Commentary: Cloud computing – A security problem or solution?

P.G. Dorey\textsuperscript{a,}\textsuperscript{*}, A. Leite\textsuperscript{b}

\textsuperscript{a} Royal Holloway, University of London, UK
\textsuperscript{b} KPMG LLP, UK

\textbf{Abstract}

The move to cloud computing is the next stage of an unstoppable trend in the breakdown of the enterprise perimeter, both technically and organisationally. This new paradigm presents a number of security challenges that still need to be resolved but sufficient change in the IT environment has already happened - so that most organisations are working in a transitional state where security exploits are happening across the enterprise boundary. In this situation, the compartmentalisation introduced by migrating to cloud services could result in much improved security.

© 2011 Elsevier Ltd. All rights reserved.

\section{1. Introduction: the rise of cloud computing}

It is clear that cloud computing has number of attractive aspects that are driving adoption (Grossman, 2009). Benefits such as cost reduction, improved provisioning and access to resources beyond that which would normally be possible in a private environment are just some of the items that are frequently mentioned. This drive to adoption is being echoed by many CIOs and is being reflected by real purchasing decisions. In a report last year by investment bankers Goldman Sachs (Goldman Sachs, 2010) 58% of enterprises consider Software as a Service (SaaS) when purchasing an application and 39% preferred the SaaS option.

But cloud computing as `software as a service' has not just happened overnight, and is very much part of a continued trend to extend IT capability and business processes beyond the traditional boundary of the enterprise. Understanding this trend is important in understanding the changing risks and so we shall explore them in more detail.

\subsection{1.1. Progression of connectivity}

The progression of connectivity in information technology has led inexorably towards more and more granular connections – moving from simple enterprise to enterprise extranet mainframe and minicomputer links in the late 1970's and early 1980's towards peer to peer connectivity by 2000. This peer to peer interaction has grown - either directly or through Internet-based brokers (like a social networking site). The evolution of connectivity with time has been well described by the Industry thought-leadership group The Jericho Forum in their business case paper for deperimeterisation (The Jericho Forum, 2007) and is summarised in Fig. 1.

External cloud computing itself is part of the progression of connectivity, where various services (from Software as a Service- Saas- at its most complete, down to Infrastructure as a service- IaaS- at its simplest) are delivered outside of the enterprise. This change in architecture requires pervasive connectivity leading to the point where the Internet itself can become the corporate network. As illustrated in their diagram (The Jericho Forum, 2007), The Jericho Forum highlights that the corporate perimeter – the secure separation of the enterprise managed network from external networks - essentially broke down some time in the early 2000's. The implications for security are clearly significant.
1.2. The ‘flat’ corporate Network

Despite the trend, enterprise security architectures have still very much continued to focus on the perimeter. In many cases this focus of security on the perimeter and ease of developing end user applications has also led to clients and servers being made intimately part of the same network in one homogenous flat structure. How this occurred is not surprising, as in the evolution of end user computing, a significant amount of application development moved towards applications designed to be run on client PCs and then, through the development of client-server architectures, these migrated onto local servers. This local ownership resulted in a management battle in the mid 2000’s where a goal of the IT department became the retrieval of those servers from ‘under the desk’ of local departments and back under management in the data centre (for example (Friedman and Rosenberg, 1999).

But even in the data centre, the legacy of departmental computing remains. As stated earlier, in many cases the way that local departmental applications were developed has tended to require administrative privileges on local PCs and in addition they also require very ‘flat’ network relationships from client to server in order for the applications to run. In our experience, additional barriers such as firewalls between client and server within the corporate network have not been common, and where it has been tried there have often been technical difficulties in achieving a good level of network segregation.

1.3. The social engineering path

A combination of fallible end-users connecting to the Internet, local administration rights and flat network relationships has provided a ready path for unauthorised access. The attackers have therefore found ways of exploiting the end user as a vector to access data on servers and systems that were otherwise reasonably protected. The method of attack has steadily escalated into a kind of ‘arms race’ (Moore and Anderson) where the attackers have exploited a particular attack, combining technical exploits and targeted social engineering such as Spear Phishing (Herley, 2010) which the security profession has attempted to counter on a case by case basis. There are many white papers that describe the methods by which malware is infiltrated into the network inside the corporate perimeter, but in general the main approach described is as illustrated in Fig. 2.

To date the most sophisticated form of such attack has been termed ‘Advanced Persistent Threat’, which (in the view of almost every security professional) is impossible to protect against with current porous-perimeter architectures, the only realistic strategy being early detection and response (The Security for Business Innovation Council, 2011).

The common steps in Advanced Persistent Threat Attack (APT) is similar to standard malware infiltration but with additional direction and intelligence, as described below (The Security for Business Innovation Council, 2011):

1. Reconnaissance to build knowledge of the organisation
2. Social engineering and/or spear phishing to target end users
3. Exploitation of vulnerabilities in an end point
4. Lateral expansion using peer relationships to roam the network
5. Escalation of privileges
   - Additional spear phishing or decrypting administrators’ passwords
6. Compromise of internal systems
7. Exfiltration of data or other objective (such as planting false information)
8. Cleanup

The above examples therefore illustrate some of the risks in transition from closed to open networks that we are facing. Whilst data itself remains open on the corporate network, and inside attack can be initiated through end user access (through the Internet, email or portable media) we have a significant and growing exposure that requires a new architectural approach to be able to manage it.

2. The risks during transition

In the view of the authors we are currently at a dangerous stage of transition from a security model based on protection that relies on a strong corporate network perimeter moving over to a data-centric model where data and information repositories themselves are protected and data is organisationally segregated from systems management.

The security dangers arise because of undeveloped thinking and understanding of the security changes during this transition period and hence an almost undetected threat is starting to be realised within many enterprises. Because many IT and security professional are still focused on the perimeter, investment in deperimeterised security technologies such as data-centric security has not yet caught up. This is not strictly just a problem for those deploying security because, until very recently, most technology vendors were also still focused on attempting to plug holes in the perimeter rather than addressing the new challenges.

As described above, we have seen the security consequences of this breakdown, as end users are able to directly access Internet web sites from within their own enterprise LAN, and openly receive email at the desktop from all Internet sources, both legitimate and malicious (such as spam). A whole industry exists to attempt to lock-down endpoints and filter incoming traffic but at best (as illustrated by the APT example) this has been only partially successful.

In most cases, security professionals and their IT colleagues have been able to do a relatively good job in protecting applications within the enterprise from direct external attack. With only a few notable exceptions, work on firewalls, proxies and improved secure applications development have gone a long way to creating robust and protected applications. However, whereas locking down applications and servers in their managed data centres has been achievable, attempts at locking down the clients has proved to be politically and technically impossible in many cases. A simple Internet search of technical IT support forums (IT Management, 2011) shows a very active debate still rages on whether full local administrative access of PCs, with the ability to load executable software, is acceptable or a security disaster because of pervasive malware. It is therefore not a big step to consider that clients operating on the same network as applications and servers can be a fundamental security weakness.

3. The security benefits of cloud computing

In the view of the authors, some aspects of cloud computing provide key elements of the necessary architectural change to segregate clients from mass data and applications. As mentioned earlier, a quick analysis of the means of data
access being used in APT espionage and similar data theft approaches; shows that there would be a benefit in better segregating shared data and applications from the network that the client sits upon. Externalised cloud computing software as a service (SaaS) applications have this advantage because they do not expose the full network stack to the clients who access the application; in an analogous situation banks do not put their internal corporate networks at risk by giving customers access to banking applications, all that is exposed- even on identity theft - is the individual account of a single customer. Arguably, SaaS cloud computing therefore offers some protection against the ‘lateral movement’, privilege escalation, and reconnaissance of APT. In the example of Fig. 2 above, there could be no further movement between stages 3 and 4 of the attack in a well-engineered cloud hosted application and the malware would remain localised on the end user’s initially infected PC.

There are further advantages of cloud computing where SaaS is provided as a utility service to many client companies. In this circumstance the cloud service provider is not uniquely connected with the target client owner of the data and so social engineering of service company staff is unlikely to be as relevant to a particular data set and therefore will be less effective as an internal data access attempt on enterprise staff. In fact it should be possible to segregate the data of customers from the information flow of the cloud provider itself as the different areas of data support completely different enterprise business processes.

Aggregation through cloud services should also bring other advantages such as economy of skill where larger teams of security professionals are more cost effective for the service provider than they would be for their clients, and also the benefits brought by centralisation of security processes, resilience and redundancy (Zissis et al., 2011). Providing services across multiple clients also gives a cloud services provider the ability to see a wider picture of attacks and security events than a single client and thus should be able to better operate an early warning response to particular attack, or give better context of whether there is particular targeting of a single client. Such benefits have already been recognised by some Internet Service Providers.

The ability of cloud service architectures to deliver improved security has already been demonstrated for a number of years with the existence of popular malware scanning security services for email and cloud-based proxies offering filtering of web browsing. Indeed commercial services even exist to support enterprise network security configuration and patch-management that are delivered from the Internet cloud.

4. Risks relating to cloud computing

Of course, moving to cloud services falls well short of completely solving the security problem; instead it refocuses security concerns onto other key areas of security engineering. A large cloud services provider is arguably a bigger target and more attractive for those who wish to cause maximum disruption through attacks such as distributed denial of service. The externalisation of the application also increases the attack surface to which it is exposed and requires robust software integrity created through the use of secure development methodologies (for example the importance of input validation and/or filtering techniques to resist attacks such as SQL injection). We should therefore be concerned where developers do not follow the necessary best practice (SAFECode, 2011).

Much of the concern around cloud security is related to third party management – the fact that the cloud service provider is not a directly managed from within the client organisation. As such the normal security issues of outsourcing appear, i.e. being concerned with the integrity, control and sustainability of the supplier and the totality of risks that the client is taking when relying on a third party. None of these concerns are new to information security; however what should be new is the wish for the cloud service to be much more of a utility in the way that it operates. A true utility should have a service relationship with many clients and not expect to have 1:1 audit relationships with each one of them. This requires a universally accepted audit certification (see below) that ideally can be reported into the client’s Enterprise Risk Management and its Governance, Risk and Compliance Reporting.

Other cloud security risks include the adequacy of segregation of data between clients as well as its geographic (and regulatory) location, technical issues such as the presence or absence of encrypted (secure) communications and virtualisation security, and fundamental architectural concerns such as a dependence on the Internet and missing choke-points that can be used to monitor system and end-user security behaviours.

The final category of concerns relate to integration with existing enterprise security processes. Many organisations have invested significantly in access control and identity management systems so that their joiners/leavers process will ensure the timely provisioning and de-provisioning of computer facilities when someone changes job or leaves. Internal networks have also used technologies such as Microsoft’s Active Directory to provide a secure single sign-on to services and applications. Both of these integration successes are challenged by cloud computing services that more often than not have their own separately managed user identifier and access password. Further loss of integration can also occur where encryption keys come under management of the third party and not the client, and also if monitoring of user access is not available for behavioural monitoring. Concerns over integration of data management further come about through corporate obligations to manage all instances of company data, such as when e-discovery is required in legal cases.

5. Focus areas for investment in cloud services security

In this paper we are discussing the potential information security benefits of cloud and advocate that the Cloud model can actually make a positive contribution to the Security posture of Service Consumers. However, we have also stated that it cannot be ignored that security challenges still remain
which can lead to hesitation in wider adoption or even fundamentally undermine the business case (Armbrust et al.). We now look at three concerns that in our opinion are priority areas for security improvement in the Cloud environment:

1. Identity and Access Management
2. Data Security
3. Trust and assurance

5.1. Identity and Access Management (IAM)

IAM is very much at the heart of Information Security in its aim to identify subjects and based on this information define which resources to which they should be allowed (or denied) access. Traditionally, IAM systems have tended to be centralised, often consisting of discrete directories covering particular areas of a single domain. The increase in interaction with 3rd parties and growth in number of applications and other technology portfolios, has led to the need for solutions that allow for a single logon to gain access to multiple resources without having to re-authenticate (secure single-sign-on).

However, customary solutions such as the use of Kerberos or PKI based schemes pose challenges when dealing with environments that involve multiple parties managed under distinct and separate security domains. The early appearance of Web based single sign-on solutions addressed the challenge of allowing users to logon once and access multiple resources, however these tended to either use proprietary protocols or have extensions to existing standards making it difficult for an enterprise to manage integration with outside parties - particularly with providers of Cloud-based services (Núñez et al., 2011).

To address these challenges, Federated identity management (FIM) has been proposed as an umbrella term covering an array of standards and technologies that allow for distribution of identity information as well as delegation of IAM related tasks across multiple parties and security domains (Shim et al., 2005). In a typical FIM system we can identify at least three parties:

1. A principal attempting to access a resource
2. The relying party (RP) who provides the service and relies on a IdP
3. Identity Provider (IdP) who provides specific information about the Principal.

Within FIM we make a distinction so that we can also distinguish between Centralised and Decentralised systems with their own characteristics:

- Centralised systems: That use a single IdP that is aware of all Principals and serves all RPs. These have posed challenges associated with concerns over a single entity having full control and the need to have all participants accept and integrate with this single entity. For this reason, centralised systems have often gained limited adoption, a good illustration of these being the case of Microsoft Passport (Menn, 2004). In the authors’ opinion such systems are appropriate in very specific use-cases in which a dominant IdP exists by default, such as in the case of government related services where a central entity has the need to view all subjects and evaluate their access requirements.
- Decentralised systems: Are cases in which multiple IdPs are present, each covering a limited set of users and appropriate trust relationships are defined that allow for identification to be performed by the IdP that holds information on the Principal. Whilst in theory this appears to be a viable option, semantic challenges arise when having to deal with links between all IdPs and RPs involved in a given circle of trust. For example, interoperability – the need for all parties to talk with the same protocol and interpret the same policies, and also the inheritance of trust between the different providers – how parties taking part in a circle of trust can know that all participants are trustworthy. However, a solution appears to appearing to address this integration and interoperability challenge, and SAML is emerging as the popular choice due to wide adoption in end user organisations as well as cloud providers. Version 2 of this standard builds on previous work and combines the aspects of SAMLv1, Shibboleth and Liberty Alliance’s Liberty-ID FF 1.2 (PingIdentity, 2011).

The Liberty Alliance (Liberty Alliance, 2011), originally drafted standards and acted as an industry body for delivery of identity standards has now disbanded and transformed into the Kantara Initiative (Kantara Initiative, 2011) with the aim of validating and certifying interoperability between different vendors of products supporting SAML. Shibboleth originally built on top of the SAML 1.0, now leverages SAML 2 and has enjoyed continued success particularly in academic environments.

In spite of emerging standards, the process of managing Identities in cloud environments still presents a level of architectural complexity. We therefore see the emergence of Identity as a Service (IDaaS) as a potential opportunity to address complexity in IAM both in cloud and even internal environments that may require access by third parties. Technology providers sitting in the middle between Service Providers, Identity Providers and Users can readily provide an adequate integration layer that is able to process and interpret multiple forms of Identity and Authorisation management and act as translators to recognised standards, such as SAML. The use of such a service in itself can facilitate the management of identity throughout its lifecycle including the provisioning/de-provisioning and the capture of relevant event information that is required for monitoring and audit purposes as well as the provision of self-service mechanisms for use by end users.

Overall, we believe, that as far as technology and standards are concerned, the current state of the art now addresses the major identity management challenges raised in the past. However barriers still remain over how to integrate with existing processes and also how to deal with the more general issues commonly raised in over cloud computing such as dependency and trust in the Service Provider.

5.2. Data Security

Adoption of cloud computing in any of its forms has the clear implication of relinquishing ownership of technology
infrastructure (with clear benefits, we should add). However, one important item is left that cloud consumers own—and that is the Data.

This presents us with a new challenge, because very commonly it has been the case that security controls are placed closer to the infrastructure level. As we move to more service based technologies it becomes harder to data owners to actually be able to enforce or impose controls at the infrastructure or even at the application layer.

The shared nature of cloud services also make it impractical for individual users to dictate controls that should be implemented in different technology stacks and raises the need for controls to be closer to the asset that they can influence i.e. security controls need to be more data-centric. With this in mind we look at data-centric controls from two perspectives: Preserving confidentiality and Architectural issues.

5.2.1. Preserving confidentiality

When discussing confidentiality, we commonly think of using encryption techniques to prevent unauthorised viewing of actual data, clearly we want this to happen while data is in transit but we also need to consider data stored at the cloud provider. This raises a challenge: how can we manage keys in this environment? Clearly we don’t want to have the actual keys exposed at the provider together with the data, in the same way we want flexibility in how data can be accessed without having to go through a central gateway that recognises or knows all required keys – use of public key cryptography is not practical as each item would need to be encrypted with as many keys as users that require access to it.

A practical alternative is the use of tokenisation—essentially, replacing bits of data that are considered sensitive (e.g. credit card information, social security number) with a dummy token. The process of translating from token to real data can either be implemented at the client endpoint or by using a separate cloud provider. Tokenisation has been mooted as an alternative that avoids the key management concerns previously described but is not without its downsides:

- We are storing redundant data (mapping of token to real value)
- We still require a centralised point that performs this translation.

Another attractive concept is that of homomorphic encryption—which presents the possibility of being able to process encrypted data in the cloud, and have meaningful results provided by that processing without actually having to decrypt the data, therefore preserving confidentiality. Whilst holding great promise this is an on-going research area, that although developing quickly, is not yet considered to be practical enough for implementation in real world applications (Gentry, 2009) (Sadeghi et al., 2010).

A further encryption approach being considered for cloud computing is Digital Rights Management (also called Information Rights Management). This is particularly valuable in certain cases, such as dealing with unstructured data like of various types, where it may not be feasible to know in advance exactly which fields need to be tokenised. In these cases, Digital Rights Management is possible solution in that it has access policies that directly envelope the data itself and define who and how information containing within can be handled. However, although promising, Digital Rights Management is not yet a simple solution to implement particularly when involving multiple parties under different domains and effectively achieving interoperability between all (Koenen et al., 2004).

It is clear that more work is needed in these areas.

5.2.2. Data architectures

Further, cloud services can use Database Models different from the more familiar Relational Databases, which in itself makes it complex to understand and to deploy known models of data control used in more traditional systems. Commonly referred to as “NoSQL” databases (Leavit, 2010), these types of data storage are currently very young in their deployment and have primarily focused on usability with security functionality being fairly immature, in the authors’ opinion. However, this is an area where significant research is taking place and we expect developments to arise in the short to medium term (Roy et al., 2010) (Yuefa et al., 2009).

Whatever the data architecture it is also important to consider data on the client devices themselves, the major challenge being how much (or how little) the device can be trusted to store sensitive data—even transiently. A further analysis of the approaches being used or considered to protect device data and create trusted device enclaves is outside of the scope of this paper, but the challenges arguably also exist for non-cloud service architectures.

One last development we believe to be of interest, is the area of geo-affinity of data, that this, the ability to specify the data and processing can only take place in a specific geography (e.g. for legal or regulatory reasons) and be able to demonstrate that this is indeed the case. In this space, it is worth mentioning an on-going collaboration between Intel, VMware and RSA aims to deliver this capability by validating the actual boot process (attestation via TPM (Trusted Computing Group, 2011), validating geo-location and further report to a centralised console (in or out of the cloud) (Intel, RSA, Vmware, 2011).

5.3. Trust and assurance

The last challenge we would like to discuss is arguably the most important and covers the trust aspects of cloud service adoption. Essentially a large part of the concern arises due to the loss of control that comes with adoption of cloud-based services and we can break this concern into two main areas:

1 - Factors under control of service provider
2 - Factors external to the service provider.

5.3.1. Factors under control of service provider

As we progress through the typical the typical service stack of Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS), the level of abstraction perceived by cloud consumers increases—essentially, as users of cloud services we lose visibility of what is happening “under the hood” and the mechanisms available to cloud
users to secure information also become more limited. In true cloud services, because of multi-tenancy, there is also limited control over how resources are shared amongst multiple tenants and in the capabilities each may be given to monitor.

Service Providers therefore face the challenge of having to provide a sufficient assurance to cloud users that these abstractions are effectively managed and secured. Appropriate diligence has not only to be performed but also demonstrated. The current norm, is for providers to base themselves on perceived industry standards such as SAS70 or security specific certification, such as ISO27001 (Amazon, 2011) (Salesforce.com, 2011), as a way to demonstrate to adequacy of security provisions implemented.

It is well understood that providers are in most cases handling large numbers of customers running on the same underlying infrastructure and it is therefore not practical to facilitate traditional client audits or reviews that would give the expected level of assurance to each organisation consuming cloud services. However, as far as some clients are concerned, there is also a perception that transparency is lacking (Amazon Cloud Outage Highlights Need For Transparency, 2011) and regardless of being able to overcome the technical challenges we have already described, the matter of having sufficient trust to embrace cloud services in large scale is still an issue to be resolved.

In a study of assurance provided by cloud providers (Chakraborty et al., 2010), the authors performed a review of publicly available information, such as Service Level Agreements, policy statements and similar data to evaluate the level of Security, Privacy and business integrity provided by 25 cloud providers. The findings are generally important but a particular point to note is that large providers tend to base security claims purely on their size as an organisation. In another finding it was identified that IaaS and SaaS providers generally were more willing to make commitments from a security perspective.

In conclusion, the ability to demonstrate attainment of security related certification and audit by 3rd parties is helpful. However this is not sufficient to overcome concerns about trust. Overall there is a need for providers to be more clear and public in their provisions and guarantees in regard to information security. The Common Assurance Maturity Model (CAMM) (CAMM, 2011) is a consensus framework for assessment of information security maturity in third party organisations that could play a role here. Of interest, CAMM together with some well known lobby organisations in the security world such Cloud Security Alliance (CSA), ISACA and the Credit Card industry’s PCI have issued a joint positional paper discussing Assurance in the 21st century which describes the need for a common approach amongst the multitude of organisations providing guidance and frameworks for assurance (Business Assurance for the 21st Century, 2011).

5.3.2. Factors external to service provider

Whatever the views of the service provider client, legislation and regulatory concerns can also hinder the ability to adopt cloud services (Mowbray, 2009). The risk of having sensitive data accessed by the service provider (without the client being made aware) is always present and difficult to address without end users applying specific controls, such as data encryption. Assuming this is even architecturally feasible (as discussed earlier). Larger providers now have the capability to allow users to specify the specific geographies where data must be stored, however this only resolves part of this problem. Ultimately this is an issue that goes beyond the Information Security aspects of Cloud computing and requires legal judgement and assessment. It is a complex problem requiring an understanding of precisely what information is being placed with the cloud provider together with the possible impact of two dimensions of legal view; Firstly, that of the regulators and laws of the client country or country of the data subject and secondly, the legal regime of the cloud hoster. For example whether information disclosure by the hoster could be mandated or information potentially made unavailable due to a legal investigation in the country where the provider is based.

5.4. Ways forward

It is clear that a multitude of options are arising that aim to deal with the three key issues we set out to discuss in this section of our paper. In the majority of cases, the challenges do not lack solutions but are even likely have too many available – this in itself represents a challenge. Development of standards across all areas of cloud will likely drive the need for interoperability. However whether winning standards and services will be as a result of the simple selection of best of breed capabilities or through other commercial dynamics coming to play is far from certain.

In an interesting way, most of the challenges described are similar to what already happens where outsourcing has taken place in a large scale, so these problems and solutions are not necessarily new. We consider that the answer to some of the challenges described likely lies in the cloud itself and in leveraging services dedicated to managing identities, resolving key management and the on-going assurance of Cloud providers. Each of these challenges is on a scale that it is unlikely that a client organisation could do on its own. And therein lays the answer that whilst cloud computing may have brought to the front challenges; it will also be the part of the solution and allow a step change in security compared with what we had in pre-cloud world.

6. Conclusions

Cloud security is regularly cited as an inhibitor for the more rapid adoption of cloud services. We agree that the new cloud services architectures need careful security treatment, but the current situation of transition between internal and external security architectures has introduced many serious internal security challenges that are proving impossible to resolve with long-standing security approaches. We therefore argue that cloud services are themselves a potential security solution.

If all cloud security challenges are not solved is it worth migrating to cloud as a security solution? The authors would argue yes for two reasons; Firstly, the transition to deperimeterisation is already well in train and no reversal seems either possible or likely. A new architectural security response is therefore essential and overdue. Secondly, the cloud services security solutions are more technical in nature and
rely less on the good security behaviours of large numbers of end users. By any measure end user awareness and campaigns to influence security behaviours will only have a limited benefit, particularly against highly sophisticated social engineering (Herley, 2010).

We believe that investment in security for cloud services in the areas of assurance, identity management and data-centric security should become the focus of vendor effort. Undue attempts at patching the growing number of holes in the corporate network security perimeter will be of lesser value. Meanwhile, security and IT teams in end-user companies should significantly redesign their security architecture so as to be able to manage, and benefit from, the increased compartmentalisation introduced by the cloud computing paradigm.

REFERENCES


Amazon cloud outage highlights need for transparency [online] s. l. CRN; 2011.


Communications of the ACM.


Chakraborty R, Ramireddy S, Raghu TS, Rao HR. 4, s.l. The plight of the targeted attacker in a world of scale. s. l. CRN; 2011.


Leavit N. 2, s.l: Promise, will NoSQL database live up to their, Vol. 43. IEEE; February 2010. 12–14.


Mowbray M. 1, s.l: The fog over the grimen mire: cloud computing and the law, Vol. 6. HP; 2009. Scripted.


Paul Dorey is a Visiting Professor at Royal Holloway, University of London and Chairman Emeritus of the Institute of Information Security Professionals. He is a Director and Founder of the consultancy firms CSO Confidential and Security Faculty Ltd., which support public and private organisations in security strategy development and security team training and coaching. His security career of over 25 years includes security and risk leadership roles at BP, Barclays Bank and Morgan Grenfell/Deutsche Bank.

Armando Leite is a Senior Manager in KPMG UK, working with the Information Protection team. He has 12 years experience in designing, building and defeating various types of infrastructures and applications. Armando’s professional focus is on supporting his clients to leverage current and new technologies to maximum business advantage whilst adequately managing associated risks. Armando is a CISSP, CISA, CCSK and is currently pursuing an MSc in Information Security at Royal Holloway, University of London, UK.