Cloud Security Guidelines

CONTENTS

INTRODUCTION

Cloud Computing has created a lot of buzz in the IT industry, especially in our information driven world. In fact, as of 2015, 88% of businesses have already adopted cloud services to leverage their business operation and well as to reinforce their ROI. However, since private cloud computing controls most HPPI and PCI-sensitive organizations using a complex web-based infrastructure, the security of the data has been one of the leading concern imposed to many IT professional. Since cloud services offer instances for many clients to utilize a single hardware, the data stored on its database has the possibility to get lost in the cloud when you didn't have a proper control over where your own data lives.

When it comes to security, it is very important that you have proper control over your cloud environment as numerous risk cannot be underestimated. To better help you identify the threats in cloud security and prevent it from ruining your long-run business, we have provided you with detailed information about the existing risk that that is incorporated in this e-book. Some of the security risk discussed in this e-book includes the extension of existing risks which evolves within a cloud computing software, management issues resulting to incompatible user and service provider functions, proliferation of unseen attack surfaces, threats within the function of the cloud security provider, as well as the proliferation of the new attack surfaces and some recommendations how to mitigate these risks.

WHAT IS CLOUD COMPUTING SOFTWARE?

In simplest term, cloud computing software is a cloud-based platform used for accessing and storing data or programs over the net instead of placing it in your computer's hard drive. Cloud is a simple metaphor for internet. Cloud storage is the counterpart of local storage, wherein all of the data and files you are working on or you wish to store is being trusted to the hand of your cloud computing software provider. Basically, there are 3 types of services in cloud security, which includes: SaaS (Software-as-a-Service), IaaS (Infrastructure-as-a-Software) and PaaS (Platform-as-a-Service).

In IaaS, cloud model provides a basic storage and processing resources for the deployment of OS (operating system) and software. While in PaaS, the cloud model enables developers and IT specialist to create applications that is used as a proprietary programming tools which is being introduced by the cloud service provider. On the other hand, SaaS allow its end-users to access powerful programs by simply using a web browsers. Regardless of the process or method used, the main aspect of cloud computing greatly involve a rapid elasticity, multi-tenancy and pay-as-you-go usage, which in return forms the basis of cloud model.

Cloud service provider greatly rely on the creation and establishment of their virtual machines (creation of application software that can be easily be de-provisioned and provisioned when needed) to drive versatility, elasticity and cost efficiency. Various virtual instances ends up sharing same physical server. But despite of numerous analysis raving about the efficiency and benefits of cloud security, there are still some risks associated to it, and sometimes they are largely unknown. Many users are also unarmed of the unforeseen sense that cloud entails when it comes to the existing security threats on the cloud. Take for example the act of 'phishing' in which an unwitting client is being tricked to expose his/her personal information due to the malicious 3rd party. And such scheme are inevitable regardless of the type or what organization you belong.

RISK 1: DATA LOSS

Data loss is the term used for the accidental loss of data and files that are not backed up—therefore adversely leading to irrecoverable data. Although the instances can revolve around to software or hardware failure, it's most likely triggered by either human error or your service provider's fault. Since the traditional data center of the organization is under the complete control of the service provider, the organization is logically the one who's protecting your data physically. And mostly, when you share your data in a shared database such as Public Cloud Hosting, there is a huge possibility for you to lose control of your own data.

Public Cloud Hosting is not a good choice especially when you are not sure if your service provider doesn't provide a backup for its users, thus subsequently making your data and other important files irretrievable. This imposes a critical security risk to the business or organization under the server. Therefore, one must ensure to opt for a security provider that offers backup in case of such unforeseen circumstances. Once you entrust your data to a Public Cloud Hosting or third party operator, there is no guarantee that you will recover your information, especially when it is the service provider or the system is the one at fault. While Private Cloud strategy can initially offer more control over the organization's data compliance especially to HIPAA standards & PCI, it is not inherently a secured choice to make.

For both consumers and organization/businesses, the effect of losing your data can be terrifying. Imagine the consequences of losing your business efforts, investment and all the things you've put in your business/organization just because you've lost some of your important data and now cannot be retrieved? Indeed, the odds of being in this scenario is very threatening. Furthermore, it would take you some time, money and effort just to retrieve your files again or recreate your documents manually. And at worst side, you'll have to start over again from scratch particularly if the damage is severe, thus putting a chaos in your organization/business.

RISK 2: DATA BREACHES

Although Data breach and Data loss is commonly used as synonym for each other, they are totally two different risks. While data loss is referred to the term for accidental loss of data and likes, data breach on the other hand refers to the malicious and illegal access or retrieval of data—a strategy that is commonly orchestrated by hackers. One of the good example of data breaching is that of what happen to Target—a second largest discount retailer in US behind Walmart. In 2014, the company was severely affected by data breaching wherein they've suffered from loss of sensitive personal information and credit card of more than 100 M of its customers. The hackers has successfully bypassed the firewall of the company's virtual machine, thus, penetrating the important files stored on their system.

When an integral component was compromised—say an application, hypervisor or a shared platform component—it exposes the whole environment into a potential breach, and worse might lead to a more severe issues such as data loss, identity theft and bankruptcy. If this happen, the cloud security provider is the one being placed at fault as they are the one who keep a complete control over your data and other important files stored in their cloud system. And when data breach happen, no one will suffer from the downside of data breaching other than your business or organization.

One the other hand, if your business or enterprise has different cloud providers, it is very important to keep your data and user's identity under your own control rather than letting these cloud providers to create a multiple islands of identity which makes it more complex to manage your data on the line. In this way, you are provided with easier back end data integration between multiple cloud providers.

RISK 3: REGULATORY COMPLIANCE AND GEOGRAPHICAL IMPLICATIONS

Each locations and jurisdictions when it comes to cyber regulatory compliance are uniquely different from one country to another. Indeed, data that's perceive to be secure/protected in one country may not be the same in the other due to the differences in the regulatory laws across regions and countries all over the globe. For example, the European Union has imposed a very strict privacy law, and hence US may not comply with the law imposed in EU on the same matter.

Furthermore, the physical severs which comprised the cloud used by different businesses or any organizations are scattered around many countries and jurisdictions, thus making it hard to pinpoint the exact whereabouts of an instance at a given time. The 'mobility' of the virtual instance can give rise to the expropriation of the business or company's property under various government agencies, and many of them may remain unconcerned about the privacy of the cloud users.

RISK 4: SHARED SERVICE THREATS

Most of the cloud services, especially public cloud servers, are supported by 'multi-tenant' frameworks—they are being shared between different organizations and users. Though resource sharing is one of the useful and highly encouraged cost reduction strategy for many companies or organizations, it still exposes cloud users under one roof from wide range of 'shared service threats'. And if a single user incurred problems or has initiated threats, there is a huge chance for the threat to spread to the rest of to the whole cloud environment, thus adversely affecting others. These threats become harder and more difficult to control compared to a single-tenant threat.

If an organization or a company was inflicted with threats caused by the other user who is also under one cloud environment, they may suffer from different downside which can lead to loss or theft. In CSP administration model, one of the most highlighted issue in terms of shared service threats has something to do with immature identity management protocol, wherein 66% of cloud users could not prove if their service provider Database Administrator are taking action to protect them from those who are abusing their 'super-user' privileges.

Furthermore, the cloud service provider can also maliciously be held responsible for such disaster in the cloud system because even low level operation staff in the CSP can have the power to abuse their access privileges to potentially damage clients. Some of the cloud technologies even go so far which allow their IT staff to have or extend access controls across different virtual environment in a network in just merely signing on. In this case, a service provider should therefore get a sophisticated Access Management Tool to help ensure that only reputed and responsible parties are qualified to have an access to sensitive or private business data.

RISK 5: USER PRIVACY & SECONDARY DATA USAGE

User's personal data are commonly stored in the cloud, particularly when they start using various social media sites. While most of these social websites are not certain about how they are going to handle their user's personal data, more and more organizations and individuals are still utilizing them for their personal and business endeavor, particularly sharing and saving their data. Moreover, these social sites comes with a 'default share all' set up for their users, which makes it possible for these cloud server provider to control everything at their end (sites like Facebook, LinkedIn, Twitter, etc.).

Since these social sites have the control over its user's data under their interface, they have the freedom to deduct some personal information of their users. Thus, you need to ensure that your cloud provider will not use your data for any secondary purposes—these data can be mined directly to the user's data under the cloud provider or indirectly based from the user's behavior (clicks, outgoing and incoming URLs, etc.). In fact, there are some social application provider which infiltrate user's data just for secondary purpose (e.g directed advertising, campaigns, etc.). No wonder why users receive some advertisement in their email once they open their personal gmail, hotmail or yahoo account.

And since these sites entertain various cloud actions which make it possible for users to make random clicks on some email links, visit fake sites or download data, the possibility of introducing new risk to the cloud environment is innumerable. Some of these actions can adversely introduce malware in the cloud system, which might ultimately develop into a full blown attack, thus affecting not only the user's data, but is also presenting threat to the cloud's security. And though this can cover major threats, these just represents the fraction of security risk that both users and cloud provider faces.

RISK 6: SOFTWARE & SECURITY MANAGEMENT RISKS

The scalability of the cloud technology do entail great economic efficiency for many organizations, yet also prove to cause many problems from software management perspective. The ability of deactivate and activate virtual machines when needed means some might remain dominant within a shared environment. And this may create a patch management concerns at some point as the sheer volume of inactive virtual machines across numerous physical environment may continually lead to a growing list of entity that are needed to be updated. And since proprietary data in the cloud technology is being transferred between end user and cloud data center via online means, the likelihood of getting your data compromised along the process is possible. In this case, the organization or user should ensure that the data is being protected at its maximum level as it is being transferred on the web.

While the interception of data in the transit should can be the main concern of every business or organization, the threats is much greater when the organization utilizing a cloud computing model was affected by destructive entities (such as virus, malware, worms, etc.) as the data is being transmitted over the net. Dormant VM’s (virtual machine) also makes it difficult to eliminate viruses or worms as new outbreaks occur, particularly when they are reactivated. And as the virus spread all over the cloud environment, unsecured data were being exposed to various risks and interceptions during the transmission.

RISK 7: MULTI-TENANCY

Multi-tenancy is the term in cloud computing which means sharing of services and resources among different clients (networking, CPU, storage/database or application stack. Multi-tenancy increases the dependence on other controls and logical segregation which ensure that one tenant cannot deliberately or inadvertently interfere with the data or security of other tenants. However, multi-tenancy can also pose different risk, and one of the major issues when it comes to multi-tenancy involves the inappropriate configuration of the tenant's side security control, which may result to proliferation of some security holes.

The cloud users must also be aware of the issues and possible conflicts between the service provider VS (virtualization software) and their personal software configuration. These can limit the efficiency of security hardening procedures because both are subjected to change over time. According to a specific survey of CIOs, more than 36% of these tenants has cited to perform improper configuration & poor implementation as the most concerning sources of risks and potential vulnerability. While SaaS users who tend to take a hands on approach in implementing application control is still on-going, one can find themselves creating a new security flaw.

RISK 8: INSIDER'S THREAT

An ‘insider threat’ is arguably one of the most damaging risk that an organization can face. The threat cause by malicious insider is amplified for consumers in a cloud services by the convergence of I.T services and clients under single management domain and combines with lack of transparency into provider’s process. For instance, provider may not reveal how they grant their employees access to virtual and physical asset, how it analyzes and report on the policy compliance and how they monitor their employees. In short, there is little or no visibility into the hiring standards and practices for the cloud employees. And this situation clearly gives an attractive opportunity for adversary—ranging from hackers, organized crime, corporate espionage and even a nation/state sponsored intrusion. With the level of access being granted, this could enable such adversary to garner confidential data or gain a total control over the cloud service without risk of detection.

The fact that insiders gain unlimited access to the company’s critical information makes them more intimidating and dangerous than losing your data. After being compromised by 3rd parties, insiders working for organizations or vendors could unknowingly or knowingly leak critical data from the cloud. From IaaS, PaaS to SaaS, a malicious insider has an increasing level of access to more sensitive or personal files wherein the cloud service provider is the one who is being placed at stake and solely responsible for the security. According to CSA, even if the encryption has implemented, if the keys aren’t kept with customers and only available at the data usage time, then the system is still susceptible to insider attack.

RISK 9: INSECURE APIS AND INTERFACES

Cloud Computing Providers exposes sets of software interfaces to set of software interfaces (APIs) that the customers use to interact and manage with their cloud services. Management, provisioning, orchestration, and monitoring are just few of the things handled by these interfaces. Furthermore, the availability and security of general cloud services is highly dependent upon the security of the basic APIs. From access control, authentication to encryption & activity monitoring, this interfaces should be designed to secure and protect users from both malicious and accidental attempts and action to circumvent policy. Moreover, 3rd parties and organizations often build upon these interfaces to provide value-added services for their customers—and this is where a complexity of new layered API takes place, which increases the risk as the organization may be required in relinquishing their credentials to 3rd parties in order to enable their organization.

The cloud has successfully empowered organizations and companies in distributing their service to wide spectrum of users. Unfortunately, this also exposes them to myriad of policy circumvention and risks, which is best controlled with APIs. Though they regulate 3rd party access, most APIs are generally unstable, and sometimes used to circumvent protocols especially in accessing data and some selected services. Thus, weak APIs and interfaces can expose your company or organization to various security issues pertaining to integrity, confidentiality, accountability and availability.

RISK 10: ACCOUNT HIJACKING

Account hijacking is not new, however, it is still one of the most daunting issue when it comes to cloud security. Attack methods like phishing, fraud and exploitation of software vulnerabilities are just few of the risks associated to it. Hackers and unwanted insiders use different strategies and methods just to infiltrate cloud systems, gain access to the extensive client's account and steal users' credential to be used in spamming, phishing and other illegal activities. Passwords and credentials are often reused, which in return amplifies the impact of such threats or security attack. An intruder who gains control of the user's account can manipulate the data, manage transactions on their end, and provide false or damaging response to your customers, therefore affecting your business or redirecting your customers to other sites.

If your account in the cloud was hijacked, it can be easily used by the attacker to gain power of your reputation, either to enhance themselves or at your expense. One of the best example herein is the large scale attack that happens at Amazon, wherein the hackers has launched a cross-site scripting attack in order to hijack customers' account in Amazon wireless retail site. If credentials and other important files are stolen, the wrong party will have the access to individual's system or account, thus may attack the critical area of your business or damage your data and use it for fraudulence. Your service or account instances might also become the new base for hijackers to carry out all their illegal activities. So to avoid this things from happening, one must employ a proactive monitoring to detect any unauthorized activity or prohibit sharing account credentials between users & services.

RECOMMENDATIONS ON MITIGATING CLOUD SECURITY RISKS

Government agencies and businesses typically demands CSP's (cloud service providers) to integrate enhanced security in order to guarantee constant operational availability. Simply put, the responsibility of securing cloud is often given to the cloud providers. Subsequently, vendors or cloud providers simply activate the claimed best security controls for cloud.

Though this might give business entities and organization the convenience, this just leaves them without understanding of what the possible risks they might face in the future. Moreover, this case can increase the probability that adversative events will interrupt cloud operation.

Even if this cases ae inevitable, still, organization may able to address the security risks inherent in the cloud. The plethora of security risk has already been previously mentioned. Now, we will proceed into exploring the possible solution to eradicate or minimize the associated risks.

CLOUD RISK MITIGATION

Efforts to resolve cloud risks need to be based on the standard methodologies. Although each idea may have different particular methodologies, all of which are created with similar core components in mind which are the following:

- To determine the needs of an organization
- Assess the risks
- Choose and implement the controls for risk mitigation
- Assess controls and detect any shortcomings
- Monitor controls to make sure they are working effectively.

Every cloud implementation usually faces a distinct risk combination. Therefore, there will never be something that can be helpful for every situation and concern considering that every users faces a unique risk profile.

Though, this isn't to say that the most sought-after and best practices aren't necessary. The truth is, these practices became the foundation of formulation of different risk mitigation strategies. But the best practices often determine a minimum benchmark for controls, risk mitigation, and other enhancement.

Security policies of cloud services focus on varying facet of cloud security, based to which cloud delivery system you are referring- **IaaS, PaaS, or SaaS:**

Infrastructure-as-a-Service policy emphasizes on maneuvering virtual machines and protecting data. This also focuses on managing access to these traditional computing infrastructure underlying the cloud's virtual machines. This policy needs to address the governance framework on risk mitigation to virtual machines. IaaS has been utilized as Command & Control centers that direct operations of botnet that is used in suspicious infrastructure updates across and within virtual machines.

Platform-as-a-Service policy emphasizes the protection of data and managing application access in complete life cycle of businesses developed and hosted by an independent vendors of software, small or large businesses. This policy need to focus on addressing risk mitigation of PaaS being utilized as Command & Control center that direct operations of botnet that is utilized for installing malware cloud applications.

Software-as-a-Service policy emphasizes the control of access over a specific application that is rented to customers whether they are government agencies, organizations, businesses or private individual. The policy needs to address risk mitigations of SaaS application vulnerable to malware application attack which allocates suspicious instance resources. For instance, the designated working hours that an application gives access to authorized employee to download important data may be suspiciously changed into non-working hours which is in favor for hackers.

HOW TO MITIGATE CLOUD SERVICE RISKS?

Risks can be mitigated in a cost-effective manner through applying best security controls. This is needed to be done in order to lower the possibility that the vulnerabilities of a particular asset can be exploited which may lead into threat implementation.

Before mitigating risks, you need to first identify the assets to be secured. The simplest approach is:

- To identify assets
- To analyze risks
- To apply necessary security countermeasures
- To conduct post-run

1. IDENTIFYING RISKS

Both cloud provider and consumer should identify the software and hardware assets and estimate replacement cost for each. Both need to maintain and occasionally update an asset inventory which can change because of organization restructuring, better failover tool, energy-efficient technologies as well as new legislations on data privacy exports across jurisdiction boundaries.

The number of software and hardware assets that consumers need to point-out when renting SaaS service are far fewer compared when using PaaS model and IaaS. For SaaS assets, the assets that need to be identified are applications, operating systems of mobile devices, and default programs. In such case, it will be necessary to limit device service inventory into SaaS applications and programs. It will not be advisable to mix personal programs with programs needs to gain SaaS access on similar device.

PaaS consumers, on the other hand, needs to pinpoint assets that is controlled. At minimum, operating system, hardware, network infrastructure, and instance resources need to be controlled by the cloud provider in PaaS set-up. The responsibility of asset identification on this system should be taken by the cloud provider.

2. ANALYZING RISKS

Risk is referred to the possibility that threat will be able to exploit the vulnerabilities of cloud services. Without cost-effective countermeasures, cloud services are prone to vulnerabilities which could launch threats once exploited.

For example, a good application is separated in modules which interact with each other to perform one or a sequence of certain tasks. This makes the process of adding a module to an application through either adding new module or using the existing ones. Once an application must a threshold module, both provider and consumer have no means of knowing if data requests or instance resources have reached its maximum capacity. They will not know whether or not a hacker has developed malicious or suspicious virtual machine on the physical server which houses healthy and risks-free virtual machines until after the effects gradually appear. Meaning, it will be too late to resolve the problem. The hacker achieved this through flooding the virtual machine with malicious queues on data request or on instance resources. The hacker lures victims to boost their virtual machine until it already reach the physical server's maximum capacity.

3. SECURITY COUNTERMEASURE APPLICATIONS

This may sound an easy concept but is relatively a difficult one when applied in real life. It is important to consider finding cost-effective security countermeasures in order to ensure that the cost of countermeasure implementation will not go higher than the provided benefits. It is a must to look for countermeasures which can effectively reduce the security risks without compromising ROI. It will be more necessary to find something that can boost ROI as well.

If the risks tend to require costly countermeasures which is far costly than the provided benefits, on the other hand, users will need to accept the fact and embrace the risks. In such case, countermeasures will be useless.

Nevertheless, if the residual risks overpower the countermeasures, users can still try repeating the risk assessment steps. This can be done if the risks identified are just a result of the first assessment. Users can repeat the assessment process to sharpen their skill on identifying assets, understanding and analyzing the risks as well as determining the depth and full breadth of probable countermeasures and the multiple ways it can be possible applied.

4. CONDUCT POST-EVALUATIONS

Though risk assessment needs to be done every after three years, it may still be needed to reassess the risk more often if particular conditions happen. Reassessment can be done if the arise of new cloud technologies can impact hardware, software, and network assets. It can also be done when new threats and new vulnerabilities emerge, new effective security countermeasure for residual risks are available , new approach on risk mitigation in conceived, when there are major changes in compliance regulations on jurisdictions as well as changes in laws and if there are major impacts that comes from organizational changes on assets.

RECOMMENDATIONS

RECOMMENDATION 1: MANAGE CONTROL

New users of cloud strategies may become quickly overwhelmed by the great number of distinguished threats of cloudscape. Prior on using the strategy, it will pay to take necessary measures to counterattack the mentioned cloud security risks and to ensure that all of the sensitive data will remain secured on a constant basis. Organizations may find it pretty hard or even nigh impossible to continue their operation in the middle of disruption threats if they will not adopt a security-first mindset. The cloud, with its limitless storage capabilities and relatively cheap cost, may lure business to place all their data on cloud networks.

However, this voluminous data nested on cloud servers usually becomes the primary obvious target for malevolent third parties. All the previously mentioned concerns over the weak access to the management control contained by workforce of the service provider create further vulnerabilities that can be an entrée point for malicious parties. Data can therefore may be easily stolen or lost. Encryption in the cloud environment is thereof a must rather than a typical option.

At least, employees' login data encryption should be thoroughly enforced so that the access to cloud will be restricted only to responsible partied. Majority of companies that offers cloud service usually offer this fundamental form of clod security. Through this service, companies can have peace of mind knowing that only the authorize individuals can have access to all the data in the cloud.

That will not just provide an additional sense of comfort over the protection of sensitive data but will also have profound inferences on the cost saving viewpoint. Restricting processing privileges on cloud to responsible users can benefit businesses with proper management of per-use billings that is typical to cloud services.

Another way to make sure that only the trusted users can gain access to sensitive data is through encrypting the data locally prior on storing it to the cloud servers. This can be a reasonable task particularly for those who use cloud as mere storage device. But this solution might not be applicable for users who needs cloud's real-time processing.

2.2 RECOMMENDATION 2: SECURITY RESPONSIBILITY AND SLA (SERVICE LEVEL AGREEMENT)

A survey conducted by Ponemon Institute highlights inquisitive discrepancy between expectations of service providers and cloud users. According to the survey, 69% of cloud service providers believe that the responsibility of cloud security are for users but only 35% of cloud users appear to agree.

With many pervasive risks which come within the territory of cloud operation, it is just understandable that service provider will take hesitation over taking the responsibility of cloud security. The liability that CPS might face can therefore be quite crippling on the long run. Nonetheless, while both CPS and user's needs to be jointly responsible for ensuring security within the virtualized environment, organizations and businesses must read thoroughly over the SLA (Service Level Agreement) to allocate clearly the security responsibilities. Through looking into SLA, both parties can also limit the volume of responsibilities that they may take.

Regardless of the protections indicated in the SLA, it is still imperative for businesses to have the capability to constantly monitor and boost their own security in cloud. This might appear quite trivial from the inception, CPS are often hesitant to offer the fundamental documentations such as breach investigation data and reports and well as user access login.

When this data are asked, CSP will often argue that they are well-equipped with necessary tools that can secure data. CSP's typically claim that they have enough tools and are able to provide security precautions to ensure that businesses data are secured without proving it.

Cloud Service providers are often relatively secretive when it comes to security practices they uphold. This may be probably because divulging information about their previous breaches may bring them into disastrous situation and may even lead into adverse consequences for brand reputation.

Furthermore, an incomplete SLA may also trigger questions about data ownership. For an instance, when business is blamed of SLA breaching with a provider, organizations or companies must be primarily concerned about data recovery. A security breach usually led CSP to indefinitely withhold the data of customer. Customer may only have hold over data ownership after numerous court decisions which might be given after a year or two or even more.

Data loss will result into subsequent inability to operate. This will surely have detrimental flow-through impact to the company customers and may impair the business reputation. Therefore, it's a must to ensure a strong SLA in order to avoid getting doomed into failure. With strong SLA in case of security breach, businesses will be able to manage a constant monitoring process and ensure seamless business operation.

2.3 RECOMMENDATION 3: SECURITY FRAMEWORK ADOPTION.

Despite of the gradually growing confusion about the cloud adoption, numerous organizations have appeared to offer businesses with reliable security framework which outline the numerous possible risks of cloud. Cloud Users can take a look on these security frameworks to manage their risk evaluation process and create a cloud security plan that thrives into a unified approach.

Some may be familiar of the IT Governance & Control's omnipresent COBIT which helps in bridging the gap in between the effective controls and general risks for business. This may be effective at some point and really do its job effectively. Nevertheless, there are more cloud specific frameworks which is better than those prominent framework. This eliminates the need for experts or executives to implement the potentially outdated frameworks into the cloud model.

ENISA has also created its own framework which helps in evaluating the risks related with cloud policies adaptation and in differentiating cloud providers. Meanwhile, users who intend to apply single model can rely on CSA or Cloud security Alliance. CSA is an organization which implements excellent practices in the virtual environment security. Its recently released CCM applies similar principles as of the abovementioned frameworks. Its main goal is to offer businesses with the essential structure, clarity and detail relating to the information security specially designed for cloud.

2.4 RECOMMENDATION 4: SECURITY-AS-A-SERVICE (SAAS) NEW SUBSET

The new subset of SaaS intends to help new users of cloud in contending security threats intrinsic to the multi-tenant cloud environment and to cloud itself. SaaS providers exist to aid the transition into cloud and offer a strong level of ease and comfort over the web operations. In core, activity is basically routed through the SaaS provider's network that creates a secure instance that is designed to monitor and detect any malicious activity. This instance will be used as web operation base, interfacing with web applications and Internet or even with similar cloud service.

Even if this type of infrastructure may show inherently lower processing, SaaS may be beneficial for inexperienced or start-up businesses to outsource security procedures to the third parties. SPs can therefore allow businesses to give full attention on their central competencies rather than of being sidetracked by the increasing cloud security threats.

Businesses can take advantage of similar economy of scale which applies to other applications on cloud. Adopting such services gives executives and opportunity to see cloud security as distinctly identifiable function with obvious cost amount associated to it.

TIPS TO LESSEN POSSIBILITIES OF RISK ACCUMULATION AND ENSURE EFFECTIVE CLOUD RISK MITIGATION

1. Necessary staffs should be well-adept with the cloud nature. Cloud users should be able to grasp the nature of cloud and the associated risks. They must also understand and hold their responsibilities and should be accountable when using it. The IT management and business owner needs to work together in order to ensure that all involved staffs possess essential skills and knowledge to embark on cloud initiative.

2. Management should authorized everything that is placed on the cloud. All data in cloud-based technology needs to be formally classified for CIA (Confidentiality, Integrity, and the Availability) and need to be assessed for the risks in the business terms. Best business practice and technical controls should also be incorporated as well as tested in order to mitigate security risks throughout an asset's life cycle.

3. Management needs to know and monitor cloud users. Necessary security controls are needed to be place on all cloud uses including the human resources activities or practices such as transfers, recruitments, termination and more. This is associated to people who are in charge of cloud use. Businesses owners need to do necessary background checks, duty segregation, user access and least privilege review controls.

4. Follow mature process in IT. All cloud-based technical infrastructure and systems development must align with the policy, be well-documented, meet the agreed requirements, appropriately resourced and be communicated to stakeholders.

5. Executives need to have oversight. Businesses as a whole should recognize that importance of cloud-based technology as well as data. There should be constant vigilance and unceasing risk monitoring to the information asset. Both providers and users need to ensure compliance with the appropriate rules and regulation, laws, frameworks and policies.

6. Management should recognize their responsibility on ensuring cloud security. The relevant business management needs to take control over the risk related with their cloud service use. Management should also establish, monitor, direct and evaluate corresponding risk management.

7. Management needs to build or buy security and management for the cloud. Before deciding to invest into cloud-based solution, it will be imperative for businesses to first look into varying consideration particularly the consideration on the security aspects. Information security and risks as well as the management and monitoring must be all taken into consideration.

8. Management should ensure compliance with associated regulation upon its use. There are certain obligations that both cloud providers and users need to adhere to. Both must comply with the legal, regulatory, contractual and policy obligation. They must also uphold to the values such as client commitment and integrity. It is also a must to ensure that cloud use is authorized and appropriate.

9. Management should monitor cloud risks. Cloud risks are inevitable but can be mitigated. Monitoring can help in the mitigation process. All cloud-based service and technology acquired or developed needs to enable timely and transparent information risk reporting that needs to be back-up by well communicated and documented escalation and monitoring process.

10. Cloud Users should adhere the best practices. All cloud-based technical infrastructure and systems development should consider the contemporary controls and technology to address the emerging risks on information which may be identified through external and internal monitoring.

CONCLUSION

Cloud is today's most powerful and potent service model which brings immense processing ability and scalability to all types and size of businesses which will lead into optimization of operation which can subsequently result into business growth and success. Businesses have successfully used this multi-tenant model to thrive forward the new generation of cutting-edge, innovative web processor and services. However, this multi-tenant environment also comes with numerous different unique set of security risks. Security risks to new and prevailing cloud users are still omnipresent and can compromise the promising benefits of cloud.

IT leaders needs to respond to the constant emergence of attack surfaces, the relative complexity of providing guaranteed security to cloud and the evolution of previous cloud security threats. Nevertheless, with a well-informed SLA and with adoption of security risk management framework that observe a unified approach, executives may successfully endure the ever-increasing security risks on the cloud and be able to effectively secure the sensitive data. Through keeping themselves completely aware of the risks, executives will be able to plan accordingly and implement safeguards to secure valued customers. This will be the only time everyone can truly reach the silver lining on the cloud.

Moreover, business can benefit through saving themselves from the detrimental consequences of risk exploitation. Through understanding the risks and the consequences associated into it and learning the risk mitigation process as well as getting insights on possible solutions, businesses will be able to have more time to focus on their core business thus leveraging their growth and success.

ABOUT LEAN SECURITY

SECURITY SOLUTIONS YOU CAN RELY ON

For dedicated managed security and IT solutions that are guaranteed effective and reliable, more online business owners are choosing Lean Security over any other internet security firm period. We are the only firm that works laterally with our clients every step of the way to ensure their needs are met and their web applications are secure at all times. When you need a team of experts who will listen and respond to your IT needs, trust Lean Security to show you what we can do for you today.

THE SECURITY SOLUTIONS YOU NEED

Headquartered in Sydney, Australia and serving the international business community, Lean Security was founded under the principle of offering our clients real-world solutions to all of their online business needs. We are more than an IT consultancy, we offer managed security solutions designed to keep your web applications secure and your business running smoothly. We are an Australian owned and operated company and you can be assured that your data is controlled by us, right here in Australia.

OUR PHILOSOPHY

Our team of experienced professionals strive to provide a higher level of service and support that our clients can't get anywhere else. We offer best in class products and rely on our over 10 years of practical security industry experience to provide our customers with truly world class online business solutions.

Lean Security showcases the best value for the IT and online security products and offers our clients a wide range of customizable services including:

- Secure Managed Cloud Hosting
- WAF Managed Service

- Managed Web Application Security Testing
- Managed DDoS Protection
- Managed Event Correlation /SEIM Solutions
- Managed Network Vulnerability Assessments

CHOOSE LEAN SECURITY AS YOUR APPLICATION SECURITY PROVIDER

We at LEAN SECURITY furnish organizations and associations with a simple and savvy method for dealing with the security dangers connected with corporate web and versatile applications. LEAN Security gives oversaw helplessness examining and web application infiltration testing administration. This implies establishing the data cen5teres without any need of equipment or programs to be installed, you can pay as per your need which means you can start with the little and then you may extend if you need more services, it totally up to you. Thirdly there will be so compelling reason to employ and prepare any web IT Security staff. Let our expert group handle all the specialized testing. And yes, you will be having a very simple fixed pricing per application (or per subscription) makes it easier to manage the budget.

At LEAN Security, we will be helping you through:

1. **Our Technology:** We use an assortment of business and open source apparatuses and items to convey the best security administrations to our clients. A rundown of the apparatuses utilized include:

   - **Nessus Vulnerability Scanner:** The most widely organized vulnerability assessment & management solution
   - **Qualys Vulnerability Scanner:** Qualys is a source of cloud security, compliance and related services for small and medium-sized businesses and large companies
   - **Metasploit:** Penetration Testing Software
   - **Netsparker:** Work as a False Positive Free Web Application Security Scanner
   - **SQLMap:** Automatic SQL injection and database takeover tool
   - **Burp Suite:** Burp Suite is an cohesive platform for execution security testing of web applications.

2. **Process:** For getting the services, you don't need to wait some weeks or even months until your website is verified by a security consultancy. Our SLAs are very simple and you get results much faster and provide you the reliability that you will not regret on your decision. Our SLA's provide:

    - **Basic Assessment** - branding web sites and mobile applications without the data collection features in 3 business days only.
    - **Standard Security Assessment** - corporate web sites with data collection functions and simple web applications (reservations, order handling etc.) in 5 business days only.
    - **Premium Assessment and Penetration Testing** - ecommerce applications or complex web applications with multiple roles and privileges in 10 business days only.

3. **Our Consultants:** Our customers will get enthusiastic account managers and project managers to help accomplish the project goals and results. Our team will help you to:

    - Analyze your business necessities and find the clarifications to address your challenges.
    - Generate a security assessment plan to meet timelines
    - Provide inclusive reporting on the position of the project
    - Intensify any issues that need quick and speedy resolutions
    - Track you resources and budget

Moreover, all your projects are checked by our skilled professionals with respected industry certifications like:

- **CISSP** - Certified Information Systems Security Professional
- **CISA** - Certified Information Systems Auditor
- **CISM** - Certified Information Security Manager
- **GPEN** - GIAC Penetration Tester
- **GCIH** - GIAC Certified Incident Handler
- **GWAPT** - GIAC Web Application Penetration Tester
- **GXPN** - GIAC Exploit Researcher and Advanced Penetration Tester