International Journal of Research Studies in Computing
April 2013, Volume 2 Number 1, 31-43

ISSN: 2243-772X
International Journal of Research Studies in
Computing
Volume 1 Number 1 April 2012
Consortia Academia

The role of the cloud provider to providing security in cloud computing

Rahimli, Ailar ✉
Multimedia University, Malaysia (a.rahimly@gmail.com)

ISSN: 2243-772X
Online ISSN: 2243-7797

OPEN ACCESS

Received: 13 December 2012 **Revised**: 9 January 2013 **Accepted**: 14 February 2013
Available Online: 10 March 2013 **DOI:** 10.5861/ijrsc.2013.275

Abstract

Cloud Computing is a service that delivers different application via the internet to the different users and also reachable from everywhere. Cloud computing same as others technology has challenges, security is main and important challenge for cloud computing. For providing the security in cloud computing can use many mechanisms but cloud provider and cloud user are playing significant role in providing the security in cloud. So, the objective of this paper found the role of the cloud provider for providing the cloud computing.

Keywords: cloud computing; security; cloud provider

The role of the cloud provider to providing security in cloud computing

1. Introduction

Cloud computing provide applications as service by software and hardware via the internet , server provide the service for user base on demand and also user pay the cost base on use of service (kushida, 2010). User can use the different application, storage, resources. Cloud computing service mode includes three types: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (Iaas) (SPI Model). Security, availability and reliability are challenges in cloud computing technology, but security between the other challenges is very important, because any technology without security system can't adopt by the users. User when will not concern about the security and reliability that, they know about how is the operation being performed. Cloud computing try that user can trust to cloud service, because cloud service concern about user, and try to provide security system in cloud computing (Frank Gens, 2009). Fujistu researched about concerning in using the cloud computing by users, and you can see the result, that most of the users concern about security in cloud computing, and after the security, stable operation and support system have highest rate.

Due to these issues, the weak security system is easy to break in cloud computing system. The security of system must be strong even for weakest users, the bigger security risks include: Weak password recovery workflows, phishing attacks, and key loggers. Security is one of the important factors in cloud computing, because cloud user face security threats are in inside and outside the cloud. The responsibility for providing security on the cloud computing divided among the cloud user, cloud provider, and third party that user use security sensitive software for providing security .cloud user is responsible for application-level security and also cloud provider is responsible for physical-level security and likely for running the external firewall policies. Provide security in intermediate layers of software stack is share between cloud user and operator. Cloud provider responsible to protect against theft or denial of service attacks by users, the last security concern for cloud user protect against cloud provider and also user need to be protected from one another.

The significance of this study show the how the cloud provider can provide security in cloud computing. Now, many methods and also software, application are available can provide security in cloud computing but in this study my scope are cloud providers in the cloud computing system who provide service to cloud users. So, explain the role of cloud provider as member of cloud computing system for providing the security in this system. The main assumption of this study, describe the role of the cloud provider in providing security in cloud computing system and the lack of the number of the companies that provide cloud computing services in undeveloped countries could be limitation of this study because if there were more companies, then the result of this research can be more developed.

Finally, many mechanisms are available to provide security in cloud computing, but in this research explain the role of the cloud provider in providing security in cloud computing in developing economics, because cloud provider more responsibility for providing the security in cloud computing.

2. Related work

Today, the primary security mechanism in cloud computing system is a virtualization. Virtualization is powerful protection and defense that protected against user to attack one another or underlying cloud infrastructure. Virtualization is good and important technology for cloud and by using physical resource such as a server that is divided into virtual resources called virtual machines (VM). Cloud provider are making sustainable effort to provide security for their system and to minimize the threat of insider attacks and this works that causes to reinforce the confidence of users. Security management of virtualization technology is required to control and reduce the security risk and run the security policy. The Cloud Security Alliance is control the issues of authentication, authorization, privacy, integrity and also data reliability and availability (Cloud Computing Alliance, 2009).

According to Chow et al. (2009), security concerned 3 items:

- Traditional security
- Availability
- Third party data control

Traditional security concerns include: the computer, network intrusions, or attacks that will be made easier or possible moving to cloud (Chow, 2009). Attack to VM-level is a problem that, this problem is related to potential vulnerabilities in the VM technology and also cloud provider vulnerabilities. The cloud user must protect the infrastructure that used to connect, interact with cloud, and also complex task that do by cloud outside the firewall in many cases.

Critical applications and data being available are center of Availability concerns (Chow, 2009). As with traditional security concerns, availability of the cloud user's own data centers is very important item because their server uptime compares with it, cloud provide argue this result. There are many single points of failure and attacks in the cloud that maybe they lack an assurance of computational integrity.

The legal implications of data and applications are complex, being held by third party (Chow, 2009). So they are many questions that remain unanswered. When the third party hold the data, in this condition there is also potential lack of control and transparency. Another side effect of the control with cloud is audit difficulty and also there are contractual obligation issues. Cloud provider espionage is the worry about the theft of company proprietary information by the cloud provider. Another possible concern is using subcontractors by contracted cloud provider.

In this section, we describe some security issues, available solutions and their pitfalls in cloud computing.

2.1 Soap messages

Web service technology is most used technology in the field of SOA in the cloud computing, the web service security system should be strong enough to optimize the security attack from different enemies. Soap is a XML base messaging framework (using foe exchanging information over a different protocol) that the security attacks can involve with it. It lets a program running in one system to call program running in another system and this is independent of any programming model. SOAP (http://www.w3.org/TR/soap/) denial of service and wrapping attack are two common attacks with soap messages. Wrapping element signature attack is the primary picture for web service security in large data centers such as: Amazon had weak items in soap request validation components in their elastic compute cloud, and so, let unprivileged and action to take place in the cloud on a victim's account. Now we show an example using Amazon web service (AWS) technology and its security.

In the first step, in the registration time, the customer must provide a self- signed certificate and an accidently generated RSA to the AWS. If not, next generally defined certificate can send to AWS with signature in this time the AWS provide command line tools to search virtual machine images (AMI-Amazon Machine Images), to perform these images, to monitor them, and finally conclude some of AMIs. This soap message can be changed by developers. The soap header includes two elements, one is the BinarySecurityToken that include the certificate said above and the second is the TimeStamp which will include the information of the creation and also expiration of this SOAP. If the soap message is transmitting unsecure layer, then the SOAP Body also the timestamps inside the soap header require to be signed (Gruschka & Iacono, 2009). Since, SSL/TLS is the protected the channel, it's an ineffective attack vector and also, as the EC2 web service let to access by simple HTTP, a in active attack would be enough to get in ownership of such request. For succession in warping attacks, just need here is that the artificial body requires having identically the same ID as the original.

2.2 Multi-core OS systems

Factored operating system is designed to show the challenge found in the systems, can provide framework from which to attention cloud security. In actually, systems have several classes that similar to FOS such as: traditional micro kernel, distributed OS's, and cloud computing infrastructure. Traditional micro control contains MACH and L4 (Accetta, Baron, Bolosky, Golub, Rashid, Tevanian, & Young, 1986). For simple operation of parallelism among server, FOS search to distribute parallelize within a server for high level function (Wentzlaff, Gruenwald, Beckmann, Modzelewski, Belay, Touseff, Miller, & Agarwal, 2009). The main motivation of FOS was to force the scalability, elasticity of demand, fault tolerance and resolve the problems in programming large system. For large system such as: cloud, an OS like as FOS is the right match to take care all appear issues. In the many a core multi-processor system, the OS managed and monitor the resource and also planning for all task. Therefore in the case of the scalability, an application is an element into a service, so it's also factored in additional service to be spread among service specific servers on a group of servers.

Figure 1 shows the FOS system functionality. As said previously, OS managed the resource. Therefore the core are dynamically spread and allocated for each of services among the servers. The periodic message is controlled to verify if all servers are working fully or not .if one of the message is losing then a server fault is found and decision can be taken to determine a new server for the specific function. Unlike the first cloud and cluster system, FOS provides one system image to an application. Items that the application interface is that of a signal machine, while the OS enforcement this interface among several machines in the cloud.

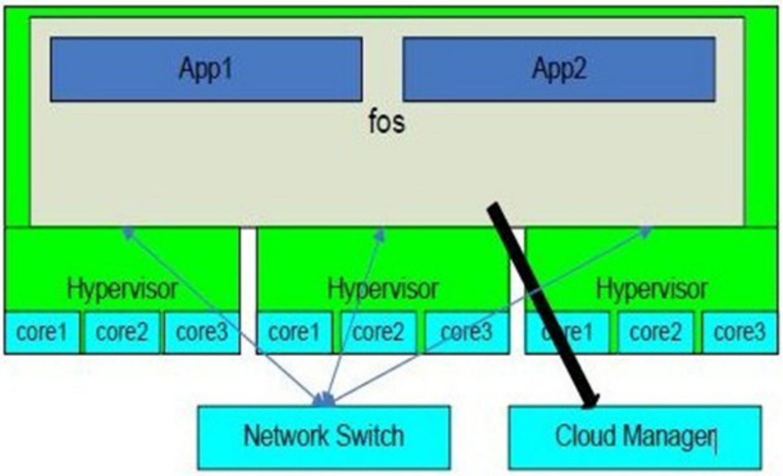

Figure 1. Hypervisor and Network Switch performs the scheduling where FOS communicates with the Cloud Manager to send scheduling command

2.3 Securing Code, Control Flow and Image Repositories

Any user in the cloud is provided an example of a virtual machine (VM): an OS, application, and many others. Virtual machine introspection (VMI) was designed in to show VMs together with livewire, a prototype IDS that use VMI to show VMs (Garfinkel & Rosenblum, 2003). A monitoring library called XEN Access is for a guest OS performing on top of XEN that request the VMI and virtual desk monitoring capabilities for accessing the memory state and disk activity of goal OS. These approach need that the system must be clean when monitoring is began, which is a fault and requires more investigation in VMI. LARES is a one type of the framework that can control an application performing in an untrust and guest VM by interesting protected into implementation a flow of process to be monitored. Since the gust as requires to be changed on the fly on insert hooks, these techniques may not be enforceable in some customized OS. All of these works have some faults when security is considered in the cloud; therefore encapsulation of the cloud computing system in a secured environment is compulsory.

2.4 Accountability in clouds

The cloud accountable means that the trustable, reliable cloud and also customer will be satisfied for using cloud by monthly or yearly charge. All attacks have impact on the accountability of cloud. Trusted computing is one of the approaches to get some of characteristic said above to make cloud accountable. Normally, it needs trusting the validity of large and complex codebase (Santos, Gummadi, & Rodrigues, 2009). A simple yet significantly powerful tool of selfish and destructive participants in a distributed system is “ambiguity”: making confidently statement to others. A small, trusted component is TrInc which combats ambiguity in large, distributed systems. TrInc provides new primitive: unique, one time in life time attestations. It’s practical, versatile and easily executable to wide area a distributed systems. Assessment shows that TrInc omits most of trusted storage required to performance append-only memory and significantly decreases communication overhead in PeerReview. Small and also simple primitives compare to TrInc will be sufficient to made cloud accountable.

3. Methodology

This research involve with one independent variable that is cloud provider and also the dependent variable is providing security in cloud computing. The questionnaire is utilized as the tools to collect from respondents. The questioner of this research includes 4 parts: Background, Attributes about the cloud computing security, security posture, and demographic of respondents of organizations. The survey instrument of this research in part one: respondent must select suitable answer, for part two: Strongly agree and Agree, for part three: 4-point-scale that ranged from “1= very confident, 2= confident, 3= somewhat confident, 4= not confident, and last part also same as part one respondents must select suitable answer. The population of this research is the cloud provider in organizations in developing economics such as: Malaysia, Singapore, and China. The sample size in this research is 103 and the method for collecting data is survey, using online survey. For data analysis makes report about the answer of respondents that provide frequency or percentage frequency tables, charts, and pie chart from respondents.

4. Discussion of result: Role of Cloud Provider

The main finding in this research is a role of the cloud provider to providing the security in cloud computing. Cloud provider and cloud user play significant role in cloud computing system especially in security of cloud computing. Cloud provider is responsible for physical security and cloud user is responsible for application level security and also Security for intermediate is shared between the user and the provider. The most of the cloud provider don’t believe that the security of their cloud service as a competitive advantages. So, they don’t more attention to this item as one of the most important responsibilities and also don’t believe their services and protect significantly secure and protect the private or sensitive information of customers.

Many cloud provider believe that customer must responsible of security of the cloud not their responsibility. They also say their application and system are not always assessment for security threats before to deployment to customers. The provider of the cloud computing technology allocated less than 10% of their operational resource to the security. Cloud provider say that the primary reason that customers used the cloud resource for lower cost and faster deployment of application. In contrast, improve the security with regulation is observed as unlikely reason for selecting cloud services.

Many of the cloud providers believe that they don’t have allocated the security personnel to oversee the security of the cloud platforms, infrastructures, and application. Provider of the private cloud resource appears that the security objective is more important in it than the provider of public and hybrid cloud. Cloud providers’ attributions about cloud computing security in the three parts:

- Security in the cloud service as competitive advantages
- Cloud server significantly protected and secures the private or sensitive information and data of the customers
- Provide security in cloud computing is one of the most important responsibilities

In the different organization, the leader of the organization concern about security of cloud computing resource provided to customer. Cloud provider must focus on the cost and speed of deployment than provide security in cloud server. The majority of cloud provider only 10% of the resource or less are allocated to security and related activities. Some cloud provider believe that many company purchase the cloud computing service for reducing the cost, improve the customer service, faster deployment time, and interest efficiently , and security is not reason for using this service by customer. So focus on cost and speed causes to create security hole and not more focus on security and data protection.

Many organizations that used the cloud believe that IT operation is most responsible for ensuring security of providers' solutions. Cloud computing system have security risk, cloud provider are more sure about their ability to ensure the recovery from considerable IT failure and ensure the physical location of data properties are in secure environment and also least confident in their ability to limit privileged user access to sensitive data and ensure appropriate data segregation requirements are met. Generally, cloud provider is more confident about their ability to perform the following offered security requirements:

- Access to highly eligible IT security personnel
- Prevent or limitation viruses and malware infection
- Secure private or sensitive information in movements
- Gaining compliance with leading self-regulatory frameworks
- Perform training and awareness for all system users

In contrast, the cloud provider is less confident about the following security requirements:

- Identify and authenticate users before the grant access
- Secure vendor relationships before sharing information assets
- Prevent external attacks
- Encrypt sensitive or private information assets whenever possible
- Specify the root cause of cyber attacks

The security technology that most of the used in the cloud computing environment:

- Fire wall
- Antivirus and anti-malware
- Encryption for data in movement
- Patch management
- Log management

And some the other security technology least used that include: Single sign-on, Data loss prevention, Correlation or event management, Access governance systems, and Encryption for wireless communication.

So the cloud providers are more responsible for providing the security of the cloud resource than the cloud user but different perception among cloud provider and cloud user about who is responsible for providing the security in cloud computing means organizations maybe more relying on their cloud vendors to ensure safe cloud computing. But the risk to data in the cloud, are interesting items that providers don't attain more that the security of cloud service as competitive advantages.

5. Conclusion

The result and finding of this study shows the cloud providers are not focus on providing the security in cloud computing but also their features priority that deliver to users such as low cost with fast deployment , improve the customer service and also increase the IT function. Cloud providers in this study conclude that they can't provide with complete assurance to service and produce are enough secure. Given the concerns about risk to organizations that have confidential and sensitive information in the cloud; hence, so users must demand to enhance the security features. However, before this event user must be aware of this responsibility to evaluate the risk of cloud computing before migrating to the cloud. It's important that the users, who are making the more of the decision to work in the cloud, must be educated about the requirement to completely application for their ability to protection information in the cloud. Finally, cloud provider and user should consider the significant of working together to create a secure and less turbulent computing environment.

6. References:

Accetta, M., Baron, R., Bolosky, W., Golub, D., Rashid, R., Tevanian, A., & Young, M. (1986). A new kernel foundation for UNIX development. In the *Proceeding of the USENIX Summer Conference* (pp. 93-113). Available from http://cseweb.ucsd.edu/classes/wi11/cse221/papers/accetta86.pdf

Cloud Security Alliance. (2009). Security guidance for critical areas of focus in cloud computing. Available from https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

Diodlo, N. (2010). Legal, privacy, security, access and regulatory issues in cloud computing. In the *Proceeding of the 2nd International Conference on Information Management and Evaluation*. Available from http://researchspace.csir.co.za/dspace/bitstream/10204/5011/1/Dlodlo1_2011.pdf

Garfinkel, T., & Rosenblum, M. (2003). A virtual machine introspection based architecture for intrusion detection. In the *Proceeding of the 2003 Network and Distributed Systems Symposium*. Available from http://suif.stanford.edu/papers/vmi-ndss03.pdf

Gruschka, N., & Iacono, L. (2009). *SOAP message security validation revisited*. Germany: NEC Laboratories Europe.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards trusted cloud computing. In the Proceeding of HotCloud. Available from http://www.mpi-sws.org/~gummadi/papers/trusted_cloud.pdf

Wentzlaff, D., Gruenwald III, C., Beckmann, N., Modzelewski, K., Belay, A., Touseff, L., Miller, J., & Agarwal.Fos, A .(2009). A unified operating system for clouds and many cores. Computer Science and Artificial Intelligence Laboratory TR. Available from http://dspace.mit.edu/bitstream/handle/1721.1/49844/MIT-CSAIL-TR-2009-059.pdf?sequence=1

Appendix

In this part, represent questionnaire and also the average of answer of respondents, because collect data in developing economics such as: Malaysia, Singapore, and China, and show all result is very much, and so just show the average of result.

I. Background	
Q1 . What types of cloud computing resources do you offer? Note that a company may provide more than one service type.	
Software as a service (SaaS)	**52**
Platform as a service (PaaS)	**17**
Infrastructure as a service (IaaS)	**34**

Q2. What types of cloud computing resources do you offer?	
Software as a service (SaaS)	**56%**
Platform as a service (PaaS)	**10%**
Infrastructure as a service (IaaS)	**34%**

Q3. What best describes your organization’s primary cloud computing deployment approach? Normalized to sum to 100%.	
Private Cloud	**17%**
Public Cloud	**57%**
Hybrid	**17%**

II. Attributions about cloud computing security (strongly agree & agree combined)	
Q4. In your opinion, who is **most responsible** for ensuring the security of cloud resources provided by your organization?	
The cloud computing service provider	**17%**
The cloud computing user	**71%**
Shared responsibility between the provider and user of cloud services	**15%**

Q5. What percent of your organization’s resources or effort is dedicated to security and control-related activities?	
Less than 5%	**33%**
Between 6% to 10%	**46%**
Between 11% to 20%	**10%**
Between 21% to 30 %	**6%**
Between 31% to 40%	**1%**
Between 41% to 50%	**0%**
More than 50%	**0%**
Don’t Know	**6%**

Q6. How important is security for meeting your organization’s IT and data processing objectives?	
Very Important	**53%**
Important	**47%**

Q7. How confident are you that cloud applications and resources supplied by your organization are secure?	
Very Confident	**48%**
Confident	**52%**

Q8. Are new cloud applications evaluated for security prior to deployment for customer organizations?	
Always	**14%**
Most of the time	**29%**
Some of the time	**47%**
Rarely	**3%**
Never	**9%**

Q9. In your opinion (best guess), what are the primary reasons why companies engage your organization for cloud computing services? Please select only three choices.	
Reduce Cost	**38%**
Increase efficiency	**13%**
Improve security	**8%**
Faster deployment time	**20%**
Increase flexibility and choice	**11%**
Improve customer service	**9%**
Comply with contractual agreements or policies	**1%**
Other	**0%**

Q10. How confident are you that your customer's security requirements are met?	
Very confident	**39%**
Confident	**61%**

Q11. Who in your organization is most responsible for ensuring that your customer's security requirements are met?	
IT operations	**21%**
Information security	**9%**
Compliance	**11%**
Legal	**15%**
Internal audit	**0%**
Help desk supervisor	**15%**
No One Person	**30%**

IV. Security Posture					
Q12 . The following matrix lists 25 attributions that define an effective IT security environment. Please assess the effectiveness of your organization's cloud computing security environment with respect to applications, platforms and infrastructure you provide to customer organizations. The four-point scale provided to the right of each attribute should be used to define your level of confidence in being able to accomplish the stated security requirement. 1 = very confident, 2 = confident, 3 = somewhat confident, 4 = not confident.					
Security objectives	AvG	1	2	3	4
Determine the root cause of cyber attacks	**48%**				
Know where information assets are physically located	**57%**				
Secure sensitive or confidential information at rest	**52%**				
Secure sensitive or confidential information in motion	**71%**				
Secure endpoints to the network	**59%**				
Identify and authenticate users before granting access	**37%**				
Secure vendor relationships before sharing information assets	**42%**				
Prevent or curtail data loss or theft	**57%**				
Prevent or curtail external attacks	**42%**				
Limit physical access to IT infrastructure	**65%**				
Ensure security governance processes are effective	**69%**				
Prevent or curtail system downtime and business interruption	**67%**				
Prevent or curtail system-level connections from insecure endpoints	**53%**				
Comply with all legal requirements	**69%**				
Achieve compliance with leading self-regulatory frameworks including	**69%**				
Prevent or curtail viruses and malware infection	**80%**				

Perform patches to software promptly	**53%**				
Control all live data used in development and testing	**55%**				
Enforce security policies	**64%**				
Access to highly qualified IT security personnel	**80%**				
Conduct training and awareness for all system users	**69%**				
Conduct independent audits	**62%**				
Ensure security program is adequately managed	**49%**				
Monitor network/traffic intelligence	**61%**				
Encrypt sensitive or confidential information assets whenever feasible	**48%**				

Q13. Please review the following list of 25 enabling security technologies. Then select each technology that your organization presently deploys in the cloud computing environment. Please include those technologies that are presently in-process of being deployed in the next 12 months.	
Access governance systems	**13%**
Anti-virus & anti-malware	**77%**
Correlation or event management	**10%**
Data loss prevention (DLP)	**8%**
Database scanning and monitoring	**34%**
Encryption for data at rest	**3%**
Encryption for data in motion	**58%**
Encryption for wireless communication	**14%**
Endpoint solutions	**22%**
Firewalls	**94%**
Identity federation	**0%**
ID & credentialing system	**30%**
Identity & access management (IAM)	**31%**
Intrusion detection or prevention	**38%**
Log management	**43%**
Network intelligence systems	**25%**
Patch management	**47%**
Perimeter or location surveillance	**19%**
Privileged password management	**23%**
Service oriented architecture (SOA) security	**27%**
Single sign-on (SSO)	**6%**
User management and provisioning	**15%**
Virtual private network (VPN)	**24%**
White listing solutions	**38%**
Web application firewalls (WAF)	**21%**

Q14a. Does your organization provide security as a service from the cloud?	
Yes	**9%**
No	**91%**
Unsure	**0%**

Q14b. Does your organization provide security as a service from the cloud?	
Yes	**33%**
No	**34%**
Unsure	**33%**

Q15. Please review the following list of 17 system control activities. Then select each activity that your organization presently deploys in the cloud computing environment. Please include those activities that are presently in-process of being deployed in the next 12 months.	
Background checks of privileged users	**3%**
Certifications (such as PCI DSS, ISO, NIST and others)	**44%**
Crisis communication procedures	**34%**

Controls assessment	**27%**
External audit	**13%**
Helpdesk activities	**76%**
IT audit	**26%**
Monitoring changes in regulatory requirements	**11%**
Policies and procedures	**65%**
Quality assurances	**52%**
Redress and enforcement	**17%**
Surveillance	**29%**
Training of data handlers	**35%**
Training of end users	**5%**
Training of security practitioners	**4%**
Vetting and monitoring of third parties	**22%**

Q16.Gartner has advanced seven cloud computing security risks. Please rate your organization’s ability to mitigate or significantly curtail this risk for IT operations in the cloud. The four-point scale provided to the right of each attribute should be used to define your level of **confidence** in being able to mitigate or curtail each risk area: 1 = very confident, 2 = confident, 3 = somewhat confident, 4 = not confident.					
	AvG	1	2	3	4
Restrict privileged user access to sensitive data	**32%**				
Ensure compliance with all applicable privacy and data protection regulations and laws	**48%**				
Ensure the physical location of data assets are in secure environments	**54%**				
Ensure proper data segregation requirements are met	**36%**				
Ensure recovery from significant IT failures	**65%**				
Investigate inappropriate or illegal activity	**49%**				
Ensure long-term viability and availability of IT resources	**48%**				

Q17. What types of confidential or sensitive information does your customers consider **too risky** to be stored in the cloud? AVG	
Consumer data	**11%**
Customer information	**19%**
Credit card information	**35%**
Employee records	**39%**
Health information	**50%**
Non-financial confidential business information	**31%**
Financial business information	**50%**
Intellectual properties	**42%**
Research data	**14%**
Other (please specify)	**0%**
None of the above	**46%**

Q18. What types of business applications do your customers consider **too risky** to be processed and housed in the cloud? AVG	
Sales and CRM applications	**25%**
ERP applications	**27%**
Human resource and payroll applications	**42%**
Financial and accounting applications	**54%**
Engineering applications	**14%**
Manufacturing applications	**5%**
Logistics applications	**4%**
Scheduling and time management applications	**2%**
Communication applications	**11%**

Other	**2%**

Q19. Does your organization have a fully dedicated security team to oversee the security of cloud applications or platforms?	
Yes	**26%**
No	**74%**

Q20. The Cloud Security Alliance (CSA) has advanced the following 14 areas as "critical areas of focus" for organizations deploying cloud computing resources. Please check each IT operation that your organization accomplishes or provides for your cloud computing customers.	
Critical areas of focus	**23%**
Governance and enterprise risk management	**48%**
Legal and contracting issues	**35%**
Procedures for electronic discovery	**26%**
Compliance and audit	**14%**
Information lifecycle management	**30%**
Portability and interoperability	**72%**
Business continuity and disaster recovery	**99%**
Data center operations	**27%**
Incident response, notification and remediation	**15%**
Application security	**28%**
Encryption and key management	**40%**
Identity and access management	**49%**
Storage operations	**13%**
Virtualization operations	**37%**

V. Organization characteristics and respondent demographics	
D1. What organizational level best describes your current position?	
Senior Executive	**4%**
Vice President	**4%**
Director	**22%**
Manager	**19%**
Supervisor	**5%**
Staff or technician	**33%**
Contractor	**2%**
Other	**6%**

D2. Check the **Primary Person** you or your supervisor reports to within your organization.	
CEO/Executive Committee	**4%**
Chief Financial Officer	**6%**
Chief Information Officer	**66%**
Chief Information Security Officer	**8%**
Compliance Officer	**3%**
Chief Privacy Officer	**0%**
Director of Internal Audit	**0%**
General Counsel	**0%**
Chief Technology Officer	**12%**
Human Resources Leader	**0%**
Chief Security Officer	**0%**
Chief Risk Officer	**3%**
Other	**1%**

D5. What industries does your organization serve?	
Airlines	**0%**
Automotive	**0%**

Agriculture	**0%**
Brokerage	**3%**
Cable	**0%**
Chemicals	**0%**
Credit Cards	**0%**
Defense	**0%**
Education	**12%**
Entertainment	**0%**
Services	**8%**
Health Care	**3%**
Hospitality & Leisure	**2%**
Manufacturing	**16%**
Insurance	**3%**
Internet & ISPs	**1%**
Government	**0%**
Pharmaceutical	**0%**
Professional Services	**5%**
Research	**2%**
Retail	**24%**
Banking	**5%**
Energy	**0%**
Telecommunications	**0%**
Technology & Software	**19%**
Transportation	**0%**

D6. What best describes your role in managing data protection and security risk in your organization? Check all that apply.	
Setting priorities	**60%**
Managing budgets	**68%**
Selecting vendors and contractors	**36%**
Determining privacy and data protection strategy	**40%**
Evaluating program performance	**63%**