing, and available bandwidth will continue to expand SaaS for video capability.

There are always people operating the technology at various points along the way. Security policies should be in place at both the customer and the service provider to ensure that people follow correctly defined actions. These actions may be authorizing a new user, updating account information, changing access privileges, enabling new equipment, etc. This is a good place for IT and security professionals to discuss their

[12] The Role of Power over Ethernet in Future Security Applications, see: https://siamembers.siaonline.org/eweb/DynamicPage.aspx?Action=Add&ObjectKeyFrom=1A83491A-9853-4C87-86A4-7D95601C2E2&WebCode=prDetail&DoNotSave=yes&ParentObject=CentralizedOrderEntry&ParentDataObject=Invoice%20Detail&ivd_prc_key=00F0718F-DFA2-42D5-8E84-B8F95D77D64B

[13] SNMP and its uses, see: http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

mutual responsibility for physical security. It is also important to include in your discussion the service provider who provides maintenance for on-site devices, as well as the SaaS provider. This discussion may uncover new responsibilities that need to be addressed. Requirements should be documented in a service level definition between the contracting parties.

What is Multi-Tenant Software?

In a Software-as-a-Service model, the term "multi tenant" has a specific meaning. It refers to the capability of an application, generally consisting of a software and database combination, to support many tenants (organizations) on a common platform, with compartmentalization[14] (separation) of each tenant's data and configuration.

For example, Company A may decide to implement an SaaS based access control and video surveillance systems across several sites having a large geographical spread, with a small number of doors and cameras at each site. Company B may decide to implement a similar system. In the multi-tenant model, each company may in actuality be sharing the same hardware and software resources located at the provider's data center, but cannot see each other's schema, data, or even have any awareness that other organizations are using the service. One example of this is the telephone system where common elements exist, but the infrastructure is "on demand" and allows the user to establish a set of configurable parameters (such as a telephone call) and maintain privacy between each user for those calls, even though many other users are using the commonly available resources.

Not all SaaS Architectures are the same

SaaS architectures may be classified as having four maturity levels. The key attributes are multi-tenancy, efficiency, and scalability.

In brief, the first two levels are ad-hoc and do not feature a multi-tenant software component as they require the installation of a separate customized instance of the application. This has a direct impact on the cost model for enterprises that seek the advantages of a competitively priced solution that will scale. Maturity levels three and four are both multi-tenant, allowing a single instance to serve all customers. The fourth maturity level has all three attributes: scalable, efficient, and multi-tenant to match demand without further alteration of the applications software architecture.[15]

A "Litmus test" of multi-tenant SaaS software, is whether the user may enable or disable levels of service (or the service entirely), without the need for human interaction at the

[14] Compartmentalization, see: http://en.wikipedia.org/wiki/Compartmentalization_(computer_science)#Encapsulation

[15] Software as a Service, see: http://en.wikipedia.org/wiki/Software_as_a_service

service provider. Can data exist "in the cloud," with the service being entirely managed by the end user administrator at the customers site?

In summary, important considerations around the maturity level of the SaaS service exist; namely, whether it may be independently configured, managed, and scaled on demand, according to the needs of the user at the time, while all data, both "in flight" and "at rest" remains secure.

The functions described above have an important impact on the SaaS cost model and whether it will prove to be commercially efficient in meeting the cost, performance, and compliance needs of the potential customer, especially if scale, security and self-management are important factors.

DIFFERENTIATING SAAS FROM REMOTELY HOSTED SOLUTIONS: QUESTIONS TO ASK

With the advent of different security manufacturers presenting different offerings "in the cloud," there is the potential for much confusion about what multi-tenant SaaS services are, and are not. The section preceding this describes the attributes of multi-tenant software. This section includes several terms that are important to consider in the multi-tenant context.

What Saas is Not

Remotely Hosted suggests remote hosting of hardware or software, but the description is not multi-tenant specific. Some services utilize a "client-server" model where software is required to be installed on specific computers at the client's site, while the server is hosted elsewhere.

Some debate exists about the role of cloud-hosted services and the ongoing role of client-server.[16] For the purpose of this description, a simple differentiator to establish whether the model is client-server or SaaS based, is to enquire whether additional software, in addition to a web browser is required to be installed (If additional software is required, then the model is not considered SaaS).

Some cloud providers are presently developing "offline" software components that cache information locally in the event that the SaaS service or connection is unavailable, and then synchronize when the service or connection is restored. This is typically representative of a client-server computing model and is nothing new. While the most visible method is to provide a piece of client software to allow functions to continue, in the physical security context, caching of information locally is already provided by the design and capability of hardware devices that cache information and transactions.

[16] The client-server model: Not dead yet, see:
http://money.cnn.com/2009/02/16/technology/copeland_oracle.fortune/index.htm

In the context of access control, panels and edge devices cache access control lists and usage data for reasons other than just availability. The decision on whether access will be granted at a door after presentation of a valid card read requires a decision and response within a few hundred milliseconds, a task that is rarely achievable on a geographically consistent basis using today's Internet technology if the network is congested or unavailable. This is why hardware devices that operate independently of a central server have intelligence at "the edge," or have capabilities and data contained within an access control panels memory.

This is also true of surveillance devices; IP video cameras have emerged that support local storage, allowing surveillance data to be stored locally and transmitted according to several circumstances, including events that require transmission (where analytics is used) and where, for whatever reason, the "at rest" storage device is unavailable.

As a general rule, security considerations exist for every device that has the ability to cache rules or event information, or pass data through the networked system. Questions such as upgrade capability, security of the data stored, and the cost of management are all considerations.

STACK-A-BOX Vs MULTI-TENANT

"Stack-a-Box," is a generic term in use that describes less scalable systems that operate locally, or in data centers to perform cloud based security functions. They generally do not participate in a service-oriented architecture,[17] nor offer the degree of scalability for the on-demand growth that the multi-tenant model requires.

They are, however, useful for single function, sole purpose situations where scale is achieved by stacking more servers together as part of a hybrid solution.

On the surface, they may seem to offer better segmentation of customer data, but such benefits are at best, questionable, if the system is network connected (as is required for a hosted model), is exposed to other network traffic, and by definition, has the potential to be penetrated. Additionally, the operating system and application requires to be kept in-sync with latest revisions, and these systems miss out on the cost benefits that are attributed to the community style model that SaaS offers. This is because of the individual attention that is required to maintain the latest revision of the application and operating system patches, which is uneconomic compared to other large-scale service oriented systems. The economics of this approach may be uncovered with a thorough technical and economic analysis.

[17] Service-Oriented architecture, see: http://en.wikipedia.org/wiki/Service-oriented_architecture

SaaS IN PHYSICAL SECURITY TODAY

In exploring the growing impact of Cloud Computing on physical and electronic security, discussion is limited to systems providing electronic security services (such as alarm monitoring, access control and surveillance).

Access control

In a traditional alarm and/or access control system, sensors are monitored by a control panel(s) usually located within the protected facility. In addition, the alarm features of the system are commonly supervised by an external monitoring facility connected via a telephone line, Internet connection or wireless communications.

Aside from alarm reporting, all other functions, such as access control administration and reporting can be conducted on site. In many cases the integrator can communicate with the panel remotely.

In contrast, in the cloud computing model, each edge sensor, networked keypad, or device containing intelligence, reports directly to software in the cloud. Management, administration and reporting are similarly handled in the cloud with the user input being provided via a web interface. Responsibility for managing the system may remain with the client or be provided by personnel as a managed service for the customer. In either case, the management activities are carried out on the service provider's equipment.

Several Service providers are offering apparently robust solutions that are integrated to varying degrees with other security services. Although some products may hold themselves out as SaaS solutions, they are in reality "remotely hosted client-server solutions." The section describing SaaS maturity levels, and multi-tenant architecture should be carefully reviewed in order to understand the true nature of the service offered to be ascertained.

Video Surveillance

The traditional approach to video surveillance systems is to locate cameras, recorders, and monitoring stations at the facility to be protected. The replacement of coaxial cable based cameras with IP cameras that transmit digital video via the Internet Protocol (TCP-IP) opened up a whole range of new possible service models. A common approach using less expensive equipment places the cameras and recorders on site in the protected facility and allows remote monitoring, and in some cases remote panning, tilting and zooming (PTZ) of the cameras. An alternative that is emerging to PTZ is the digital equivalent, where a higher resolution image is captured, by a fixed camera (usually megapixel)[18] over a wider field of view. Magnification of the image is achieved

[18] Digital and analog video, and megapixel functionality, see: http://en.wikipedia.org/wiki/Closed-circuit_television_camera

by real time cropping of the image "on the fly." Because the image is such high resolution, pixilation of the image, which distorts the quality, is averted and sufficient information is presented to ensure that the image is still sufficiently viewable.

The emergence of hosted video solutions, whereby the actual video data is transmitted and stored at a remote site, is emerging. The majority of present service offerings are best suited to applications that require a lower frame rate and resolution because of the limitations of many network systems to transmit large continuous volumes of data produced by the camera. The present rule of thumb is that for each DSL connection,[19] two to four video surveillance cameras per location, at a frame rate of 5–7 frames per second may be supported, which is often suitable for overview video. However, these systems can deliver very powerful solutions for organizations with a surveillance requirement across several dozen, hundreds, or even thousands of locations as a standard, quickly deployable solution, with little capital outlay. Where higher internet upload speeds are available, higher resolution and frame rate solutions are available as Video Software as a Service (VSaaS) offerings.

Intrusion Detection

Entire intrusion detection solutions can be managed via SaaS. Several commercial solutions targeted for small business are available. Sensors and a control panel are located at the premises, with all management and data forwarding occurring remotely.

Visitor Management

Visitor management is an area where economy of scale can make a real difference in the sophistication available to most companies. Formerly, the initial acquisition cost limited the deployment of these systems to larger companies with the majority of businesses managing visitor access manually.

Several vendors exist and it is common for such vendors to offer the ability to connect with both cloud and traditional vendors to exchange data. The use of Application Programming Interface (API) tools to interconnect cloud-based databases together to exchange identity and transaction information is becoming common and referred to as "Inter-Cloud" connectivity. Although XML[20] is very common to implement such connectivity for either a cloud to cloud, or cloud to traditional systems, several other alternatives are evolving.

Mass Notification

Mass notification systems may be the ideal cloud application. The cloud computing model strongly supports system objectives. The hosted system is remote from the client facility, making it less likely to be affected by natural disasters. Multiple clients sharing

[19] Digital Subscriber Line, see: http://en.wikipedia.org/wiki/Digital_Subscriber_Line

[20] Extensible Markup Language (XML) API, see: http://en.wikipedia.org/wiki/Web_service

infrastructure are afforded a great economy of scale since these systems are used infrequently but must be scaled to meet peak demand.

Market Trends

The advantages of SaaS operating in the cloud can be significant. There are great gains to be realized in economy of scale, sophistication of feature sets and increased management capabilities.

Based on a recent survey by the Gartner Group, basic service issues such as performance, customer service reliability and risk management are among the considerations that slow the implementation of SaaS.[21] Interestingly, these factors vary by the country surveyed with the United States receiving a better report card than Great Britain. Furthermore, present adoption of SaaS in the USA is significantly greater than Europe.[22]

On balance, it is certain that SaaS services are flourishing. As with all new technologies, present concerns will be fully explored and when resolved, these services will gain a significant percentage of new installations and make inroads against the local computing model. The business benefits outlined that SaaS affords, make a compelling case for consideration in many security service portfolios.

We are now only seeing the tip of the iceberg in terms of the types of systems that may move into the cloud. One emerging factor is that vendors are expanding their services horizontally. This will result in interrelationships between systems that we have not anticipated and could result in more dominant SaaS offerings.

Law enforcement is one area which is primed for explosive growth. Current budget constraints are a strong factor motivating agencies at all government levels to adopt SaaS, because of the “pay-as-you-go” nature of the service offering.

Offsetting this, are concerns for privacy and security, which are often greater than those of their civilian counterparts. Currently, Fusion Centers and other information sharing systems are currently receiving the most attention but, as the security concerns are resolved, it is possible that SaaS may extend to all phases of police and other emergency services work.

---

[21] Gartner User Survey Analysis, Software as a Service, Enterprise Applications Markets Worldwide, 2008, see: http://www.gartner.com/DisplayDocument?id=802221

[22] Rainstor report and commentary, see: http://www.eweekeurope.co.uk/news/news-solutions-applications/uk-companies-still-fret-over-saas-and-the-cloud-2797

Current and future applications will grow in sophistication and may include:

- Video surveillance and analytics
- Traffic control
- Access control to public infrastructure
- Mass notification
- Incident management

The potential for integration of multiple types of services here is even greater than that which is now occurring in the private sector. This will improve law enforcement effectiveness, but will also create enormous privacy and ethical concerns.

SaaS Adoption Drivers

As with any industry, the drive to reduce program costs as well as increase the efficiency and effectiveness of security operations has become the pre-eminent goal. Maximizing security effectiveness and efficiency is a daily challenge, especially with the growth of technology as a tool to support security operations. As never before, security management and practitioners must show that the return-on-investment for ongoing security is appropriate and measureable.

Economics

Economics is high on the list of drivers for the security industry when considering SaaS, as it offers a solution to alleviate the capital expenditure burden that technology can impose on a security department's budget. The move to a SaaS solution allows an end-user to diminish the extent to which capital is used. Additionally, rather than having system hardware and application software on-site, which requires ongoing management and maintenance and the costs that go with it, the project may be augmented with "pay-as-you-go" operational expenditure, for services.

If we consider physical access control alone, the opportunities to reduce the costs of installing, maintaining, upgrading, expanding and measuring system performance may be significant, depending upon the size and configuration of the system. As an example, a common physical access control system will, at minimum require:

- Pre-project planning and design;
- Physical infrastructure e.g. conduit and cabling, field panes, credential readers, door hardware mechanisms etc;
- Head-end workstations;
- System and archive servers;
- System updates and service packs;
- Credential issuance and management;
- System Performance Monitoring and trouble shooting; and
- System reporting and response.
- Staff training

The foregoing is not an exhaustive list. Depending on the size, configuration and level of integration of the system with other protections other components and activities would be added to the foregoing list.

Security practitioners who manage or work with access control systems know that a significant amount of effort and emphasis must be placed on the management and performance components of the system. Tracking, installing and managing system

software updates and service packs can be a time consuming job, which has significant ramifications if not completed in professional and timely manner and the ability to mitigate risk can be severely impacted.

From an end-user perspective the immediate savings that may be expected from utilizing SaaS as a security solution will include:

- Availability of planning and design information from SaaS professionals based on their experience with other similarly sized projects;
- Elimination of headend-equipment (system and archive servers) costs;
- Elimination of application software license costs;
- Elimination of application and system management and maintenance costs;
- Reduction in design and implementation time;
- Reduction in system performance measurement costs;
- Reduction in data center space requirements for system head-end equipment;
- Reduction in the amount of data storage at the end-user facility or operation;
- Reduction in system expansion planning, and design costs.
- Ability to increase and decrease capabilities on-demand.
- Overall, significantly diminished capital expenditure requirements.

From the above list of potential savings, the reduction in the amount of computer infrastructure that a user would normally purchase is not the most likely reason they would consider a move to a SaaS solution. A key driver for potential end-users are the savings that accrue through elimination of multiple software application licenses and the financial return on eliminating the time and effort to maintain the application itself, as much of the responsibility is moved to the SaaS provider. This responsibility will also normally include complementary software upgrades and full support of the application's environment.

Another important benefit is an increase in consistent capability. SaaS provides a very effective platform for speedy implementation of enterprise class security tools on a consistent basis, across a wide geography, that is especially useful for organizations with multiple small to medium sized facilities (e.g., a global network of chain stores or office facilities), where a standard footprint, and consistent security posture is desired.

In addition to transferring the responsibility of maintaining the software application to the SaaS provider, the end-user also benefits from the speed at which the application is updated following improvements to the application itself. Because of the community nature of SaaS, this process occurs at no additional expense to the end-user and should be relatively transparent with respect to the operation of the system itself.

The downside of the automated upgrade approach, however, is that the end user has little or no control over version and feature changes to the application itself (e.g., in the event that an application is changed to support a security process in a different way, the

users ultimately have to operate the application in the manner that the SaaS application developer has decided). Several IT vendors of SaaS software, have softened the impact of these changes, by providing a change window where the user is given a window of time to migrate to the newer version of the SaaS application, but this is not commonplace yet. For larger users where this may be an issue, staying current with manufacturer roadmap implementations is useful, as is participation in any communication mechanisms (user feedback groups) about product feature enhancements.

A further way to mitigate the impact that changing critical features over time has is to inquire about the ability of the hosted application to exchange data with other sources, using a Software Development kit (SDK) or Application Programming Interface (API). Most vendors support this approach and although other technologies exist, the use of the XML API is common (as mentioned previously in the section about visitor management). Using this approach, a particular function (e.g., the handling of identities) may occur outside the core SaaS application, and the data that is critical to the function of the SaaS application, may be populated and managed from the externally connected system. This is becoming a common trend for synchronizing an organizations "person identities" (that may be contained in a Human Resources database) by sending them to the SaaS application for linking with physical credentials that allow access.

SaaS providers will allude to the fact that it is less expensive to use cloud-based applications and that the end-user is relieved of the expense of setting-up their own servers and data storage areas. Although this may certainly be the case, claims such as this should be put to the test in each instance to ensure it is worth the move to a SaaS solution and that the total cost of ownership and eventual return on effort are quantified and fully explored. The Total Cost of Ownership (TCO) model is an excellent way to compare the SaaS solution against the traditional method used to implement security technology project. Likewise, working with an organization's finance department to conduct a financial analysis of capital projects, using tools such as IRR (Internal rate of return), assist the security professional in analysis and in gaining support for projects that meet the essential financial criteria of the organization considering the project.

Efficiency

Although a reduction in capital and operating expenses is very attractive, an equally critical consideration is whether moving to a SaaS option will increase security's efficiency and overall effectiveness.

The journey to increased effectiveness is only maximized if efficiencies in time, effort and budget are realized and contribute to a performance measurement process. It appears self evident that if a SaaS solution will eliminate the need for an end-user to physically house, manage, maintain and support an application such as access control then increased efficiencies in the security function should be achievable. Shedding the

management of the software application process alone releases security resources to concentrate on other tasks that are critical to their corporations and organizations.

Another noteworthy efficiency inherent to SaaS solutions is the ability to access the service remotely via the Internet from anywhere at any time. This ability has contributed to the term coined as "on demand computing." This feature provides for greater control and management overview of the process as well as the opportunity to trouble shoot on-site problems from a remote location. That being said, this feature can also be incorporated in traditional "on-premise" systems; however, experience shows that it is not normally implemented or enabled in the majority of situations, as there are several barriers to a "manage anywhere" system. One example is the insistence of some vendors to open corporate firewalls for the convenience of remote management, due to the crude design of that vendor's technology. This approach frequently (and correctly) meets resistance from corporate IT security departments as it lowers the security posture of the organization by potentially reducing the security.

Efficiencies are not readily accrued in all instances as the end-users must accept and buy into the SaaS process and learn to work with it. This is often an issue of change management and recognition that the end-user is not the sole participant in a critical security protection such as access control. For some technical security resources, this will be the first time an important component of the overall security program is not under their sole control.

Other SaaS Drivers

Other drivers are also moving organizations and individuals towards an understanding that SaaS may be a viable option for use in the security environment. In recent years escalating use of the Internet to browse for information, complete transactions such as on-line banking and shopping, book travel and even day-trade have increased the confidence of individuals using the Internet.

The rapid expansion of networked computing across all industry has also demonstrated to users that they do not need the application they are using, or the data it delivers to be resident on their local machine. This has been well proven with technologies such as virtualization.[23] Other business practices, such as outsourcing IT services and the acceptance of the convergence of IT and physical security programs have prepared security professionals to consider SaaS as a viable security option.

In more recent years the decision to move towards a SaaS solution does not mean that an end-user must accept a "one size fits all" situation. SaaS providers offer solutions that can be configured to the end-user's environment and business needs just as if it were a traditional "on-premise" installation.

[23] Virtualization, see: http://en.wikipedia.org/wiki/Virtualization

Existing Barriers to SaaS

Although software as a service has been available for some time over a range of business environments, initial reluctance on the part of the security community included issues surrounding data privacy and protection. Some potential end-users remain reluctant to have their security data stored on the provider's servers rather than on their own which are secured within their facility. A response to this might be to store the end-user data on a third party's server(s) rather than those controlled by the SaaS provider. The core issue revolves around the ability of users to access their data and is giving rise to the consideration of code escrow services (in the event that SaaS providers were to cease business for economic or other reasons).

Other impediments to deploying a SaaS solution also may include government and industry imposed regulations or compliance as well as issues surrounding existing legacy systems and the expense of updating them so they can be interfaced with a SaaS solution. As always, concerns will be raised regarding the security of the end-user data once it is stored "in the cloud". That being said, these concerns can be addressed through security monitoring and periodic auditing, which can be completed by the end-user or a third party.

As an example of potential security concerns, a 2008 Gartner Inc., survey of SaaS user entities reported that a majority of the participants indicated that "no policies had been instituted to govern the evaluation and use of SaaS."[24] This is not necessarily the fault of SaaS providers, but rather the end-users who pay for the service.

End-users need to be clear and specific with their questions to the SaaS provider in the early stages of the planning process.

Detailed questions addressing the following areas need to be asked:

- Fit with requirements;
- Demonstrated performance;
- Guaranteed availability – at what price;
- Data security;
- Security of the process itself;
- Degree of available customization and cost; and
- Degree of available integration.
- Service level definition tools.
- Independent audit and compliance of processes and data security.

[24] Gartner Survey Finds 90 Percent of Respondents Expect to Maintain or Grow Usage of SaaS, see: http://www.gartner.com/it/page.jsp?id=823713

Regardless of the foregoing, results from that same survey indicated that 90% of respondents had intentions to maintain or increase their usage of SaaS. A principal driver for this was reported as a result of a "lower total cost of ownership."

Total Cost of Ownership

As noted earlier, the Total Cost of Ownership (TCO) with respect to any major technology implementation needs to be delineated in the early stages of considering a SaaS implementation. There are several TCO models such as the Total Economic Impact™ (TEI)[25] method from Forrester Research, which can be used to determine the ultimate costs to implement a SaaS versus the traditional "on premise" security technology project.

In most instances financial considerations for traditional "on premise" versus SaaS solutions for the same type of project are similar to those shown below.

Components Required to Complete Project *(Note that some components will vary in each model)*	**Project Costs to the End-User**	
	Traditional "on-premise"	**SaaS**
On-site infrastructure (control panels, conduit, wiring and related hardware) Somewhat less for SaaS solutions.	√	√
Hardware (Application & Archive Servers)	√	
Application Software Licensing	√	
Application monitoring, maintaining, upgrading and training	√	
SaaS Subscription fees		√
On-site Deployment Costs	√	√
On-site Support Costs (system maintenance)	√	√
Data Center Staffing costs	√	
Data Center Space Costs	√	
Data Center Operation and Maintenance Costs	√	

Whichever method is chosen to complete the project, the impact to the total cost of ownership is a result of different project components. As an example, the cost of licensing application software, maintaining and upgrading it is a significant factor in the "on-premise" option while the SaaS subscription fees is a significant factor to be considered if that option is selected.

The TCO process allows a potential SaaS user to develop a detailed parallel estimate of project and ongoing costs. The depth to which the TCO is taken is an end-user decision; however, the normal operational life cycle of the system being considered can be used as a guide.

[25] Total Economic Impact methodology, see: http://www.forrester.com/TEI

Furthermore, liaison with the organization's financial department will also yield benefits by using available resources and tools to analyze the financial impact of each scenario being considered.

Industry and Market Fit

Most research suggests that the industry and market "fit" for SaaS to provide services to the security environment is well founded. The provision of security services and technology has grown to a global scale and shows no signs of slowing. In fact, recent studies indicate that the rate of adoption of SaaS is actually increasing as the business model becomes proven, and the technology and surrounding processes mature.

Organizations and corporations are increasingly operating in established and emerging foreign marketplaces. These locations may or may not offer local technical capabilities to operate and maintain technology at the desired level. In these situations, SaaS provides an effective solution by ensuring the operation, maintenance, upgrading and training of the application being used is continuously addressed and operates consistently across its end-user facilities. For geographies that do not have a stable economic or political situation, or lack consistent infrastructure security, SaaS services provided from a remote location are able to provide a useful tool to mitigate the risk of data exposure or availability of service.

Having data centers located in disparate geographies is not without its challenges, however. For example, organizations that provide SaaS hosted services to their cousins in the European Union have compliance challenges to deal with. These are based around personally identifiable information and data privacy, and raise questions about jurisdiction and sovereignty. For example, a US company seeking to provide SaaS services to customers resident in EU countries, has to decide whether to submit to the exclusive jurisdiction within the EU, or whether to achieve compatibility with compliance requirements in other ways. The US Department of Commerce, in concert with the European Commission, has established a safe harbor framework that allows US companies to participate in a program that satisfied requirements.[26]

The ability of the SaaS solution to provide a consistent level of operation regardless of the geographic region, in which a facility is located, is a highly desirable feature. As an example, a company may wish to collect specific security data from its global facilities for use in its strategic or tactical planning process. As each contributor accesses the same SaaS application the data could be reported in a consistent manner across all of the operations to gather key use metrics. Management can readily identify if one or

[26] Safe Harbor, see: http://www.export.gov/safeharbor/eu/eg_main_018365.asp

more contributors are not operating in a compliant fashion. This data collection however, needs to be considered in light of each countries privacy laws, so as not to run afoul of regulatory and compliance requirements.

The future for SaaS in the security market has very strong growth potential as reported in recent industry reviews. According to a recent Gartner Inc., report "Software as a service is forecast to have a 19.4% compound annual growth rate through 2013 for the aggregate enterprise application markets, more than triple the total market CAGR of 5.2%."[27] This in part is attributed by many to the fact that "SaaS presents a leaner" alternative" to traditionally installed systems.

With an expectation that SaaS adoption will continue to grow dramatically over the next few years, we should also expect to see more diverse and enhanced SaaS offerings. Up until this point, the SaaS industry has generally demonstrated a capability to change as a service provider and offer end-users customized solutions to meet its end-user needs.

Security and Market Segments for SaaS

Market segments for SaaS are readily defined based on the traditional, yet critical security responsibilities. These include access control, identification management and credential issuance, closed circuit video (video surveillance), intrusion detection, and security officer management and scheduling, as well as services which are emerging based around analysis and Physical Security Information Management (PSIM)[28]. It should be noted that the SaaS costs to provide service across all of the foregoing security segments will not follow the same uniform pricing approach. It is incumbent that the end-user ensures that some form of total cost of ownership process has been completed to identify potential cost differences between SaaS solutions such as access control versus video surveillance.

SaaS solutions for security related programs such as Business Continuity Management and Emergency (Disaster) Response are currently available and have proven their worth in corporations which have geographically dispersed facilities or who have globally based resources.

Other security related market segments that offer increased potential for SaaS end-users include Security Incident Reporting, Asset Tracking and High-Value Inventory Controls, Pre-Employment Screening, Computer Based Security Training and Skills Based

[27] Gartner market trends report, see:
http://www.gartner.com/DisplayDocument?ref=g_search&id=965313

[28] Physical Security Information Management - PSIM, see:
http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000552012

Management. Any one of the foregoing are being offered in one form or another; however, the integration of any one of these applications into the SaaS environment provides benefits to the end-user such as consistency of use, economy of scale, a likely reduction in IT personnel or effective re-tasking of those resources as well reduced capital costs to the end-user.[29]

The depth of the capability of SaaS to provide solutions for security related needs has not been fully plumbed as yet. As SaaS providers expand their involvement in the security market more opportunities will present themselves.

[29] Cloud Computing – A Smart Business, see: http://www.securitybuyer.com/Cloud-Computing-A-Smart-Business

SAAS SECURITY CONSIDERATIONS

Security Considerations

Although there are many benefits to cloud computing, there are also significant security considerations when considering the move to the cloud, and in considering a cloud provider. Although it is assumed that providers are largely responsible for the security of the applications they offer, customers are responsible for the assurance of operational security. As with all new technologies, there are new risks to be discovered, and old risks to be re-evaluated.[30] The Cloud Security Alliance (CSA)[31] provides an excellent source for further reading about security and has the stated mission: "To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing". The CSA paper titled "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1" provides guidance about architecture, governance, and operations.[32]

Data Confidentiality

Don't assume that storage or transmission of your physical security system data is secure or not accessible by intruders. Data in the cloud is generally in a shared environment along with other customers where encryption may not be feasible due to cryptographic key management and other design issues. What is currently evolving are agreed-upon implementations for encryption with interesting research work from several firms.[33] For now, data is tagged and stored with a unique customer identifier to enforce data isolation among the many customers.

Data Remanence

A risk in cloud services is that sensitive information might be inadvertently exposed to unauthorized parties. When eliminating files containing highly sensitive information, a simple delete or a one time overwrite may not be sufficient. Data deleted from the cloud environment does not always disappear. Once your data is uploaded to your provider it is nearly impossible to know the number of backup copies that were made and this is a major problem for data remanence. Data remanence is also a challenge when storage media is no longer needed or is retired. For information on how to

[30] A Practical Guide to Cloud Computing Security, see: http://www.avanade.com/_uploaded/pdf/practicalguidetocloudcomputingsecurity681482.pdf

[31] Cloud Security Alliance, see: http://cloudsecurityalliance.org/

[32] CSA document, see: http://www.cloudsecurityalliance.org/csaguide.pdf

[33] Encryption Is Cloud Computing Security Savior, see: http://www.networkcomputing.com/security/encryption-is-cloud-computing-security-savior.php

address data remanence, refer to the NIST Publication.[34] In the absence of other widely available industry standards for data eminence, many companies have voluntarily adopted NIST guidelines and standards.

Data Availability

As mentioned, availability is a critical component to consider. Your quality-of-service should be explicit in a service level agreement (sometimes referred to as a service level agreement)[35] with your cloud provider. You may be saving money, but what would happen if your physical security systems were down for a full day or during peak business hours? Your Seas provider must have a recovery plan in the event of a disaster. The data and application infrastructure should be replicated across multiple sites to prevent total failure and the time to complete the restoration should be contained in a service level agreement with the provider.

Data Ownership

You may be allowing your provider to have unlimited usage rights when the contents of your data is placed on the provider's computing network. You have the copyright to the data, but its value can be greatly reduced if the provider decided to share it. Data ownership is largely a legal issue, which needs to be addressed in the contractual terms and conditions with your provider. Any individual or entity that builds consumer products or publishes original works should seek legal advice before using the services of a cloud provider.

Data Privacy

If you plan to store or transmit information that is considered protected (e.g., under the European Data Protection Directive and its member states or US laws), you must consider privacy and appropriate terms and conditions with your cloud provider to comply with every jurisdiction. The following questions should be explored with the cloud provider:

- What are the compliance requirements?
- What kinds of privacy data will be placed in the cloud?
- Where are the subjects of the data located?
- Where will the cloud provider store the data?
- Where will the servers be located?
- Will the data be transmitted to other locations that prohibit cross-border data transfers?
- Can the data be isolated or restricted to a specific geographical location?

[34] NIST Special Publication, 800-88, "Guidelines for Media Sanitization", see: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

[35] Service Level Definition/Agreement, see: http://en.wikipedia.org/wiki/Service_level_agreement

Viability of Cloud Provider

In the event the Seas provider becomes insolvent, acquired by another company, or untenable, you must be sure that key data will remain available to you. There should be a plan with the provider for migrating the data to another provider or back to your in-house IT environment. Data portability may be especially difficult if the cloud provider does not use procedures or standard data formats or service interfaces that could guarantee portability.

External Parties.

SaaS providers may need to rely on external facilities to manage systems, networks, hosts, applications and storage. Does your trust with your provider extend to external parties? When the SaaS provider uses external parties, appropriate controls based on a risk assessment should be reflected in an agreement and implemented[36]. At a minimum, non-disclosure agreements should be used when processing, storing, or transmitting sensitive information that involves external parties.

Identity and Access Management.

A challenge in any cloud provided service is Identify and Access Management[37] (IAM). It is especially challenging when managing the access for diverse user populations such as employees, contractors, and partners. Your IT security specialist should be involved with architects, designers, and the SaaS provider to help address key requirements for IAM that include:

- The IAM policy (if one exists);
- Provisioning of accounts to users, including those who are administrators with privileged access;
- Single sign on support based on identity federation standards;
- Strong authentication using two-factors or more;
- Role based access control features that promote least-privilege;
- Auditing and logs required by policies and regulatory compliance.

Compliance

Care should be taken to ensure that the migration of physical security and IT perimeter controls to a cloud provider does not put your investment in protecting compliance-related data at risk. In some cases, using a cloud infrastructure may imply that certain kinds of compliance cannot be achieved to appropriately track and provide protection for the data.

---

[36] A Practical Guide to Cloud Computing Security, see:
http://www.avanade.com/_uploaded/pdf/practicalguidetocloudcomputingsecurity681482.pdf

[37] Identity and Access Management commentary, see:
http://www.experteditorial.net/securitysquared/2009/04/its-all-about-identity-and-access-management.html

Organizations should establish whether the provider should provide a capability to restrict where the application or data is hosted, to address relevant legal and regulatory requirements. In general, compliance management is the responsibility of the customer using SaaS services. ISO 27002 addresses such compliance and states:

> *Compliance with legal requirements. Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.*
>
> Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow as alluded to earlier).

It may also be that the cloud provider being considered already participates in an independent audit as part of a compliance program already in place. In some cases it may be possible to reduce the organization's cost of compliance, and actually show this as a cost reduction in the ROI analysis, by utilizing the compliance program of the provider (e.g., Statement of Auditing Standards No. 70: Service Organizations – "SAS-70" type I & II)[38] if it fulfills the organizations compliance requirements and results in lowered costs. Often, the cost may actually be less to implement specific controls that are incremental to the service providers existing program, than the cost of an entire existing program to achieve compliance.

Vulnerability and Security Patch Management.

Although the cloud provider is largely responsible for technical vulnerabilities of the infrastructure supporting SaaS, there are aspects for which the customer remains responsible, such as end-point computing devices (e.g., laptops, desktops, and smart phones), and the application interfaces with the SaaS provider. It is important to note, that thought should be given to discussions related to real and contractual risks related to failure of non-performance of security controls of the provider. Mitigation options should be considered to handle risks. For an overview of General Security Risk Assessment, see the ASIS guideline.[39]

---

[38] Statement of Auditing Standards No. 70: Service Organizations, see: http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations

[39] ASIS International General Security Risk Assessment Guidelines, see: http://www.asisonline.org/guidelines/published.htm

Most Cloud providers will seek to contract (transfer) out of risks related to security failures and careful thought should be given to scenarios that may expose the organization to risk and its costs.

SaaS applications residing in the cloud environment should undergo regular vulnerability testing. Hackers are continuously looking at and scanning web applications that are Internet facing for application vulnerabilities.

For vulnerability examples see the Open Web Application Security Projects (OWASP) top 10 web application vulnerabilities.[40]

There are several ways that cloud providers secure their systems and conduct vulnerability testing. These include:

- Self tested and secured
- Tested and secured by the provider hosting the equipment
- Independently tested by a third party and secured in concert with the cloud vendor and applicable hosting provider
- Customer tested (with the providers permission)

ISACA, serving IT governance professionals, has produced an auditing procedure, which provides useful suggestions.[41]

ISO 27002 also addresses vulnerability management and states: *Technical Vulnerability Management. Objective: To reduce risks resulting from exploitation of published technical vulnerabilities. Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.*

Security patch management is a critical component in technical vulnerability management for protecting host systems, network appliances, and applications from unauthorized users. Your SaaS provider should demonstrate regular assessments for new patches of all software (operating systems, applications, and database) involved with the delivery of their service**.**

Intrusion Detection, Incident Response.

When managing and mitigating risks that involve intellectual property, regulatory compliance, fraud, and possible privacy data breaches both the customer and the cloud

[40] OWASP Top 10 Project, see: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[41] ISACA - Security assessment–penetration testing and vulnerability analysis, see: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31608

provider are responsible for managing intrusion and incident response. ISO 27002 provides the following guidance:

> *Reporting information security events and weaknesses. Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.*
>
> Formal event reporting and escalation procedures should be in place. All employees, contractors, and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information.
>
> *Management of information security incidents and improvements. Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.*
>
> Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents. Where evidence is required, it should be collected to ensure compliance with legal requirements.

Investigation for inappropriate, non-compliant or illegal activity is made more difficult in a cloud environment. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. Contractual agreements should be sought with the cloud provider to support specific forms of investigation.

Law Enforcement.

Cloud computing is not without technical challenges for law enforcement. When there is illegal activity or suspicious activity, law enforcement will need to engage with the cloud provider. If computers of the cloud provider are seized as evidence or shut down, this could seriously impact the availability of applications or access to data. Laws and investigative procedures for collecting evidence are evolving, and require development to meet the challenges of cloud computing.

Crimeware-as-a-Service (CaaS).

Software packages (e.g., "crimeware" toolkits) are beginning to emerge as a Software-as-a-Service. The improved economies and scale for which cloud computing and SaaS brings to business also has given rise for cyber criminals which can exploit new vulnerabilities where the cyber criminal or attacker does not directly perform the activities related to data that is being compromised. This trend has provided new challenges for software security providers who provide such services.

E-DISCOVERY AND CLOUD COMPUTING

The intersection of Cloud Computing and Use of Digital Evidence

The impact of Cloud Computing on the stakeholders who work with Digital Evidence will be very profound. These stakeholders; Law Enforcement, Corporate Investigations and the Legal industry need to start to prepare for the changes. The 'assumptive paradigm' that these stakeholders have used in both the physical world and the digital world up is that up and until this point, evidence collection has been about physical possession. When collecting both physical and digital evidence a physical source (such as a file cabinet, laptop, PDA or physical location) has been used to identify relevant information. In the Cloud Computing environment, no easily identifiable physical location exists from which to collect data from.

The major issues confronting these Digital Evidence Stakeholders are; Location & Access, Technology, Privacy & Admissibility. The remaining section will address these issues. The issues listed below should not be perceived as being a comprehensive list of issues, but rather, the highest-level issues that can be easily anticipated.

Location & Access

When the need to collect Digital Evidence occurs in a Cloud Computing environment, where should one start? In the past, a custodian's desktop or laptop computer would be the ideal place to not only start, but collect a majority if not all of the Digital Evidence that was needed. In a Cloud Computing environment a specific Desktop/Laptop is not required. The challenge is to identify where Digital Evidence is located in a Cloud Computing environment. The custodian's primary Desktop/ Laptop will hold key information as to the location (source) of Digital Evidence in the Cloud. If the Desktop/ Laptop was not used to access the Cloud; however, it will be highly unlikely that the residual pointers will point to Digital Evidence in the Cloud. In essence, Digital Evidence in the Cloud may be spread across many computers, many countries and many formats.

The location of Digital Evidence may be the first but not the only challenge that will confront Stakeholders. Having legal access to information in the Cloud may become the next challenge faced. Depending on the method used to collect the Digital Evidence, actual physical access may be necessary. The fundamental question, "Who has ownership of the data in the Cloud?" must be answered. If permission to acquire the

Digital Information is needed, does the Stakeholder need permission from the User, Cloud Service Provider or Both? Assuming that the Digital Evidence Stakeholder knows where Digital Evidence is located and obtains a legal tool to compel disclosure (in US jurisdictions a subpoena, or in some commonwealth countries an Anton Piller[42] order), where is this served? These are the major issues that must be resolved and raise issues of cross border data flow, sovereignty and jurisdiction.

Technology

The technical complexities of the Cloud will cause the Digital Evidence Stakeholders some challenges. Most data in the Cloud will exist in Proprietary Databases with the Cloud Provider. Assuming that the Digital Evidence Stakeholder could make an evidentiary grade copy of the evidence, their next challenge will be how to analyze and view the evidence outside of the application that it was created in.

The Digital Evidence Stakeholder may have few choices to analyze the data. The Digital Evidence Stakeholder will either need to have the Cloud Provider provide a Proprietary application to view the Digital Evidence or ask the Cloud Provider to provide a "Virtual Sandbox" for which Digital Evidence can be analyzed on the Cloud Provider network. From an evidentiary perspective both options are not going to be workable solutions without a lot of considerations concerning objectivity.

Additionally, the typical tools that have been used by the Digital Evidence Stakeholders up and until this point are not likely to be effective in conducting analysis of the evidence and so this issue will need to be addressed. It is likely that a next generation of search and analysis tools may need to be created.

Privacy

The major issue at play with Cloud Computing is the reality that all participants' data becomes intermingled with every other person's data being hosted in that application. When Digital Evidence is primarily located on a desktop/laptop there is a natural boundary, which provides privacy protection in that it limits the intermingling of other individual's data. Depending on the scope of the Digital Evidence Search in the Cloud, privacy issues may need to be resolved.

[42] Anton Piller Order, see: http://en.wikipedia.org/wiki/Anton_Piller_order

Admissibility

The Legal system in the United States has always taken a strong paternalistic view on Evidence and recently Digital Evidence. The primary resource around the "Rule of Evidence" is found in the Federal Rule of Evidence (FRE).[43] The Federal Rule of Evidence (FRE) has adopted a number of Rules 1001 – 1008, which is sometimes known as the "Best Evidence Rule."[44] The purpose is to allow a copy of the original evidence if the original evidence is not available and the copy of the evidence can be authenticated. This plays a huge part in the use of getting Digital Evidence accepted into the US Legal System as being Admissible. There are a number of other requirements to having Digital Evidence accepted as "Admissible", so this commentary should not to be perceived as a comprehensive dialogue on Admissibility.

To establish Admissibility of Digital Evidence it must be proven that the copy of the Digital Evidence with the Original Evidence was authenticated. It must also be demonstrated that the copy is accurate, and that credible methods of making the copy were used. The tool-set of Digital Evidence Stakeholders has usually worked well when the original evidence is tied to a physical location, or specific piece of hardware. In the Cloud computing environment, this becomes much more difficult because traditional precedents are difficult to apply. Solutions to address these issues will need to be considered and developed by Digital Evidence Stakeholders.

Other Considerations

The four issues above provide a list of the most formidable challenges to the Digital Evidence Stakeholders. However, there are some distinct benefits that Cloud Computing may provide. Specifically, the leap in logic is not too substantial to assume that Cloud Computing Providers will either provide a best practice for the handling of Digital Evidence, or that they may become regulated. In the alternative, legal precedent is likely to prevail as it does with other disputes related to evidence collection and jurisdiction.

In any of the above scenarios, Digital Evidence collection will likely become standardized, leading to the provision of better, and more consistent results in digital evidence collection. For example, a business that infrequently or never collects digital evidence in its own IT environment may be challenged to follow proper digital evidence collections practices. Furthermore, present legal precedent has evolved so that organizations that do not comply with the relevant best practice, and consult with their legal counsel during proceedings, may be penalized. Therefore, a business that hosts its data in the Cloud will likely benefit from the Digital Evidence collection procedures that the Cloud Providers employ.

---

[43] Federal Rule of Evidence, see: http://www.law.cornell.edu/rules/fre/

[44] Best Evidence Rule, see: http://www.michaelariens.com/evidence/commentary/bestevidence.pdf

Cloud Computing will likely cause a whole set of legal issues that will require careful examination. For example, Metadata is "Data about Data". This could be when a record was created, modified and by whom. When a customer uses the Cloud, Metadata will be created about the data in the Cloud. In this situation, who owns the metadata in the Cloud (The client or Cloud Provider)? Would you answer the question the same way if you knew that the Metadata was intermingled with other client's data?

Conclusion

Cloud Providers will find themselves in the role of needing to provide Service Level Agreements (SLA) for Digital Evidence collection for their clients. Some Cloud Providers may elect to use special masters to play the specific role in Digital Evidence Collections, to avoid providing testimony that might be adverse to its clients and protect confidentiality.

The virtues of Cloud Computing are powerful to businesses and governments seeking to implement this newest technological innovation. The move toward Cloud Computing will require adherence to risk management principles that support businesses and governments to move beyond the challenges, and seek innovations that make the process more effective. The solutions and processes that are developed today are likely to become the best practices of tomorrow. Therefore; we recommend that all interested parties of the Cloud Computing universe come together in a common interest to create "Best Practices for Cloud Computing."

Summary of Footnotes

1. NIST Definition of Cloud Computing, see: http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc
2. Understanding Public Clouds, see: http://www.keithpij.com
3. "Understanding Public Clouds" http://www.keithpij.com
4. "Understanding Public Clouds" http://www.keithpij.com
5. Corporate and product examples in this section and throughout the document are provided for explanatory purposes. Inclusion does not denote endorsement by ASIS International.
6. Client-Server, see: http://en.wikipedia.org/wiki/Client-server
7. Server Farm, see: http://en.wikipedia.org/wiki/Server_farm
8. Gartner - Market Trends: Software as a Service, Worldwide 2008-2013, see: http://www.gartner.com/DisplayDocument?ref=g_search&id=965313
9. NFPA 101 Life Safety Code, see: http://www.nfpa.org/aboutthecodes/list_of_codes_and_standards.asp
10. How Web-hosted Software-as-a-Service (SaaS) Lowers the Total Cost of Ownership (TCO) for Electronic Access Control Systems, see: http://www.brivo.com/benefits/cost
11. How Web-hosted Software-as-a-Service (SaaS) Lowers the Total Cost of Ownership (TCO) for Electronic Access Control Systems, see: http://www.brivo.com/benefits/cost
12. The Role of Power over Ethernet in Future Security Applications, see: https://siamembers.siaonline.org/eweb/DynamicPage.aspx?Action=Add&ObjectKeyFrom=1A83491A-9853-4C87-86A4-F7D95601C2E2&WebCode=prDetail&DoNotSave=yes&ParentObject=CentralizedOrderEntry&ParentDataObject=Invoice%20Detail&ivd_prc_key=00F0718F-DFA2-42D5-8E84-B8F95D77D64B
13. SNMP and its uses, see: http://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
14. Compartmentalization, see: http://en.wikipedia.org/wiki/Compartmentalization_(computer_science)#Encapsulation
15. Software as a Service, see: http://en.wikipedia.org/wiki/Software_as_a_service

16. The client-server model: Not dead yet, see: http://money.cnn.com/2009/02/16/technology/copeland_oracle.fortune/index.htm
17. Service-Oriented architecture, see: http://en.wikipedia.org/wiki/Service-oriented_architecture
18. Digital and analog video, and megapixel functionality, see: http://en.wikipedia.org/wiki/Closed-circuit_television_camera
19. Digital Subscriber Line, see: http://en.wikipedia.org/wiki/Digital_Subscriber_Line
20. Extensible Markup Language (XML) API, see: http://en.wikipedia.org/wiki/Web_service
21. Gartner User Survey Analysis, Software as a Service, Enterprise Applications Markets Worldwide, 2008, see: http://www.gartner.com/DisplayDocument?id=802221
22. Rainstor report and commentary, see: http://www.eweekeurope.co.uk/news/news-solutions-applications/uk-companies-still-fret-over-saas-and-the-cloud-2797
23. Virtualization, see: http://en.wikipedia.org/wiki/Virtualization
24. Gartner Survey Finds 90 Percent of Respondents Expect to Maintain or Grow Usage of SaaS, see: http://www.gartner.com/it/page.jsp?id=823713
25. Total Economic Impact methodology, see: http://www.forrester.com/TEI
26. Safe Harbor, see: http://www.export.gov/safeharbor/eu/eg_main_018365.asp
27. Gartner market trends report, see: http://www.gartner.com/DisplayDocument?ref=g_search&id=965313
28. Physical Security Information Management - PSIM, see: http://www.securitymagazine.com/Articles/Column/BNP_GUID_9-5-2006_A_10000000000000552012
29. Cloud Computing – A Smart Business, see: http://www.securitybuyer.com/Cloud-Computing-A-Smart-Business
30. A Practical Guide to Cloud Computing Security, see: http://www.avanade.com/_uploaded/pdf/practicalguidetocloudcomputingsecurity681482.pdf
31. Cloud Security Alliance, see: http://cloudsecurityalliance.org/
32. CSA document, see: http://www.cloudsecurityalliance.org/csaguide.pdf
33. Encryption Is Cloud Computing Security Savior, see: http://www.networkcomputing.com/security/encryption-is-cloud-computing-security-savior.php

34. NIST Special Publication, 800-88, “Guidelines for Media Sanitization”, see: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
35. Service Level Definition/Agreement, see: http://en.wikipedia.org/wiki/Service_level_agreement
36. A Practical Guide to Cloud Computing Security, see: http://www.avanade.com/_uploaded/pdf/practicalguidetocloudcomputingsecurity681482.pdf
37. Identity and Access Management commentary, see: http://www.experteditorial.net/securitysquared/2009/04/its-all-about-identity-and-access-management.html
38. Statement of Auditing Standards No. 70: Service Organizations, see: http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations
39. ASIS International General Security Risk Assessment Guidelines, see: http://www.asisonline.org/guidelines/published.htm
40. OWASP Top 10 Project, see: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
41. ISACA - Security assessment–penetration testing and vulnerability analysis, see: http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID=31608
42. Anton Piller Order, see: http://en.wikipedia.org/wiki/Anton_Piller_order
43. Federal Rule of Evidence, see: http://www.law.cornell.edu/rules/fre/
44. Best Evidence Rule, see: http://www.michaelariens.com/evidence/commentary/bestevidence.pdf