Spyridon Samonas

Insider fraud and routine activity theory

Conference Item [eg. keynote lecture, etc.]

Insider fraud and Routine Activity Theory: A Thought Experiment

Spyridon Samonas
London School of Economics and Political Science

Abstract

This paper examines three scenarios of insider fraud based on empirical data from an upper-tier budget hotel in London, as part of a thought experiment on insider fraud. The scenarios are presented in the form of crime scripts and are reviewed under the theoretical framework of the Routine Activity Approach, which is widely used in crime science. The discussion that follows reflects on the theoretical underpinnings of the Routine Activity Approach and raises wider issues and concerns relating to information security, such as the adoption and implementation of controls against the insider threat.

Keywords: Insider threat, insider fraud, Routine Activity Approach, cyber-crime.

1. Introduction

In the past few years an assortment of government (Cappelli et al., 2009; Cummings et al., 2012) and not-for-profit organisations (CIFAS, 2012), as well as professional services firms (E&Y, 2012; PwC, 2012), have been releasing reports on information security or fraud that consistently highlight issues pertaining to computer-enabled fraud. According to PwC's (2012) latest Information Security Breaches Survey (ISBS) 53% of large and 12% of small organisations in a sample of 447 respondents reported an incident of theft or fraud involving computers between February-March 2011 and 2012. Confirming the popular assertion that insider fraud spiked during global financial downturn (2009), computer-enabled theft and fraud instigated by staff tripled between 2008 and 2010, and have remained at historically high levels

ever since despite substantial investments in security awareness training (*ibid*)[1]. In large organisations this type of fraud has doubled over the last two years, whereas in small businesses it is still relatively rare, albeit several times more common than in 2008 (*ibid*).

However, information security expenditure against insider fraud and theft remains a low priority. Analysing data from 743 Information Technology (IT) professionals, the recent report on insider fraud conducted by the Ponemon Institute (2013) shows that only 44% of them say their organization views the prevention of insider fraud as a top security priority; and that such perception has actually declined since 2011. In the latest Global Information Security Survey conducted by Ernst & Young (2012), out of the 1,836 respondents only 18% would be spending more on forensics and fraud support over the next year, 7% would be spending less, and a whopping 75% reported that they would be spending the same. Despite fraud featuring in the top-five of threats and vulnerabilities that have most increased the risk exposure of the respondents over the last year prior to the survey, it scores slightly below the middle of the list of top information security priorities over the next year (E&Y, 2012). In a similar vein, PwC's latest ISBS indicates that protecting other assets, such as cash, from fraud is the least important driver for information security expenditure – in fact, only 1% of the respondents considered protection from theft as the main driver (PwC, 2012).

Insiders are responsible for some of the biggest frauds ever recorded (NFA, 2012). Insider fraud is presumably costing organisations all over the world billions of US dollars in damages every year (Hoyer et al., 2012). One of the major difficulties of studying insider fraud is that it is underreported, and so its financial impact on organisations can only be loosely estimated (NFA, 2012). Consequently all relevant studies and reports are based on limited data, mostly because cyber incidents are usually not revealed when discovered, and so it is difficult to pinpoint their

[1] Throughout this paper *ibid* is used to direct the reader to the immediately preceding reference or footnote citation.

frequency, impact or root causes (CIFAS, 2012; Dekker et al., 2012). This not only adversely affects the credibility of insider fraud studies, but also impedes policy making at a national and international level.

Information security scholars and practitioners often argue that people are the first line of defense, but they are also are the main cause of security breaches (Angell and Samonas, 2009; Pironti, 2013; Samonas and Angell, 2010; Samonas, 2012). In this respect one of the biggest threats to information security is not the latest variation of some new malware that exploits technical vulnerabilities, rather, the malicious actions or inadvertent errors of trusted employees (Pironti, 2013) that operate 'inside the firewall' (Warkentin and Willison, 2009). This is mainly due to the fact that the controls and tools employed to protect organisations against external threats are inherently insufficient to address the insider threat (Schultz, 2002; Theoharidou et al., 2005). As Warketin et al (2009) note, the insider threat is, in many cases, disregarded "in a rush to protect the perimeter with ever-increasingly sophisticated perimeter controls". Being a subset of the insider threat, insider fraud is nowadays more relevant than ever (Hoyer et al., 2012), especially considering that people are becoming increasingly creative in the use of computers and networks as enablers for traditional fraud schemes (Lincke and Green, 2012; NFA, 2012).

This paper draws on the Routine Activity Approach to discuss three scenarios of insider fraud as part of a thought experiment in a budget hotel in London. Each of these scenarios is presented with the help of a 'crime script' (Willison, 2006; Willison and Backhouse, 2006), and refers to the manipulation of cash bookings within the hotel's reservations system.

2. Insider threat and fraud in cyber-crime

Dhillon et al (2004) argue that computer-related crime is a ubiquitous variant of all crime. In this respect, the term 'cyber-crime' is commonly used as an overarching concept that encompasses so many different actions and incidents pertaining to crime. Citing Newman (2009), Hartel et al (2010) provide a comprehensive definition

of cyber-crime as “behaviour in which computers or networks are a tool, a target, or a place of criminal activity”. Drawing on Furnell (2002), Yar (2005) suggests that cyber-crime can be distinguished into ‘computer-assisted’ and ‘computer-focused’ crime. The former type of crime includes ‘traditional crime’ that pre-dated the Internet and is still being committed with the help of computers (Hartel et al., 2010), such as fraud, theft or money laundering (Yar, 2005). The latter type refers to the ‘criminogenic’ features of computers and networks (Hartel et al., 2010), and specifically to those crimes that essentially have a parasitic relationship with technology and the Internet, such as hacking or viral attacks (Yar, 2005). From a legal standpoint, cyber-deception and theft that involves stealing money or property is only one of the categories of cyber-crime along with cyber-trespass, cyber-pornography and cyber-violence (Wall, D., 2001 cited in Yar, 2005).

The focus of this paper is on insider threat and insider fraud that are computer-assisted and can be classified under cyber-deception and theft. At a conceptual level, insider threats mainly refer to the intent of dishonest employees to commit some form of cyber-crime (Dhillon and Moores, 2001; Warkentin and Willison, 2009; Willison and Backhouse, 2006), as opposed to external threats that are attributed to hackers and viruses, or acts of God, such as flooding and earthquakes (Willison and Backhouse, 2006). Perhaps the first distinction between external and internal (or else insider) threats to computer systems appears the late 1980s when Denning (1987) formulated an intrusion-detection model to identify attempted system break-ins by outsiders, as well as abuse by insiders who misuse their privileges (Hartel et al., 2010).

Warkentin et al (2009) and Hartel et al (2010) suggest that there is a significant body of Information Security literature that deals with insider threats that essentially ranges from Denning’s (1987) seminal paper to the work of Dhillon, Backhouse, and most recently to Willison’s research on opportunities for computer crime and crime prevention techniques (Dhillon, 1999; Dhillon and Moores, 2001; Dhillon et al., 2004; Warkentin and Willison, 2009; Willison, 2003, 2006; Willison and Backhouse, 2006). Loch et al (1992) develop a taxonomy of computer system threats based on the

distinction between external and internal threats. Each of the two main types of threats is split into human and non-human, which in turn are further branched into intentional and accidental. An updated taxonomy developed by Warkentin (1995) includes a distinction between low-grade and high-grade threats, with the latter being a malicious individual or organisation that seeks to exploit vulnerabilities and maintain intrusions towards maximising long-term gain (Warkentin and Willison, 2009).

In an attempt to assess the effectiveness of ISO17799 on insider threats, Theoharidou (2005) presents an overview of the different classifications of insider threats that appear in the relevant literature, and which are based on a variety of criteria, such as the type of access that the insider has or the aims, intentionality and technical expertise of the insider. As with much of the terminology examined in information systems research, there is an abundance of definitions attached to insider threat (Cappelli et al., 2009; Cummings et al., 2012; Schultz, 2002; Silowash et al., 2012; Theoharidou et al., 2005; Willison, 2006). Quoting Greitzer et al (2010), Hoyer et al (2012) consider insider threat as the departure of human behaviour from compliance with security policies, irrespective of whether this is the result of malice or simply disregard for said policies. However, Cappelli et al (2009) provide a more elaborate definition that is both sufficient and suitable for the purposes of this paper:

"A malicious insider threat to an organization is a current or former employee, contractor, or other business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems."

It appears that Capelli et al (*ibid*) have truly captured the changing character of information security in the above definition. Over the past few years the concept of the 'insider' has become somewhat restricted, and in many cases irrelevant due to the fact that privileged access to the assets of an organisation is given to employees,

volunteers, consultants and contractors (Brancik, 2007; NFA, 2012; Ponemon, 2013). Access is also given to business partners or fellow members of a strategic alliance, whereas contractors nowadays include employees of a Cloud Service Provider, which is a fairly new and different contractual relationship compared to outsourcing (Hartel et al., 2010). Thus a more sophisticated and prudent alternative to the term 'insider' would be a '(person with) specialised access' (*ibid*).

In fact, insider threat comprises Intellectual Property theft, IT sabotage, fraud, espionage, and accidental insider threats (Silowash et al., 2012). The difference between fraud and theft within this classification of insider threats is relatively straightforward. However, fraud and theft are two terms that are often misused and treated as synonymous, even though they are not. In the UK legislation, there is a clear line between theft and fraud. Under the Theft Act 1968, a person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it, either with a view to gain or for the thief's own benefit. The Fraud Act 2006 eventually repealed certain provisions regarding theft of property by deception, which essentially formed the basis of the revision of the Theft Act in 1978. According to the Fraud Act 2006, there are three main types of fraud; namely fraud by false representation, failing to disclose information, and abuse of position. The latter type, which is directly pertinent to the scope of this paper, refers to breaches where a person dishonestly abuses a position of employment to make a gain for him/herself or another; or to cause loss to another or to expose another to a risk of loss. Interestingly, the law may regard that a person has abused his/her position, even though his/her conduct consisted of an omission rather than an act of commission.

In the U.S., the first law on computer fraud was the Computer Fraud and Abuse Act of 1984, which evolved into the Title 18 U.S. Code, Section 1030 federal law that governs computer-enabled fraudulent activity. Section 1030 punishes any intentional, unauthorized access to 'protected' computers, namely computers that are used by financial institutions, the federal government, or in foreign or interstate commercial and communication activities (Brancik, 2007).

Following a distinction similar to the one applied to threats, fraud can be divided into external and internal fraud, depending on whether or not the perpetrator is an employee (Lincke and Green, 2012). Insider fraud is generally considered a subset of the insider threat problem (Hoyer et al., 2012). The underlying theme in many definitions of insider fraud (ACFE, 2012; Cappelli et al., 2009; Cummings et al., 2012; Lincke and Green, 2012; Silowash et al., 2012), is the abuse of trust or position for personal gain as illustrated in the Fraud Act 2006. Such abuse can take different forms, such as corruption, asset misappropriation, and financial statement fraud, and implies that the insider has access to the organisation's assets and systems, and even the ability to influence the outcomes of organisational processes (ACFE, 2012).

With the use of IT as a fraud enabler in mind, Silowash et al (2012) define insider fraud "an insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to an identity crime (e.g., identity theft or credit card fraud)". In a similar vein, Cummings et al (2012) consider a malicious insider as capable for disrupting operations, corrupting data, exfiltrating sensitive information, or generally compromising an IT system, causing loss or damage.

The next sections presents an overview of the Routine Activity Approach, which is the primary theoretical perspective used in this research.

3. The Routine Activity Approach

The Routine Activity Approach (RAA) is a sociological theoretical perspective that was developed by Lawrence Cohen and Marcus Felson in their effort to explain criminal trends in the United States between 1947 and 1974 as a result of changes in labour force participation and single-adult households (Cohen and Felson, 1979). RAA has been instrumental in informing Situational Crime Prevention (SCP) techniques (Theoharidou et al., 2005; Willison, 2006; Willison and Backhouse, 2006), and has been widely used in Crime Science – which, in contrast to Criminology,

studies incidents and the short-term motives of offenders, and not their personality or social background (Hartel et al., 2010; Theoharidou et al., 2005).

The theory suggests that the organisation of routine activities in everyday life constructs 'variable opportunity structures for successful predation' (Yar, 2005). The conceptual framework of the theory consists of 'three minimal elements of direct-contact predatory violations' (Cohen and Felson, 1979), which were originally conceived to address violent assaults, or crimes where one person takes or damages the property of another (Willison and Backhouse, 2006). The three elements involve (1) a potential offender, (2) a suitable target and (3) the absence of capable guardians (see Fig. 1). These elements could be considered as three sufficient and necessary conditions for a crime to be committed, since it is their spatial and temporal convergence that gives rise to opportunity for crime. By implication the theory implies that a crime does not occur when there is lack of even one of these elements (*ibid*).

Fig. 1: Application of Routine Activity Theory in Crime

Source: (Choo, 2011)

Yar (2005) presents a succinct description of the core assumptions of RAA:

> *"Thus, at a general level, the theory requires that targets, offenders and guardians be located in particular places, that measurable relations of*

spatial proximity and distance pertain between those targets and potential offenders, and that social activities be temporally ordered according to rhythms such that each of these agents is either typically present or absent at particular times."

One other important aspect of RAA is the assumption that there are always motivated offenders at hand inclined to commit crime should a favourable opportunity present itself. Rational choice theory has clearly influenced RAA, which also assumed that motivated offenders carry out a risk assessment prior to committing a crime by calculating the anticipated benefits, costs and risks involved (Choo, 2011; Willison and Backhouse, 2006; Yar, 2005). For instance, the suitability of a target can be estimated according to its fourfold constituent properties that are usually rendered in the acronym VIVA (Value, Inertia, Visibility and Accessibility) and that refer to two of the elements of RAA (Hartel et al., 2010; Yar, 2005), namely the lack of capable guardians and finding a window of opportunity to strike at a target.

Quoting Tseloni et al (2004), Yar (2005) defines guardianship as 'the capability of persons and objects to prevent crime from occurring'. In RAA, the role of guardians is crucial, either through a direct intervention that acts as a deterrent, or by merely staying in close proximity to the target, thus reminding the potential offender that someone is watching vigilantly (*ibid*). In the context of computer-assisted cyber-crime, capable guardians usually take the form of internal controls. Indeed, the different kinds of controls that can be employed to safeguard organisations against insider cyber-criminal activity have been extensively discussed in the information security literature (Willison and Backhouse, 2006). Dhillon et al (2001) make a distinction between technical, formal and informal controls drawing on the TFI model (Samonas, 2012). Technical controls are the most traditional and mostly address issues pertaining to access management (Dhillon and Moores, 2001; Willison, 2006). Formal controls usually involve rule-following, and may relate to regulatory compliance as well as to compliance with prescribed organisational processes (*ibid*) and information security policies. Finally, informal controls mainly refer to the provision of an all-round information security education and to the

cultivation of a security culture, within which obedience is valued and incident reporting is positively encouraged (Furnell and Thomson, 2009). Dhillon et al (2001) stress the importance of striking the right balance between controls while noting that in many cases computer-assisted crimes occur when a current employee circumvents existing controls.

Quite often, organisations fall victims of their employees because they fail to take information security seriously, and so in this way they ultimately create security loopholes that are ready to be exploited by insiders. The following table summarises the eight factors that, according to Willison et al (2006), lead to the formation of opportunity structures for crime in organisations (see Fig. 2).

RAA operates at a societal or organisational level and one of the main question that it poses is how to minimise opportunities for crime within the context of the routine activities of potential offenders (Hartel et al., 2010; Lincke and Green, 2012). Hartel et al (2010) propose the adoption of five principles of opportunity reduction, which essentially refer to the three main elements of the theory; some of these principles also appear in the work of Choo (2011) and Lincke et al (2012). The principles include the increase in the effort and risks of crime, the reduction of the potential rewards and the provocations that invite criminal behaviour, and finally the removal of excuses for criminal behaviour.

Factors leading to deficient security	**Description**
Organisational complacency towards IS security	Failure of some organisations to implement even the most basic controls, leaving their systems vulnerable
Erroneous perceptions of IS security risks	Measures may be implemented to address risks that in reality are relatively minor, at the expense of those areas where the risks are high but receive little attention
Technical perspective of IS security	The 'distorted image' of security held by managers is often equated with a myopic understanding of the problem area and how it should be addressed

Funding of IS security	The technical perspective often leads to a poor return on investment owing to the inability of those responsible for security to understand and address the necessary and related managerial aspects of security (e.g. implementing a security policy), while they concentrate too heavily on technical safeguards
The inter-related nature of security controls	Security is very much like a house of cards: inadequate consideration for one area will impact on another, possibly creating those conditions that help to form an opportunity
Implementation of inappropriate controls	If the safeguards introduced provide an inadequate level of security then the IS will be left vulnerable. However, the same is also true if the safeguards are perceived by staff as unworkable in the organisational context
Safeguard implementation	Poor implementation can negate any improvements in security for which a safeguard was designed
Compliance reviews	Many organisations fail to check whether their controls are operating as intended. As a consequence those safeguards which are failing to perform leave an IS vulnerable

Fig. 2: Opportunity formation through deficient security

Source: (Willison and Backhouse, 2006)

Finally, in terms of assessing its practical contribution, RAA as a subset of SCP has proven to be suitable for addressing the insider threat (Willison, 2006). Choo (2011) asserts that RAA is an all-encompassing theoretical lens for cyber-crime studies. However, Yar (2005) argues that, while appropriate for the use of computer-assisted cyber-crime, RAA falls short in explaining issues that pertain to computer-enabled cyber-crime due to the novel way in which socio-interactional activities take place in the virtual environments of cyberspace. Indeed, despite attempts to enhance the conceptual framework of the theory so that it addresses contemporary aspects of crime by adding new elements, such as the 'intimate handler' or the 'crime

facilitators or dis-inhibitors' (Willison and Backhouse, 2006), RAA seems to be fully applicable only to terrestrial cyber-crimes.

4. Empirical findings

This research paper reflects on empirical data that were gathered by the author between November 2012 and January 2013, during his assignment as Deputy Front-of-House Manager in a 160-bed 'upper-tier' budget hotel in London (Roper and Carmouche, 1989). The data refer to standard organisational processes and regulatory compliance procedures, and were used to construct three hypothetical cases of insider computer-assisted fraud. The three cases were emulated on the hotel's computerised reservations system operating in the training mode. The result was that all three fraud schemes were viable.

Each scenario refers to hotel bookings paid in cash and on the day of check-in. It is assumed that the offender is an insider with advanced user privileges higher than say a receptionist, for instance a Deputy Front-of-House Manager, Shift Leader, or Duty Manager. Also, one major underlying assumption that is fairly reasonable to make is that accountants and internal auditors are not expected to access any particular bookings or the user logs attached to them for that matter, with one notable exception: when bookings have either a positive (guest or group has underpaid), or a negative (guest or group has overpaid) balance in the respective ledger accounts upon checkout. This is a quite common phenomenon considering the sheer volume of bookings placed with a hotel, and could be called the 'zero balance trap'. The bookings outside the 'zero balance trap' turn up in many reports as outstanding, and so tampering with their accounts is extremely likely to be detected – unless, of course, the 'guardians' have been compromised in some way and there is widespread collaboration and conspiracy for fraud inside the organisation.

The presentation of the findings can be broadly classified as a thought experiment, in that it is a narrative of an experimental situation that is explicitly constructed in

order to destroy or challenge the current paradigmatic position, or to support an emerging paradigmatic position (Introna and Whitley, 2000). Because of obvious moral and ethical concerns (*ibid*) the three scenarios discussed here were only emulated and not attempted in practice. They only aim at challenging the existing organizational paradigm of the hotel and its current *modi operandi* with regard to the creation of security loopholes through deficient information security.

The detailed activity entailed in each scenario is presented with the help of a crime script, which is based on the fundamental premise that any crime consists of a series of stages (Willison and Siponen, 2009). The separation of a crime into distinct stages seems to have considerable analytical utility in the case of computer-assisted crimes. More specifically, criminal activity can occur at the input, throughput or output stages (Dhillon, 1999; Dhillon et al., 2004). Input crimes are committed when a rogue employee enters false or manipulated information into a computer system. Throughput crimes epitomize the 'low and slow' approach (Cummings et al., 2012), or what is widely known as 'salami slicing' (Dhillon, 1999), which refers to small amounts being taken off a large number of accounts and then directed to a separate account that belongs or is controlled by the offender. These crimes are committed throughout a prolonged period of time, during which the offender tries to avoid raising any eyebrows with his actions and stays 'below the radar'; hence, the 'low and slow' attribute. Finally, output crimes are relatively unsophisticated and committed by concealing or misusing bogus inputs, or by postponing detection (*ibid*). Interestingly, manifestations of almost all of the aforementioned categories of crime (input, throughput and output) appear in each of the three crime scripts that are examined in this paper.

Crime scripts focus on the operational aspects of crime and they were originally developed to help in the design of more sophisticated SCP techniques (Willison and Backhouse, 2006; Willison and Siponen, 2009). By analysing the flow of criminal thought and activity, crime scripts can help policy makers and practitioners identify blind spots and crystallise patterns of malicious actions, in an effort to develop more robust and effective internal audit controls. Within the context of RAA, crime scripts

can pinpoint flaws in existing security control measures, help compile a list of potential targets; but most of all, they can examine a wide range of opportunities for fraud that vary in sophistication, risk and difficulty of execution. It is a pragmatic way of looking at fraud as it focuses on the conception and execution of a fraud scheme from the perspective of the offender. The format of each crime scripts presented here follows the general script that appears in the work of Willison (2006) and Willison et al (2006); the first column represents the stage in the script, and with each stage comes a corresponding behaviour.

In terms of the technological aspect of the scenarios, the computerised reservations system used in the hotel is a widely used, scalable system that can cover the whole spectrum of the hotel industry, and therefore, it can also accommodate the needs of smaller and/or lower-end hotel units or hotel chains. However, customizing the software to suit the needs of a large, but low-end, hotel was a highly demanding task that appears to have created all sorts of complications in the overall use of the system. Most notably, it seems that the alignment of the business processes of the hotel together with the processes inscribed in the system by its developers requires considerable effort on the part of the hotel staff, and the top management in particular. Although standard hotel operations, such as the back- and front-offices, are indeed very similar in most hotels, they are not and they cannot be exactly the same across the entire hotel industry. Before going 'live', the particular system underwent extensive customization according to the special needs of the hotel in order to be brought to an operable state; that is, in a position to handle the main bulk of the hotel's operations.

During the customization process, many features of the system were deemed unnecessary and they were, therefore, disabled. Some of the features that were retained and used proved to be particularly helpful in the day-to-day operations of the hotel. For example, the reception staff can simultaneously check in and out a group of guests on the system, provided that all the members of the group arrive and depart together. Indeed this has saved much time and effort, since in the previous reservation system every single guest of the hotel had to be individually

checked in and out, regardless of whether they were part of a group reservation or not.

Scenario no.1

The first scenario is rather simple and, to a certain extent, naïve in conception; and it entails a high level of risk of discovery for the perpetrator. It revolves around the use of reverse or adjustment postings in guest ledger or Accounts/Receivable (A/R) accounts, with the latter being the accounts primarily used for group bookings. Certain groups pay any outstanding balances, sometimes after their check out day, depending on the arrangements they have with the hotel - hence, the need for an A/R account.

According to the scenario, the offender manipulates the input of cash payments they receive for bookings, whilst trying to withhold, rather than hand to the customer, any receipts automatically generated by the computerised reservations system upon settling the payment. In that way, the payment is noted on the system in the first place, and then reversed or partially adjusted, so the offender can fairly easily pocket the cash that is left outside the safe deposit box.

For instance, a guest pays £100 in cash for a booking. The offender takes the payment settles it on the system and then fully or partially undoes the settlement of the payment, as if no payment was received for that particular booking. If the customer does not ask for a receipt, they cannot prove that they have paid in cash and may be asked to pay again! The major drawback of this scenario is that reverse and adjustment postings, also known as negative postings, always appear in banking reconciliation and the end-of-day (night audit) sequence reports that run early in the day, so that the system can generate charges for all in-house guests and roll out to a new ‘business day’. Negative postings can only be performed by users with advanced privileges and usually raise a red flag. Consequently, in that case, middle and senior management and accountants can enquire why the postings were made and who authorised them. In view of the above, the crime script would read as follows (see Fig. 3).

Stage	Script Action	Situational Control
Preparation	Deliberately gaining access to the organisation	Pre-employment screening
Entry	Authorised as employee	-
Pre-condition	Look for cash bookings Advanced user privileges	Better screening of who gets advanced privileges and why. Periodic review of all users with high user privileges.
Instrumental pre-condition	Process check-in of cash bookings by the offender	Segregation of duties; staggered breaks
Instrumental initiation	Access the reservations system; receive cash payment	Password use for performing certain actions in the system
Instrumental actualization	Apply negative posting	Password required for performing this action; system prompting the user to indicate authoriser
Doing	Keep the amount of cash that is not going to be settled on the system	-
Post-condition	Put the amount of cash settled on the system (if any) in an envelope and in the hotel's drop safe	Amount has to be double-checked and signed for by a colleague
Exit	Log out of system	Check the negative postings report in the end-of-day sequence; access the user log of the booking in question

Fig. 3: Crime script for negative postings scenario

Adapted from: (Willison and Backhouse, 2006)

Scenario no.2

The second scenario is based on the manipulation of room rates and applies only to those bookings that are not automatically placed on the system through an Online Travel Agent (OTA). It has moderate risk and medium to high financial reward. Upon placing a booking on the system, the end-user must select an agent to designate where the booking comes from and then a rate for the booking; so that the guest is charged for the nights they stay in the hotel. The rates are given 'code names' that summarise their properties; for example, the rate code 'HOTELCOM5' may reflect the special rate that a hotel gives to bookings coming from Hotels.com for stays over

5 nights. In this case, the agent would be the OTA named Hotels.com. Each agent can be associated with an assortment of rate codes that reflect the base rate, as well as a variety of other rates for different periods of time and other special circumstances (for example, special discounts for Bank Holiday weekends etc). Selecting the right agent and rate is essential, since the agent field is used to calculate the revenue that comes from a particular agent, and by extension, the commission that the hotel will need to pay to them. In short, a single rate code associated with a particular agent gets attached to every booking.

Rate manipulations works as follows. Prior to check-in, end-users with advanced privileges can give discounts to the selected rate of any booking, either as a percentage of the nightly rate or as a set amount. The system then prompts the end-user to indicate who authorized this discount and what for. For example, if the nightly rate is £100, a privileged end-user can give a 100% discount for every night included in this booking, as long as they indicate who was the more senior member of staff that granted them the right to do it and for what reason. The offender can make considerable profit; if they receive a payment in cash on the day of check-in, give a hand-written receipt instead of the standard one that is generated by the system, keep the cash, discount the rates and then settle an amount lower than the original balance, they get away with pocketing the difference. So, even if the guest is given a receipt, the offender can still commit the fraud, unless the receipt has been generated by the system. Insufficient controls can cost a lot of money to the hotel in this scenario. One major problem with this fraud is the commission paid to agents. If the offender is giving discounts to non-direct bookings, namely to bookings that have been made through OTAs, then there will be a discrepancy between the commission that the hotel was expecting to be invoiced for and the actual amount of money they are going to be invoiced by OTAs, which will be higher – so, the hotel suffers from the cash theft, but also from the loss of revenue, which is sometimes difficult to pinpoint.

Another version of rate manipulation that is even more difficult to detect also occurs when privileged end-users change the ‘room type to charge’ field on a booking; and

so, instead of double or triple, they charge the guest a single room, without them knowing. In this context, the crime script for the second scenario is the following (see Fig. 4).

Stage	Script Action	Situational Control
Preparation	Deliberately gaining access to the organisation	Pre-employment screening
Entry	Authorised as employee	-
Pre-condition	Look for cash bookings Advanced user privileges	Better screening of who gets advanced privileges and why. Periodic review of all users with high user privileges.
Instrumental pre-condition	Check for cash booking not associated with OTAs; process check-in of these bookings	-
Instrumental initiation	Access the reservations system	Password use for performing certain actions in the system
Instrumental actualization	Apply discount to nightly rates; receive cash payment	Password required for performing this action; system prompting the user to indicate authorizer; senior staff has to approve the discounts
Doing	Keep the amount of cash that is not going to be settled on the system	-
Post-condition	Put the amount of cash settled on the system (if any) in an envelope and in the hotel's drop safe	Amount has to be double-checked and signed for by a colleague
Exit	Log out of system	Random checks for irregularities in rates or OTA invoices

Fig. 4: Crime script for rate manipulation scenario

Adapted from: (Willison and Backhouse, 2006)

Scenario no.3

The third scenario is the most sophisticated of the three, has relatively high rewards and a moderate to low risk, and is based on the routing of charges. Routing refers to the ability to route charges from one room to another for certain (or all) charges in a

given period. Charges can be automatically separated on a guest's folio, or can be moved off the guest's folio altogether to another guest room or a Posting Master (PM). The idea behind this scenario is relatively more complex. A privileged user roots (transfers) the charges of one room to a PM (virtual) room. The guest makes a payment in cash and gets a receipt for the payment. Then, the offender pockets the cash and either applies a negative posting to the PM room, or leaves the PM as is with an outstanding balance. PM rooms are mostly used as 'buffers' for group bookings in conjunction with A/R accounts – charges are being temporarily transferred to them for a variety of legitimate reasons that facilitate the day-to-day business; in this respect, it is normal for them to carry occasional negative postings and/or outstanding balances. So, no red flags there. The existence of a rooting is indicated in the booking profile and it is clearly visible to anyone who is accessing the booking for whatever reason. However, it can be deleted as easily as it is established, after the fraud has come full circle. The crime script for the third scenario should read as follows (see Fig. 5).

Stage	**Script Action**	**Situational Control**
Preparation	Deliberately gaining access to the organization	Pre-employment screening
Entry	Authorised as employee	-
Pre-condition	Look for cash bookings Advanced user privileges	Better screening of who gets advanced privileges and why. Periodic review of all users with high user privileges.
Instrumental pre-condition	Check for cash bookings	-
Instrumental initiation	Access the reservations system	Password use for performing certain actions in the system
Instrumental actualization	Set up routing to PM room; receive cash payment	Password required for performing this action
Doing	Keep the amount of cash that is not going to	-

	be settled on the system	
Post-condition	Put the amount of cash settled on the system (if any) in an envelope and in the hotel's drop safe; delete routing	Amount has to be double-checked and signed for by a colleague
Exit	Log out of system	Random checks for irregularities in routings

Fig. 5: Crime script for routing scenario

Adapted from: (Willison and Backhouse, 2006)

Drawing on RAA, the following section discusses the findings from the three crime scripts that were presented in the current section and raises wider issues and concerns relating to information security.

5. Discussion and analysis

Notwithstanding their recognised contribution to the improvement of crime prevention, RAA, SCP and all the other theoretical frameworks that are adopted in cyber-crime science (Hartel et al., 2010) are inherently insufficient to address fraud fully, which is ultimately a complex social phenomenon that often unfolds in the most unimaginable ways (Kroll, 2012). Theory involves categories, and categories lead to a permanent production of blind spots (Luhmann, 2002). However, certain important issues and concerns are raised even from a purely theoretical consideration of insider threat and fraud, and despite the fact that the scope of this paper is rather limited to computer-assisted cash fraud in a hospitality environment.

The thought experiment presented in this paper shows an assortment of possible and, most worryingly, feasible cash fraud schemes in a hospitality environment. The findings are in line with, and supported by, much of the literature on insider threat and fraud. An indicative example of this is the recent study on cyber fraud in the U.S. financial services sector conducted by the Computer Emergency Response Team (CERT) of the Insider Threat Center at Carnegie Mellon University (Cummings et al.,

2012). The following list integrates the main points that can be derived from the thought experiment with most of the findings of the CERT study (*ibid*):

- Scenarios no. 2 and 3 favour a 'low and slow' approach, which can lead to more damage and escape detection for longer;
- All scenarios are not very technically sophisticated. No programming or hacking skills are necessary, besides an in-depth knowledge of the business model of the organisation, as well as a good grasp of certain aspects of the logical model of the computerised system;
- The most serious threat comes from users with privileged access and/or a managerial position. Managers have the power to alter business processes and manipulate subordinate employees;
- In scenarios no. 2 and 3, fraud can be uncovered only by random audits, a co-worker suspicion, or a customer complaint (when a customer files a formal complaint for not getting a receipt for their payment).

Following the examination of each scenario and its respective crime script under the theoretical lens of RAA, a few points need to be raised further. Whilst it is fairly reasonable to assume that there always will be motivated offenders in organisations, the same does not apply for suitable targets, namely opportunities for crime, or absent guardians. The crime scripts suggest that opportunities for insider fraud relate to the disharmonies often found in the technical, formal and informal aspects of the systemic integrity of an organisation (Samonas, 2012).

Technical opportunities typically arise from lax rules or inconsistencies in the computerised bureaucracy of information systems (Angell and Samonas, 2009; Samonas and Angell, 2010; Samonas, 2012). Looking at the hospitality industry in particular, modern state-of-art hotel revenue management systems can adequately manage enormous volume of reservations and daily financial transactions, as well as multiple points-of-sale. However, they simply cannot prevent fraud at all levels. Hotels can easily get bogged down in customising the Commercial-Off-The-Shelf (COTS) software they choose to use, and which is purportedly scalable to suit any size hotel and serve all segments of the market. Yet, the flexibility, modularity, and

scalability of this COTS software can turn from a promised business strength to an elusive weakness.

Actually, it is not that rare for a poor or incomplete customisation and configuration of the software to happen, since it is an activity usually performed in haste, and in certain cases, with minimal resources to hand (Samonas, 2012). In this respect, opportunities for crime arise from the technical deficiencies that are created when something falls through the cracks during the extensive customisation of the software. For example, the easiness with which routing is created and then deleted to cover the tracks of the fraudster in scenario no. 3 is clearly the result of poor configuration of the system.

Quite evidently, opportunities at the formal level of the organisation refer to organisational procedures and processes; but also to rule following and compliance – an issue that touches upon the creation of opportunities for crime at the informal level. One fine example of this category of opportunities is the management of access control. Besides its purely technical considerations, the management of end-user privileges is an extremely delicate and important matter. Privileges tend to accumulate over time as employees change departments and accept new job responsibilities (Cummings et al., 2012).

In scenario no. 1, negative postings can only be performed by end-users who have been granted advanced use privileges, not by receptionists or other temporary employees. This is a fair and appropriate measure, which, however, can be subverted when managers bypass the standard procedure for granting higher access privileges to some of their employees. Busy managers can easily fall into the trap of disclosing their password to a subordinate employee who is willing to take some of their manager's workload. Having in mind what is best for the day-to-day business and/or their partial relief from certain repetitive tasks, managers may abuse their power and make all the necessary arrangements for an end-user to be given higher privileges, without taking into account what are the standard requirements in such a case. Adding another aspect to this, Dhillon et al (2001) note that employees from

certain cultures may be keen on putting faith in personal relationships at the expense of company procedures.

But even when privileges are granted for all the right reasons, it is imperative for the organisation to establish periodic checks and reassessments on how these privileges have been allocated and are being used. Otherwise, the effectiveness of the measure will be incomplete and will allow malicious employees to take undue advantage of their position. So, when a crime occurs, the guardians are not necessarily absent, as RAA assumes; it is quite possible that the guardians are present, but blind. The blindness of the guardians primarily stems from the organisational complacency towards information security or even the erroneous perceptions of information security risks (Willison and Backhouse, 2006); however, this blindness may also be the result of an orchestrated insider attack against the organisations nerve centre. The 'zero balance trap' is an indicative example of the former case. In their effort to battle through augmented daily workloads, organisations often overlook certain controls, thus allowing the rise of opportunities for crime. The latter case is extremely serious and may involve elements of industrial espionage and/or sabotage (Kroll, 2013).

The revisiting of end-user privileges also brings about issues pertaining to trust – which opens up an array of possibilities for insider fraud. Whenever computerised bureaucracy is hindering certain aspects of the normal operation of an organisation, trust is instrumental in providing employees with discretionary powers to act independently and improvise in order to sufficiently address 'irregular' situations (Angell and Samonas, 2009; Samonas and Angell, 2010; Samonas, 2012). However, trust is a double-edged sword (Samonas and Angell, 2010; Samonas, 2012), especially if it is granted without adequate supervision (Dhillon and Moores, 2001). In scenario no. 1, for instance, a Front-of-House manager could fairly easily abuse the powers entrusted to him by defrauding through 'salami slicing'; namely, by applying negative postings to certain cash bookings, and then signing off these postings as necessary, making sure to back everything up with a fictional story about a 'difficult' guest. In the context of a computer crime case study, Dhillon et al (2004)

advocate the merits of trust and argue that when trust is replaced by control, the organisation will experience some sort of disruption.

The various internal controls and other audit mechanisms that are used in modern organisations can achieve their potential only when organisations realise the inter-related nature of controls (Willison and Backhouse, 2006), and strike the right balance between technical, formal and informal controls (Dhillon and Moores, 2001; Dhillon et al., 2004). To this end, almost a decade ago Dhillon et al (2004) were calling for more pragmatic measures to be built on good management practices and trust-based communication, which encourages individuals to take responsibility for their actions. In the past 15 years the relevant literature has provided a variety of recommendations for the prevention, detection and deterrence against insider threat and insider fraud. To a greater or lesser extent, these recommendations have been gradually integrated into information security standards, such as the International Organization for Standardization (ISO) and International Electrotechnical Commission's (IEC's) standard 27002 (ISO/IEC 27002), the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, or the CERT Resilience Management Model (CERT-RMM). In the 'Common Sense Guide to Mitigating Insider Threats', Silowash et al (2012) present 19 best practices to mitigating insider threats and take the painstaking effort to map these practices to the ISO/IEC 27002, the NIST SP 800-53 and the CERT-RMM.

However, despite all this knowledge and expertise on information security, E&Y speaks of a great gap between the actual and the desirable levels of security in modern organisations, and identifies the high velocity of change in cyber-crime as one of the main cause for this, among others. In order to understand fraud and take meaningful measures to prevent it, security professionals and policy makers need to get into the offender's shoes, as much as possible – they need to think like an offender. Fraudsters are usually creative when it comes to plotting a fraud, and they generally possess an abundance of skills, knowledge, resources, authority, and motive (Warkentin and Willison, 2009). This is vividly illustrated in ancient Greece. A plethora of references that revolve around Metis, the Goddess of wisdom and

cunning thought, can be found in Greek mythology; and so, fraud has been around for thousands of years. In the concept of metis, which was heavily practiced by mortals and Gods, ancient Greeks encapsulated “a form of intelligence that applied to a wide range of practical activity”; they used the very same term to express “intellectual behaviors, combining flair, savvy, alert anticipation, flexibility of mind, feint, resourcefulness, prudence, a sense of opportunity, diverse skills and patiently acquired expertise” (Klein, 1986).

In the case of computer-assisted insider fraud, insiders are not only aware of the policies, procedures, and technology of their organization; they are also aware of the organization’s vulnerabilities at a technical, formal and informal level (Hartel et al., 2010; Silowash et al., 2012). Information security professionals and policy makers are struggling to think like a fraudster, when the reverse is true; motivated offenders are more likely to be successful when trying to think like law enforcers. And there seems to be a lag between the manifestations of these two lines of thought; fraudsters are not always smarter, but they are definitely faster in keeping up with constant change, in changing their colours and blending in with the environment – and in this respect, they should be treated as leaders rather than followers.

6. Conclusion

Connoly et al (Connolly and Haley, 2008) have argued that the hospitality firm of the future should be “flexible, agile, and aggressive by reducing bureaucracy and formalization and by being more open to risk and innovation”; this was, indeed, excellent advice for any organization, not just hospitality firms. Five years later, this sounds like wishful thinking. Despite the bleak picture that is being painted by external and internal threats, complacency about security is gaining momentum (Hartford, 2012; Kroll, 2012). Some organizations are clearly striving for failure (Ciborra, 2000, 2002), thinking that they are covering all the bases, when, in fact, they cover relatively few. They are shortsighted and thrive on a belief that everything is working well, ignoring the potential detrimental consequences of their actions; they are inviting a major security breach that will ‘scar’ them and make

them operate in a 'reactive mode' that will essentially lead to more insecurity and anxiety (Dhillon et al., 2004; Samonas, 2012).

The obvious way to deal with the insider threat and fraud is perhaps more control. However, although technology is designed to control uncertainty, it actually creates "new and riskier contingencies" than the ones it was originally supposed to deal with (Kallinikos, 2006, 2007); in this respect, more control is less. Willison et al (2006) argue that one of the longstanding problems of information security is its alignment with business objectives. The reasonable need of organizations to mitigate risks that are pertinent to information security ends up getting misunderstood by employees, who quite often treat controls, risk countermeasures and other safeguards as a constraint that they need to circumvent to make their day-to-day work easier (Samonas, 2012; Willison and Backhouse, 2006).

In a similar vein, information security professionals also argue that a heavy investment on information security can have an adverse effect on business, leading to inefficiencies and loss in productivity (Cowan, 2012). As Cowan notes (2012), it is a battle between security and productivity; security measures must neither be so restrictive that they affect business processes and the flow of information, nor too relaxed, thereby causing harm. Nevertheless, disobedience and non-compliance, regardless of where and how they come from, can only create more windows of opportunity for crime; and so, the safeguards are actually introducing risks instead of addressing them (Willison and Backhouse, 2006). Slightly paraphrasing the lyrics of a famous Queen song "too much love will kill you": "too much security will kill you – just as sure as none at all".

Every organisation is in some way unique and faces different kinds and levels of exposure to insider threat and fraud. And the only way to address this variety is with a variety of appropriate actions (Ashby, 1958). There is no panacea for the threat of insiders and the constantly rising opportunities for crime; but most of all, there is no such thing as complete security and total peace of mind. It is encouraging to see that information security scholars and practitioners urge organisations to be truly

pragmatic and abandon their grandiose plans that often lead to complacency (Booz, 2011), deficient security and exposure to even more risk. Information security involves people, and for this reason alone, it is destined to thrive only on bespoke solutions that carefully consider the hazards and weaknesses, the strengths and the opportunities for growth; and, of course, hope for the best.

References

ACFE (2012) *Report to the Nations on Occupational Fraud and Abuse: 2012 Global Fraud Study,* Association of Certified Fraud Examiners, http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf, last accessed on 2nd April 2013.

Angell, I. O. and Samonas, S. (2009) The Risk of Computerized Bureaucracy, *Journal of Information System Security,* **5,** 2.

Anonymous (2009) Internal Fraud Likely to Rise In Wake of Economic Crisis, *Treasury & Risk,* 10-10.

Ashby, W. R. (1958) *An introduction to cybernetics,* Chapman and Hall, London.

Booz (2011) *Resilience in the Cyber Era: Building an Infrastructure that Secures and Protects,* An Economist Intelligence Unit research program sponsored by Booz Allen Hamilton, http://www.boozallen.com/media/file/resilience-in-the-cyber-era.pdf, last accessed on 7th April 2013.

Brancik, K. (2007) *Insider Computer Fraud: An In-depth Framework for Detecting and Defending against Insider IT Attacks,* Taylor & Francis.

Cappelli, D. M., Moore, A. P., Trzeciak, R. F. and Shimeall, T. J. (2009) *Common Sense Guide to Prevention and Detection of Insider Threat, 3rd Edition—Version 3.1,* Software Engineering Institute, Carnegie Mellon University and CyLab, http://www.cert.org/archive/pdf/CSG-V3.pdf, last accessed on 1st April 2013.

Choo, K.-K. R. (2011) The cyber threat landscape: Challenges and future research directions, *Computers & Security,* **30,** 8, pp. 719-731.

Ciborra, C. (2000) *From control to drift: the dynamics of corporate information infastructures,* Oxford University Press, Oxford.

Ciborra, C. (2002) *The labyrinths of information: challenging the wisdom of systems,* Oxford University Press, Oxford.

CIFAS (2012) *Staff Fraudscape: Depicting UK's Staff Fraudscape,* Credit Industry Fraud Avoidance System - The UK's Fraud Prevention Service, http://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-0-StaffFraudscape_2012.pdf, last accessed on 7th April 2013.

Cohen, L. E. and Felson, M. (1979) Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review,* **44,** 4, pp. 588-608.

Connolly, D. and Haley, M. (2008) Information Technology Strategy in the Hospitallity Industry, In *The Sage handbook of hospitality management*, (Eds, Wood, R. C. and Brotherton, B.), Sage, Los Angeles.

Cowan, D. (2012) *Comment: Too Much Security May Affect Business Processes,* Infosecurity, 27 June 2012, http://www.infosecurity-magazine.com/view/26550/comment-too-much-security-may-affect-business-processes/, last accessed on 7th April 2013.

Cummings, A., Lewellen, T., McIntire, D., Moore, A. and Trzeciak, R. (2012) *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector (Technical Report CMU/SEI-2012-SR-004),* Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm, last accessed on 24th March 2013.

Dekker, M., Karsberg, C. and Daskala, B. (2012) *Cyber Incident Reporting in the EU: An overview of security articles in EU legislation,* European Network and Information Security Agency, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu/at_download/fullReport, last accessed on 1st April 2013.

Denning, D. E. (1987) An Intrusion-Detection Model, *Software Engineering, IEEE Transactions on,* **SE-13,** 2, pp. 222-232.

Dhillon, G. (1999) Managing and controlling computer misuse, *Information Management & Computer Security,* **7,** 4, pp. 171-175.

Dhillon, G. (2001) *Information security management : global challenges in the new millennium,* Idea Group Pub., Hershey, PA.

Dhillon, G. and Moores, S. (2001) Computer crimes: theorizing about the enemy within, *Computers & Security,* **20,** 8, 715-723.

Dhillon, G., Silva, L. and Backhouse, J. (2004) Computer crime at CEFORMA: a case study, *International Journal of Information Management,* **24,** 6, 551-561.

E&Y (2012) *Fighting to close the gap: Ernst & Young's 2012 Global Information Security Survey,* Ernst & Young UK; Insights on governance, risk and compliance, http://www.ey.com/Publication/vwLUAssets/Fighting_to_close_the_gap:_2012_Global_Information_Security_Survey/$FILE/2012_Global_Information_Security_Survey___Fighting_to_close_the_gap.pdf, last accessed on 7th April 2013.

Furnell, S. (2002) *Cybercrime: Vandalizing the information society,* Addison Wesley, London.

Furnell, S. and Thomson, K.-L. (2009) From culture to disobedience: Recognising the varying user acceptance of IT security, *Computer Fraud & Security,* **2009,** 2, 5-10.

Greitzer, F. L. and Frincke, D. A. (2010) Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation, In *Insider Threats in Cyber Security - Advances in Information Security, 49*, (Eds, Probst, C. W., Hunker, J., Gollmann, D. and Bishop, M.), Springer US, pp. 85-113.

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

http://eprints.eemcs.utwente.nl/18500/03/0_19_CCS.pdf, last accessed on 2nd April 2013.

Hartford (2012) *The Hartford Small Business Data Protection Survey,* Conducted by the Pert Group on behalf of the The Hartford Financial Services Group, http://newsroom.thehartford.com/News-Releases/Small-Business-Owners-Despite-Being-Increasingly-Targeted-Believe-Data-Breach-Unlikely-50c.aspx, last accessed on 7th April 2013.

Hoyer, S., Zakhariya, H., Sandner, T. and Breitner, M. H. (2012) *Fraud Prediction and the Human Factor: An Approach to Include Human Behavior in an Automated Fraud Audit*, 45th Hawaii International Conference on System Sciences Proceedings, IEEE Computer Society, 4-7 January 2012, Grand Wailea, Maui, HI, USA,

Introna, L. D. and Whitley, E. A. (2000) About experiments and style: a critique of laboratory research in information systems, *Information Technology & People,* **13,** 3, pp. 161-173.

Kallinikos, J. (2006) *The consequences of information: institutional implications of technological change,* Edward Elgar, Northampton, MA.

Kallinikos, J. (2007) Information technology, contingency and risk, In *Risk, complexity and ICT*, (Eds, Hanseth, O. and Ciborra, C.), Edward Elgar, Cheltenham ; Northampton, MA.

Klein, R. (1986) The Mētis of Centaurs: Book review of 'Les Ruses de L'Intelligence: La Metis des Grecs' by Marcel Detienne and Jean-Pierre Vernant, *Diacritics,* **16,** 2, pp. 2-13.

Kroll (2012) *Global Fraud Report,* Kroll Advisory Solutions, http://www.krollcybersecurity.com/media-center/global-fraud-report.aspx, last accessed on 7th April 2013.

Kroll (2013) *The Insider Threat: Why Chinese hacking may be the least of corporate worries,* Kroll Advisory Solutions White Paper, http://www.krolladvisory.com/library/Insider_Threat_WP_022213_THT_042_2013_Final.pdf, last accessed on 7th April 2013.

Lincke, S. and Green, D. (2012) *Combating IS Fraud: A Teaching Case Study*, Americas Conference on Information Systems, Seattle, Washington, 9-11 August 2012, http://aisel.aisnet.org/amcis2012/proceedings/ISEducation/2/.

Loch, K. D., Carr, H. H. and Warkentin, M. E. (1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding, *MIS Quarterly,* **16,** 2, pp. 173-186.

Luhmann, N. (2002) *Theories of distinction: redescribing the descriptions of modernity,* Stanford University Press, Stanford, Calif.

Newman, G. R. (2009) Cybercrime, In *Handbook on Crime and Deviance*, (Eds, Krohn, M. D., Lizotte, A. J. and Hall, G. P.), Criminology and Criminal Justice Series, Springer Science, pp. 551-584.

Pironti, J. (2013) *The Changing Role of Security Professionals,* Infosecurity: 15 January 2013, http://www.infosecurity-magazine.com/view/30212/the-changing-role-of-security-professionals/?goback=%2Egde_1368287_member_212195880, last accessed on 7th April 2013.

Ponemon (2013) *Risk of Insider Fraud: Second Annual Study,* Ponemon Institute, http://www.attachmate.com/assets/Ponemon_2012_Report.pdf, last accessed on 7th April 2013.

PwC (2012) *Information Security Breaches Survey: Technical report,* PricewaterhouseCoopers UK, http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf, last accessed on 7th April 2013.

Roper, A. and Carmouche, R. (1989) Budget Hotels – A Case of Mistaken Identity?, *International Journal of Contemporary Hospitality Management,* **1,** 1.

Samonas, S. and Angell, I. O. (2010) The Power of Discretion in IS Security, *Journal of Information System Security,* **6,** 2.

Samonas, S. (2012) *Managing Computerized Bureaucracy: Opportunities and Hazards,* PhD Thesis, Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science, London, UK.

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

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. and Flynn, L. (2012) *Common Sense Guide to Mitigating Insider Threats, 4th Edition (CMU/SEI-2012-TR-012),* Software Engineering Institute, Carnegie Mellon University, http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm, last accessed on 24th March 2013.

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

Tseloni, A., Wittebrood, K., Farrell, G. and Pease, K. (2004) Burglary Victimization in England and Wales, the United States and the Netherlands, *British Journal of Criminology,* **44,** 1, pp. 66-91.

Wall, D. (2001) Cybercrimes and the internet, In *Crime and the internet*, (Ed, Wall, D.), Routledge, London.

Warkentin, M. E. (1995) Information system security and privacy, In *Emerging Information Technologies, Advances in Telematics*, Vol. 2 (Ed, Hanson, J.), Ablex Publishing, Norwood, NJ.

Warkentin, M. E. and Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat, *European Journal of Information Systems,* **18,** 2, pp. 101-105.

Willison, R. (2003) *Opportunities for computer abuse: assessing a crime specific approach in the case of Barings Bank,* Ph.D. Thesis, Department of Information Systems, London School of Economics and Political Science, University of London, London.

Willison, R. (2006) Understanding the perpetration of employee computer crime in the organisational context, *Information and Organization,* **16,** 4, pp. 304-324.

Willison, R. and Backhouse, J. (2006) Opportunities for computer crime: considering systems risk from a criminological perspective, *European Journal of Information Systems,* **15,** 4, pp. 403-414.

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

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