A Framework of Opportunity-Reducing Techniques to Mitigate the Insider Threat

Towards Best Practice

Keshnee Padayachee
Institute for Science and Technology Education
University of South Africa
Pretoria, South Africa
Email: padayk@unisa.ac.za

Abstract—**This paper presents a unified framework derived from extant opportunity-reducing techniques employed to mitigate the insider threat leveraging best practices. Although both 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. Situational Crime Prevention theory is the most evolved criminology theory with respect to opportunity-reducing techniques. Hence, this theory will be the basis of the theoretical framework. The derived framework highlights several areas of research and may assist organizations in implementing controls that are situationally appropriate to mitigate insider threat.**

Keywords-Insider Threat; Abuse and crime involving computers.

I. INTRODUCTION

According to the SpectorSoft 2014 Insider Threat Survey [1], 61% of IT professionals (n=355) indicated that they were unable to deter insider threats, while the US State of Cybercrime Survey [2] found that 32% of executives (n=500) of US businesses, law enforcement services and government agencies claim that 'insider crimes are more costly or damaging than incidents perpetrated by outsiders'. An 'insider' is any individual who has legitimate access to an organisation's information technology (IT) infrastructure [3] while an 'insider threat' uses the authority granted to him/her for illegitimate gain [4]. Malicious insider actions can range from compromising information confidentiality to integrity and/or availability [5]. Examples of attacks include unauthorised extraction, duplication or exfiltration of data, tampering with data, deletion of critical assets, etcetera [6]. The motivations of malicious insiders range from apathy to espionage, sabotage, terrorism, embezzlement, extortion, bribery, corruption and ignorance [7]. In general, it has been proffered by Cornish and Clarke [8] that while both motivation and opportunity play a critical role in crime in the physical world, opportunity may be the 'trigger' to committing a crime. The aim of this paper is assess the current set of opportunity reducing techniques to contain the insider threat against the principles of best practices for insider threat mitigation. This assessment will be used as a basis to derive a unified framework to mitigate the insider threat leveraging best practices.

Farahmand and Spafford [9] found that most law enforcement agents use the fraud triangle to investigate the insider threat. The fraud triangle, which is used as a framework to explain crime, is composed of three elements – pressure (i.e. motivation), opportunity and rationalisation [10]. A comprehensive insider threat strategy will involve addressing all three elements of the fraud triangle. However, this paper focuses primarily on the opportunity element of the fraud triangle. Motivations are difficult to analyse as they are based on human emotions. In contrast, it is easier to identify opportunities and to develop pragmatic strategies to minimise crime. There is duality between rationalisation and opportunity as, if the insider cannot rationalise a crime, then it is not considered to be a good opportunity for crime. Felson and Clarke [11] 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 or justification (i.e. rationalisation) to commit a crime, there has to be an opportunity to commit the crime.

According to Willison [12], it is valuable for researchers to consider computer crimes in terms of criminology theories, as they are, after all, crimes. Willison [12] proposes that the techniques advocated by Situational Crime Prevention theory could reasonably be adopted by information security practitioners. This theory has been applied to the insider threat (see [12-14]) and to general information security concerns (see [15] and [16]). In criminology, four theories of crime embody the opportunity theory perspective: Rational Choice theory [17], Routine Activities theory [18], Crime Pattern theory [19] and more recently Situational Crime Prevention theory [20]. Situational Crime Prevention theory is the most evolved theory with respect to opportunity-reducing techniques. Hence, this theory will be the basis of the theoretical framework.

An effort is made in this study to derive a framework that may be used to develop a unified strategy to mitigate the insider threat and to identify areas of potential research. The framework combines a benchmark of best practices with the formal description of situational crime prevention. The

978-1-4799-7755-0/15/$31.00 ©2015 IEEE

objective of this research is to determine the extent to which Situational Crime Prevention satisfies the principles of best practices for insider threat mitigation. The rest of the paper is structured as follows: Section II presents the theoretical framework for the study. Section III evaluates the current status of opportunity-reducing techniques. Section IV presents a discussion on the findings and the paper concludes with Section V.

II. THEORECTICAL FRAMEWORK

The Situational Crime Prevention theory considers five categories of opportunity-reducing measures. Each measure is further divided into 25 specific techniques [8] which are intended for the physical landscape (see table I)

TABLE I. TECHNIQUES OF SITUATIONAL CRIME PREVENTION

Category	Subcategories
Increase the effort	Target hardening (i.e. increasing the difficulty of carrying out the crime [21]); control of access to facilities; screen exits; deflecting offenders; controlling tools (i.e. tools that may be used to cause harm [14])
Increase the risks	Extending guardianship; assisting natural surveillance; reducing anonymity; utilising place managers; strengthening formal surveillance
Reduce the rewards	Concealing targets; removing targets; identifying property; disrupting markets; denying benefits
Reduce provocations	Reducing frustrations and stress; avoiding disputes; reducing emotional arousal; neutralising peer pressure; discouraging imitation
Remove excuses	Setting rules; posting instructions; alerting conscience assisting compliance; controlling drugs and alcohol (this subcategory will not be considered in this study as it is unrelated to the information system domain)

These techniques were given 'digital analogies' by Beebe and Roa [15], Willison [12], Coles-Kemp and Theoharidou [14], and Hinduja and Kooi [22]. The 'increase the effort' category involves ensuring criminal opportunities are difficult to execute which may discourage offenders, while the 'increase the risks' category involves increasing 'the risk of detection, resistance and apprehension' associated with maleficence [21]. The 'reduce the rewards' category' involves reducing the benefits of the crime [21]. Beebe and Roa [15] argue that lowering the perceived net benefit gained by cyber criminals may deter them from committing the crime. Nonetheless, in their opinion typical deterrents like sanctions 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.

'Remove excuses' involves neutralising the rationalisations of a criminal [21]. The aforementioned category is significant for opportunity reduction because 'if offenders can be prevented from rationalising and excusing their criminal actions, they will be open to feelings of guilt and shame' [12]. If an insider is unable to excuse and justify an offence, then the offence is not considered to be a suitable opportunity [16]. For instance, insiders may rationalise their actions by perceiving cybercrime as a victimless crime [23].

The 'reduce provocations' category involves removing 'noxious stimuli from the environment' [21] that may precipitate a crime. This category considers the emotional side of crime which involves situations that act as triggers or precipitators to an individual who is already motivated [8]. Examples of situations that precipitate maladaptive behaviour include frustrations caused by failures of equipment and services, and invasion of privacy [24]. Wortley [25] indicates that precipitator controls constitute more of a 'soft' approach, compared to the 'hard' approach of the previously discussed categories. Highly constrictive controls can lead to stress and frustration and hence precipitate crime. For example, increasing the effort with stringent access controls may impact usability. Hence, it is important for organisations to balance precipitator controls with cost-benefit controls.

In the next section, extant information security techniques recommended for reducing opportunity from the perspective of the Situational Crime Prevention theory are mapped to a contemporary set of best practices.

III. MAPPING OF OPPORTUNITY-REDUCING TECHNIQUES IN INFORMATION SECURITY AGAINST BEST PRACTICES

Willison [12], as well as Coles-Kemp and Theoharidou [14] mapped the ISO/IEC 27002 standard [26] to Situational Crime Prevention theory. In the next elaboration, the current techniques recommend for Situational Crime Prevention is benchmarked against 19 best practices identified by Silowash et al. [27].

TABLE II. BEST PRACTICES FOR INSIDER THREAT MANAGEMENT [27]

19 Best Practices for Insider Threat Management	
#1.	Consider threats from insiders and business partners in enterprise-wide risk.
#2.	Clearly document and consistently enforce policies and controls.
#3.	Incorporate insider threat awareness into periodic security training for all employees.
#4.	Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour.
#5.	Anticipate and manage negative issues in the work environment.
#6.	Know your assets.
#7.	Implement strict password and account management policies and practices.
#8.	Enforce separation of duties and least privilege.
#9.	Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
#10	Institute stringent access controls and monitoring policies on privileged users.
#11	Institutionalise system change controls.
#12	Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
#13	Monitor and control remote access from all end points, including mobile.
#14	Develop a comprehensive employee termination procedure.
#15	Implement secure backup and recovery processes.
#16	Develop a formalised insider threat programme.
#17	Establish a baseline of normal network behaviour.
#18	Be especially vigilant regarding social media.
#19	Close the doors to unauthorised data exfiltration.

As these best practices were developed from an analysis of more than 700 real world case studies (see table II), it is clear

that this evaluation is based on the most definitive list of best practices recommended to mitigate the insider threat to date.

Guido and Brooks [28] also established a set of practices based on a systematic review of well-known insider threat best practices. The practices offered by Guido and Brooks [28] are considered in instances where the best practices listed in table II are deficient. This benchmarking process superimposes these best practices on Situational Crime Prevention in order to derive a pragmatic framework to mitigate the insider threat (see Appendix A).

A. Increase the effort

The 'increase the effort' category describes interventions that increase the difficulty associated with maleficence

The information security analogy proposed for 'target hardening' (i.e. increasing the difficulty of carrying out the crime [21]) include anti-virus software [12], vulnerability patching [15] and 'sensitive system isolation' [14]. Antiviruses are susceptible to misuse. Vulnerability patches may be exploited if organisations do not apply the patches immediately [29]. 'Sensitive system isolation' may be more susceptible to insider threats, as storing all the sensitive and confidential data in one location makes it an easy target [30] which defeats the purpose of 'target hardening'. In this subcategory it was established that Practice #7 (i.e. 'Implement strict password and account management policies and practices') parallels the essence of this subcategory.

Authentication [14] has been proposed to 'control access to facilities'. Clearly authentication must be mediated by access control in order to be an effective means of controlling access to data in the virtual world. However traditional access control such as role-based control is also susceptible to the insider threat as the system grants access as long as the access is authorised Hence, finer-grained authentication and access control may be an effective means of addressing the technique of 'control access to facilities'. It is evident that practice #10 (i.e. 'Institute stringent access controls and monitoring policies on privileged users') is most appropriate to this subcategory.

Firewalls, which have been proposed as a digital analogy to 'screen exits' [12] are 'of limited use, given that the majority of insider threat activity occurs within an enterprise's perimeter' [28]. Clearly this subcategory parallels practice #19 (i.e. 'Close the doors to unauthorised data exfiltration').

The information security controls proposed for 'deflecting offenders' include: honeypots [15]; key splitting [14]; 'segregation of duties' [12] and pre-screening [12]. 'Segregation of duties' prevents misuse since duties and responsibilities are separated [26]. The techniques in this subcategory parallel practices #4 (i.e. 'Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour') and #8 (i.e. 'Enforce separation of duties and least privilege').

Web access controls [14], 'controlling downloads' [12], 'termination procedures' [12] and 'least privilege' [14]) have been proposed as information security measures with respect to 'controlling tools' (i.e. tools that may be used to cause harm). The filtering of downloads is an essential control as insiders may download illicit tools like keystroke loggers or stenographers [31] to aid them in committing maleficence. The principle of 'least privilege' is another fundamental control, however, its practical enforcement may be limited due to fluctuations in work responsibilities. It is clear that this subcategory can be superimposed to practices #8 (i.e. 'Enforce separation of duties and least privilege') and #14 (i.e. 'Develop a comprehensive employee termination procedure'). It is proposed that 'filtering of downloads' is an essential control hence this should also be adopted as a best practice.

B. Increase the risks

This category proposes interventions that increase the negative consequences associated with maleficence. The information security control that is suggested for 'extending guardianship' involves the management of mobile facilities [12]. This is significant as the privacy offered by remote access 'provides a tempting opportunity for insiders to attack with less risk' [32]. This correlates with best practice #13 (i.e. 'Monitor and control remote access from all end points, including mobile').

The information security controls that are recommended for 'assisting natural surveillance' include incident reporting [14] and visualisation tools [15]. Cappelli et al. [32] further qualify this process by affirming that there should be a specific Insider Incident Response Plan. This correlates with practice #16 (i.e. 'Develop a formalised insider threat programme') which includes incident management. Silowash et al. [27] asserts that an insider threat programme should include 'an established incident response plan that addresses incidents perpetrated by insiders, has an escalation chain, and delineates authorities for deciding disposition.'

The information security controls that are recommended to facilitate 'reducing anonymity' include audit trails and event logging [12]. This relates to practice #12 (i.e. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions').

The information security techniques proposed for 'utilising place managers' include a two-person sign-off [12] and 'resource usage monitoring' [15]. A two-person sign-off will help "reduce the risk of extortion" [27]. Two-person controls mirror the thematic concept of multiparty control. Multiparty control is more suitable to the 'utilising place managers' technique, as it involves employees who could naturally monitor the environment as a deterrent [21] while 'monitoring resource usage' may be more suitable to 'strengthening formal surveillance' technique. Multiparty controls was not considered a best practice by either Silowash et al. [27] or Guido and Brooks [28]. Hence it is suggested that multiparty controls should be adopted as a best practice for insider threat mitigation.

Intrusion detection is recommended as a control for 'strengthening formal surveillance'[12]. Intrusion detection systems may not be sensitised to the commands issued by a malicious insider and may appear to be part of his/her normal duties [33]. Hence practice #17 (i.e. 'Establish a baseline of normal network behaviour') may assist in developing more

effective intrusion detection systems and resource usage monitoring. Formal surveillance can be strengthened by change controls and configuration management tools where the former ensure the proper management of all changes made to the network and the latter detect changes to source code and application files [34]. This addition correlates with practice #11 (i.e. 'Institutionalise system change controls'.)

C. Reduce the rewards

The 'reduce the rewards' category is accomplished by decreasing the perceived benefits associated with committing crime.

The information security analogy for 'concealing targets' involves restricting public domain information, for example constraining the information that is revealed on the organisation's website [12]. This is an essential control, as social engineers may exploit information provided on an organisation's website, while insiders may use the organisation's intranet to identify opportunities. However, there is no equivalent best practice for this subcategory. Hence it is proposed that the process of restricting public domain information should be adopted as a best practice for insider threat mitigation.

'Removing targets' is a related technique that involves the obscuring of targets by deploying Clear Desk and Clear Screen controls as recommended by the ISO/IEC 27002 standard [26]. No equivalent best practice could be linked to this subcategory. Hence Clear Desk and Clear Screen controls are suggested as a best practice for insider threat mitigation.

Watermarking [15], digital signatures [12] and 'information classification' [15] have been recommended as information security analogies for 'identifying property'. Watermarking is rendered ineffective if the insider has access to the original object [35]. Digital signatures may prove useful for non-repudiation; however, they require additional validation such as time stamps [36]. Asset management (ISO/IEC 27002) is more encompassing than mere 'information classification' as it includes accountability for assets [26]. Hence a fitting best practice would be practice #6 (i.e. 'Know your assets').

Encryption [12], Automatic Data destruction Mechanisms [15], Continuity Management [14] and Incident Management [14] are offered as information security techniques analogous to the 'denying benefits' technique. Encryption may be cracked by insiders using keystroke loggers [34] or by the mere fact that insiders have privileged access [37]. The automatic destruction of data by mechanisms that wipe out sensitive data instantly reduces the suitability of a target [38]. Business Continuity Management and Information Security Incident Management are clauses from ISO/IEC 27002 [26]. Manage Continuity also implies Disaster Recovery [39]. This correlates with best practice #15 (i.e. 'Implement secure backup and recovery processes').

With regard to the 'disrupting markets' technique, open source products or freeware are recommended as information security controls. This may not be financially viable. There is no corresponding practice that could be linked to this subcategory. Hence it is suggested that in general there should be processes to disrupt the markets that benefit from cybercrime that should be adopted as a best practice for insider threat mitigation.

D. Reduce provocations

The 'reduce provocations' category consists of techniques that are aimed at decreasing the emotional triggers that may precipitate a motivated criminal to commit an offence. This paper proposes a more coherent term to designate the 'reduce provocations' category namely 'reduce precipitators' in order to focus on the situational factors rather than purely on the emotional side of crime. The purpose of this new designation is to reflect the pluralistic nature of cybercrime interventions (i.e. technological, psychological, sociological and organisational). Adaptions of this nature are congruent with the principles of Situational Crime Prevention. Cornish and Clarke [8] posit that the application of Situational Crime Prevention theory must be predicated on the crime itself. As each crime is unique, the opportunity-reducing measures must also differ.

Some of the proposed analogies are more generic than specific to the cyber security domain. For the emotional side such as 'reducing frustrations and stress', 'avoiding disputes', 'reducing emotional arousal' can be mitigated by practice #5 (i.e. 'Anticipate and manage negative issues in the work environment') which is an overarching practice.

The technique of 'discouraging imitation' may be resolved by 'rapid repair' of damage inflicted on an organisation's information technology (IT) infrastructure, for example, the prompt repair of a defaced website [12]. This can be correlated with practice #15 (i.e. 'Implement secure backup and recovery processes').

Coles-Kemp and Theoharidou [14] recommend security usability and user participation in the risk analysis process as possible information security controls for 'reducing emotional arousal'. User participation in general would be beneficial, as the insider threat may be precipitated by security policies or controls that are misunderstood, poorly communicated or inconsistently applied [27], as well as by a lack of procedural fairness [40]. Hence, it may be useful to involve users in the entire information security life cycle from development to implementation. Security usability could be a step towards reducing the insider's negative response towards information security controls. Users should be able to figure out how to perform security tasks and they should be comfortable with the user interface [41]. As discussed earlier this was correlated with practice #5 (i.e. 'Anticipate and manage negative issues in the work environment').

Disciplinary processes [14] have been recommended as a means of 'neutralising peer pressure'. This may not be apt to this category – controls that identify elements of peer pressure would be more suitable. Social engineering is a virtual form of peer pressure. An insider may act as a social engineer and implement techniques like desk snooping or shoulder surfing to gather evidence with which to manipulate another insider as a means of identifying opportunities [31]. Hence, it is recommended that this technique be expanded so as to neutralise the effect of social engineers. This parallels practice #18 (i.e. 'Be especially vigilant regarding social media'). Practice #18 should also include a clause about social

engineers. While Practice # 1 (i.e. 'Consider threats from insiders and business partners in enterprise-wide risk') is also relevant, an insider may be influenced by 'outsiders' to commit maleficence.

E. Remove excuses

The 'remove excuses' category is accomplished by interventions that decrease the rationalisations that criminals may use to justify their behaviour.

In terms of 'setting rules', the techniques parallel practices #2 (i.e. 'Clearly document and consistently enforce policies and controls') and #9 (i.e. 'Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities').

In terms of 'posting instructions', e-mail disclaimers [15] are recommended as a comparable information security control, aside from the typical controls like information security policy. There is no equivalent practice found in the set of benchmark practices. However, the best practice of 'Issue rules of behaviour to all users and implement banners on all systems' proposed by Guido and Brooks [28] is appropriate to this subcategory.

Single sign-on [12] and 'a single point of reference for security' [14] have been proposed as information security controls to realise the 'assisting compliance' technique. Single sign-on is a process where an insider is given one password across all systems, which assists with usability and may be centrally controlled [42]. According to Kelly [43], having a single password has several advantages: users are unlikely to write it down or to constantly call the help desk to assist with the resetting of passwords. These advantages reduce the exposure of the insider to social engineering attacks. Single sign-on is considered to be an aspect of Centralised User Management [44]. This notion extends to the 'single point of reference for security' technique, which involves the centralised management of information security policies. Hence, 'Centralise Insider Threat Management' should be proposed as a best practice for 'assisting compliance'. While best practice #3 (i.e. 'Incorporate insider threat awareness into periodic security training for all employees') is absolutely essential in assisting compliance.

In terms of 'alerting conscience', the information security controls that are recommended include copyright protection [14], a code of ethics [14] and 'multi-level warning banners' [15]. Copyright protection is addressed by the 'setting rules' category. Practice #3 ('Incorporate insider threat awareness into periodic security training for all employees') would be an adequate way to alert conscience. However, Guido and Brooks' [28] best practice recommendation of 'Issue rules of behaviour to all users and implement banners on all systems' is more appropriate in this case.

A summary of the correlation of the practices per category is shown in fig 1. The cost-benefit type categories such as 'increase the effort', 'increase the risk' and 'reduce the reward' challenge the rational insider to calculate the net value of the crime. The 'remove excuses' and 'reduce precipitators' categories, on the other hand, are indirect controls that force an insider to consider a crime opportunity from a rational perspective without being driven by provocations or justifications. It is clear that the best practices focus more on the costs of cybercrime rather than the reducing the benefits of cybercrime.

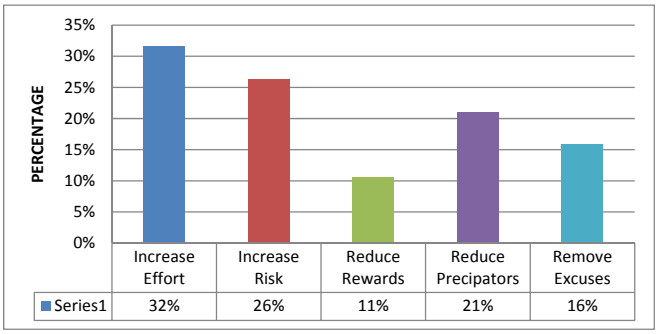

Figure 1. A Summary of percentage correlations of best practices per category

IV. DISCUSSION OF FINDINGS

In this evaluation, it was found that all 19 best practices derived from empirical research were satisfied by Situational Crime Prevention. This implies that Situational Crime Prevention is highly compliant with best practices. This implies that implementing Situational Crime Prevention is an example of best practice. However, the application of Situational Crime Prevention will require considering these best practices from an opportunity-reducing lens.

Some best practices were overarching and fitted more than one subcategory. Notably six of the 24 subcategories could not be linked with the best practices from Silowash et al. [27], while two of these subcategories were satisfied by one of the best practices proposed by Guido and Brooks [28]. However, four techniques were incomparable to a best practice. To be precise, 16.67% techniques were incomparable to a best practice. This clearly highlights the gaps where insider threat programmes are lacking. The category of 'reduce the rewards' category were found to be the most incongruent to best practices – specifically the sub-categories of 'concealing targets', 'removing targets' and 'disrupting markets'. The author provided recommendations in instances where there were no analogous best practices (see Appendix A).

In a similar study, Beebe and Roa [15] claim that the majority of security interventions are introduced to increase the perceived effort, while limited controls increase the perceived risk and reduce the anticipated rewards. Their study enumerated the number of techniques per category. In the current study, it is evident that the majority of best practices are aimed at increasing the effort and the increasing the risk of cybercrime, while the least number of practices are aimed at reducing the rewards of cybercrime. Removing the excuses (i.e. justifications) for maleficence is also found to be inadequate. In this evaluation it is clear the reducing the rewards associated with crime is a highly overlooked area with respect to best practices. This implies that even though the cost of crime is high, the rewards are still attractive.

V. CONCLUSION

This paper makes three significant contributions to the understanding and mitigating of insider threat. Firstly, the framework derived here may be used as a proactive mitigation strategy – it seeks to conceptualise the element of opportunity in terms of the insider threat. The framework may be used to implement information security controls that should empower information security administrators to prevent and possibly counteract the insider threat. Future research will involve evaluating the framework that was derived from opportunity-based criminology theories and best practices. Secondly, in the process of deriving the framework, several areas of potential research were revealed. The third contribution involves benchmarking best practices with respect to Situational Crime Prevention. This analysis has demonstrated the extensibility of the extant security best practices that could be enhanced with an opportunity-reducing dimension. The main contribution made by this article is the multidimensionality of the framework, which provides a new solution space in which to reason about mitigating insider threat from a best practices and an opportunity-reducing perspective.

REFERENCES

[1] SpectorSoft (2014) SpectorSoft 2014 insider threat survey. Available: http://downloads.spectorsoft.com/resources/infographic/spectorsoft-2014-insider-threat-survey.pdf (Last accessed 31 January 2015).

[2] PwC, CSO magazine, CERT® Division of the Software Engineering Institute at Carnegie Mellon University, and United States Secret Service (2014) US cybercrime: Rising risks, reduced readiness. Available: http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2014-us-state-of-cybercrime.pdf (Last accessed 31 January 2015).

[3] G. B. Magklaras and S. M. Furnell, "A preliminary model of end user sophistication for insider threat prediction in IT systems," Computers & Security, vol. 24, pp. 371–380, August 2005.

[4] E. E. Schultz, "A framework for understanding and predicting insider attacks," Computers & Security, vol. 21, pp. 526–531, October 2002.

[5] M. Maybury, P. Chase, B. Cheikes, D. Brackney, S. Matzner, T. Hetherington, B. Wood, C. Sibley, J. Marin, and T. Longstaff, "Analysis and detection of malicious insiders," MITRE CORP, Bedford, MA, 2005.

[6] M. B. Salem, S. Hershkop, and S. J. Stolfo, "A survey of insider attack detection research: beyond the hacker," in Insider Attack and Cyber Security. vol. 39, S. J. Stolfo, S. M. Bellovin, A. D. Keromytis, S. Hershkop, W. S. Smith, and S. Sinclair, Eds. New York: Springer, 2008, pp. 69–90.

[7] 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, pp. 1–9, January 2011.

[8] D. B. Cornish and R. V. Clarke, "Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention," in Theory for Practice in Situational Crime Prevention (Crime Prevention Studies). vol. 16, M. J. Smith and D. B. Cornish, Eds. New York: Criminal Justice Press, 2003, pp. 41–96.

[9] F. Farahmand and E. H. Spafford, "Understanding insiders: An analysis of risk-taking behavior," Information Systems Frontiers, vol. 15, pp. 5–15, March 2013.

[10] J. T. Wells, Principles of Fraud Examination. Hoboken, NJ: Wiley, 2008.

[11] M. Felson and R. V. Clarke, "Opportunity makes the thief: Practical theory for crime prevention," Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London Police Research Series Paper 98, 1998.

[12] R. Willison, "Understanding the perpetration of employee computer crime in the organisational context," Information and Organization, vol. 16, pp. 304–324, January 2006.

[13] R. Willison and M. Siponen, "Overcoming the insider: Reducing employee computer crime through situational crime prevention," Communications of the ACM, vol. 52, pp. 133–137, September 2009.

[14] L. Coles-Kemp and M. Theoharidou, "Insider threat and information security management," in Insider Threats in Cyber Security, C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, Eds. US: Springer, 2010, pp. 45–71.

[15] N. L. Beebe and V. S. Roa, "Using situational crime prevention theory to explain the effectiveness of information systems security," in SoftWars Conference, Las Vegas, Nevada, pp. 1–18, December 2005.

[16] N. L. Beebe and V. S. Roa, "Improving organizational information security strategy via meso-level application of situational crime prevention to the risk management process," Communications of the Association for Information Systems, vol. 26, pp. 329–358, March 2010.

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

[18] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," American Sociological Review vol. 44, pp. 588–608, August 1979.

[19] P. Brantingham and P. Brantingham, "Crime Pattern Theory," in Environmental Criminology and Crime Analysis, R. Wortley and L. Mazerolle, Eds. New York: Macmillian, 2008, pp. 78–93.

[20] R. V. Clarke, "Introduction," in Situational Crime Prevention: Successful Case Studies, R. V. Clarke, Ed. Guilderland, NY: Harrow and Heston, 1997, pp. 1–43.

[21] T. R. Smith and J. Scott "Policing and crime prevention," in Crime prevention, D. A. Mackey and K. Levan, Eds. 1st ed Burlington, Massachusetts: Jones & Bartlett, 2011, pp. 61–88.

[22] S. Hinduja and B. Kooi, "Curtailing cyber and information security vulnerabilities through situational crime prevention," Security Journal, vol. 26, pp. 383–402, June 2013.

[23] J. B. Barlow, M. Warkentin, D. Ormond, and A. R. Dennis, "Don't make excuses! Discouraging neutralization to reduce IT policy violation," Computers & Security, vol. 39, pp. 145–159, November 2013.

[24] R. Wortley, "A classification of techniques for controlling situational precipators of crime," Security Journal, vol. 14, pp. 63–82, 2001.

[25] R. Wortley, "A two-stage model of situational crime prevention," Studies on Crime and Crime Prevention, vol. 7, pp. 173–188, 1998.

[26] ISO/IEC 27002:2005 (2005) Information technology—security techniques—information security management systems—code of practice for information security management. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297 (Last accessed 1 September 2014).

[27] G. Silowash, D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall, and L. Flynn (2012) Common sense guide to mitigating insider threats, 4th Edition (CMU/SEI-2012-TR-012). Software Engineering Institute, Carnegie Mellon University. Available: http://www.sei.cmu.edu/reports/12tr012.pdf (Last accessed 31 January 2015).

[28] M. D. Guido and M. W. Brooks, "Insider threat program best practices," in 46th Hawaii International Conference on System Sciences (HICSS), Grand Wailea, Maui, Hawaii pp. 1831–1839, January 2013.

[29] W. A. Arbaugh, W. L. Fithen, and J. McHugh, "Windows of vulnerability: A case study analysis," IEEE Computer, vol. 33, pp. 52–59, December 2000.

[30] A. Jones and C. Colwill, "Dealing with the malicious insider," in 6th Australian Information Security Management Conference, Perth, pp. 87–100, December 2008.

[31] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," Information Security Technical Report, vol. 15, pp. 112–133, August 2010.

[32] M. Cappelli, A. P. Moore, T. J. Shimeall, and R. Trzeciak (2006) Common Sense Guide to Prevention/Detection of Insider Threats Available: https://www.cylab.cmu.edu/files/pdfs/CERT/CommonSenseInsiderThreatsV2.1-1-070118-1.pdf (Last accessed 10 May 2014).

[33] J. Myers, M. R. Grimaila, and R. F. Mills, "Towards insider threat detection using web server logs," presented at the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Knoxville, Tennesse, USA, 2009.

[34] M. Cappelli, A. P. Moore, and T. J. Shimeall (2006) Common sense guide to prevention/detection of insider threats Available: http://www.cert.org/archive/pdf/CommonSenseInsiderThreatsV2.11070118.pdf (Carnegie Mellon University, CyLab and the Internet Security Alliance, Tech. Rep.) (Last accessed 10 May 2014).

[35] N. P. Sheppard, S.-N. Reihaneh, and P. Ogunbona, "On multiple watermarking," in ACM Multimedia Conference workshop on Multimedia and security: new challenges Ottawa, Ontario, pp. 3–6, September-October 2001.

[36] J. Zhou and R. Deng, "On the validity of digital signatures," ACM SIGCOMM Computer Communication Review, vol. 30, pp. 29–34, April 2000.

[37] R. Walton, "Balancing the insider and outsider threat," Computer Fraud & Security, vol. 11, pp. 8–11, November 2006.

[38] P. H. Hartel, M. Junger, and R. J. Wieringa, "Cyber-crime science = crime science + information security," Centre for Telematics and Information Technology University of Twente, Enschede TR-CTIT-10-34, 2010.

[39] Isaca, COBIT five: for information security. USA: Information Systems Audit, & Control Association, 2012.

[40] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Roles of information security awareness and perceived fairness in information security policy compliance," presented at the 15th American Conference on Information Systems(AMCIS), San Francisco, California, 2009.

[41] A. Whitten and J. D. Tygar, "Why Johnny can't encrypt: A usability evaluation of PGP 5.0," presented at the 8th USENIX Security Symposium, Washington D.C., 1999.

[42] A. Pashalidis and C. J. Mitchell, "A taxonomy of single sign-on systems," in Proceedings of the 8th Australasian Conference on Information Security and Privacy (ACISP). vol. 2727, R. Safavi-Naini and J. Seberry, Eds. Wollongong, Australia: Springer-Verlag, 2003, pp. 249–264.

[43] M. Kelly (2002) Is single sign on a security risk? . Available: http://www.giac.org/paper/gsec/811/single-sign-security-risk/101711 (Last accessed 21 September 2013).

[44] S. Heilbronner and R. Wies, "Managing PC networks," IEEE Communications Magazine, vol. 35, pp. 112–117, October 1997.

APPENDIX A

Framework of Situational Crime Prevention: Towards Best Practices						
	Techniques					**No of Best Practices.**
Increase Efforts	*Target Hardening* Implement strict password and account management policies and practices **(#7)**	*Control of Access to Facilities* Institute stringent access controls and monitoring policies on privileged **(#10)**	*Screen Exits* Close the doors to unauthorised data exfiltration **(#19)**	*Deflecting Offenders* Beginning with the hiring process, monitor and respond to suspicious or disruptive behaviour **(#4)** Enforce separation of duties and least privilege**. (#8)**	*Controlling Tools* Enforce separation of duties and least privilege**. (#8)** Develop a comprehensive employee termination procedure. **(#14)** Filter Downloads of Illicit Tool$^{\beta}$s	*6*
Increase Risk	*Extending Guardianship* Monitor and control remote access from all end points, including mobile **(#13)**	*Assisting Natural Surveillance* Develop a formalised insider threat programme **(#16)**	*Reducing Anonymity* Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions **(#12)**	*Utilising Place Managers* Institute multiparty controls$^{\beta}$	*Strengthening Formal Surveillance* Institutionalise system change controls **(#11)** Establish a baseline of normal network behaviour **(#17)**	*5*
Reduce Rewards	*Concealing targets* Restrict public domain information (both internally and externally) $^{\beta}$	*Removing Targets* Implement Clear Desk policy and Clear Screen policies$^{\beta}$	*Identifying Property* Know your assets **(#6)**	*Disrupting Markets* Disrupt the markets that benefit from cybercrime$^{\beta}$.	*Denying benefits* Implement secure backup and recovery processes **(#15)**	*2*
Reduce Precipitators	*Reducing Frustrations and Stress* Anticipate and manage negative issues in the work environment **(#5)**	*Avoiding Disputes* Anticipate and manage negative issues in the work environment **(#5)**	*Reducing Emotional Arousal* Anticipate and manage negative issues in the work environment **(#5)**	*Neutralising Peer Pressure /Social Engineers* Consider threats from insiders and business partners in enterprise-wide risk **(#1)** Be especially vigilant regarding social media **(#18)**/ social engineers$^{\beta}$	*Discouraging Imitation* Implement secure backup and recovery processes **(#15)**	*4*
Remove Excuses	*Setting Rules* Clearly document and consistently enforce policies and controls **(#2)** Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities **(#9)**	*Posting Instructions* Issue rules of behaviour to all users and implement banners on all systems$^{\alpha}$	*Alerting Conscience* Issue rules of behaviour to all users and implement banners on all systems$^{\alpha}$	*Assisting Compliance* Incorporate insider threat awareness into periodic security training for all employees **(#3)**.		*3*
	Note: α Best Practices proposed by Guido and Brooks [28]. β Best Practices proposed by the author.					