Cloud Computing Storms

Stephen Biggs, Stilianos Vidalis
Information Operations Research Group, University of Wales, Newport, UK

Abstract

Cloud Computing (CC) is seeing many organisations experiencing the 'credit crunch', embracing the relatively low cost option of CC to ensure continued business viability and sustainability. The pay-as-you-go structure of the CC business model is typically suited to SME's who do not have the resources to completely fulfil their IT requirements. Private end users will also look to utilise the colossal pool of resources that CC offers in an attempt to provide mobile freedom of information. However, as with many opportunities that offer legitimate users enormous benefits, unscrupulous and criminal users will also look to use CC to exploit the loopholes that may exist within this new concept, design and business model. This paper will outline these loopholes and attempt to describe the perfect crime conducted within a cloud environment.

1. Introduction

Computer crime is a lucrative activity that continues to grow in its prevalence and frequency [1][2][3][4]. This statement is the reality behind any new technology, whereby legitimate users are compromised by those seeking to benefit in unscrupulous ways, usually, though not entirely, for financial gain. Rogers and Seigfried [4] suggest, 'the increase in criminal activity places a strain on law enforcement and government agencies.' Statistics suggest that over the past few years cyber-criminal activity has increased dramatically. More and more Law Enforcement agencies around the world are forced to adapt the techniques they employ, in order to be able to cope with the rapid change in the nature of the crimes they are charged with investigating. During 2009, the authors conducted a survey of the High Tech Crime Units (HTCU's) around the UK, with the results clearly indicating that the current practice of investigating cloud facilitated cyber-crime is outdated and fundamentally wrong.

The shift from document-based evidence to electronic-based evidence has necessitated a rapid change in the current practice, but that change on its own is not enough. Digital forensics and the many principles and guidelines by which digital forensic investigators throughout the world abide, can vary to some degree, though the underlying principles are very similar. The very backbone of the forensic community however, is being tested at present and the authors believe that the digital community and more importantly, the law enforcement agencies of the UK are not yet prepared for the potential rise in cloud facilitated cyber-crime. This concept is fuelling debate globally, with many UK Police chiefs ignoring the warnings. This is fundamentally wrong and could result in catastrophic consequences being felt locally, nationally and globally. The major developments in the world of computing in the last 5 years can only exacerbate the poor decision making processes of many high ranking law enforcement officers.

According to Gartner Consulting [5], 'investigating inappropriate or illegal activity may be impossible in cloud computing.' Gartner [5] warns: 'Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centres.' Heterogeneous large scale distributed virtual computing infrastructures therefore, to which the cloud environment belongs, is the focus of the research being conducted. If there are no contractual commitments to support specific forms of investigations then investigations and discovery requests are likely to be impossible.

Treacy and Bruening [6] state; 'Cloud Computing is not clearly defined.' This statement evidently relates to the many guises in which cloud computing can appear, with many vendors vying for a competitive market share that will ensure company growth and sustainability. The cloud model can vary somewhat between each of the many vendors that have identified a lucrative market, from which they want a sizeable share. Dastigr [7] suggests, most high profile vendors will provide a professional and safe cloud computing environment, however, many unscrupulous businesses and underworld providers may look to exploit the need for cloud services and offer cut price deals in order to attract business. The authors somewhat disagree with Dastigr, where the push by vendors for cloud customer supremacy, may outweigh the responsibilities vendors have as opposed to their profit margins. Evidence shows that law enforcement agencies in the UK, strongly believe that organised crime and other types of threat agents are already using heterogeneous large

scale distributed virtual computing infrastructures for conducting a wide variety of cyber-crimes.

The fear then is that obtaining artefacts of evidential value from such environments is virtually impossible.

This paper will describe what happens, how it happens and when it happens from the perspective of an investigator performing digital forensic investigations within the United Kingdom, based on the primary research conducted as part of the CLOIDIFIN research project [8]. The authors will also describe a perfect crime scenario, conducted in a by utilising cloud resources. A definition of cloud storms will be highlighted.

2. Digital Investigations

Digital investigators in the UK abide by the guidelines laid down by the 'Association of Chief Police Officers (ACPO) Good Practice Guide for Computer-Based Electronic Evidence' [9]. These guidelines provide information necessary to ensure investigations are performed to high exacting standards. Within those guidelines there are four key principles regarding computer based electronic evidence [9]. ACPO further states that: 'In order to comply with the principles of computer based electronic evidence, wherever practicable, an image should be made of the entire target device.' This however is becoming more and more impractical, where devices can now store many TB of data at very low cost. The ACPO advice here is: 'Partial or selective file copying may be considered as an alternative in certain circumstances e.g. when the amount of data to be imaged makes this impracticable.'

Digital evidence is, by its very nature, extremely fragile. It can be altered, damaged, or destroyed by improper handling or examination. For this reason it is imperative that precautions are taken to document, collect, preserve and examine evidence of this type. A failure here can render a case inadmissible in court, with many hours of investigation wasted as a result [9].

Vacca [10] states: 'Computer forensics is the principle of reconstructing the activities leading to an event and determining the answers to 'What did they do?' and 'How did they do it?' The many varying definitions however, all conclude that computer/digital/cyber-forensics is the science of proving what has happened previously, how it happened, where it happened and who made it happen.

Digital forensics has had to endure a continuous evolutionary process to maintain a level playing field with the perpetrators of cybercrime over recent years. That process must continue at pace to ensure that investigators are armed with the appropriate up-to-date tools and knowledge to continue their battle as newer and more complex ways of facilitating those crimes are created.

Traditional forensic methodologies permit the investigators to seize equipment and conduct their investigation from the relative security of a lab environment. This is known within the digital forensics field as 'dead analysis' and is still judged as the industry standard practice for the forensic investigator.

The tools used by an investigator can also vary, with each tool performing in similar ways, yet preferences can occur by the very nature in the way they perform tasks. The most common tools an investigator may use include: EnCase by Guidance Software [11], Forensic Tool Kit by Access Data [12] and $Helix_3$ [13] which is an open source tool kit. There are many others, though the three highlighted are the most commonly used and industry accepted tools [8]. These tools are extremely powerful and can locate artefacts of evidential value, even if the suspect has deleted the data that is considered compromising.

E-discovery and live forensics are two evolving areas of digital forensics that an investigator can add to their portfolio of weapons to combat e-crime. The term e-discovery carries many definitions, yet for the purposes of this paper, it is defined as: 'Electronic discovery (e-discovery or eDiscovery) refers to any process in which electronic data is sought, located, secured, with the intent of using it as evidence in a civil or criminal legal case.' E-discovery can be carried out offline on a particular computer or it can be performed on a network. EnCase have launched their own eDiscovery [11] suite and this is yet another powerful tool available to law enforcement agencies in their fight against cybercrime.

Live forensics is another method in the fight against cybercrime, which is the means and technique of obtaining artefacts of evidential value from a machine that is running at the time of analysis. This could prove pivotal in cases where evidence is obtained from the machines volatile Random Access Memory (RAM) for instance.

3. Cloud Computing

In recent years, desktop computing has traditionally seen users run copies of software programs on every computer they own and use. All of the files created by those software programs are stored on the local machine that created them or the network to which they are connected. If a computer is connected to a network, the other machines connected to that network can share those files, yet computers beyond that network will have no access to the data.

Cloud computing is software that runs not on PC's or company servers but instead on computers and

servers available on the Internet. The cloud offers private end-users and companies of all sizes a colossal pool of resources at remote locations without the need to invest in their own hardware and software infrastructure. Miller [14] states: 'Key to the definition of cloud computing is the "cloud" itself. For our purposes, the cloud is a large group of interconnected computers. These can be personal computers or network servers; they can be public or private.'

Although there has yet to be collaboration from the IT community on a specific definition for cloud computing, Menken [15] concurs: 'Cloud computing can be defined as the use of computer technology that harnesses the processing power of many inter-networked computers while concealing the structure behind it.' The cloud concept of virtualisation and remote access may prove to be a difficult paradigm for some users, yet the concept is seen by many as the next epochal technological milestone, in what has already seen rapid advances in computing since Gordon E. Moore made his prediction in an Electronics Magazine article: 'Cramming more components onto integrated circuits' in 1965. The data created by cloud applications are stored at many remote data centres worldwide. The companies at the forefront of this new cutting edge concept include, Amazon, Google, Salesforce, Yahoo and Microsoft. The vendors state that the data are secure and are backed up in the event of a catastrophic event at any of their data centre locations, therefore, appealing to the security conscious users within the digital information community.

Cloud computing therefore, offers users the ability to access their documents, , applications, images and movie files, from any device capable of connecting to the Internet, from virtually anywhere in the world. With this concept, the inevitability is that it will grow and grow, as users become more independent from their traditional desktop machines and require portability, coupled with the ability to share all their data resources with whomever, whenever and wherever they choose. The concept also allows business users to move away from the office space and perform their daily tasks at remote locations. With the advent of 3G, the third generation enabled network, offering cloud access from virtually any location in the world, facilitating that movement whilst maintaining an Internet connection to the data required for everyday tasks.

4. Cloud Computing Concerns

Service Level Agreements (SLA's) must be robust if they are to be effective in combating cybercrime. For example, hacking, distributed denial of service (DDOS) attacks, phishing, pharming, distribution of malware, viruses, trojans, spyware and worms will test the resilience of cloud vendors to rebuff such attacks and how they deal with the perpetrators of such crimes. SLA's also highlight that the promotion and facilitation of child pornography or other illegal activities will contravene policy and agreement and the law, yet policing such activity and making those cyber criminals culpable will also test the ways in which vendors monitor this type of activity.

The inevitability however, that with new technologies will come new ways of facilitating old crimes and/or the creation of new crimes is a sobering reality. Vendors must ensure that their agreements evolve at a suitable pace. They must also ensure that their policies do not just act as a smoke screen, policing the conditions laid down is imperative if the cloud is not going to become a harbour for the criminal underbelly that will look to exploit any weaknesses. Vendors must liaise with law enforcement agencies in an attempt to minimise the impact that cloud technology will have on vendor credibility and law enforcement involvement. The path ahead is uncharted and what happens may have significant consequences if the relationship is not sound.

It is believed that many of the vendors of cloud computing may not have fully encompassed the issues surrounding the usage of the cloud. The inevitability that unscrupulous users will identify and exploit any weaknesses that the cloud model possesses is a stark reality. Vendors, in their quest to secure a lucrative market share may have undermined the possibilities of attack and misuse of their cloud resources. The likelihood that the creation, storage, processing and distribution of illicit material will present major legal issues, is also a grave reality. The problems that will arise from cross-border legislation, due to the many locations of cloud data centres, coupled with the potential for data to be stored across those centres has the potential to impact significantly on the digital investigator and their ability to conduct effective investigations. The race to envelop that market share may be driven at a pace where critical issues are dealt with retrospectively and not given sufficient forward thinking throughout the development stage.

The biggest fear for many users of the cloud model is security. Presscott [16] questions: 'Why aren't enterprises falling over themselves to buy and use cloud services?' In the survey of over 170 businesses, more than 50% were concerned about the security issues surrounding the use of cloud resources. Many of the vendors claim to be investing huge sums to ensure data security both digitally and physically at their data centres. However, the old adage that nothing is 100% secure remains a real and possible threat to data integrity. The premise that risks can NOT be eliminated completely, yet can only be minimised to an

acceptable level is how users of cloud services must view their usage strategies.

Espiner [17] warns, 'Cloud-computing services are on the rise but the security around them is not yet mature enough to trust…' This appears to be a common thread among security experts, whereby they warn that insufficient investment and the desire by vendors to subscribe vast quantities of users into their cloud may hamper the security issues associated.

Mansfield-Devine [18] comments and questions: 'Cloud computing is hot, but are we running ahead of our ability to ensure a secure environment? If you are smart, you have invested significant resources in securing the perimeter of your organisation. You feel safe behind the firewalls, DMZ's, VPN's and fiercely enforced policies. Then along comes cloud computing and suddenly your users are keeping valuable and even business-critical data outside the perimeter, beyond your control…'

It is this concept of going against all security foundations of the recent past that cloud vendors are asking users to encompass and trust. John B. Horrigan [19] of the PEW Research Center, a non-profit "fact tank", in September 2008 conducted research titled 'Use of Cloud Computing Applications and Services'. Horrigan (2008) states that, 'Cloud computing takes hold as 69% of all internet users have either stored data online or used a web-based software application.' From this information, it can clearly be seen that the inevitable expansion and global acceptance of cloud services will pressurise further law enforcement agencies and investigators already inundated with huge workloads. The Confidentiality, Integrity and Availability (CIA) model of information security is going to be pushed to the ultimate test where cloud computing is concerned.

The questions posed by Hobson [20] raise major issues over 'Confidentiality'. When using cloud services, Hobson implies, and then asks: 'If you are giving your data to a third party, you have no control over it. So who have you given it to? What is the access to the data? Who sees it? Can it be taken and used by someone else? Who administers this? What assurance do you have that your data is confidential? Are you happy with a contractual warranty? If so, what is your recourse if the contract is breached?'

Hobson expands these questions to 'Integrity' and asks: 'Are you convinced as to the integrity of your data? Can it be tampered with? If it was tampered with, would you know? – Most people would not. Are you satisfied with the segregation of data? What is the chance of "leakage" and how is this protected and tested?'

He finalises his comments on the CIA model with 'Availability'. Hobson suggests that if your data is not available to you, for whatever reason, then it is rendered useless. What must be considered here is that in the United States, any data leakage or compromise of personal data, relevant authorities must be informed within a given timescale, even if the data was encrypted. This varies slightly from state to state, yet it is believed that this type of accountability will be encompassed in the future in the UK and possibly the rest of the EU. This imposes a requirement on the vendor to inform the user of the cloud resources of any compromise of data, yet the knowledge of that compromise lies solely with the cloud vendor, until such a time that the user is made aware.

One such security breach is currently being investigated. Rao [21] writes: 'The Electronic Privacy Information Center (EPIC) has asked the Federal Trade Commission to investigate the privacy and security measures of Gmail, Google Docs and Google's other "cloud computing" services for consumers.' Rao [21] highlights that a recent security breach at Google surrounding Google Docs is a stark reminder that putting consumers' data in the cloud, could have dire consequences. The sound resonating from the research to date is that the future is uncertain and what lies ahead with cloud security issues will be a topic for continued debate for some time to come.

A major issue from a legal perspective is one that may have been overlooked by both vendor and user. The legislation surrounding the location of digital data storage and its relation to the user location can leave users, vendors and investigators with issues of compliance and from an investigators point of view, serious cross-border red tape with which to deal with. Warwick Ashford [22], writing for Computer Weekly in December 2008 comments: 'Regulatory or legal requirements are often forgotten, and this can expose businesses using cloud computing to unnecessary risk says Andrew Scott, partner at law firm Dickinson Dees.' The Data Protection Act, for example, requires businesses to control the way personal data is processed and stored, but this is extremely difficult with cloud computing, says Scott. It is also unlikely that businesses will have any of the control they need over where the data is stored or have any real assurances that no data is left behind after the contract ends.

The 'European Directive on Data Protection' [23] which encompasses all the key issues of article 8 of the European Convention on human rights, has been reviewed by the Information Commissioners Office, who in 2008 called for a re-examination of the EU Directive, which will include promoting and supporting legislative change. The report suggests: 'In the 13 years since the Directive came into force, the world has seen dramatic changes in the way personal data is accessed, processed and used. At the same

time, the general public has become increasingly aware of the potential for their data to be abused.'

The major concern however, that UK law enforcement agencies will want to monitor closely, is the use of CC by paedophiles. Sadly, this type of crime accounts for between 70%-80% of an investigator's workload and the cloud could prove to be a haven that the paedophile may wish to exploit to fulfil his heinous needs. If data content is not monitored by cloud vendors, then this type of remote storage and relative anonymity of the cloud account holder, may further stretch law enforcement resources beyond breaking point. Couple this with the cross-border legislation and red tape that an investigator may encounter, many of these crimes will go unpunished if this is exploited by people fulfilling their needs by child exploitation. The authors believe it would be possible to conduct paedophile activities anonymously and without trace to the device accessing the images within the cloud.

5. Cloud Storms

Cloud storms can be defined as the issues that arise from the concerns raised in the previous section. The definition of storm offers several meanings, dependent on the scenario being referred to. The Oxford English Dictionary (2010) defines the term "storm" as: 'A violent disturbance of the atmosphere.' Or 'Move angrily or forcefully in a specified direction.'

A cloud storm therefore, can refer to the many ways in which perpetrators of cyber-crime can violently disturb the cloud model, methodologies, technologies and those charged with maintaining the equilibrium from a vendor point of view. Cloud storms will furthermore create tempestuous times ahead for law enforcement agencies and so too the courts responsible for hearing such criminal cases.

One must be mindful when utilising cloud resources; 'every silver lining has a cloud..!' This statement is the belief the authors hold in that the cloud does indeed have many benefits, yet the potential for the crimes listed below to have an adverse effect on the model, can only overshadow the benefits felt by legitimate users.

The authors believe, corroborated by the fears of the industrial partners associated with this research that paedophile activity, ID theft, fraud, malware and also insider intrusion will undoubtedly sharpen the edge that cyber-criminals currently enjoy over law enforcement agencies worldwide within a cloud environment.

Insider intrusion is a major threat to data held in the cloud, whereby the measures a cloud vendor takes when employing system technicians/administrators must rival that of those measures taken when employing airport staff. This alone is not enough however, when you consider that many breaches of security have unearthed flaws in airport security by media journalists posing as legitimate staff. What is to say that organised crime and/or the cyber-criminal off the street will not look to infiltrate cloud data farms in the hope that they can profit in some way from the compromise of this valuable commodity? This threat clearly identifies that no amount of security will provide a 100% secure environment. The authors believe that time will ultimately see cloud infrastructures, resources and physical domains being compromised by insider attacks, which are already prevalent in today's society and affect businesses adversely every year.

Malware will also generate an unsettled cloud front, with the identification by cyber-criminals of assets worth £billions collectively among vendors. These malicious software attacks will test continuously the resolve of the cloud administrators to rebuff the unwanted attention of this type of attack that will look to penetrate the security perimeters of these titanic data pools. Once compromised, vast quantities of personal data will become available to cyber-criminals, actively benefiting from the theft of the many personal identities gleaned from the cloud resource. These attacks will primarily occur, though not entirely for financial gain. A report by CNN earlier this year highlighted [24], 'In January, Google announced its web-based Gmail system had been compromised by a malware attack originating in China. As a result of the breach, Google announced it would stop censoring its Google.cn search engine and possibly end business operations in the country.' This compromise is proof that malware is already finding its way into the data centres of the major players of cloud resources and will almost certainly continue to cause many problems for vendors, customers and system administrators alike.

The potential compromises of the cloud listed above, ultimately culminate into many instances of identity (ID) theft. The theft of personal data sadly, is big business, with cyber-criminals looking at new ways of infiltrating colossal databases held by the many cloud vendors offering their flavour of online storage. Many vendors with data farms outside of the United States, are still not be required by law to inform customers or relevant authorities of any outages that occur, they can merely brush these instances under the proverbial carpet. The authors have posed direct questions to UK law enforcement officials with the reply that it is unlikely that the UK will follow the United States' lead in the notification of this type of critical outage to the relevant parties, certainly in the near future.

Another major concern of the authors and their industrial partners, is the rising scale of paedophile

activity across the Internet. Section 6 below will highlight this concern where hypothetical perfect crime scenarios are described. These scenarios are currently being tested as part of the ongoing research into cloud technologies and their impact on digital forensics and the detailed results will follow in subsequent papers.

The technical knowledge of the perpetrators of this heinous crime is becoming ever more advanced and the availability of this knowledge via portals such as YouTube etc. is but a mouse click away. The authors believe that technology, although may not be breeding new criminals, is most definitely facilitating new criminals. The Internet has seen a huge rise in individuals, who prior to the information superhighway phenomena, were once just curious about paedophilic activity, can now feed that desire in the comfort of, and in some cases, their family home. This can only add to the pressures felt by law enforcement agencies, who at present are only treading water and just managing to keep their heads above the surface. The frenzy of activity by paedophiles today, facilitated by cloud resources is like seagulls following a trawler, in the hope that defenceless pickings will present themselves and feed their heinous desires.

Where a warrant is served and a computer is running at that premises, according to ACPO guidelines, traditionally, unless a trained first responder is available, the machine is pulled at the electric plug to isolate it. This essentially destroys vast amounts of potential evidence in RAM and more pertinently, any connections to cloud instances will be lost. The need for trained first responders therefore, is acute and without these experts, artefacts of evidential value will have vanished. The authors consider, this scenario will also create stormy times for digital forensic investigators trying to piece together the jigsaws of crime that suspects are accused of.

Having a first responder on-site however, will only be the starting point. Obtaining data of evidential value from data centres will also present law enforcement agencies with a major tempestuous hurdle. The Mutual Legal Assistance Treaty (MLAT) is a costly way to obtain artefacts of evidential value from outside the local jurisdiction of a HTCU. The cost is not only financial but additionally the time and man hours it takes to obtain evidence via these diplomatic channels is extensive. The concern also lies with completeness and the possibility of contamination of the evidence. If evidential data is stored alongside innocent data on a cloud server, what measures are taken to ensure the image provided to law enforcement will only contain data associated with the suspect and that the evidence acquired is complete? Juries will have the arduous task of deciding whether or not there is reasonable doubt of cross-contamination in cloud related cases and it is the authors' belief, until case law can set precedent, that these cases will be very difficult process through the strict judicial system of England & Wales.

6. "The Perfect Crime"

With sombre crimes involving paedophilia hitting the news headlines more and more recently, the authors' concerns surrounding the use of cloud resources and services to facilitate these heinous crimes, has resulted in two hypothetical "The Perfect Crime" scenarios being considered.

Statistics prove that cyber-crime is augmenting and the impact of this has yet to be fully felt by law enforcement and society in general.

The perfect crime scenario suggested by the authors will encompass not only paedophilia, but also cloud facilitated fraud and identity theft. These crimes are currently testing the resolve and aptitude of all law enforcement agencies internationally.

With digitisation fuelling and facilitating crime, where previously for instance curious paedophiles may not have fulfilled their needs by accessing 'Indecent Images of Children', these individuals can now access those images with little risk of being caught. The birth of the cloud as we see it today, however, can now facilitate this crime and offer the perpetrator almost total anonymity. Law enforcement agencies in the UK and most likely the rest of the world are just not ready to tackle the scale of the potential problem that the cloud will create when it comes to detecting and bringing to justice cloud facilitated crimes.

The way in which the perfect crime could be committed involves the use of freely available cloned or stolen credit card details. The use of these details are utilised to buy two instances of cloud resources where the illegal images can be stored. If either of these are compromised and taken down, the other will act as back-up for the images being stored. To access these images, a third cloud instance running a virtual private network (VPN) is accessed by the user, which essentially would leave the cyber-criminal virtually undetectable. The images stored remotely, would then lower the risk of any evidence being found locally to almost zero. If the VPN is accessed via Internet cafes, libraries or even via one of the many open networks that exist in the UK, the perfect crime is a stark reality.

Open networks, iphone, the new ipad and other Internet ready media devices capable of accessing the Internet via wireless means, can only exacerbate the problem.

Another way the authors believe a perpetrator of paedophilic images can remain virtually undetectable and commit the perfect crime, is to utilise the freely available PortableApps suite to access their illegal images of children in the cloud. By doing so, the

authors consider that no artefacts of evidential value will be left on the local machine utilised to access these images and the only evidence to link the perpetrator to the images located in the cloud will be contained on the device that was used to store this application, such as a thumb drive.

The authors are currently in the process of testing these theories and will ultimately continue pressing for law enforcement involvement and the proactive policing of this potential crime wave.

7. Conclusions

Cloud computing is here to stay, yet the journey may take the model through some stormy waters. The concept will undoubtedly alleviate many issues for countless users, yet it will inevitably attract the unscrupulous like sharks to a feeding frenzy. How vendors deal with this and who they involve in the process will have significant impact on how those unscrupulous vultures are repelled.

The cloud model will continue to offer users state-of-the-art applications and infrastructures at affordable prices, with the level of support that can rival in-house IT services. Vendors will inevitably come and go and it will be imperative that users establish effective SLA's to ensure any of the vulnerabilities highlighted do not have a detrimental effect on their business or way of life in adverse situations. The vulnerabilities will surface in time, as they have done with all new technological milestones and it will be testament to those charged with dealing with those vulnerabilities that will ensure the effects are not catastrophic.

The authors believe that for a digital investigation of cloud related cyber-crimes to be effective and stand up to the rigorous and eagle eyed gaze of the judicial system in England and Wales, it must embrace and incorporate certain key changes. These changes must begin with the overhaul of International legislation that will police the boundaryless face of the Internet and the technology that is facilitated by it, cloud computing. If global unity is not embraced, the impact of cloud computing on digital forensics will be acute and the number of crimes that will go unpunished will be great. Cloud computing will undeniably help many businesses and individual private end-users to function in these uncertain economic times, yet the full impact that the cloud model will have on the digital forensic community is unknown. The Internet has shrunk the world in terms of communication and knowledge availability, it is therefore a recommendation of this paper that those small steps be taken by the respective governments to address the issue before it escalates out of control.

A recommendation that can be dealt with nationally within the UK, is the training and imparting of the relevant knowledge to those charged with policing and investigating cyber and cloud related crimes. During CLOIDIFIN the authors identified that few HTCU's are ready or will be ready in the near future to tackle investigations of cloud based crimes and that investment in resources, infrastructure and training is essential if the impact of the cloud model is not going to render HTCU's with cases that push them further towards the edge of failure.

Testing of a cloud resource has highlighted that SLA's and the terms and conditions agreements are ineffective if they are not implemented correctly. It is all well and good stating certain actions are against policy, yet if they are not policed suitably, they are rendered useless. The authors therefore recommend that vendors continue to ensure policies are written and evolved to prevent issues of non-compliance, yet urge the vendor to manage and instigate methods and procedures to police those that are in contravention of those policies.

This paper concludes that the full impact that cloud computing will have on law enforcement agencies and private cyber investigators will only be tested when cases are brought before the courts and sufficient case law is initiated to set the benchmark for this type of case. At present, law enforcement agencies are not in a favourable position to fight the battle against cloud facilitated cyber-crime and it is the belief that senior police officers and politicians are behaving like the proverbial ostrich, with their heads firmly planted into the sand in the hope the problem will inexplicably disappear.

International unity is also vital requisite if the cyber criminal is not going to prosper as a direct result of cloud resources and technology.

6. References

[1] CASEY, E. *Handbook of Computer Crime Investigation.* Academic Press. Boston. 2002

[2] KRUSE, W. & HEISER, J. C*omputer Forensics: Incident Response Essentials.* Addison Wesley. New York. 2002

[3] RICHARDSON, R. 2008. *CSI Computer Crime and Security Survey.* [WWW] http://www.gocsi.com/forms/csi_survey.jhtml (March/April 2009)

[4] ROGERS, M. K. & SEIGFRIED, K. The Future of Computer Forensics: A Needs Analysis Survey. *Computers & Security,* **Volume 23** (1), 2004. pp. 12-16.

[5] GARTNER. 2008. *Tough questions: Gartner tallies up seven cloud-computing security risks.* [WWW] http://www.mbtmag.com/article/CA6578305.html (September 2008 - April 2009)

[6] TREACY, B. & BRUENING, P. Cloud Computing – data protection concerns unwrapped. *Privacy and Data Protection PDP*, **Volume 9** (3), 2009. pp. 13.

[7] DASTIGR, F. Head of ICT Torfaen County Borough Council. 2nd April 2009. *Personal Communication.*

[8] BIGGS, S. J. *CLOIDIFIN Research Project.* University of Wales, Newport. 2009. (Vidalis, S – Project Supervisor)

[9] ACPO. 2007. *Association of Chief Police Officers – Good Practice Guide for Computer Based Electronic Evidence.* [WWW] http://www.acpo.police.uk/asp/policies/Data/ACPO%20Guidelines%20v18.pdf (September 2008 – April 2009)

[10] VACCA, J. R. *COMPUTER FORENSICS Computer Crime Scene Investigation.* 2nd edn. Charles River Media Inc. Hingham, Massachusetts. 2005.

[11] EnCase by Guidance Software. [WWW] http://www.guidancesoftware.com/default.aspx 2009

[12] Forensic Toolkit (FTK) by Access Data. [WWW] http://www.accessdata.com/downloads.html 2009

[13] Helix3 by e-fense. [WWW] http://www.e-fense.com/products.php 2009

[14] MILLER, M. *Cloud Computing – Web-Based Applications That Change the Way You Work and Collaborate Online.* United States of America. Que Publishing. 2008.

[15] MENKEN, I. *Cloud Computing – The Complete Cornerstone Guide to Cloud Computing Best Practices.* United States of America. Emereo Pty Ltd. 2008.

[16] PRESCOTT, M. 2009. *Internet Revolution – Cloud Control.* [WWW] http://www.internetevolution.com/document.asp?doc_id=170782&image_number=1 (February-April 2009)

[17] ESPINER, T. 2008. *Can business trust "immature" cloud computing? Not yet, warn experts.* [WWW] http://software.silicon.com/security/0,39024655,39362814,00.htm (January – April 2009)

[18] MANSFIELD-DEVINE, S. Danger in the clouds. *Network Security.* **Volume 2008** (12), pp. 9-11. 2008.

[19] HORRIGAN, J. B. 2008. *PEW INTERNET – Use of Cloud Computing Application and Services.* [WWW] http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Cloud.Memo.pdf.pdf (March/April 2009)

[20] HOBSON, D. 2009. *Global Secure Systems: Into the Cloud we go.....have we thought about security issues?* [WWW] http://www.globalsecuritymag.com/David-Hobson-Global-Secure-Systems,20090122,7110 (March/April 2009)

[21] RAO, L. 2009. *The Perils Of Cloud Computing: Privacy Group Wants To Take Your Gmail Away.* [WWW] http://www.techcrunch.com/2009/03/17/the-perils-of-cloud-computing-privacy-group-wants-to-take-your-gmail-away/ (April 2009)

[22] ASHFORD, W. Managing The Risks In The Cloud. *Computer Weekly.* Reed Business Information Ltd. Sutton, Surrey. pp. 8 2nd December 2008

[23] European Union Directive 1995 on Data Protection. Reviewed in 2009.

[24] FARRAR, L. 2010. *How safe is cloud computing?* [WWW] http://edition.cnn.com/2010/TECH/03/12/cloud.computing.security/index.html (March 2010)

