iS
CHANNEL

Joe Blogg's Hacking Supercomputer

A discussion on how the inexpensive and pervasive availability of Cloud Computing to the Common Man is forcing the metamorphosis of Information Systems Security

Abhishek A Sanyal
MSc Analysis, Design and Management of Information Systems (2010/11)
Information Systems and Innovation Group
Department of Management
London School of Economics and Political Science

KEYWORDS

Responsibility Modeling

Mechanism Cracking

Business Model for Information Security

Structures of Responsibility

ABSTRACT

The inexpensive and pervasive availability of Cloud Computing to the Common Man is leading to an increase in malicious attacks such as SIP Brute Force Attacks on Wireless Encrypted Networks, also widely known as Mechanism Cracking. In such attacks, the Common Man has the ability to harness the power of Cloud Computing equivalent to a Supercomputer, at a fraction of the cost and with added nefarious benefits. In this paper, the metamorphosis of the field of Information Systems Security (ISS) due to this specific type of cloud-based mechanism-compromising attack is explored. Siponen's proposed model built upon interactions amongst ISS research communities is taken as the Conceptual Model throughout the study undertaken in this paper so as to maintain a single theoretical lens even while making use of multi-dimensional views of the same problem. ISACA's Business Model for Information Security is utilized for Causal Analysis to arrive at potential causes, and Backhouse's Structures of Responsibility (as a part of Responsibility Modeling from Siponen's proposed model) is adopted as a specific ISS approach to explore potential Mitigating Measures. The paper is careful to only descriptively discuss potential causes and mitigations, and not concretely prescribe them. It is envisaged that the paper will give further impetus to research in the domain of ISS related to cloud-based mechanism-compromising attacks, especially in the area of people-centric ISS with a focus on the definition and interaction of roles and responsibilities of organizational actors.

INTRODUCTION

The paper starts off with a brief description of some relevant information security incidents and explores their importance to Information Systems Security (ISS). Progressing further on the same lines, the paper codifies these security incidents to represent unambiguously their validity to ISS. Keeping in view the importance of a conceptual model to look for "a theory which can support the multiple images of a problem and at the same time bring in consistence" (Backhouse et al, 1996) and "in order to review the vast literature in ISS through a conceptual framework that helps us not only to classify the works but also to trace their intellectual origins" (Dhillon et al, 2001), the paper makes use of a Conceptual Model put forward by Siponen (2005) as the generic lens for discussion. Focusing on the human element of ISS, and to maintain a combinatory approach between interpretivism and positivism, the paper elects to use Responsibility Modeling (Backhouse, 1996) as the specific angle for discussion of a people-centric ISS. The factors obtained from the Root Cause analysis of the problem statement being studied in this paper, identified primarily by using a prevalent industry-wide framework known as ISACA's Business Model for Information Security, are studied through the specific lens of Responsibility Modeling. As the focus of the Paper is on people-centric ISS, the Paper puts forward a dual analysis of the factors based on an application of Responsibility Modeling to Risk Analysis & Security Policy and Monitoring of IT Assets & Secure Service Provisioning. Interestingly, this analysis poses a conundrum involving questions related to a trade-off scenario between innovation and privacy, which provide further scope for research.

The Incidents and their Importance to Information Systems Security (ISS)

In an article that appeared on www.infoworld.com, "a German white-hat hacker named Thomas

Corresponding Author
Email Address: abhisheksanyal@alumni.lse.ac.uk (A.A. Sanyal)

Roth claimed that he had found a way to use Amazon's EC2 cloud and some custom software to crack the password of WPA-PSK-protected networks in around 20 minutes. With some tweaks to his software, which tests 400,000 passwords per second using the EC2 cloud's compute power, Roth said that he could reduce that cracking time to 06 minutes, about 1.68 USD worth of time on Amazon's EC2 cloud (Amazon's EC2 cloud is priced at 0.28 USD per minute for use of its services). GPU-assisted servers were previously available only in supercomputers and not to the public at large, according to Roth; that's changed with Amazon's EC2" (Samson, 2011).

Using Cloud Computing for hacking is increasing at a very fast pace as reported in an article on www.voiptechchat.com. "Complaints of rampant SIP Brute Force Attacks coming from servers with Amazon EC2 IP addresses are causing many administrators to simply drop all Amazon EC2 traffic" (Posner, 2010).

In an article on www.theregister.co.uk, David Campbell, a security consultant has sounded an ominous warning for the ISS community – "As it becomes possible now for the black-hat hacker community to get their hands on large amounts of computing power, we as security professionals are going to need to re-assess threat models that we thought previously were not a factor. Using stolen credit cards, they could create a Supercomputer that would be faster potentially than what the three-letter agencies have and they wouldn't be paying for the CPU cycles" (Goodin, 2009).

"The promise of Cloud Computing to eliminate the costs of deploying and maintaining large numbers of servers is no doubt a boon to businesses looking for inexpensive ways to tackle special computing chores. However, some who stand to benefit the most may not be the most savory of enterprises" (Goodin, 2009).

The series of events related to hacking by the use of Cloud Computing in an easily available and highly cost-effective mode represent the requirement for a metamorphosis in Information Systems Security (ISS). Such a metamorphosis of ISS is needed in order to address the issues raised by the access to and utilization of computing power akin to a Supercomputer for hacking by the common man (Joe Bloggs). This paper discusses this metamorphosis from the specific angle of Responsibility Modeling while maintaining a generic, single lens (i.e., a conceptual model) throughout the discussion.

Codification of the incident as a representation of its importance to ISS

In a special publication of the National Institute of Standards and Technology called "Guidelines on Security and Privacy in Public Cloud Computing" (Jansen et al, 2011), the incidents being cited by this paper have already been codified representing the importance of such incidents to ISS.

"As with any technology, Cloud Computing services can be turned towards improper or illicit activities. A couple of noteworthy instances have already occurred that give a sense of what might be expected in the future: (i) Botnets - In many ways, Botnets assembled and controlled by hackers are an early form of Cloud Computing. Cost reduction, dynamic provisioning, redundancy, security, and many other characteristics of Cloud Computing apply. Botnets have been used for sending spam, harvesting login credentials, and launching injection attacks against websites. Botnets could be used to launch a denial of service attack against the infrastructure of a cloud provider. The possibility that a cloud service could become infiltrated by a Botnet has already occurred; in 2009, a command-and-control node was discovered operating from within an IaaS-Cloud. Spammers have also purchased cloud services directly and launched phishing campaigns, ensnaring recipients with malware via social engineering techniques, and (ii) Mechanism Cracking - WiFi Protected Access (WPA) Cracker, a Cloud Computing service ostensibly for penetration testers, is an example of harnessing cloud resources on demand to determine the encrypted password used to protect a wireless network. With Cloud Computing, a task that would take five days to run on a single computer takes only 20 minutes to accomplish on a cluster of 400 virtual machines. Because cryptography is used widely in authentication, data confidentiality and integrity, and other security mechanisms, these mechanisms become, in effect, less effective with the availability of cryptographic key-cracking cloud services. Both cloud-based and traditional types of systems are possible targets. CAPTCHA cracking is another area where cloud services could be applied to bypass verification meant to thwart abusive use of Internet services by automated software" (Jansen et al, 2011).

This paper will focus only on the aspect of Mechanism Cracking i.e., using Cloud Computing to hack into the encrypted passwords used to protect wireless networks as it is pertinent to the incidents being cited in this paper. The other aspect involving the use of Cloud Computing for Botnets will not be discussed in this paper as it is not relevant to the incidents being cited in this paper.

THE GENERIC LENS FOR DISCUSSION

Requirement of a conceptual model

"As researchers, we are faced with a major question: what sort of conceptual approach do we need in security research? The answer is indeed not an easy one. Growing interest in security demands a broader perspective but concrete alternatives have not been provided. Problems are to be viewed in a multidimensional manner. What is needed is a theory which can support the multiple images of a problem and at the same time brings in consistency" (Backhouse et al, 1996).

"In order to review the vast literature in ISS, we need a conceptual framework that helps us not only to classify the works but also to trace their intellectual origins. It is important to understand the theoretical concepts that form the basis of methodological approach. Such understanding allows researchers to cut through the surface details that overlays different approaches and hence indicate the philosophical assumptions of the approaches" (Dhillon et al, 2001).

The model proposed by Siponen depicting the backgrounds and influences of different ISS approaches in terms of interaction amongst (i) Disciplines, (ii) Research Communities of ISS, and (iii) Modern ISS approaches provides such a conceptual model and therefore, has been taken as the Generic Lens for discussion in this paper (Siponen, 2005).

Description of the conceptual model

The model proposed by Siponen starts off from the IS/MIS Security community and takes an interpretivist approach at analyzing whether today's systems would be more resilient and secure from a survivability (Karya et al, 2001) or, viability (Hutchison et al, 2000) point of view. Inside the same research community and using the interpretivist approach, Siponen makes use of the angle of Security-modified Systems Development to look at the utility of methods such as (i) ISS Planning (Straub et al, 1998), (ii) Logical Control Specification (Baskerville, 1989), and (iii) ISS Spiral Model (Booysen et al, 1995).

Next, the model proposed by Siponen moves on to the discipline of Software Engineering and looks at ISS from the angle of Semantic Responsibility Analysis (Backhouse et al, 1996) while maintaining a combinatory approach between interpretivism and positivism. This angle lets Siponen explore the efficacy of ISS based on the people aspect and especially related to the importance of roles and responsibilities of organizational actors.

Should ISS be customized or localized in terms of business and information needs or, is there a need to have a standardized or, global ISS solution design and deployment? This is the question, which is probed by Siponen when he looks at two positivist modern ISS approaches coming from the research communities of Computer Security and Database Security viz. (i) Business Process Modelling (Rohm et al, 2000), and (ii) Information Modelling (Smith, 1989). As the last endogenous factor from the model proposed by Siponen, a positivist approach of Cryptology from the discipline of Mathematics is taken by Siponen to look at ISS. This angle allows him to evaluate whether it can be possible to achieve robust ISS on the basis of encryption algorithms alone?

THE SPECIFIC ANGLE FOR DISCUSSION

The Human Element of ISS

"Notable among the earlier work on Risk Analysis in ISS is Parker's Program (Parker, 1981), Fisher's Methodology (Fisher, 1984) and Warman's Framework (Warman, 1993). All three approaches use risk analysis as a means to design controls for ISS keeping in view the various threat categories but giving primacy to the social aspects in establishing security. Risk analysis prompted yet another stream of thought, espoused by Lane (Lane, 1985) that behaviour of people is a major and a central factor in security and should be the first factor to receive attention" (Backhouse et al, 1996). "Lane proposes that in an organization, staff with special responsibility should be designated. This, he feels, is an effective way of reducing risks in computer based systems. He also proposes the division of responsibility and the division of knowledge about the system amongst many personnel" (Backhouse et al, 1996).

It can be seen from the work done by Lane, Parker, Fisher and Warman that people are a major and central factor in ISS, and arguably, should be the first factor to receive attention. At this point, the paper anchors the notion of people-centric ISS, which is built further upon in the next section.

'Who Is Expected and Allowed To Do What'

"Information security is important in proportion to an organization's dependence on information technology. When an organization's information is exposed to risk, the use of information security technology is obviously appropriate. Current information security technology, however, deals with only a small fraction of the problem of information risk. In fact, the evidence increasingly suggests that information security technology does not reduce information risk very effectively" (Blakley et al, 2002). Blakley goes on to argue further that "we must reconsider our approach to information security from the ground up if we are to deal effectively with the problem of information risk" (Blakley et al, 2002).

"Where information risk is well enough understood and at least in broad terms stable, information security starts with policies. These policies describe 'who should be allowed to do what' to sensitive information" (Blakley et al, 2002).

Continuing further with the same line of reasoning as Blakley, it is obvious that organizational policies can only be defined as 'who is allowed to do what' if it is known that 'who is expected to do what', and this knowledge comes from modeling the importance of roles and responsibilities of organizational actors. At this point, the paper anchors the notion of business process modeling for ISS, which is built further upon in the next section in conjunction with the notion of people-centric ISS.

Responsibility Modeling

Synthesizing the notions of people-centric ISS and business process modeling for ISS, the paper chooses Responsibility Modeling as the specific angle / specific ISS approach for discussion. From the discipline of Software Engineering (in the proposed model by Siponen), Responsibility Modeling allows a specific angle of discussion while maintaining a combinatory approach between interpretivism and positivism.

The use of the specific angle of Responsibility Modeling in this paper will facilitate the discussion of the efficacy of ISS for Cloud Computing related malicious activities based on the people aspect and the importance of roles and responsibilities of organizational actors.

CAUSAL ANALYSIS OF JOE BLOGG'S HACKING SUPERCOMPUTER: A PERSPECTIVE FROM THE BUSINESS MODEL FOR INFORMATION SECURITY

The Information Systems Audit and Control Association (ISACA) proposes a Business Model for Information Security for Causal Analysis, which is made up of Preventive, Corrective and Detective Controls (ISACA, 2009).

"The Business Model for Information Security (BMIS) presents a holistic, dynamic solution for designing, implementing and managing information security. As an alternative to applying controls to apparent security symptoms in a cause-and-effect pattern, BMIS examines the entire enterprise system, allowing management to address the true source(s) of problems while maximising elements of the system that can most benefit the enterprise. By studying all factors that introduce uncertainty and correlating all factors for understanding actual organisational needs, BMIS complements any framework or, standard already in place. It will assist enterprises in effectively managing information risk to minimise threats and ensure confidentiality, integrity and availability of information assets while harnessing enterprise information assets to create value" (ISACA, 2009).

This paper will use ISACA's Business Model for Information Security to attempt a Causal Analysis of Joe Blogg's Hacking Supercomputer based on available information in the public domain only (Samson, 2011 ; Posner, 2010 and Goodin, 2009).

Failure of Preventive Controls

On one hand, Amazon has a Security Policy in place for the Cloud Computing services it offers to clients. However, the percolation and enforcement of the Security Policy may not be adequate as the series of incidents have shown in which Amazon personnel failed to show or, act according to any standard guidance. This representative behaviour by Amazon can also be extrapolated to the possibility of a weak Risk Analysis, which traditionally is supposed to underpin the Security Policy.

On the other hand, the organizations being affected by Joe Blogg's Hacking Supercomputer have also showed some of the inertia such as associated with personnel from Amazon: inability to act in a coherent manner, unavailable and inadequate guidance and a Risk Analysis that did not cater for such attacks.

This paper will consider inadequate Risk Analysis and weak enforcement and percolation of Security Policy as failure of Preventive Controls in the case of Joe Blogg's Hacking Supercomputer.

Failure of Detective Controls

Multiple incidents have shown over time that Amazon has failed to detect and act on suspiciously malicious activities being carried out through IT assets under direct management and control of Amazon itself. Granted that ownership of public IP addresses hosting the Amazon EC2 cloud change frequently but monitoring of use during the tenancy term by different tenants can still be carried out by Amazon by logging simple parameters such as: "(i) Source and Destination IPs, (ii) Destination Port and Protocol, (iii) Accurate Date, Time and Time Zone of malicious activity, and (iv) Intensity and frequency of malicious activity in appropriate logs" (Posner, 2010). Similar lacunae exist on the side of the victim organizations also as even when system administrators could detect the SIP Brute Force Attacks on their Wireless Encrypted Network, they could do so more in a post-mortem manner rather than in a proactive manner; an example of this is system administrators dropping traffic from all Amazon EC2 cloud IP addresses and recommending the same radical approach both upstream and downstream (Posner, 2010).

This paper will consider inadequate monitoring of IT assets for malicious activity as failure of Detective Controls in the case of Joe Blogg's Hacking Supercomputer.

Failure of Corrective Controls

Once the SIP Brute Force Attacks have taken place, Amazon was left stranded with poor customer relationship management and an inability to commit that such attacks would not take place from Amazon's infrastructure in the future. This attitude from Amazon has actually resulted in a conundrum for Amazon's clients represented by two sides: (i) "Although Amazon takes pains to ration resources it makes available to single customers, it was possible to get around such limitations using a single credit card. Presumably, it would be even easier to bypass those controls using hundreds or thousands of stolen credit cards, something that is trivial for criminals to get a hold of" (Goodin, 2009), and (ii) "what role should Amazon and other public-cloud service providers play in preventing customers from using their services to commit crimes? Clearly, these services are being exploited to commit crimes. Yet is it reasonable to expect a provider to scrutinize and monitor all of its customers' activities in a Big Brother-like manner, in the name of preventing potential crimes from being committed? Few customers would likely accept that sort of invasiveness" (Samson, 2011).

This paper will consider inability to commit to secure service provisioning as failure of Corrective Controls in the case of Joe Blogg's Hacking Supercomputer.

From the Causal Analysis, the paper identifies the primary causes of Joe Blogg's Supercomputer (for the sake of discussion in this paper) as: (i) Inadequate Risk Analysis and weakly enforced and percolated Security Policy, (ii) Inadequate monitoring of IT assets, and (iii) Inability to commit to secure service provisioning.

It is pertinent to note here that all the causes can be thought to be underpinned by weak people-centric ISS and inadequate mapping of expected business & security processes to actual roles and responsibilities of organizational actors. In such a scenario, Responsibility Modeling will facilitate further discussion on the Mitigating Measures for Joe Blogg's Hacking Supercomputer.

MITIGATING MEASURES FOR JOE BLOGG'S HACKING SUPERCOMPUTER: APPLICATION OF RESPONSIBILITY MODELING

Structures of Responsibility (Backhouse et al, 1996)

Brief Description

"In analysing organisations as patterns of behaviour, one very important aspect of social causality becomes evident: that is responsibility" (Backhouse et al, 1996). The framework proposed by Backhouse endeavours to analyze the various aspects related to responsibility, in the form of Structures of Responsibility.

"These structures provide a means to understand the manner in which responsible agents are identified; the formal and informal environments in which they exist; the influences they are subjected to; the range of conduct open to them; the manner in which they signify the occurrence of events; the communications they enter into and above all the underlying patterns of behaviour. The framework assumes reality to be the outcome of human interactions which generate shared norms and experiences. Through the responsible agents identified we can relate the norms, patterns of behaviour, and experiences to their referents, which are actions effected in the real world. In preparing a schema, it is important to identify the agents who determine what takes place, and what behaviour is realised. Every agent in the organisation under consideration has a determinate range of possible conduct. This range aggregates to the behaviours that are afforded by that environment. Having defined the enterprise in terms of patterns, of actions, of behaviours and of responsible agents, a semantic schema is prepared by arranging them in a sequence of existence dependency. In preparing a schema, it is important to identify the agents who determine what takes place, and what behaviour is realised. Every agent in the organisation under consideration has a determinate range of possible conduct. This range aggregates to the behaviours that are afforded by that environment" (Backhouse et al, 1996).

"Such dependency forms the fundamental principle in developing a semantic schema showing ontological dependencies and its representation takes the form of an Ontology Chart. An Ontology Chart represents the invariants in any domain as patterns of behaviour to be realised by agents acting therein. Those invariants on the right of the chart can only be realised when those on their left have been realised.

The chart is a way of modeling what behaviour can be realised in any domain, but where the restrictions are only existential and not given by rules or conventions. Each invariant pattern is shown as a node in the chart and the analysis task is to elicit for each node the responsible agents and the norms used by the organisation in practice when the patterns of actions represented are actually instantiated. Where a node has two antecedents, then both these must be realised if the invariant is to be realised. The chart is used to provide a very stable model for analysing the domain, since it contains little that will change over time. It is a useful platform from which we can study the norms and structure of an organisation. In most cases the responsible agents will make their decisions in the line with prevailing norms, rather than arbitrarily" (Backhouse et al, 1996).

Application – Risk Analysis and Security Policy

"The security functions of most organisations have formal mechanisms for designing and maintaining secure systems. Such approaches may suffice in cases where the norms are very strong, and it is relatively easy to identify responsible agents in a conventional manner. However, if the norms are not strong and the environment is informal, it can be quite difficult to attribute responsibility and identify key decision makers" (Backhouse et al, 1996).

For Risk Analysis, it is not only important to identify, evaluate and manage the risks an organization faces but also make sure that the people conducting the exercise are making use of formal mechanisms. In the scenario where formal mechanisms for Risk Analysis are being used, it is relatively easy to attribute responsibility and identify key people with discretionary powers, which in turn leads to better Risk Analysis. A practical manifestation of this phenomenon is the much required ability of a Risk Analysis to remain current with changes in the organizational landscape, which would not be possible if key decision makers could not be identified and responsibility could not be explicitly attributed. In the case of Amazon and the victim organizations, the organizational landscape has evolved to either provide or, use cloud-based services respectively but, their Risk Analysis has most probably lagged behind.

With Cloud Computing being considered as a disruptive innovation, it is only more necessary that organizations adopting Cloud Computing on either the buy-side or the sell-side keep their Risk Analysis contemporary.

The definition of a Security Policy generally takes off from where Risk Analysis concludes as a Security Policy can be seen as a representation of the Risk Analysis that is now being made public, at least to all employees of the organization, and has visible commitment and approval of the organization's top management. However, the enforcement and percolation effects of the Security Policy are a different story altogether. The enforcement of a Security Policy is easier in a situation where "norms are strong and it is relatively easy to identify responsible agents in a conventional manner" (Backhouse et al, 1996); The same situational context would also hold true for percolation of a Security Policy i.e., framing and deploying the low-level guidelines / standard operating procedures. In case the Risk Analysis (taken to be placed on the left hand side of an Ontology Chart) is inadequate, the Security Policy would be inadequate too (taken to be placed on the right hand side of an Ontology Chart) keeping in mind that an Ontology Chart is a semantic schema in which existence dependency is modelled in the form of organizational patterns. Following on, with a weak Security Policy, it is only natural that its enforcement and percolation would be weak too. In the case of Amazon and other victim organizations, the action of personnel responsible were characterized by a lack of coherence or, direction and therefore point towards a high probability having an underlying weak or, inadequate Security Policy.

Thus, for organizations on either side of cloud-based services, the definition, enforcement and percolation of a Security Policy is, perhaps arguably, of paramount importance.

Application – Monitoring of IT Assets and Secure Service Provisioning

"In identifying the responsible agents and capturing the norms associated with each action, we are in a position to understand the underlying repertoires of behaviour. By looking at the informal environment, the semantic schema is able to capture the structures in their cultural context. This enables the analyst to understand the object system better. In managing and developing information systems security in an organisation, such an approach can aid in illuminating concepts such as attribution of blame, responsibility, accountability and authority." (Backhouse et al, 1996).

One of the basic tenets of ISS, and also widely known as Detective / Monitoring Controls, is the requirement of monitoring IT infrastructure / IT assets underpinning IT services that are being either provided or, consumed. On the same lines, UK's Office of Government Commerce (OGC) also recommends monitoring and control of IT assets that underpin IT services from a security perspective in their publication: IT Infrastructure Library (ITIL). Continuing further on the same lines, USA's IT Governance Institute (ITGI) also recommends monitoring and control of IT assets as they believe that 'what cannot be measured, cannot be controlled'. Monitoring of IT assets gives an organization the ability to act proactively rather than conduct mitigation post-mortem. The paper considers an organization with an inadequate Risk Analysis and weak Security Policy as 'informal' in the context of ISS and so an Ontology Chart of the informal controls environment in an organization would place monitoring of IT assets on the left hand side while proactive action by the organization would be placed on the right hand side. It is easily discernible here, keeping in mind the existence dependency, that inadequate monitoring of IT assets underpinning IT services will lead to weak or, total lack of proactive actions from organizations. The paper also observes that the semantic schema of these responsibility structures points towards a cultural laxity, which in turn is a manifestation of inadequate Risk Analysis and Security Policy. For Amazon and other victim organizations, monitoring of IT assets was observed as an area lacking proper focus and therefore both parties could take action only in a post-mortem manner.

Hence, the requirement of monitoring of IT assets cannot be underscored further for organizations on either side of Cloud Computing.

Cloud Computing is neither the only nor the first innovation that has fallen prey to the conundrum of provisioning secure services but still not impinging on privacy. One of the most pertinent examples of this conundrum is illustrated by the problem faced by Banks in monitoring and taking action on Credit Card fraud: Banks can monitor and take action on 'suspicious activity' on Credit Cards only if the Bank has collected sufficient customer information related to spending behaviour to define 'normal activity'. The paper observes here that the best way to manoeuvre this conundrum is through a balancing act, which is not biased towards either side. As an illustration of this balancing act, the solution adopted by Banks on the ground can be explored further: On one hand, Banks collect information on spending behaviour and prepare a schema of 'normal activity' only by an opt-in feature that customers have to subscribe to in order for Banks to take proactive action on 'suspicious behaviour'; On the other hand, for customer who have not opted-in, Banks tend to adopt a de facto approach and set 'spend limits' per type of Credit Card beyond which all activity is considered suspicious and tackled accordingly.

A similar kind of conundrum is observed for Joe Blogg's Hacking Supercomputer: "Using stolen credit cards, they (i.e., hackers) could create a Supercomputer that would be faster potentially than what the three-letter agencies have and they wouldn't be paying for the CPU cycles" (Goodin, 2009). The paper notes here that this specific failure of Corrective Controls is manifested only on the sell-side of Cloud Computing and not on the buy-side i.e., providers of cloud-based services such as Amazon and not consumers of cloud-based services should be evaluating this Corrective Control. In the series of incidents mentioned in this paper, Amazon could have adopted a more people-centric ISS and monitored patterns in service payments (i.e., rents) correlated to patterns of service usage to identify abuse / use for malicious intent and still be able to take proactive action, rather than relying on building up patterns of consumer behaviour and relying on technological solutions for post-mortem action.

It is thus abundantly obvious that providers of cloud-based services have to explore secure provisioning of services as a part of not only their business model but also as an integral part of their ISS, and that the measures adopted would have to rely on people-centric ISS rather than technology in order to satisfy privacy requirements of consumers.

CONCLUSION

The use of Cloud Computing by hackers to simulate the computing power of a Supercomputer is definitely changing the way traditional ISS has been defined and maintained. Even though the solution to this new challenge to ISS will most probably come as an amalgamation from multiple ISS approaches, this paper only focussed on the study of underlying causes and potential mitigating measures from a people-centric ISS and Responsibility Modeling viewpoint. Such a perspective adopted in this paper enabled the contextually situated study of ISS for Mechanism Cracking, keeping the people aspect of ISS in the centre with a portrayal of its interaction with roles and responsibilities of organizational actors in the foreground through the ISS approach of Responsibility Modeling.

The paper made use of the Business Model for Information Security and identified (i) Inadequate Risk Analysis, and weakly enforced and percolated Security Policy, (ii) Inadequate monitoring of IT assets, and (iii) Inability to commit to secure service provisioning as the primary potential causes allowing the use of Cloud Computing for Mechanism Cracking.

Further study regarding potential mitigating measures was done through Structures of Responsibility (as a part of Responsibility Modeling). The paper benefitted from the use of an Ontology Chart to map organizational patterns and define situation specific potential mitigating measures, which were logical resultants from existence dependencies / ontological dependencies from the semantic schema. In short: (i) Contemporary Risk Analysis, (ii) Enforced and percolated Security Policy, and (iii) Monitoring of IT assets underpinning IT services (for proactive action), were taken as potential mitigating measures for both, buy-side and sell-side of Cloud Computing, while commitment to secure service provisioning (without impinging on privacy), was taken to be a potential mitigating measure for only the sell-side of Cloud Computing.

The paper will provide further impetus to research in the domain of ISS related to cloud-based mechanism-compromising attacks, especially in the area of people-centric ISS with a focus on the definition and interaction of roles and responsibilities of organizational actors. Such a focus is required in the metamorphosis of ISS in the face of Joe Blogg's Hacking Supercomputer as once again it has been proved that, arguably, the weakest link in security is most often the human.

REFERENCES

Backhouse, J. and Dhillon, G. (1996) Structures of Responsibility and Security of Information Systems. European Journal of Information Systems. 5(1) pp. 2-9.

Baskerville, R. (1989) Logical Controls Specification: An Approach to Information Systems Security. Systems Development for Human Progress. pp. 241–256.

Blakley, B., McDermott, E. and Geer, D. (2002) Information Security is Information Risk Management. NSPW '01. Cloudcroft, New Mexico, USA.

Booysen, H. and Eloff, J. (1995) A Methodology for the Development of Secure Application Systems. Proceedings of the 11th IFIP TC11 International Conference on Information Security.

Dhillon, G. and Backhouse, J. (2001) Current Directions in ISS Research: Towards Socio-organizational Perspectives. Information Systems Journal. 11 pp. 127-153.

Fisher, R. (1984) Information Systems Security. Englewood Cliffs, Prentice-Hall.

Goodin, D. (2009) Amazon's EC2 Brings New Might to Password Cracking. http://www.theregister.co.uk/2009/11/02/amazon_cloud_password_cracking/ (accessed 22 February 2011).

Hutchinson, W. and Warren, M. (2000) Using the Viable Systems Model to Develop an Understanding of Information System Security Threats to an Organisation. Proceedings of the 1st Australian Information Security Management Workshop.

ISACA (2009) An Introduction to the Business Model for Information Security. 2009 Edition. Chicago (Illinois), USA.

Jansen W. and Grance T. (2011) Guidelines on Security and Privacy in Public Cloud Computing. Draft NIST Special Publication. US Department of Commerce, National Institute of Standards and Technology (NIST), USA.

Karya, M., Kokolakis, S., and Kiountouzis, E. (2001) Redefining Information Systems Security: Viable Information Systems. Proceedings of the IFIP TC11 16th International Conference on Information Security (IFIP/SEC '01). June 11–13 Paris, France.

Lane, V. (1985) Security of Computer Based Information Systems. Macmillan, London.

Mao, W. and Gratch, J. (2006) Evaluating a Computational Model of Social Causality and Responsibility. 5th International Joint Conference on Autonomous Agents and Multi Agent Systems. Hokkaido, Japan.

Posner, F. Amazon's EC2 SIP Brute Force Attacks on the Rise. http://www.voiptechchat.com/voip/457/amazon-ec2-sip-brute-force-attacks-on-rise/ (accessed 22 February 2011).

Rohm, A. W. and Pernul, G. (2000) COPS: A Model and Infrastructure for Secure and Fair Electronic Markets. Decision Support Systems. 29(4) pp. 434–455.

Samson, T. Amazon's EC2 Enables Brute Force Attack. http://www.infoworld.com/t/data-security/amazon-ec2-enables-brute-force-attacks-the-cheap-447 (accessed 22 February 2011).

Siponen, M. (2005) Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods. Journal of Information and Organization. 15 pp. 339-375.

Smith, G. W. (1989) The Semantic Data Model for Security: Representing the Security Semantics of an Application. Proceedings of the 6th International Conference on Data Engineering.

Straub, D. W. and Welke, R. J. (1998) Coping with Systems Risk: Security Planning Models for Management Decision Making. MIS Quarterly. 22(4) pp. 441–464.

Warman, A. (1993) Computer Security Within Organizations. Macmillan, London.