ABSTRACT

Since the rise of cloud computing there has been a continuous debate about its security. This debate has been complicated by the fact that few cloud providers have offered detailed insights into their operations, and the technology used in clouds is not well known to the general public, making it difficult for IT outsiders to get an understanding of cloud security. This paper gives insights into the operations of an actual cloud by sharing the expertise of several CSC cloud security professionals who have detailed insights into the CSC cloud, as they work with it on a daily basis. Four myths of cloud computing are examined and debunked. These myths are: (i) customers can attack each other easily in a cloud, (ii) cloud users are protected by standard security, (iii) clouds are volatile and vulnerable and (iv) clouds cannot be transparent.

Keywords: cloud computing, cyber security, cloud security, CloudCompute, BizCloud, BizCloud VPE, ISO 27001

1. INTRODUCTION

About 15 years ago, when information security issues became known to the general public, the security problems concerned software that was in direct use by end-users: for example email was affected by viruses that spread through email attachments, and spam created an earlier form of denial of service by overloading users’ mailboxes. Vulnerabilities in these end-user systems are still present today, but in addition to that, a large part of the IT infrastructure has shifted away from the end user. Enterprises replaced email workflows with their own information systems and Excel spreadsheets were transformed into actual database-driven applications, maintained by a professional staff and running inside the corporate data center. The culmination of these developments is cloud computing, which in turn allows enterprises to shift away from managing their own infrastructure, instead relying on the services provided by cloud providers.

Apart from the business drivers and effects of this trend – the replacement of upfront investments in IT by a pay-per-use model – this trend also reduced the possibility for the general public and corporate user to understand information security issues, as they were no longer visible through personal experience. A database can be understood as an Excel sheet, but a database security problem such as a transaction log running full does not have any equivalent in Excel that is meaningful to a user in the same way. Likewise, a denial of service attack on a financial institution causes unavailability of the user’s banking app on her iPad, but she has no mental representation of the vast infrastructure that is running in connection to the app which is affected by the attack. The damage done to the institute is, however, far more sophisticated depending on the way the back end allows connectivity to the outside world. Global transactions and broker information could also be victim to the attack as well as various internal systems, all outside the view of the end user.
Clouds, which are not directly managed or maintained by their enterprise users or the general public, face the same issue: How can security risks be really understood if the technology is fairly new and there is no direct experience of what cloud is? One way to gain an understanding of the cloud and cloud security is to actually start using the cloud – simply paying with one's credit card and starting up compute resources in a cloud like Amazon’s EC2. However, even though this can be an enlightening experience for users, it does not provide insights into the infrastructure that supports this process and the corporate business processes running behind clouds. As such, there is the need for more insight into the nature of cloud security. Obtaining this information is difficult, however, because cloud vendors are not willing or are unable to give much insight into their operations. Important reasons for this are intellectual property protection, the need to protect the security of customers, and also technical issues associated with creating detailed reports of the cloud’s operations.

Still, first-hand information about cloud security is crucial in understanding what information security is about today, and to make informed decisions about whether to adopt clouds. It is the objective of this paper to share some insights into an actual cloud, through the experiences of three professionals working for a cloud provider, in this case CSC. These three professionals work as account security manager, IT architect and program manager respectively. In this paper they (from now on “we”) will shed light onto the CSC cloud as it is currently in use by enterprises all over the world. The method to do this is by discussing several commonly held beliefs about clouds:

1. Customers can attack each other easily in a cloud.
2. Clouds provide standard security.
3. Clouds are volatile.
4. Clouds are not transparent.

Before we discuss these myths in detail, we will explain a little bit about the CSC cloud (and especially the IaaS cloud) to set the stage. We conclude the paper with a summary of our results.

2. THE (CSC) CLOUD

In this section we will briefly explain cloud offerings in general and zoom in to the CSC IaaS cloud that will be examined in this paper. To begin, contrary to what many individuals and some companies proclaim, cloud isn’t as much a technical revolution as it is a business model. Cloud is a way of managing and handling resources, their usage and their cost. Cloud IaaS dices (or “virtualizes”) complex traditional IT resources into parts (storage, compute and network) and delivers these to customers in individual blocks with a flexibility that has not been seen before. Customers no longer need to install hardware solutions to cope with their peak activity. With cloud services, businesses don’t have to take into account their business development in the next five years; they can simply use as much as they need at that moment in time, using standard infrastructure components from the Cloud Service Provider (CSP). In turn, these building blocks can also be used to deliver higher-level services, such that a cloud can even incorporate complete workflows and application suites, such as Microsoft Office, and ERP systems like SAP.

This division between low-level clouds and higher level services is clear in the definition from the NIST (Peter Mell, 2011), which defines three basic service models for cloud (Figure 1). On the Infrastructure-as-a-service (IaaS) layer, the CSP provides the infrastructure for the management of

---

1 http://aws.amazon.com/ec2/
2 Note: This paper represents the authors’ experiences and personal views and opinions. The authors have taken substantial effort to support their claims, using their professional expertise and cross-checking of statements. However, the views and statements do not necessarily coincide with CSC’s corporate view and the actual state of the CSC cloud might be different than expressed in this paper. In addition to that, the reader is advised to carefully read the conclusions and recommendations section at the end of this paper to understand the paper’s limitations and the means to address these when assessing cloud security risks.
compute resources, usually in the form of virtual machines. The next level is formed by Platform-as-a-Service (PaaS), where the CSP offers an execution environment in which cloud consumers can run their applications. Finally, the CSP can also offer complete applications at the Software-as-a-Service (SaaS) layer.

CSC, as a CSP, is mostly active in two service models, namely the IaaS and the SaaS levels. To begin with the latter, CSC offers email services and virtual desktops services that can automatically scale with the number of users (Managed desktop, Clinical desktop and Secure desktop). In addition to that, CSC also deploys different cloud-based Big Data solutions and SaaS services such as Cordys applications and healthcare applications such as Lorenzo as-a-service. Concerning IaaS, CSC offers the following varieties:

- **CloudCompute** – A multi-tenant enterprise cloud service running from CSC’s data centers. In this model, customers deploy virtual machines into the CSC cloud, which is shared by different tenants.
- **BizCloud** – An on- and off-premises private cloud solution. In this model, customers get their own private cloud, installed in their own data center or at a CSC data center, which is managed by CSC. A service organization can be set up for the customer to comply with security requirements specifically required by a customer (for example, due to governmental regulations).
- **BizCloud Virtual Private Edition** – A private cloud deployed into a CSC data center that is delivering dedicated compute resources combined with logically segregated network and storage.

Unless stated otherwise, in the remainder of this paper we will consider CloudCompute when discussing the CSC cloud. For more information about this cloud we refer to the website.³

Technically, the CSC cloud is based on the “Vblock” architecture, a highly standardized cloud building block design, which is developed by VCE⁴ with components from VMware (virtualization), Cisco (networking) and EMC (storage). A picture of a Vblock is shown in Figure 2. There are three service levels within the cloud offering (Figure 3).

---

⁴ [www.vce.com](http://www.vce.com)
<table>
<thead>
<tr>
<th>Service Description</th>
<th>Silver</th>
<th>Gold</th>
<th>Platinum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Availability SLA (Minimum) Based on Availability Requirements for the Requested Environment</td>
<td>99.50% 3.6 Hrs / Month</td>
<td>99.90% 43 Min / Month</td>
<td>99.95% 22 Min / Month</td>
</tr>
<tr>
<td>Critical Incident Response Time</td>
<td>30 Min</td>
<td>30 Min</td>
<td>15 minutes</td>
</tr>
<tr>
<td>Operating System and Patch Management</td>
<td>Operating system management not available</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Anti Virus, Monitoring, Backup and Patch Management</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Platform Replication</td>
<td>-</td>
<td>Optional</td>
<td>Included (dual data center)</td>
</tr>
</tbody>
</table>

**Figure 3. Cloud Service Tiers**

Having described the range of cloud offerings, their associated service levels, and at a high level, what CSC is delivering, we will now turn to the first myth.

### 3. MYTH ONE: CUSTOMERS CAN ATTACK EACH OTHER EASILY

A very persistent myth concerning cloud computing is that different customers can attack each other easily from within the cloud. The assumption behind this is that customers share a pool of resources and can therefore more easily infiltrate other clients’ systems or data. Specifically it would be possible for an attacker to purchase resources on a cloud, position herself on the same physical machine as the target and launch her attack on other clients hosted on the same physical infrastructure. Given the security on CSC clouds, an attack of this type is unlikely to be successful. To explain this, we will use Figure 4, which represents a simplified public IaaS solution.

**Figure 4. Customers in Cloud and Attack Vectors**

In this figure, we see customer environments 1 and 2, which are each on the same cloud, with customer 2 being the attacker (red), and customer 1 being the victim (green). In this case, customer 1 also connects its own internal network (a situation common for many IaaS solutions). The parts that are managed by the CSP are shown in blue.
Now, what are the attack vectors and how likely is an attack? A first argument we would like to make is that it is not possible to simply become a customer in the CSC enterprise cloud. Unlike other clouds such as Amazon or Rackspace, an attacker is unable to simply draw her credit card and start using CSC’s enterprise cloud services. CSC’s enterprise cloud customers go through a rigorous verification process before they are able to utilize resources. This drastically limits the chances of attacks, as malicious customers cannot remain anonymous in the CSC cloud as they could in a more open public cloud. We will now examine four basic attack vectors:

1. Attacks on the virtualization or hypervisor layer that separates customers
2. Vulnerabilities within the management layer provided by the cloud service provider (everything in blue)
3. External attacks from the Internet (red)
4. Internal customer network threats (hopping from one client internal network across to another)

3.1 ATTACKS ON THE HYPERVISOR LAYER
At the core of customer separation is the hypervisor layer, which splits the CPU of the hardware into compute cycles that can be used by different virtual machines belonging to different customers. In effect, this creates a sandbox for the customers. It does not function natively on the host and can only access host resources through a separate control layer commonly named the hypervisor.

Cloud computing utilizes sets of hypervisors to distribute and assign resources. In fact, at the cloud layer, sets of virtual devices are sandboxed and offered to clients as if they were completely separated data centers. Thus, cloud computing is very dependent on the quality of the hypervisor security. Are they secure enough? In fact, within the CSC Cloud the hypervisor provides a very strong barrier between virtual machines and thus between different customers.

Evidence suggests that there have been very few attacks where a virtual machine has been able to elevate its privileges due to a hypervisor attack or to gather data from other virtual machines. One of the most interesting attacks was carried out on Amazon’s EC2 platform, where researchers were able to steal a cryptographic key in a side channel attack (Zhang, 2012). However, first of all, these types of cryptographic attacks are mainly of theoretical interest, as the conditions used in this attack would be unlikely to take place within normal business practice. Second, the hypervisor is relatively small in terms of its code base and open attack surface. An operating system such as Windows is thousands of times larger than the hypervisor, which is thus much more likely to remain bug free.

3.2 MANAGEMENT LAYER
Furthermore, we consider the fact that the hypervisor (as is the case with all IT services) must be patched and maintained. New versions and updates provided by suppliers must be installed through a management interface, which in turn is vulnerable for attacks. However, unlike normal software patching, the management interface of a hypervisor can be completely isolated from the end-user resources running on top of it by placing it on a separate management network. As a result, a malicious customer cannot use it to launch a direct attack. This design has been verified in penetration tests. The same argument is valid for other resources (networks and storage), which also have separate management channels that are not accessible by customers. It is worth noting that the risks increase when customers have more access rights to the management layers, for example in the form of web services.

3.3 INTERNET
Another approach for a customer is to simply launch an attack over the Internet, as most customers also connect their cloud to the Internet. CloudCompute offers a variety of defenses against these types of attack ranging from basic firewalls to more advanced mechanisms. We don’t see any reason...
to believe that the cloud is less secure than a traditional hosting environment in a data center. To the contrary, because the cloud is serving multiple clients, the security mechanisms are often at a higher level than can be deployed by an individual customer. The security resources of the cloud can be leveraged for different customers, such that, for example, 24x7 security monitoring for all customers can be cheaper than 8x5 (working hours) monitoring for one customer. In addition, the cloud’s bandwidth is much higher than that of an ordinary customer, giving it more means to reduce the chance of a successful denial of service attack.

3.4 CUSTOMER NETWORK
A more insidious way is to attack the customer through its own network, for example through end-user laptops or servers in non-cloud data centers. To limit the chance of successful attacks of this type, cloud users can use desktop virtualization services, combined with firewalling, to reduce the attack surface from their office locations. This type of attack is nonetheless more likely than a direct attack on the cloud, as basic service management remains a challenge for even the most security conscious enterprises. End users are vulnerable to phishing attacks, in spite of all the security awareness training that is given. From that point of view, the cloud is clearly not the weakest link.

3.5 CONCLUDING REMARKS
As we have seen, there is little reason to believe that clouds offer more attack paths for customers to attack each other compared to more traditional service delivery methods. Hackers will attack at the most vulnerable point in an infrastructure. Given the fact that hacking the cloud itself is problematic, they will likely follow other means to gain access to a client’s systems. This debunks the myth that one cloud customer can easily attack another one.

4. MYTH TWO: CLOUD USERS ARE PROTECTED BY STANDARD SECURITY (AND DON’T NEED TO BE INVOLVED)

The advantage of any cloud delivery model is that it is standardized and leveraged: a customer can quickly utilize basic services at a low cost. For all cloud services (IaaS, PaaS and SaaS) security functions such as availability management and network intrusion detection are handled by the service provider without any intervention from the client. In many cases the service provider is able to demonstrate that the service is compliant to specific security standards such as ISO 27001. Thus, customers can simply rely on certification (to which we will return in Section 6) and the baseline security that is covered under this. We don’t believe this is correct and this is especially clear at the IaaS level, which we will focus on here.

4.1 BASELINE SECURITY AND CLIENT CUSTOMIZATION
We first examine the issue of baseline security – the basic security controls (technical and operational) that make up the cornerstone of cloud security. As we argued in Section 3, basic security should be substantially within a cloud because of the shared multi-tenant aspects of the cloud. In the CSC cloud (as is likely the case in other clouds) baseline security involves an elaborate mixture of security controls across the entire ISO 27001 spectrum (ranging from physical security to human resources to incident management). Does that mean, however, that the client should rely on this baseline security? The recommended answer is no.

Security cannot be handled by the service provider alone, translating customer business requirements automatically into the right level of security. No matter how good the technical capability of the CSP, there will be an interface between the customer and the CSP (the “last mile”) that must be customized and managed. Networking services, user account management, patching and release management all require attention from both customer and service provider to organize securely. This is especially true at the IaaS level, but also for the higher levels, where customers must integrate identity and

\[^6\] Actual monitoring by CSC is also dependent on the service level chosen by the customer.
access management with the cloud vendor to allow their users access to services such as ERP or email. These services, even with the best automation possible, are not turnkey and will require customization for the foreseeable future. As an example, DDOS attacks have highlighted the limitations of directly accessing resources over the Internet, and customers continue to create their own network connections to access their cloud resources to meet high availability requirements.

Furthermore, CSPs also offer support services (for example, patching and security management) and must perform upgrades to their infrastructure. All these processes impact the customer and must be communicated. An ISP that connects consumers to the Internet can choose its own maintenance windows and working methods, but a CSP must work in collaboration with the customer to ensure that her business processes are not unnecessarily affected. Concerning security, the issues might become so complex that a specific person is appointed (the account security manager) whose sole job is to enforce secure collaboration, ensuring that the CSP and the clients appreciate their mutual obligations around security and therefore can maintain the security and integrity of the cloud that has been deployed.

4.2 ADDITIONAL SECURITY SERVICES AND ALTERNATIVES
No matter how good the baseline security services are, there remain situations in which it is not sufficient. Security is also a cost component, and this means that security cannot be limitless applied. Thus, what can be done to mitigate the limitations of baseline security in a cost-effective way? Essentially, after a risk assessment has demonstrated that the cloud does not meet the customer’s security requirements, two options remain:

- Complement the cloud with additional security mechanisms.
  This is the easiest option: On top of the baseline security mechanisms, new and customer tailored services are deployed. Advanced chargeable services can include host intrusion prevention, SIEM tools and audit log assurance services, and custom reporting within existing security controls (such as reports of administrative connections) and database and system encryption.

- Create another baseline security model.
  A reality that must be faced is that there are situations where the baseline itself cannot be extended with security services. As an example, this can be because the delivery model is global, and customers might have the requirement that only CSP personnel from a specific country or with specific security clearances are able to work on their systems. One solution is to set up a separate delivery team who will manage a separate instance of the cloud (a BizCloud in the case of CSC). Another option is that CSC returns specific maintenance tasks back to the customer (for example, by reducing the service level from Gold to Silver), who can find a suitable organization to perform these. A final solution is to offer specific security guarantees to a customer, for example a customer-specific scope extension of ISO 27001 (see also Section 6 about certifications).

4.3 CONCLUDING REMARKS
There is a large difference between provisioning compute resources and security resources. The former ("give me two extra virtual machines") is substantially easier than the latter. Security – both technical and operational – must be explicitly put into the system design before resources can be scaled up, and the customer must be involved in the process. CSPs are working on making security as easy as other compute resources, but this takes considerable effort, and risk assessments will continue to require customer involvement and involvement of the CSP. In dealing with cloud security, a cloud risk assessment can have three basic outcomes:

1. The cloud baseline suffices.
2. The baseline does not suffice and additional security measures and processes will be required.
3. The baseline does not suffice and must be redesigned.
5. MYTH THREE: CLOUDS ARE VOLATILE AND VULNERABLE

The third myth we aim to address is the volatile nature of clouds. In the view of many enterprises as well as the general public, clouds are constructed in such a way that data can flow freely between servers worldwide and applications can be created and destroyed without leaving a trace. Yesterday sensitive data might have been stored in Sydney, today it is in Hyderabad, and tomorrow it will be copied to an unsecured data center located on a small island in the Caribbean. For the CSC cloud, we will address this myth from three perspectives.

5.1 DATA CENTERS
CSC uses a limited set of data centers, shown in Figure 5. A customer decides which location (or locations in case of disaster recovery) it intends to use and CSC will utilize only that data center or that geography, which is put into the contract. In addition to that, the CSC public cloud is limited to those data centers that pass the security requirements (e.g., ISO 27001). This gives physical protection to the data itself, protecting it from natural and man-made disasters and ensuring that CSC has comprehensive processes and procedures in place to protect client information.

Figure 5. CSC Cloud Data Centers Worldwide

5.2 OVERALL NETWORK INFRASTRUCTURE
CSC has a worldwide data network, but by default it does not provide full automatic connectivity between data centers or load balancing between multiple data centers in the way that, for example, Google load balances Gmail traffic between different sites. Customers must explicitly request network connectivity, and often they will opt for a dedicated connection from their office locations to the CSC data centers to ensure high availability. Changing data centers remains possible but must be anticipated, as in the case of a dual data center implementation. All this contributes to a more rigid and more secure cloud.

5.3 DELIVERY OF COMPUTE RESOURCES
The working unit of a cloud is the virtual machine (VM), on which an enterprise installs its services and applications. How easy is it to create new VMs, run malware on them and delete them? The answer
starts with the fact that CSC is always involved in this process – the environment is controlled through a certified change management process. All changes for VMs are initiated by the customer and go through a standardized change management system that is an integrated part of the service delivery model. CSC does give customers the option to take back some of this control if they require and arrange the management themselves. This is done by reducing the service level, and in that case the security depends more on the customer’s own security processes. Could VMs then be transferred off site to another data center, or even to any location on the Internet? Again, depending on the customer’s requirements, CloudCompute has specific features for VM synchronization to facilitate disaster recovery, but again, these can only be used between sites that have been connected beforehand, and can only replicate existing machines to a known site. This reduces the chance that an attacker can simply move a VM outside of the original data center. Reporting of VM activity can be provided to demonstrate that the customer’s workload is indeed resident in the designated sites.

5.4 CONCLUDING REMARKS

Clouds do not have to be volatile; in fact, they can be made very structured and almost rigid in approach if required. This improves the security guarantees that can be given to a client regarding the systems running in the cloud and, specifically, we can know where our data is residing.

6. MYTH FOUR: CLOUDS CANNOT BE TRANSPARENT

As we already mentioned in the introduction, given the amount of mythology around cloud, it is difficult for the public to understand the workings of clouds. In fact, a common assumption is that clouds can become so vast and complex that they are practically unmanageable, and that it is hard for the even the CSP to retain control over them. Does that mean that cloud transparency is impossible?

To begin, CSC has earlier been working on the cloud transparency protocol, which describes a mechanism for cloud users to find out key security information about a cloud, based on standard reports generated by cloud providers (Ron Knode, 2010). Such a protocol has not been implemented by any cloud provider (including CSC) yet. In the remainder of this section we will therefore explain the current achievements of the CSC cloud regarding transparency: how CSC’s security controls are working and how they ensure that the cloud is bounded. We will break this down in three parts:

- Securing standard global cloud offerings with technical and procedural controls.
- Using a certification process and procedures to monitor compliance of those security standards.
- Targeted penetration testing designed to evidence secure logical separation of clients, data, and services.

6.1 TECHNICAL AND PROCEDURAL CONTROL FRAMEWORK

For each level of secure services a model is designed to meet the specific security requirements of ISO27001. CSC uses one set of global master controls for its security, which is applied to all cloud deployments. The delivery models are designed with this in mind: management and support services can be penetration tested and risk assessed to provide evidence that a client’s data is secure and safely managed in that multi-tenant infrastructure. Specifically in the United Kingdom, where CSC offers cloud services to the UK Government (HMG), the security levels HMG IL2 and IL3 are also applied, which require specific security controls. These controls provide transparency of service definitions and solutions.

6.2 CERTIFICATION

An important issue (if not the most important) of a certification is its scope. What is covered and what is excluded? Generally, cloud certifications can be split in three parts:

1. Data center certification, with the specific focus on physical and procedural security.
2. Technical management of the data center.
3. Cloud services themselves, which can be delivered from many different delivery organizations.

Ideally, clouds should be certified at all these levels. Generally there are three ways that this is achieved. First, there are external auditors for the CSP. For CSC specifically, ISO 27001 certification is carried out by a specialist auditor, who periodically visits the sites that are in scope, reports on the security status and makes recommendations for improvement.

Second, CSC’s cloud designs are not only assessed by external auditors but also undergo governmental scrutiny. In this section we focus on the situation in the UK. Following on from 27001 in the UK, CSC has achieved IL2 level of security and is working towards IL3. UK Government provides a framework of guidance on acceptable/appropriate levels of security. Each level of security requires an increasing level of probative auditing and testing, looking at levels of control and security from patching through to data aggregation. The process is based on an approved offering architecture that the UK Government agrees with the CSC security cloud consultants. From this architectural review a list of potential security challenges are raised, and it is those in conjunction with best practice that create the framework for a penetration test plan wholly designed to test the environment to its limits.

Third, customers can also perform audits (or more precisely, ask their auditor to do this for them, for example in an ISAE 3402 audit). In that case the audit can request specific information about relevant security controls for its customers, and physically attest in which rack the cloud resources are allocated on which their business processes are running.

6.3 PENETRATION TESTING

Apart from auditing, a frequently used method to gain assurance of a cloud’s security status is through penetration testing. Customers can request penetration tests from CSC directly, or hire a partner to perform them. For the UK Government, an ongoing programme of penetration testing to demonstrate a cloud’s continued protection is an important part of offerings. The objective is to demonstrate not just ongoing vigilance of potential problems but also early sight of potential new threats and risks as soon as they are known. Overall, testing must be broader than the pure cloud and includes:

- Testing the external environment (Internet).
- Testing internally from inside a corporate network, looking for not only threats in the cloud but all that is connected to it, including the organization’s own infrastructure and client-connected infrastructure.
- Testing all the familiar areas such as firewalls, load balancers, Vblocks, management pods, virtualization tool sets and management tool sets.
- Utilizing both automated scanning tools and manual interventions.
- Vigilance regarding new threats – maintaining version and patch concurrency to identify and mitigate newly identified vulnerabilities as soon as the supplier raises the alert.

6.4 CONCLUDING REMARKS

Insight into cloud security (“assurance”) begins with the CSP writing down its internal policies of how it deals with information security, and how they are applied to the cloud. Next, the CSP is audited by external auditors. Customers can request audits and gain insight into whether controls that are specifically important to them are implemented. Also, cloud service reporting can be provided to the customer, covering configuration compliance, threat protection, auditable activity, security events and access reports. Finally, penetration testing can offer a bottom-up view on the workings of the cloud.

7. CONCLUSIONS

In this paper we have reviewed and debunked several popular myths regarding cloud computing. Customers cannot attack each other easily, standard cloud security is hard to achieve, you can actually ascertain where your data is in the cloud, and yes, clouds can even be transparent. The CSC
cloud is not as flexible (or elastic) as the clouds from Google or Amazon, but that is not a concern for most enterprise loads. CSC balances the need for security with the flexibility of the cloud ethos. This gives assurance to customers about where their data is stored (and will be stored tomorrow), along with a known, visible security model.

Even though this paper provided firsthand experience about cloud security, it is important to understand that the cloud is not without risks and we were unable to elaborate on this in every detail—both concerning the existence of risks as well as their mitigations. Delving into greater detail than this paper provided will show how those risks can be further mitigated; a full ISO 27001 statement of applicability for a cloud covers more than 100 controls, which is beyond the scope of this paper. Also, CSC detailed designs and security controls provide increased assurance, but of course these are covered by intellectual property restrictions. Finally, risk assessments, highlighting what we see are the important issues as well as the findings of external auditors over the years, offer real insights into increased security assurance and protection of client data.

How, then, can we assess the security of the cloud in a complete manner? For this, we should refer to myth three; this assessment starts with the prospective cloud adopter. A customer that is protecting nuclear secrets has very different workloads and requirements compared to a hospital that must guard its medical files (not to mention different financial resources). Any customer has to compare her own situation and needs to that of the cloud. If the cloud (in one of its variants) meets the requirements or is more secure than the current status, it can be worth migrating. Finally, for a complete picture of cloud risks, prospective cloud consumers can of course contact CSC's cyber consulting cloud practice group, who makes risk assessments based on specific customer requirements and public material (mainly the Cloud Security Alliance security models), as well as its proprietary intellectual property and expertise gained from the CSC cloud. In any case, we hope that this paper has improved the understanding of cloud risks and contributed to the debate on cloud security.

---

8 [https://cloudsecurityalliance.org/](https://cloudsecurityalliance.org/)
ABOUT THE AUTHORS

André van Cleeff works as a Security Specialist for CSC Netherlands. His primary tasks concern account security management for CloudCompute and general cyber security consulting. acleeff@csc.com

Niels Lagerweij is a Technology Architect for CSC Netherlands. He designs solutions and migration scenarios for customers running on or planning to move to CSC’s cloud solutions. nlagerweij@csc.com

Susie Allwood is a Cloud Programme Director for CSC EMEA Northern Region and has been managing CloudCompute ISO 27001 certification and Restricted Cloud program. sallwood2@csc.com

ACKNOWLEDGMENTS

The authors would like to extend their gratitude to the members of the Cloud Team across Europe and Global CSC for their ideas and thoughts, as well as to the Cyber team for collaboration and support. Specifically, we thank Michael Dutton, Ben Haworth, Lyzia van Iterson and Alex Smink for reading and commenting on earlier drafts of this paper.

REFERENCES


About CSC
The mission of CSC is to be a global leader in providing technology-enabled business solutions and services.

With the broadest range of capabilities, CSC offers clients the solutions they need to manage complexity, focus on core businesses, collaborate with partners and clients and improve operations.

CSC makes a special point of understanding its clients and provides experts with real-world experience to work with them. CSC leads with an informed point of view while still offering client choice.

For more than 50 years, clients in industries and governments worldwide have trusted CSC with their business process and information systems outsourcing, systems integration and consulting needs.

The company trades on the New York Stock Exchange under the symbol “CSC.”

DISCLAIMER
The information, views and opinions expressed in this paper constitute solely the authors’ views and opinions and do not represent in any way CSC’s official corporate views and opinions. The authors have made every attempt to ensure that the information contained in this paper has been obtained from reliable sources. CSC is not responsible for any errors or omissions or for the results obtained from the use of this information. All information in this paper is provided “as is,” with no guarantee by CSC of completeness, accuracy, timeliness or the results obtained from the use of this information, and without warranty of any kind, express or implied, including but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will CSC, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this paper or for any consequential, special or similar damages, even if advised of the possibility of such damages.