A Rational Choice Theory Perspective of Deploying Honeypots to contain the Insider Threat

Keshnee PADAYACHEE
School of Computing, University of South Africa
Pretoria, Gauteng 0003, South Africa

ABSTRACT

The aim of this paper is to provide an understanding of the insider threat using rational choice theory. Specifically, the decision-making process of a maleficent insider in the presence of a luring honeypot is reviewed. Understanding these decisions may assist in designing technological solutions that are deployed at opportune decision points to contain the insider threat. To test the premise, an insider threat mitigation strategy derived from the rational choice modeling perspective is presented.

Keywords: Rational Choice Theory, Honeypots, Deterrent Control, Insider Threat and Compliance.

1. INTRODUCTION

According to the CyberSecurity Watch Survey [1], 33% of respondents believe that the insider threat is becoming more costly as insiders are becoming increasingly more sophisticated. Examples of attacks include unauthorized extraction, duplication or exfiltration of data, tampering with data, deletion of critical assets, etc. [2]. The term ‘insider threat’ refers to any individual who works in an organization and uses the authority granted to them for illegitimate gain (see Schultz [3] for a detailed discussion of the term). Honeypots may be a way of containing the insider threat [4] that is, limiting the damage caused by an insider by deflecting the malicious insider to a honeypot. However, it is problematic to use a honeypot to prosecute an individual and this type of lawsuit could damage a company’s reputation. Hence it is more practical to contain the insider threat and guide the insider to compliance. In this paper, rational choice theory (RCT) modeling is employed to devise a strategy to lure and contain the insider threat using honeypots. This type of analysis assists in determining at which decision points to activate interventions to redirect the insider threat to compliance.

A honeypot is an information system resource whose value lies in the unauthorized use of that resource [5]. Using honeypots should confirm an insider’s actions and potentially analyze their motivations and their resources [4]. Recently there has been a trend towards recommending honeypots or decoys to counter the insider threat (see [6] and [7]). However, in general there are several ethical and legal considerations that need to be taken into account. Hence in this article honeypots are reviewed within the broader context of insider threat mitigation. In a sense a honeypot is a ‘pre-e-crime’ detection strategy where the insider is given the opportunity to commit a crime controlled by insider threat mitigation. In this pre-e-crime scenario, RCT is used to determine intervention points for insider threat mitigation thus guiding the insider to compliance.

Compliance with information security is an adaptive response, while non-compliance is a maladaptive response [8]. ‘Deterrent controls are intended to discourage individuals from intentionally violating information security policies or procedures’ [9] and discourage a maladaptive response, whereas positive-reinforcements encourage an adaptive response. Compliant information security behavior refers to the set of core information security activities that have to be adhered to by end-users to maintain information security as defined by information security policies [10]. Pahnila et al. [11] considered both positive-reinforcement and negative-reinforcement in terms of compliance. They considered sanctions, ‘threat appraisal’, ‘coping appraisal’ and normative beliefs as negative-reinforcements while ‘information quality’, ‘facilitating conditions’, rewards and habits as positive-reinforcements [11]. Some of these factors are relevant to this paper, however aspects such as coping appraisal and threat appraisal are not. These are based on the assumption that an insider will comply because they are concerned that their actions will jeopardize the organization’s information security [11]. However, this is not a concern for the insider threat whose sole intention is maleficence. While sanctions are derived from General Deterrence Theory (GDT), normative beliefs are based on the perception of peer behavior [11]. This paper will only consider negative-reinforcement from the GDT perspective [12]. D’Arcy and Hovav [13] considered the countermeasures that deter internal systems’ misuse, namely awareness of security policies, monitoring, preventative software and training. GDT has its roots in RCT. GDT is moderated by certainty of detection, severity of punishment and the swiftness of detection [14]. GDT focuses more on the cost of the crime, while RCT considers both the cost and the benefits of the crime [15].

RCT is relatively basic; it assumes that a criminal makes decisions based on a cost-benefit analysis [16]. RCT involves increasing the perceived effort of crime, increasing the perceived risks, reducing the anticipated rewards and removing the excuse for crime [17]. Recently there has been a trend towards using RCT to explain the insider threat. For instance, Li et al. [18] used RCT to examine an employee’s intention to comply. In their study, Bulgurcu et al. [19] also applied RCT to understand insiders. The authors considered the benefits of non-compliance. According to Willison [20], RCT is highly appropriate to understanding insider threat. He argues that these types of theories complement existing security strategies and help to identify offender behavior and their associated criminal choices. These insights are useful in developing safeguards.

An effort was made in this study to employ RCT to develop a strategy to contain the insider threat. The rest of the paper is structured as follows: Section 2 contains a discussion of the concept of a honeypot as a lure to contain the insider threat. In

Section 3, RCT is examined with regard to its suitability in understanding the insider threat. Rational choice modeling is used in Section 4 to model the decision-making process of an insider in the presence of a luring honeypot and the paper concludes with Section 5 and possible future research opportunities.

2. DEPLOYING HONEYPOTS AS A LURE TO CONTAIN THE INSIDER THREAT

According to Spitzner [5], honeypots are more than just a computer or a physical resource. A honeypot may be anything from a Windows program to an entire network of computers. According to Spitzner [4], there are several advantages to using honeypots for the insider threat:

1) Small data sets: Only collect data when an attacker is interacting with them; hence easier to analyze and manage.
2) Reduced false positives: They are superior to other forms of detection strategies because an interaction with a honeypot is guaranteed to be illicit.
3) Catching false negatives: Other techniques may fail if there is a new type of attack, unlike a honeypot, as any interaction with one implies an anomaly.
4) Encryption: It does not matter if an attack is encrypted, the honeypot will capture the activity.
5) Highly flexible: Honeypots are adaptable from a simple honeytoken which may be embedded in a database to an entire network of computers.
6) Minimal resources: Honeypots require minimal resources.

According to Bowen et al. [21], the following are properties that honeypots (decoys) must have in order to bait an insider:

1) Believable: Decoys must appear to be authentic.
2) Enticing: They must be attractive to the insider.
3) Conspicuous: They must be visible to the insider.
4) Variability: Decoys should not be easily identifiable.
5) Non-interference: A decoy should not hinder, obstruct or impede normal operation.

Gupta et al. [22] identify the characteristics of luring in terms of a context honeypot. A context honeypot is used to identify a probable privacy violator. However, certain principles hold in general:

1) A suspected user can be lured only once by the same technique.
2) False negatives must be close to zero – for example, a criminal who is not lured escapes monitoring.
3) False positives should be kept low – for example, an innocent user is lured and is kept under observation for no reason.
4) Lure data will remain static until confirmation/elimination of suspicion over a suspected user – the data disclosed to the suspect must remain static so as not to raise the suspicions of the insider.
5) The suspected user must be oblivious of the luring.
6) Lure data will be different for each suspected user.

It is important for a luring honeypot to maintain the characteristics identified by Gupta et al. [22] and Bowen et al. [21]. Bowen et al. [21]) also specify that a decoy should be detectable (i.e. decoys must generate an alert). However, a honeypot will not be effective if the insider threat decides not to select a honeypot if they recognize that the luring honeypot is in fact a trap. Hence interactions with a honeypot should be detectable to the system administrator but not to the insider threat.

According to Spitzner [4], 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 only capture actions related to this activity. Additionally, there are legal and ethical challenges. Spitzner [23] provides a comprehensive review of legal challenges associated with honeypots: entrapment, privacy and liability. Entrapment may be used as a defense to escape prosecution. Honeypots may violate an individual's right to privacy. There is also the issue of liability if an organization's honeypot is used to cause others harm [23]. The ethical question centers on whether it is ethical 'to pose a computer system as something it is not' [24]. Hence, the current research also considers integrating controls such as deterrent controls and positive-reinforcement with honeypots to guide the insider to compliance. In the next section, the concept of a luring honeypot is considered from an RCT perspective.

3. THE RATIONAL CHOICE PERSPECTIVE

The basis of RCT is that criminals formulate an assessment of the costs and benefits prior to and whilst committing an offence. An individual does not only consider the formal sanctions such as imprisonment but also the informal sanctions such as embarrassment [15]. Furthermore, the individual considers both the tangible benefits of a crime such as financial gain as well as the intangible benefits [15].

RCT is classified under the basic category of opportunity theories of crime as described by Felson and Clarke [17]. This consideration of RCT as an opportunity theory provides a rationale for examining luring honeypots under the same reflection. The premise of a honeypot is that it is a device deployed to provide an individual with malicious intent with an opportunity to commit a crime. According to Felson and Clarke [17], 'opportunity plays a role in causing in all crime'.

In order to consider the insider threat as a crime of opportunity, it is practical to reflect on some of the principles of opportunity theory as discussed by Felson and Clarke [17]. There are also some properties that may attract, detract or generate more crime [17]. In this context honeypots are attractors, whereas deterrents are detractors. For the insider threat, committing a major offence can result in other minor offences being committed and vice versa [17]. Sometimes a minor offence may provide a 'camouflage' for major offences. Honeypots can therefore provide a gateway to discovering major offences and deterrent controls may deter a minor offence thereby removing 'pre-criminal conditions' to a much more serious offence. The properties of value, inertia, visibility, accessibility (VIVA), based on the routine activities theory, provide a point for evaluating objects that are suitable targets [25]. Hence in order for a honeypot to be an effective lure, aspects such as high value, low inertia, high visibility and easy accessibility have to be considered as well. In a physical crime scenario, low inertia refers to an object that is transportable [17]. Perhaps, in the sense of cyberspace, low inertia could refer to data that can be easily disseminated on a network. A crime prevention method may provide the added benefit of diffusion [17]. The benefits of diffusion may occur when an insider assumes that the deterrent controls in one system may be applicable to other systems too.

It is crucial to recognize that a deterrent may result in maleficence being displaced to another part of the system.

In this study RCT was employed to understand the decisions of an insider in the presence of a luring honeypot. This involved considering controls that may inhibit the insider from committing maleficence. These controls influence the insider to perceive that the effort or risk of committing such an offence is more than they have estimated. According to Felson and Clarke [17], criminals rarely have a complete understanding of the costs involved. Controls that increase the awareness of information security policy may assist in 'removing the excuses' (i.e. rationalizations) of an insider. Willison [26] postulates that 'if offenders can be prevented from rationalizing and excusing their criminal actions in specific settings, they will be open to feelings of guilt and shame', thus preventing further crime.

RCT is not beyond reproach. Rational choice theorists often defend the theory by stating that criminals are not 'purely rational' as the notion of rationality is 'bounded' by factors such as time, ability and values [15]. Critics of RCT assert that rarely do criminals formulate a complete assessment of the costs and benefits prior to committing a crime [15]. It is clear that RCT is not the best tool to predict criminal behavior, rather it is a tool to predict the possible decision points of a criminal act. At a pragmatic level, one of the motivations for opting for RCT for this study was to leverage the decision models for RCT provided by Clarke and Cornish [27]. It is evident that the RCT perspective may be used as a 'heuristic device or a conceptual tool' rather than a theory [28]. These decision models expose the rational choices that a criminal makes at every stage of a crime. In the next section, these models are reformulated to consider the insider context.

The current research 'deconstructs' the methodology of using honeypots as lures to contain an insider and considers how an insider would view such a decoy and how they would react from a rational theory perspective within a holistic mitigation strategy.

4. RATIONAL CHOICE MODELING

Clarke and Cornish [27] assert that the models for rational choice do not have to be complete but merely 'good enough' to provide empirical directions for query or to derive policy. The models are derived from criminology and were developed for considering burglaries. In this paper these models are reapplied from a fresh perspective considering the insider threat. The processes of crime involvement are initial involvement, event, continuance and desistance. The models are schematic representations of the key decision points in criminal behavior. The decision models are not flowcharts. It is not necessary to model all four processes. The continuing involvement model was not considered because it focuses on the success of the crime.

Initial Involvement

The first process is the initial involvement model (see Figure 1). Here the insider represents a unification of previous learning and background factors (apathy, low self-control, opportunistic behavior, etc. [29]). The dimensions of the previous learning factor are derived from Bowen et al. [6]. They recommend that honeypots or decoys be designed levels of sophistication that characterize the insider threat, ranging from insiders with a low level of sophistication to the highly privileged. An insider at a low level of sophistication relies on what can be discerned from a cursory scan, while a highly privileged insider threat will know that there are decoys in the system and will attempt to disable or avoid them. The previous learning also includes past deviant behavior [29] which is a predictor for future deviant behavior. The generalized needs are derived from the motivations of malicious insiders and range from espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption, and ignorance to apathy [30].

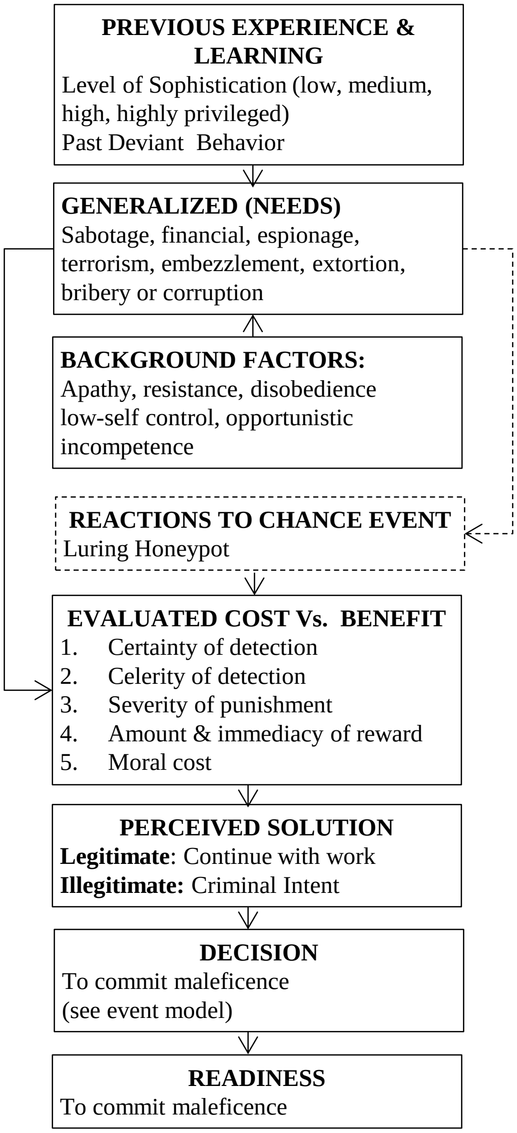
PREVIOUS EXPERIENCE & LEARNING
Level of Sophistication (low, medium, high, highly privileged)
Past Deviant Behavior
GENERALIZED (NEEDS)
Sabotage, financial, espionage, terrorism, embezzlement, extortion, bribery or corruption
BACKGROUND FACTORS:
Apathy, resistance, disobedience low-self control, opportunistic incompetence
REACTIONS TO CHANCE EVENT
Luring Honeypot
EVALUATED COST Vs. BENEFIT
1. Certainty of detection
2. Celerity of detection
3. Severity of punishment
4. Amount & immediacy of reward
5. Moral cost
PERCEIVED SOLUTION
Legitimate: Continue with work
Illegitimate: Criminal Intent
DECISION
To commit maleficence
(see event model)
READINESS
To commit maleficence

Figure 1: An initial involvement model precipitated by a luring honeypot

The insider may have malicious intent and decides whether they are ready to commit maleficence. However, the insider may be presented with an opportunity by a luring honeypot to commit an offence. At this juncture the insider will evaluate the 'cost versus benefit', and determine their readiness to commit the offence. 'Readiness' implies that the insider is lying in wait for the perfect opportunity to commit an offence.

There are two important decision points in this model: firstly, the readiness to commit maleficence and, secondly, the decision to commit maleficence, which may be precipitated by the luring honeypot. The decision to commit maleficence may be made simultaneously with the chance event or the chance event may precipitate the decision to commit maleficence.

The significance of the initial model is that it may be used for input into the properties that need to be taken into account to develop a truly effective honeypot lure. These input properties may be used to define the visibility, inertia, value and accessibility of the lures. Additionally the frequency of the honeypot lures (i.e. how often an insider should be targeted by lures) is another input property that needs to be considered. These five properties will need to be adapted to various degrees depending on the previous experience and learning; generalized needs and background factors. For instance, a highly sophisticated insider may be lured by a honeypot that appears to be a technical challenge. Hence, lowering the accessibility of the lure may provide this technical challenge. It may also be pragmatic to model lures based on the insider's motivation. For example, an insider that is motivated by financial gain will be lured by a honeypot that appears to be of high value. An insider's background may influence how they react to a lure. For example, insiders who are opportunistic or have low-self-control may need to be targeted more frequently by honeypot lures as they are more susceptible to crime. These factors may be determined by profiling.

The Event Model

The event model shows the sequence of decision-making nodes involved when an insider decides to accept the luring honeypot (see Figure 2). The alternative route, where a user decides to commit the offence without being lured, is not considered as it eliminates the honeypot in the process. In the event model, the user chooses the honeypot lure, trusting it to be real data, because it is believable, enticing, etc.

The significance of this model lies in the fact that it demonstrates that the opportunity for intervention is at the point where the insider has decided to accept the lure. At this juncture deterrent controls may be deployed to increase the perceived effort or risks of committing the crime. The lure is attacked if it is believed to be of high value, has high visibility, low inertia (e.g. easily forwarded in an e-mail) and is easily accessible. While the event model intends to attract the insider; the aim of applying deterrent controls is to subtly 'train' the insider to be compliant and furthermore the deterrent controls should target the 'supposed offence' being committed.

The aspects that deter non-compliance include sanctions, monitoring and policies, and technological controls such as usage control deterrents [29]. Usage control deterrents include conditions and obligations on the usage of data [31] and intend to deter rather than deny access. Note, the original concept of usage control deterrents did not consider how these conditions or obligations may be used from an RCT perspective to increase the costs associated with maleficence. Usage control deterrents may be used to increase the perceived risk and effort associated with the offence and may diminish the excuses for committing maleficence. They also increase awareness about the legitimate uses of organizational data and increase the effort required to access the data by stipulating conditions and obligations on the use of the data. These conditions and obligations should be aligned with information security policies.

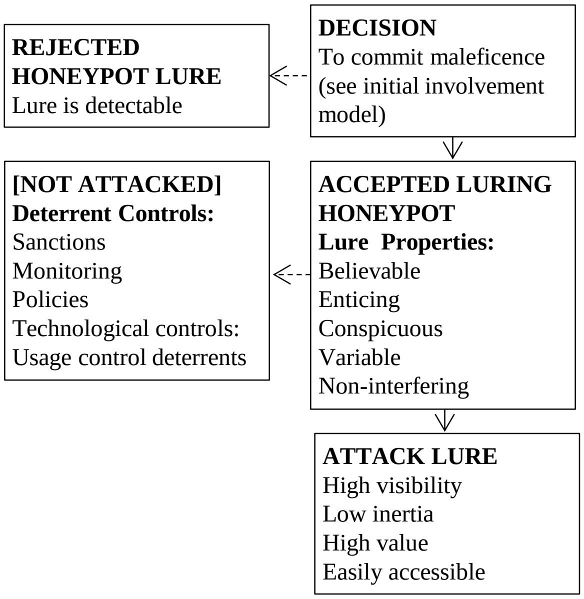

Figure 2: An event model integrating luring honeypots and deterrent controls

Desistance Model

This model (see Figure 3) is based on the aversive experiences of an insider during the course of offending (i.e. the deterrents) and variations in positive-reinforcement. Positive-reinforcements may include improved 'information quality' (i.e. improving the perceived usefulness of information); 'facilitating conditions' (i.e. providing a supportive work environment); rewards and mandating good security habits [11]; and organizational commitment. These positive-reinforcements may encourage the insider in the best case scenario to comply or in the worst case scenario to consider other crimes (displacement).

The rejected alternatives show areas of discontentment. For example, an insider may be disgruntled due to working long hours. Wortley [32] describes several types of situations that result in maladaptive behavior. The conditions that correlate with the virtual world include frustrations caused by failures of equipment and services, and invasion of privacy. Organizations need to be aware of these types of conditions as by reducing areas of discontentment, insiders will be less likely to engage in maleficence.

In this derivation, it is envisaged, that containment events via honeypots and the deterrent events will contain and deter a maladaptive response. On the other hand, positive reinforcement events will increase the likelihood of an adaptive response. Desistance implies either an end to all maleficence activity or displacement (i.e. another type of crime). It is assumed that once an insider accepts one honeypot lure, they will be presented with more honeypot lures for the purposes of reconnaissance.

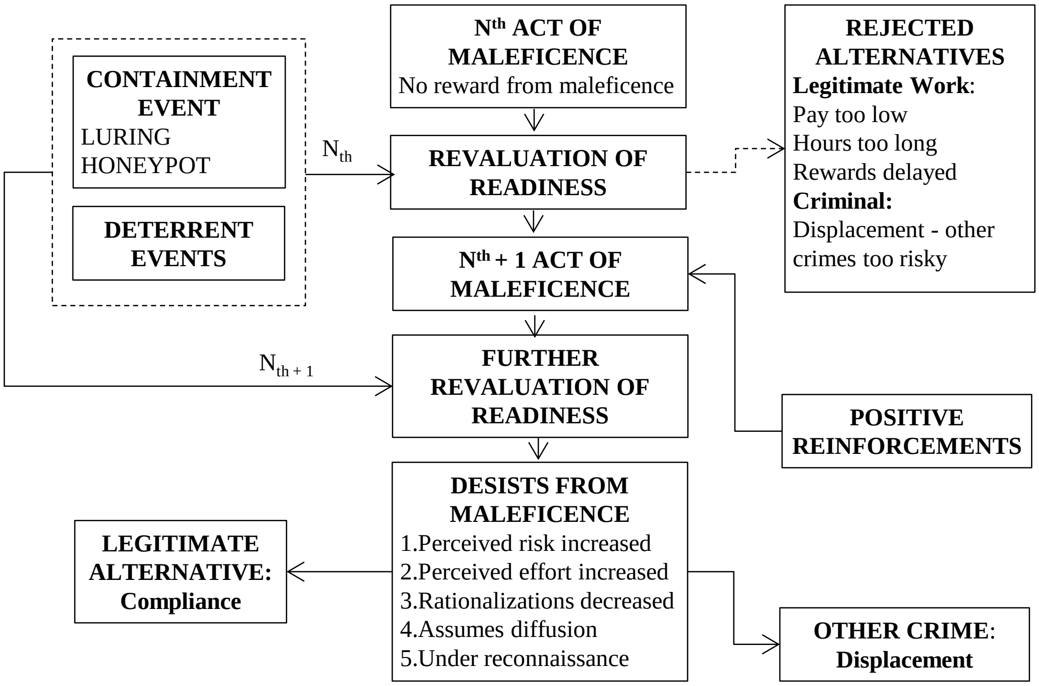

Figure 3: Desistance model integrating honeypots into a holistic mitigation strategy

In this context it is anticipated that deterrent controls and positive-reinforcements may result in malicious insiders desisting from further offences. Desistance involves the insider considering the following: the costs of the crime (i.e. perceived risks and perceived effort); the justifications for the crime (i.e. rationalizations); diffusion and currently being under reconnaissance.

The significance of this model lies in the fact that it shows junctions where organizations can intervene if the insider ignores the deterrence strategy and continues with attacking the honeypots. This implies that the insider requires further interventions which may require the use of positive-reinforcements to encourage compliance.

The other important juncture considering the rejected alternatives that is those negative aspects in the work environment that are precipitating the insider to continue with attacking honeypots despite the interventions. Organizations also need to consider the possibility that interventions have caused the insider to displace the crime. Hence there is a need to have contingency plans for this outcome.

Implications for Practice

The models are not intended to be all-encompassing. The models derived here may be used as a proactive mitigation strategy which seeks to change behaviors and motivations. This technique of viewing polarizing concepts of luring, deterring and positive-reinforcement may offer a strategy for organizations deploying honeypots without the legal pitfalls.

According to Clarke and Cornish [27] this type of modeling helps focus on a specific crime and helps develop a policy as it breaks the crime process down into a smaller components which allows for policies to target these specific components. This type of analysis helps the development of measures to increase the effort of offending and decrease the associated rewards and defenses.

5. CONCLUSIONS

In this study rational choice modeling was used to understand how to effectively lure and contain the insider threat from further maleficence. It is based on a containment strategy where the insider is deflected to honeypots instead of attacking real data while deterrent controls and positive-reinforcements attempt to negotiate them into compliance. It is based on an approach where insiders are lured successively and re-conceptualizing their notions about the costs of committing the associated offence by discouraging maladaptive responses and encouraging an adaptive response. Future research will involve implementing and evaluating the strategy that was derived. The rational choice models derived offer a broader perspective in terms of considering the psychological and organizational components, and where interventions may be deployed.

6. REFERENCES

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

[2] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research: Beyond the Hacker", **Insider Attack and Cyber Security**, Advances in

Information Security S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, W. S. Smith and S. Sinclair, eds., pp. 69-90, New York: Springer US, 2008.

[3] E. E. Schultz, "A framework for understanding and predicting insider attacks", **Computers & Security**, Vol. 21, No. 6, 2002, pp. 526-531.

[4] L. Spitzner, "Honeypots: Catching the insider threat" in 19th Annual Computer Security Applications Conference (ACSAC 2003), Las Vegas, USA, 2003, pp. 170-179.

[5] L. Spitzner, "Honeytokens: The other honeypot", http://www.securityfocus.com/infocus/1713 (accessed 12 March 2012).

[6] B. M. Bowen, M. B. Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Designing host and network sensors to mitigate the insider threat", **IEEE Security & Privacy**, Vol. 7, No. 6, 2009, pp. 22-29.

[7] J. White, and B. Panda, "Implementing PII honeytokens to mitigate against the threat of malicious insiders" in IEEE International Conference on Intelligence and Security Informatics (ISI'09), 2009, p. 233.

[8] A. Vance, M. Siponen, and S. Pahnila, "How Personality and Habit affect Protection Motivation", Workshop on Information Security and Privacy (WISP 2009), Phoenix, Arizona, 2009, pp. 14-21.

[9] H. F. Tipton, "Types of information security controls", **Handbook of Information Security Management**, M. Krause and H. F. Tipton, eds., pp. 1357-1366, Boca Raton: CRC press, 2007.

[10] M. Chan, I. Woon, and A. Kankanhalli, "Perceptions of information security in the workplace: Linking information security climate to compliant behavior", **Journal of Information Privacy and Security**, Vol. 1, No. 3, 2006, pp. 18-41.

[11] S. Pahnila, M. Siponen, and A. Mahmood, "Employee's Behavior towards IS Security Policy Compliance" in Proceedings of the 40th Hawaii International Conference on System Sciences Hawaii, 2007, p. 1561.

[12] G. E. Higgins, A. L. Wilson, and B. D. Fell, "An Application of Deterrence Theory to Software Piracy", **Journal of Criminal Justice and Popular Culture**, Vol. 12, No. 3, 2005, pp. 166-184.

[13] D. D' Arcy, Hovav, A., "Does one size Fit All? Examining the differential effects of IS Security Countermeasures", **Journal of Business Ethics**, Vol. 89, 2009, pp. 57-71.

[14] D. D'Arcy, and T. Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of disparate findings", **European Journal of Information Systems**, Vol. 20, 2011, pp. 643-658.

[15] G. F. Vito, J. R. Maahs, and R. M. Holmes, **Criminology: Theory, Research, and Policy**, 2nd edition, Boston: Jones & Bartlett Learning, 2006.

[16] D. B. Cornish, and R. V. Clarke, "Understanding crime displacement: An application of rational choice theory", **Criminology**, Vol. 25, No. 4, 1987, pp. 933-947.

[17] M. Felson, and R. V. Clarke, 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, 1998.

[18] H. Li, J. Zhang, and R. Sarathy, "Understanding compliance with internet use policy from the perspective of rational choice theory", **Decision Support Systems**, Vol. 48, No. 4, 2010, pp. 635-645.

[19] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness", **MIS Quarterly**, Vol. 34, No. 3, 2010, pp. 523-548.

[20] R. Willison, "Understanding the perpetration of employee computer crime in the organisational context", **Information and Organization**, Vol. 16, No. 4, 2006, pp. 304-324.

[21] B. M. Bowen, M. B. Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo, "Baiting inside attackers using decoy documents" in Security and Privacy in Communication Networks: 5th International ICST Conference (SecureComm 2009), Athens, Greece, 2009, pp. 51-70.

[22] S. K. Gupta, R. G. Damor, A. Gupta, and V. Goyal, " Luring: A framework to induce a suspected user into a context honeypot" in IEEE Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007), 2007, pp. 55-64.

[23] L. Spitzner, "Honeypots: Are They Illegal?", http://www.symantec.com/connect/articles/honeypots-are-they-illegal (accessed 12 March 2013).

[24] M. E. Kabay. "Honeypots, Part 4: Liability and ethics of Honeypots",http://www.networkworld.com/newsletters/2003/0519sec2.html (accessed 13 March 2013).

[25] L. E. Cohen, and M. Felson, "Social change and crime rate trends: A routine activity approach", **American Sociological Review**, Vol. 44, No. 4, 1979, pp. 588-608.

[26] R. Willison, and J. Backhouse, "Opportunities for computer crime: Considering system risk from a criminological perspective", **European Journal of Information Systems**, Vol. 15, No. 4, 2006, pp. 403-414.

[27] R. V. Clarke, and D. B. Cornish, "Modeling offenders' decisions: A framework for research and policy", **Crime and Justice**, Vol. 6, 1985, pp. 145-185.

[28] D. B. Cornish, and R. V. Clarke, "The rational choice perspective", **Environmental Criminology and Crime Analysis**, R. Wortley and L. Mazerolle, eds., pp. 21-47, Uffculme, UK: Willan Publishing, 2008.

[29] K. Padayachee, "Taxonomy of compliant security behavior", **Computers and Security**, Vol. 31, No. 5, 2012, pp. 673-680.

[30] K. Nance, and R. Marty, "Identifying and visualizing the malicious insider threat using bipartite graphs," in 44th Hawaii International Conference on System Sciences (HICSS), Koloa, Kauai, Hawaii, USA, 2011, pp. 1-9.

[31] K. Padayachee, "An aspect-oriented approach towards enhancing optimistic access control with usage control ", Computer Science University of Pretoria (Doctoral-Thesis) Pretoria, 2009.

[32] R. Wortley, "A classification of techniques for controlling Situational Precipators of Crime", **Security Journal**, Vol. 14, 2001, pp. 63-82.