A Conceptual Opportunity-based Framework to Mitigate the Insider Threat

Keshnee Padayachee
University of South Africa
Pretoria, South Africa
padayk@unisa.ac.za

***Abstract*—The aim of this paper is to provide a conceptual framework to mitigate the insider threat from an opportunity-based perspective. Although motive and opportunity are required to commit maleficence, this paper focuses on the concept of opportunity. Opportunity is more tangible than motive, hence it is more pragmatic to reflect on opportunity-reducing measures. Opportunity theories from the field of criminology are considered to this end. The derived framework highlights several areas of research and may assist organisations in designing controls that are situationally appropriate to mitigate insider threat. Current information security countermeasures are not designed from an opportunity-reducing perspective.**

Keywords—insider threat; rational choice theory; routine activities theory; situational crime prevention theory

I. INTRODUCTION

Based on the CyberSecurity Watch Survey [1], 46% of the respondents considered maleficence caused by insider attacks as more damaging than outsider attacks. An 'insider' is any individual who has legitimate access to an organisation's information technology (IT) infrastructure [2]. The insider threat involves more than a disgruntled employee; it may also include insiders who no longer work for the company but whose system credentials are still valid, or it may include a system developer who has in-depth knowledge of the system [3]. According to Chinchani et al. [4], several challenges are associated with the insider threat. They claim that security administrators consider the insider threat as unpreventable and that insiders have a higher success rate with maleficence as they are familiar with security controls. Furthermore, the authors specify that most tools are aimed at neutralising external threats. Examples of attacks include unauthorised extraction, duplication or exfiltration of data, tampering with data, deletion of critical assets, etc. [5]. The motivations of malicious insiders range from espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption and ignorance, to apathy [6]. According to Cornish and Clarke [7], both motivation and opportunity play a role in crime; however, opportunity may be the 'trigger' to committing a crime. In this paper, the principles of opportunity theory are employed to devise a framework for the purposes of mitigating the insider threat by considering various perspectives. This type of analysis assists in determining in which situations to activate interventions to redirect the insider threat to compliance.

Theoharidou et al. [8] assert that the insider threat issue may benefit from a 'pluralistic approach' that would be enriched by ideas from well-established criminology theories. Various theories attempt to understand why criminals commit crime. Some theories of crime have their basis in either sociology, psychology or biology. These theories often consider the motivations for crime. However, opportunity theories of crime focus on opportunities that have to be present in order for crime to occur. Motivations are difficult to analyse as they are based on human emotions. In contrast, it is easier to conceptualise opportunities and to develop strategies to minimise crime. Felson and Clarke [9] indicate that, unlike other factors that may be associated with crime, opportunity is the 'root cause' of all crime. It is evident that while one may have the motivation, there has to be an opportunity to commit the crime.

Four theories of crime embody the opportunity theory perspective, namely Rational Choice theory [10], Routine Activities theory [11], Crime Pattern theory [12] and more recently Situational Crime Prevention theory [13]. Rational Choice theory has been a dominant theory in economics. Becker [14] first identified the relationship between rational choices and crime. He postulated that some people are criminals not because 'their basic motivation differs from that of other persons, but because their benefits and cost differ'. Recently there has been a trend towards using the theory of Rational Choice to explain the insider threat (see [15] and [16]). While Rational Choice theory is focused on the individual, Routine Activities theory gives more attention to the larger society [9]. The latter theory is based on the convergence of three elements: motivated offenders, suitable targets, and the absence of capable guardians in time and space [11] to explain why crime occurs. Crime Pattern theory in turn is concerned with the spatial and temporal distribution of crime and seeks to detect 'patterns both in criminal events and for criminals that are scale independent' [12]. The premise is that crime is not random. Here the issue is 'to discover and prevent opportunities for crime in the daily commute and other patterns of movement of potential offenders' [17]. Situational Crime Prevention theory is based on Routine Activities and Rational Choice theories and asserts that the opportunities for crime should be reduced [7]. This theory has been applied to the insider threat by [18] and to general information security concerns by [19] and [20].

According to Willison [21], it is valuable for researchers to consider computer crimes in terms of criminology theories, as they are, after all, crimes. Theoharidou et al. [8] also assert that criminology theories would enrich the current arsenal of information security countermeasures that appear to be

derivatives of General Deterrence theory. According to Willison [21], Situational Crime Prevention and Rational Choice theories are highly appropriate to understanding insider threats. Willison [21] proposes that the techniques advocated by Situational Crime Prevention theory could reasonably be adopted by information security practitioners. However, it has been argued that the spatial and temporal elements of Crime Pattern and Routine Activities theories are difficult to apply in the cybercrime landscape (see [22] and [17]). This discrepancy provides a significant potential for further research within the cyber security domain and highlights a secondary aim of the framework, namely to identify research gaps between opportunity theories and their application to cybercrime

An effort is made in this study to derive a conceptual framework that may be used to develop controls to mitigate the insider threat and to identify areas of potential research. The rest of the paper is structured as follows: Section II presents related work on the current mechanisms deployed to manage the insider threat. The role of opportunity with regard to mitigating the insider threat is elaborated on in Section III. Section IV presents the opportunity-based framework and the paper concludes with Section V and possible future research opportunities.

II. Related Work

Mechanisms to undermine the insider threat include monitoring, detection, mitigation [23] and deterrence. For example, Data Loss Prevention (DLP) tools may be used to monitor data usage, to detect and mitigate insider threats [24]. Currently the countermeasures that deter the abuse of internal systems focus on four factors, namely awareness of security policies, monitoring, preventive software and training [25]. Monitoring alone is not sufficient for managing the insider threat. Monitoring captures the intent but not the motivation and it is difficult to identify patterns of misuse [3]. While deterrents mechanisms cannot provide insight into the actual act of insider threat [21]. A methodical review of technological tools available to minimise the insider threat may be found in Zeadally et al. [26].

Several researchers have advocated profiling to predict future threats (see [5], [27], [28] and [29]). An accurate profile of the insider threat may help to identify threats both prospectively and retrospectively [30]. However, as Hunker and Probst [3] claim, profiling has its drawbacks as it assumes that human behaviour is predictable. However profiling may be useful in an integrated approach. This approach was adopted by Salem and Stolfo [31] who suggested that profiling be combined with honeytokens (i.e. honeypots) in order to increase the coverage for suspicious insider activity.

Although intrusion detection systems have been deployed to manage the insider threat, these systems are typically designed for the external threat rather than the insider threat. According to Bowen et al. [23], intrusion detection mechanisms present a number of challenges ranging from false positives to difficulty in correctly identifying anomalous behaviour. Zeadally et al. [26] remark that intrusion detection systems may be ineffective if an insider leaves no traces behind because he/she has knowledge of how to disable the intrusion detection system [27].

Unlike intrusion detection systems, honeypots do not suffer from false positives as any interaction with a honeypot is bound to be illicit [32]. A number of studies have been conducted on using honeypots to detect and identify the insider threat (see [23] and [33]). For example, McGrew et al. [33] found that honeypots succeed in ‘sandboxing’ (i.e. containing) activities of an insider threat. However, according to Spitzner [32], honeypots have several disadvantages. There is a risk that an attacker may use a honeypot to harm other systems. Honeypots are only of value when an attacker interacts with them and they manage to capture actions related to this activity. Several legal [34] and ethical concerns [35] are also associated with deploying honeypots. In a way, the deployment of honeypots is an opportunity-based technique, as they provide an opportunity for an insider to commit maleficence. This notion is also supported by Kandias et al. [29], who used honeypots to determine if insiders exploited this opportunity. However the benefit of this technique is that maleficence is contained to the honeypot. Moreover honeypots may also act as a warning device for more serious maleficence as malicious activity in a honeypot may also indicate malicious activity elsewhere in the system.

Given the shortcomings associated with each technique, some researchers have considered an integrated approach. Brdiczka et al. [36] used profiling and anomaly detection to detect the insider threat. Salem and Stolfo [31] combined profiling and honeypots to reduce false positives. It is clear that managing the insider threat requires a wide-ranging approach and that no technique of its own accord is satisfactory. Some studies considered the opportunity dimension to create insider threat prediction tools (see [28] and [29]), in addition to attributes such as capability and motive. Theoharidou et al. [8] conducted an examination on ISO17799 (a standard for information security at the time) and its relationship to managing the insider threat. The authors considered several criminology theories that could be used to enhance the standard. They found that crime theories like Situational Crime Prevention theory were not contemplated in the standard as they did not consider the opportunity side of crime. This omission in the standard is an indication that the notion of opportunity requires further exploration.

III. Understanding the Insider Threat from an Opportunity Theory Perspective

When considering the insider threat as a crime of opportunity, it is practical to reflect on the ten principles of opportunity theory as proposed by Felson and Clarke [9]. This may lead to a better understanding of the insider threat and pave the way for the development of effective information security controls. Each of the subsequent subsections corresponds with a principle from Felson and Clark [9].

A. Opportunity plays a role in causing all crime

This implies that an insider has to be given the opportunity to commit an offense. The property of ‘opportunity’ was considered previously by Kandias et al. [29] with regard to

predicting insider threat. Their model viewed opportunity as a function of change of work behaviour, the system role of the insider (i.e. novice, advanced, administrator) and honeypot use. Other factors such as personality are difficult to use as predictors of crime [9].

B. *Crime opportunities are highly specific*

Reducing crime opportunities for insiders will have little impact on the outsider; hence strategies should be different for each type of attacker [9]. This may be the reason why intrusion detection systems are not effective to contain the insider risk, as the insider has knowledge of how to circumvent the system. Furthermore, outsiders and insiders use different paths or approaches to attack systems [37]. Gardiner [38] distinguished between insiders and outsiders in terms of capability, opportunity and motive. The required capability for an insider to commit a crime is low as compared to an outsider, because the opportunity for an attack is greater for the insider than for the outsider. While the insider's motive is more personal than random [38]. The current research focuses on opportunity, which appears to be a greater likelihood for the insider than for the outsider.

Wood [39] described the attributes of an insider threat as access, knowledge, privileges, skill, risk, tactics, motivation and process. An insider has 'unfettered' access to parts of a system and he/she may even have privileged access. A highly privileged user may know that there are decoys in the system and will attempt to disable them [40]. An insider's tactics are based on his/her goals, and the process describes the stages that lead the insider to commit maleficence. The process ranges from the intrinsic motivation of the insider, to identifying a target, to planning and finally launching the attack [39]. The propensity for risk and the motivation factors are intrinsic to the insider. The knowledge and skills factors are related to the particular insider's capability. It is clear that insiders require the knowledge and skills to commit maleficence. However, an insider's privileges and access rights may further embolden him/her to consider crime. For example, an insider who has access rights to confidential information has a greater opportunity to commit crime. Hence controlling the granularity of access may be an opportunity-reducing measure.

C. *Crime opportunities are concentrated in time and space*

According to Crime Pattern theory, crime opportunities are not equitably distributed in time and space, in other words, they are 'clustered' [12]. For example, an insider may prefer to commit an offense after office/business hours when the transgression is assumed to be less conspicuous. There are elements in crime that are 'crime generators', 'crime attractors' and 'crime detractors' [12]. For example, some locations are *hotspots* for crime – known as crime generators and crime attractors [41]. Crime generators provide many opportunities for crime, while crime attractors are locations where offenders seek out victims in a premeditated way [41]. Crime generators are locations where large numbers of people are assembled, such as a shopping mall. Crime attractors are for instance, neighbourhoods where criminals seek out known opportunities for crime [41]. Understanding these concepts in the virtual context may be the key to minimising the insider threat. For example, a crime detractor may consist of deterrent controls. Crime attractors and crime generators may be contained by using honeypots to deflect the insider.

D. *Crime opportunities depend on everyday movements of activity*

According to Crime Pattern theory, offenders follow a spatial-temporal movement pattern in their daily life [12]. Criminals are likely to commit initial crimes near these learned paths or activity nodes. The nodes include activities around the home, work, shopping and entertainment spaces, known as the activity space of the criminal [12]. It is possible to consider the personal, recreational and work activities that the insider performs online and to formulate a virtual triangle. This triangle could consist of social networking sites, online recreational activities and the organisation's intranet.

Firstly, the social networking node represents the personal node. Molok et al. [42] maintain that social networking has caused damages to organisations due to the leakage of information by their employees on these types of platforms. For example, a disgruntled employee may disclose proprietary information about his/her employers on a social networking site. This new platform adds an entirely new dimension to the insider threat problem. Nuha and Molok [43] found that insiders are responsible for disseminating work-related information on social networking sites such as Facebook, which poses a threat to an organisation's information security. A second important node to be wary of is online recreational activities such as online gambling. Exploring this node, Molok et al. [42] argue that an insider who is gambling may have financial problems and may easily be influenced online to divulge confidential information in exchange for money. Thirdly, the organisational intranet represents the work node. Understanding the 'nodes' or activity spaces along which an insider conducts work, recreation and personal activities in the virtual context may be key to discovering insider maleficence. This notion is based on Crime Pattern theory.

E. *One crime produces opportunities for another*

Felson and Clarke [9] indicate that a major crime can result in other smaller crimes being committed and vice versa. 'In sum, the most opportune targets at the outset become even more opportune after they have been first victimized', hence deterrents that 'prevent crime also have best chance to succeed when focused on these cases' [9]. Consequently a single act of insider maleficence may be the key to discovering further acts of maleficence and serve to provide timely interventions. Hunker and Probst [3] suggest using optimistic access controls as these allow the insider attacks to continue unhindered while evidence is gathered, and to contain the effects in a honeypot. The Optimistic Access Control with Usage Control model, designated the OAC(UCON) by Padayachee [44], may be a useful technique to this end.

F. *Some products offer more tempting crime opportunities*

The properties of Value, Inertia, Visibility, Accessibility (VIVA), based on Routine Activities theory, provide a point for evaluating objects that are suitable targets [11]. Objects that have high value, low inertia and high visibility and are easily

accessible are more attractive to criminals [9]. These properties may therefore be useful in designing containment controls such as honeypots and have to be considered to create an effective luring honeypot to contain the insider threat. In a typical crime scenario, low inertia refers to an object that is transportable [9]. In the cyberspace context, Yar [22] indicates that the inertia property may be related to the volume of data and the frustration caused by downloading large volumes of data.

G. Social and technological changes produce new crime opportunities

The notion that a product goes through a life cycle applies here. The life cycle consists of: innovation, growth, mass marketing and saturation [9]. (Note that this not related to the software engineering life cycle.) Felson and Clarke [9] assert that a consumer product at the innovation stage is not attractive to criminals as it is still difficult to use. A product in the growth stage is more appealing as the product is more user-friendly. In the mass marketing stage, the demand increases. At saturation stage the product is again not very attractive, as the demand for the product is now low. Reducing the life cycle to the core, it is clear that innovation is a precursory 'crime attractor'. The intellectual property of a product at innovative stages is highly valuable. Yar [22] describes the value property of VIVA as being related to intellectual property issues. However, once the product is marketed, this value erodes.

H. Opportunities for crime can be reduced

Whereas Rational Choice, Routine Activities and Crime Pattern theories consider opportunity as a factor, Situational Crime Prevention theory is directly concerned with opportunity-reducing techniques. Beebe and Roa [19] employed Situational Crime Prevention theory to evaluate the effectiveness of information system security controls. These authors considered sixteen of the twenty-five techniques in Situational Crime Prevention theory and linked each technique to existing information security controls. Willison and Siponen [18] considered the insider threat from a situational crime prevention stance to define crime scripts.

Situational Crime Prevention theory considers five categories of opportunity-reducing measures. Each measure is further divided into specific techniques [7]. Some of the techniques are given 'digital analogies' derived from Beebe and Roa [19], which are listed in brackets next to the corresponding technique:

- 'Increase the effort' includes target hardening (firewalls), control of access to facilities (authentication), screen exits$^{\alpha}$, deflecting offenders (honeypots), controlling tools/weapons (masking IP addresses)
- 'Increase the risks' includes extending guardianship (intrusion detection systems$^{\beta}$), assisting natural surveillance (visualisation tools), reducing anonymity$^{\alpha}$, utilising place managers (reporting policies$^{\beta}$), strengthening formal surveillance (auditing and logging reviews)
- 'Reduce the rewards' includes concealing targets (minimising reconnaissance information$^{\beta}$), removing targets (information and hardware segregation), identifying property (watermarking), disrupting markets$^{\alpha}$, denying benefits (encryption)
- 'Reduce provocations' includes reducing frustrations and stress$^{\alpha}$, avoiding disputes$^{\alpha}$, reducing emotional arousal$^{\alpha}$, neutralising peer pressure$^{\alpha}$, discouraging imitation$^{\alpha}$
- 'Remove excuses' includes setting rules (user agreements), posting instructions$^{\alpha}$, alerting conscience (code of ethics), assisting compliance (hacker challenges), controlling drugs and alcohol (cyber ethics training)

Since Beebe and Roa's [19] derivation was based on an earlier model of Clarke [13], some of the physical techniques do not have corresponding digital analogies. Some of the categories in the older model have been replaced by newer techniques. Elements marked with β (beta) indicate that they have been transposed from Beebe and Roa's [19] analogy. For example: 'extend guardianship' may be associated with 'intrusion detection systems'; 'utilise place managers' may be associated with 'reporting policies'; 'conceal targets' may be associated with 'minimising reconnaissance information'. The 'reduce provocations' category which was not considered by Beebe and Roa [19] hence does not have any corresponding digital techniques − indicated by α (alpha). The 'reduce provocations' category considers the emotional side of crime [7]. This category appears to be linked to motivation however provocations do not motivate a criminal, they are triggers or precipitators to an individual that is already motivated [7]. The issue of precipitators is largely an overlooked area of information security. Wortley [45] describes several types of situations that precipitate maladaptive behaviour. Some of these conditions correlate with the virtual world include: frustrations caused by failures of equipment and services, and invasion of privacy. Organisations need to be mindful of these types of conditions as by reducing provocations, insiders be less likely to engage in crime. Provocations may also be reduced by improved security usability. According to Whitten and Tygar [46], security software is usable if the end-users are successfully able to perform security tasks and if they are comfortable with the interface. The last category of 'removing excuses' is a significant area for opportunity reduction because 'if offenders can be prevented from rationalising and excusing their criminal actions in specific settings, they will be open to feelings of guilt and shame' [21] – thus potentially preventing them from committing further crime.

It is evident that the analogies are purely from a technical information security control perspective however it may be prudent in future research to consider the management perspective of information security. This could involve reviewing information security standards.

I. Reducing opportunities does not usually displace crime

Desistance implies either an end to all maleficence activity or displacement (i.e. another type of crime) [10]. According to Laub and Sampson [47] there is no clear definition of

desistance. However for purposes of this research the definition by Shover [48] is assumed: desistance is defined as the 'voluntary termination of serious criminal participation'. Rational Choice theory predicts that a criminal will only displace a prevented crime when the benefits exceed the costs – hence displacement is a threat to prevention [9]. It is crucial to recognise that a prevention or deterrent strategy may result merely in maleficence being displaced to another type of cybercrime.

J. *Focused opportunity reduction can produce wider declines in crime*

A crime prevention method may provide the added benefit of diffusion [9]. There is a hypothesis that an individual that is deterred from committing a crime in one circumstance assumes that the deterrence mechanism applies to other circumstances as well. This phenomenon is known as diffusion of benefits [9]. For example, the University of Surrey owned three car parks where cameras were set up in one car park. This intervention reduced crime in the other car parks too, even though there was no surveillance at the other car parks [9].This may occur when an insider assumes that the deterrent or prevention controls in one component of a system may be applicable to other components as well.

IV. THE FRAMEWORK

The principles discussed in Section III are dichotomized into two dimensions (see Fig. 1). The *opportunity-reducing* dimension represents the opportunity-minimising measures and effects (i.e. *opportunity-reducing efforts* and *opportunity-reducing effects). Opportunity-reducing effects* consider those properties that result from the *opportunity-reducing efforts* for crime. The *opportunity-inducing* dimension considers the context that induces crime. This dimension includes the activity space that emerges from the triangulation of *Social Networks*, the *Intranet* and *Online Recreation* nodes and the *hotspots* in this activity space. The hotspots represent crime attractors and crime generators.

A. *The Opportunity-Reducing Dimension*

An *opportunity-reducing effort* considers those efforts that may reduce crime by minimising associated opportunities. *Opportunity-reducing effort* measures consist of Situational Crime Prevention techniques and Routine Activities measures that intersect with one another to some extent. Situational Crime Prevention techniques include increasing the effort of crime, increasing the risks, reducing rewards and provocations, and removing excuses for crime.

As described in Section III, each category of opportunity-reducing techniques is divided into specific techniques. In some facets, it is easy to parallel Situational Crime Prevention techniques with information security countermeasures. However, other techniques do not have obvious equivalents with cyberspace, for instance 'disrupt markets', which appears to be out of the domain of cyberspace. This type of application of the theory demonstrates a fatal flaw in directly transposing a criminal theory to cyberspace and requires one to account for the differing contexts. The basic premise of the framework is that opportunity reducing measures needs to be mapped to the virtual space, instead of 'forcing' an unnatural relationship. Hence this framework reverts to the basic idea of opportunity as precursor to crime. Revisiting the issue in terms of the insider threat (similar to [20]), the framework focuses on the macro-level. Beebe and Roa [19] claim that the majority of security interventions increase the perceived effort, while limited controls increase the perceived risk and reduce the anticipated rewards. As there are even fewer controls that actually remove the insider's excuse for maleficence, this is an area of future research. Reducing the provocations for the insider threat consequently constitutes an entirely new area of research.

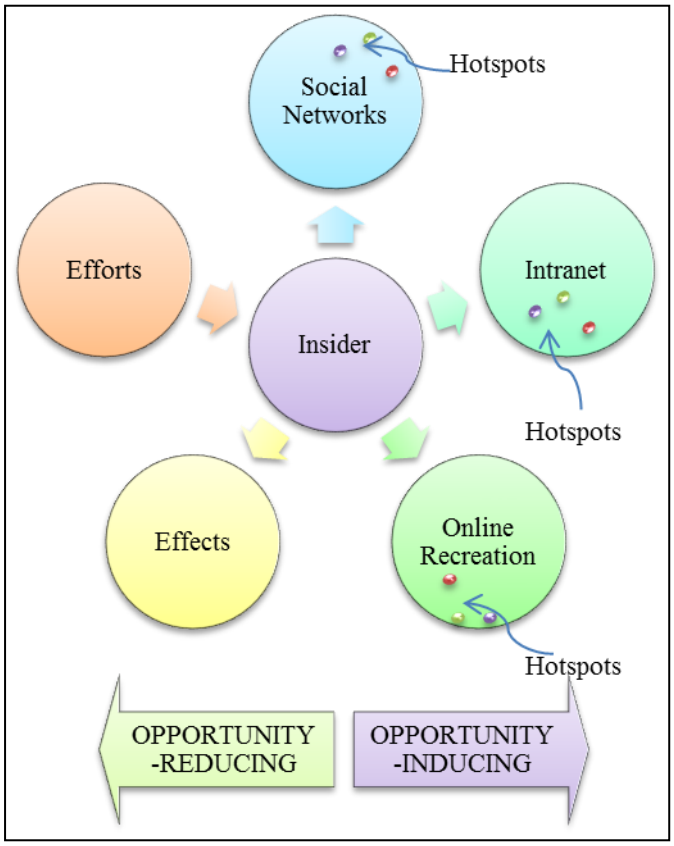

Fig. 1. *An Opportunity-based Framework to mitigate the Insider Threat*

Beebe and Roa [19] argue that lowering the perceived net benefit gained by cybercriminals from crime may deter them from committing the crime. Nonetheless, in their opinion typical deterrents like punishments are inadequate. They believe that the answer may lie in considering deterrents that do not only magnify the perceived effort required and inflate the perceived risk of being caught, but also decrease anticipated rewards. Cusson [49] argues that Deterrence theory may be made more powerful by considering the situational crime prevention perspective. (This is yet another area of further research.) General Deterrence theory has its roots in Rational Choice theory. Deterrence theory is moderated by certainty of detection, severity of punishment and the celerity of detection [50]. From an information system security

context, 'deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures' [51]. Typically organizations rely on anti-virus systems and password protection schemes [52] as deterrents. Deterrence theory focuses more on the cost of the crime, while Rational Choice theory considers both the cost and the benefits of the crime [53]. Furthermore, according to Cusson [49], Deterrence and Situational Crime Prevention theories have two commonalities. Both theories assume that the offender is a rational actor and that fear is induced by increasing the risks associated with the offense.

Situational Crime Prevention currently considers the technique of 'extending guardianship' – one of the 25 techniques, which is borrowed from Routine Activities theory. However, Situational Crime Prevention may be further strengthened from the perspective of Routine Activities theory, which would involve decreasing the suitability of targets and reducing the offender population. Decreasing the suitability of targets involves considering the VIVA properties. This could involve identifying those information assets that are of high value and addressing their visibility, access and level of inertia, in other words, identifying *hotspots* from the *Opportunity-inducing* dimension. Reducing the offender population could be achieved through profiling which is effective in an integrated approach. Yar's [22] examination of Routine Activities theory found that the core concepts of the theory are to some degree 'transposable' to crimes in virtual environments. However this examination clearly warns that criminology theories cannot be applied without considering the uniqueness of the virtual world. The framework derived here is the first step towards identifying areas that require new techniques to counter the insider threat. In terms of *opportunity-reducing efforts*, organisations should ensure that information security techniques cover all elements so as to truly mitigate the insider threat.

Organisations need to take cognisance of the fact that a crime prevention strategy may result in *desistance* or *diffusion*, which represent the dimension of *opportunity-reducing effects*. *Diffusion* is a benefit of prevention strategies, as the insider assumes that the entire system is rigged with deterrents and prevention strategies. Hence diffusion itself is an opportunity-reducing technique. This presents another area of future research, namely how to maximise the benefits of diffusion in the cyberspace to undermine the insider threat. *Desistance* implies *displacement* or the end of all maleficence. The latter is best possible outcome, as it implies that even though the insider may have had the opportunity to commit a crime, he/she desisted due to the prevention strategies. In a worst-case scenario *displacement* is chosen, in other words if the insider does not view an opportunity in one area, he/she simply chooses another avenue. For example, if the insider does not see an opportunity to commit a crime on the organisation's intranet, he/she may choose an easier option such as a social networking site. For this reason organisations should have appropriate contingency plans in place.

B. The Opportunity-Inducing Dimension

The elements of the *opportunity-inducing* dimension are interconnected. The activity space (*Social Networks, Intranet, Online Recreation* nodes) intersects with the target space (the *hotspots),* which is where crime occurs. To understand this relationship, consider each node. The *Intranet node* represents an organisation's IT infrastructure. In this context, an example of a *hotspot* could be the creation of innovative products, which is a crime attractor. The *Social Network* node represents insiders' social networking activities, therefore a *hotspot* could be an outsider who tempts the insider to reveal confidential data. The *Online Recreation* node represents activities such as online games. A *hotspot* could in this case be an outsider who takes advantage of an insider who is vulnerable. These are the nodes along which the insider operates. The identification of potential targets requires much research, given the ubiquitous nature of social networking in recent years. Social Networks actually constitute an example of a *hotspot* that is a crime generator.

The *opportunity-inducing* dimension considers those contextual factors that provide an opportune gateway to commit crime. Designing controls that consider an insider's pathways may be a way of containing the insider threat. Organisations should delineate activity spaces as areas of information security weakness, to identify *hotspots*. Though it may not be possible to minimise all *hotspots,* having awareness of these properties and setting up contingency controls and policies in terms of these properties may be the key to containing the damage leveraged by the insider threat. The proposed framework clearly highlights several areas of potential research. Hartel et al. [17] also emphasized the gap between opportunity theories and their application to cybercrime, and point out that there is a potential for multidisciplinary research.

C. Potential Research Opportunities

In terms of research opportunities that were revealed by the framework, there is firstly a need to revisit Situational Crime Prevention techniques from a purely cyber security perspective, rather than constraining the current theory intended for the physical landscape to cyberspace. Secondly, it would be prudent to revisit Deterrence theory from a Situational Crime Prevention perspective. Thirdly, as crime theories like Pattern theory and Routine Activities theory are based on time and space, more research is required to determine how to re-conceptualize *hotspots* in the physical domain to cyberspace. The framework derived here makes a first attempt at understanding the spatial context of computer crime by considering the virtual activity spaces of insiders relative to the notion of *hotspots*. Fourthly, the concept of social networking elevates the concept of the insider threat to a different dimension, and this constitutes a significant area of research.

V. CONCLUSION

This research makes two contributions. Firstly, the framework derived here may be used as a proactive mitigation strategy – it seeks to conceptualise the property of opportunity in terms of the insider threat. The derived framework may be used to design information security controls that would empower administrators to prevent and possibly counteract the insider threat. Future research will involve evaluating the

conceptual framework that was derived from opportunity-based criminology theories.

Secondly, in the process of deriving the framework, several areas of potential research were revealed, which is a major contribution of this paper. As discussed in Sections III and IV, the current set of information security techniques is inadequate for insider threats. Since these techniques were not developed taking opportunity-reducing considerations into account, there is a need for them to be reconfigured under opportunity-reducing considerations. There is also a possibility to develop an entirely new collection of techniques, for example tools that can identify areas of crime attractors and generators, and tools that can triangulate an insider's pathways in cyberspace by considering his/her social networking, online recreation and organisational intranet activity spaces for reconnaissance purposes.

The insider threat is clearly a source of concern for any organisation, and in the context of cloud computing, it could become an even greater threat. From a cloud computing perspective, the concept of the insider is multi-contextual. It ranges from the rogue administrator of a cloud service to an insider 'who uses cloud systems to carry out an attack on an employer's local resources' [54]. The framework presented in this paper is an attempt to analyse insider threat security measures from an opportunity-reducing perspective and it presents a preliminary step in tackling this imminent concern.

ACKNOWLEDGEMENT

The author would like to acknowledge the University of South Africa for supporting this research.

REFERENCES

[1] CSO MAGAZINE, USSS, CERT, & Deloitte. (2011). 2011 Cybersecurity Watch Survey: Organizations need more skilled cyber professionals to stay secure. Available from www.cert.org/archive/pdf/CyberSecuritySurvey2011.pdf. (Accessed 12 March 2013).

[2] Magklaras, G.B. & Furnell, S.M. (2005). A preliminary model of end user sophistication for insider threat prediction in IT systems. *Computers & Security*, *24*(5): 371-380.

[3] Hunker, J. & Probst, C.W. (2011). Insiders and insider threats-an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *2*(1): 4-27.

[4] Chinchani, R., Iyer, A., Ngo, H.Q., & Upadhyaya, S. (2005). *Towards a theory of insider threat assessment.* Paper presented at the International Conference on Dependable Systems and Networks, Yokohama, Japan.

[5] Salem, M.B., Hershkop, S., & Stolfo, S.J. (2008). A survey of insider attack detection research: Beyond the Hacker. In S.J. Stolfo, S.M. Bellovin, A.D. Keromytis, S. Hershkop, W.S. Smith, and S. Sinclair (Eds.), *Insider Attack and Cyber Security* (Vol. 39, pp. 69-90). New York: Springer US.

[6] Nance, K. & Marty, R. (2011). *Identifying and visualizing the malicious insider threat using bipartite graphs.* Paper presented at the 44th Hawaii International Conference on System Sciences (HICSS), Koloa, Kauai, *Hawaii*, USA.

[7] Cornish, D.B. & Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies*, *16*: 41-96.

[8] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6): 472-484.

[9] Felson, M. & Clarke, R.V. (1998). Opportunity makes the thief: Practical theory for crime prevention (Police Research Series Paper 98). Policing and Reducing Crime Unit, Research, Development and Statistics Directorate. London: Home Office. (pp. 1-36).

[10] Clarke, R.V. & Cornish, D.B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and Justice*, *6*: 145-185.

[11] Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*: 588-608.

[12] Brantingham, P. & Brantingham, P. (2008). Crime Pattern Theory. In R. Wortley and L. Mazerolle (Eds.), *Environmental Criminology and Crime Analysis* (pp. 78-93). New York: Macmillian.

[13] Clarke, R.V. (1997). Introduction. In R.V. Clarke (Ed.) *Situational Crime Prevention: Successful Case Studies* (pp. 1-43). Guilderland, NY: Harrow and Heston.

[14] Becker, G.S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2): 169-217.

[15] Li, H., Zhang, J., & Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, *48*(4): 635-645.

[16] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3): 523-548.

[17] Hartel, P.H., Junger, M., & Wieringa, R.J. (2010). Cyber-crime Science = Crime Science + Information Security. *Technical Report TR-CTIT-10-34*. Enschede: Centre for Telematics and Information Technology University of Twente.

[18] Willison, R. & Siponen, M. (2009). Overcoming the insider: Reducing employee computer crime through situational crime prevention. *Communications of the ACM*, *52*(9): 133-137.

[19] Beebe, N.L. & Roa, V.S. (2005). *Using situational crime prevention theory to explain the effectiveness of information systems security*. Paper presented at the Proceedings of the 2005 SoftWars Conference, Las Vegas, NV.

[20] Beebe, N.L. & Roa, V.S. (2010). Improving Organizational Information Security Strategy via Meso-Level Application of Situation Crime Prevention to the Risk Management Process. *Communications of the Association for Information Systems*, *26*(1).

[21] Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organization*, *16*: 304-324.

[22] Yar, M. (2005). The Novelty of 'Cybercrime'An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4): 407-427.

[23] Bowen, B.M., Salem, M.B., Hershkop, S., Keromytis, A.D., & Stolfo, S.J. (2009). Designing host and network sensors to mitigate the insider threat. *IEEE Security & Privacy*, *7*(6): 22-29.

[24] Silowash, G.J. & King, C. (2013). Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources (Technical Report). *Software Engineering Institute, Carnegie Mellon University*, Available from http://repository.cmu.edu/sei/708. (Accessed 10 July 2013).

[25] D'Arcy, D. & Hovav, A. (2009). Does one size Fit All? Examining the differential effects of IS Security Countermeasures. *Journal of Business Ethics*, *89*: 57-71.

[26] Zeadally, S., Byunggu, Y., Dong, H.J., & Liang, L. (2012). Detecting insider threats: Solutions and trends. *Information Security Journal: A Global Perspective*, *21*(4): 183-192.

[27] Schultz, E.E. (2002). A framework for understanding and predicting insider attacks. *Computers & Security*, *21*(6): 526-531.

[28] Magklaras, G.B. & Furnell, S.M. (2002). Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers & Security*, *21*(1): 62-73.

[29] Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., & Gritzalis, D. (2010). An insider threat prediction model. In S. Katsikas, J. Lopez, and M. Soriano (Eds.), *Trust, Privacy and Security in Digital Business* (Vol. 6264, pp. 26-37). Berlin Heidelberg: Springer.

[30] Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. *Digital Investigation*, *2*(4): 261-267.

[31] Salem, M.B. & Stolfo, S.J. (2012). Combining baiting and user search profiling techniques for masquerade detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *3*(1/2): 13-29.

[32] Spitzner, L. (2003). *Honeypots: Catching the insider threat.* Paper presented at the Proceedings of the 19th Annual Computer Security Applications Conference(ACSAC 2003), Las Vegas, USA.
[33] McGrew, R., Rayford, B., & Vaughn, J.R. (2006). *Experiences with honeypot systems: Development, deployment, and analysis.* Paper presented at the Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Maui, HI, USA.
[34] Spitzner, L. (2010). Honeypots: Are They Illegal? Available from http://www.symantec.com/connect/articles/honeypots-are-they-illegal. (Accessed 12 March 2013).
[35] Kabay, M.E. (2003). Honeypots, Part 4: Liability and ethics of Honeypots. Available from http://www.networkworld.com/newsletters/2003/0519sec2.html. (Accessed 13 March 2013).
[36] Brdiczka, O., Liu, J., Price, B., Shen, J., Patil, A., Chow, R., Bart, E., & Ducheneaut, N. (2012). *Proactive insider threat detection through graph learning and psychological context.* Paper presented at the IEEE Symposium on Security and Privacy Workshops (SPW), San Francisco, USA.
[37] Quassai, Y. & Panda, B. (2012). Insider threat mitigation: preventing unauthorized knowledge acquisition. *International Journal of Information Security, 11*(4): 269-280.
[38] Gardiner, B. (2003). E-Business Security in RAG order, Dublin Institute of Technology, Dublin, Ireland. Available from http://www.comp.dit.ie/rfitzpatrick/MSc_Publications/2003_Bryan_Gardiner.pdf. (Accessed 9 May 2013).
[39] Wood, B.J. (2000). *An insider threat model for adversary simulation.* Paper presented at the Proceedings of the Research on mitigating the Insider Threat to Information Systems, Arlington, Virginia.
[40] Bowen, B.M., Salem, M.B., Hershkop, S., Keromytis, A.D., & Stolfo, S.J. (2009). *Baiting inside attackers using decoy documents.* Paper presented at the Security and Privacy in Communication Networks: 5th International ICST Conference (SecureComm 2009), Athens, Greece.
[41] Brantingham, P. & Brantingham, P. (1995). Criminality of Place: Crime Generators and Crime Attractors. *European Journal of Criminal Policy and Research, 3*(3): 1-26.
[42] Molok, N.N.A., Ahmad, A., & Chang, S. (2010). *Understanding the Factors of Information Leakage through Online Social Networking to Safeguard Organizational Information.* Paper presented at the 21st Australasian Conference on Information Systems (ACIS2010), Brisbane, Australia.
[43] Nuha, N. & Molok, N.N.A. (2011). *Disclosure of Organizational Information by Employees on Facebook: Looking at the Potential for Information Security Risks.* Paper presented at the Proceedings of the Australasian Conference on Information Systems (ACIS), Sydney, Australia.
[44] Padayachee, K. (2009). An aspect-oriented approach towards enhancing optimistic access control with usage control. *Computer Science*. Pretoria: University of Pretoria (Doctoral-Thesis).
[45] Wortley, R. (2001). A classification of techniques for controlling Situational Precipators of Crime. *Security Journal, 14*: 63-82.
[46] Whitten, A. & Tygar, J.D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.* Paper presented at the Proceedings of the 8th USENIX Security Symposium, Washington D.C., America.
[47] Laub, J.H., & Sampson, R. J. (2001). Understanding desistance from crime. *Crime and justice*: 1-69.
[48] Shover, N. (1996). *Great Pretenders: Pursuits and Careers of Persistent Thieves*. Boulder, Colorado: Westview Press.
[49] Cusson, M. (1993). Situational deterrence: Fear during the criminal event. *Crime Prevention studies, 1*: 55-68.
[50] D'Arcy, D. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of disparate findings. *European Journal of Information Systems, 20*: 643-658.
[51] Tipton, H.F. (2007). Types of information security controls. In M. Krause and H.F. Tipton (Eds.), *Handbook of Information Security Management* (6 ed., pp. 1357-1366). Boca Raton: CRC press.
[52] Lee, S.M., Lee, S., & Yoo, S. (2003). An integrative model of computer abuse based on social control and general deterrence theories. *Information and Management, 41*(6): 707-718.
[53] Vito, G.F., Maahs, J.R., & Holmes, R.M. (2006). *Criminology: Theory, Research, and Policy* (2 ed.). Boston: Jones & Bartlett Learning.
[54] Claycomb, W.R. & Nicholl, A. (2012). *Insider Threats to Cloud Computing: Directions for New Research Challenges.* Paper presented at the IEEE 36th Annual Computer Software and Applications Conference(COMPSAC), Izmir, Turkey.