# A Human Factors Contribution to Countering Insider Threats: Practical Prospects from a Novel Approach to Warning & Avoiding

Dr Mils Hills[1] and Anjali[2]

[1] Associate Professor in Risk, Resilience & Corporate Security, Northampton Business School

[2] MBA researcher, Northampton Business School

**Abstract**

Any organisation is susceptible to a breach of security from outside: hacking, product contamination, theft of intellectual property and so on. Although all of these are risks to an organisation and can be highly deleterious to its financial health and reputation, the threat posed by a malevolent insider can be even more challenging. Whilst there has been a large quantity of academic articles and industry surveys produced on the theme of Insider Threats - the majority of this published work is descriptive or details the effects of insiders' actions.

This paper provides initial thoughts around some practical and pragmatic steps to being to gain clarity on the challenge of insider threat and how organisations may draw on novel approaches to grow early warning, response and mitigation against Insider Threats. The paper also discusses the importance of security culture and risk communication.

**Key Words:** Insider Threat; nudge; sentinel events; early warning; weak signals

[1] Associate Professor in Risk, Resilience & Corporate Security, Northampton Business School

[2] MBA researcher, Northampton Business School

## Introduction

The detection and countering of Insider Threats is a significant challenge for a business or organisation of any size, operating in any industry and in any country. Employees and others with access to sites and systems are often touted as being the organisation's greatest strength, however through either malicious action or unintentional consequence, they can also be the source of a great deal of cost and, even, of corporate destruction (Magklaras *et al*, 2006). Technical measures in terms of access control, background screening, workplace surveillance, layered computer security may reduce some risks, but the residual and potential challenge posed by employees, contractors and others is significant. In an era where Intellectual Property (IP), corporate reputation, regulatory compliance and governance are all rare and scarce resources – ways to anticipate and mitigate Insider Threats are highly desirable, although difficult to develop (HoMER, 2012).

This paper reports ongoing conceptual research conducted by the authors, and our early indications of practical prospects for improving security against Insider Threats in corporate and governmental contexts. These prospects, translated into real-world environments, will enable end-users to have both an enhanced understanding of and ability to sense and engage with Insider Threat.

In this paper, we first review the nature of the challenge of Insider Threats, then present cases illustrating the very real effects of successful exploitation of Insider Threats to both large and small enterprises. We also review definitive guidance from the UK government and corporate sources, not least to indicate their shortcomings. The next section sets out our two main conceptual developments that add value and edge to existing and well-meaning guidance: **(1) Early Warning from weak signals and sentinel events**, and **(2) the use of risk communication strategies to enable (1) to function**. We further indicate how both of these conceptual advancements could deliver advantage to an organisation by extracting more value from existing and new sources of data. Finally, the security culture of organisations needs to be nudged into a new era – we suggest some possible ways of doing this.

## Background: The Rise of Insider Threat

Whilst governments and military forces have always had to contend with the endless battle of espionage and counter-espionage, Insider Threat has only started to be a well-recognised threat to companies since the early 1980s. Among information system threats, the Insider Threat is the greatest – a trusted person inside a system (Warkentin

and Willison, 2009). The nature of an Insider Threat's degree of destructive potential varies with the type of industry or workplace that s/he is embedded into or has access to. Generally, the Insider Threat is revealed when individual behaviour betrays their existence – for example they are found to be in breach of policies, regardless of whether there is any motive to cause harm (Greitzer *et al*, 2013). The term is generally used to refer to anyone with authorised access and malicious intent, although we argue that unintentional consequences of human actions should also be included.

Insider Threats can be former or current employees, business partners, contractors (Chinchani et al, 2013) or others with real or assumed grounds to access a site or systems. Insider Threats may achieve their effects through sabotage, theft, fraud or poor judgment – as we write this paper, the world's second largest retailer (Tesco) has made headlines around the world, seemingly because they failed to take action on early warning signals from their auditors about what could amount to an Insider Threat (Bird 2014). We argue that Tesco's £250 million profit overstatement (and subsequent suspension of senior executives and Serious Fraud Office investigation) appears to be a case of Insider Threat perpetrated by one or more people (Jefferies 2014), and in which systems may have played merely a supporting role in the misdemeanour.

Prior to this recent event (and others in the news, such as the LIBOR-fixing trial) Nick Lesson is a famous name who made headlines for the downfall of what was then the UK's oldest financial institution – Barings Bank – using his detailed knowledge of systems and processes to conceal his activities. Leeson is a perfect example of a single Insider Threat who caused massive harm to an organisation solely to fulfil his greed (Agar, 2014). In another high profile case of a security breach, and perhaps old-fashioned espionage, U.S. soldier Bradley Manning (latterly Chelsea Elizabeth Manning) was sentenced to 35 years in prison for sharing classified files with WikiLeaks. This resulted in what has been reported to be the largest loss of classified information in American history (Tate and Londoño, 2013).

In terms of cyber-security, the picture is equally bleak. The UK Ministry of Justice (MOJ) was recently fined £180,000 by the Information Commissioner's Office (ICO) over security failings of basic prison information system in England and Wales. One of the prisons lost a back-up hard-drive containing unencrypted, confidential information - absolute negligence on the part of the employee. Prison service provided new drives with self-encryption option which was not 'turned on' while working (Smolaks, 2014). In a similar incident, the MOJ was fined £140,000 after sensitive information was emailed to three prisoners' families (BBC, 2013).

The business environment has transformed to one where crucial information can be taken from (and incredibly devastating malware can be taken into) organisations on tiny media devices. Business depends on the confidentiality, integrity and availability of data. Safeguarding information and the systems that hold it is the primary objective of cyber-security. However, there are human challenges to the resilience of the very best technical security systems. For example, the authors have been made aware of a recent informal experiment done by a UK bank, where there was a 100% success rate as employee's picked-up USB sticks that was dropped in company's car park. The employees intended to access the USB sticks, being curious as to their content.

According to a 2014 Information Security Breaches survey reports, a heartening decrease in events is reported, although, still, 81% of large organisations and 60% of small businesses suffered due to security breach. However, the average cost of these breaches has risen drastically (Department for Business Innovation & Skills, 2014). Given that many of these breaches will have been caused or facilitated by Insider Threats (poor security policy – not changing default router passwords through to deliberate attempts to damage systems or steal data) – the importance of being able to detect and deal with these *before* costs are incurred is clear.

Hence, on reviewing the literature, it has become imperative, according to Weinberg *et al,* (2014) for CEOs, CIOs (Chief Information Officers), Board members, heads of corporate and cyber security as well as business continuity and crisis functions to recognise the need to achieve the following:

- Protection of key information assets – "Crown Jewels"
- Risk assessments in terms of company's reputation, impact on business needs to be done
- Vulnerability assessments
- Assurance that key security policies are in place?
- Analysis of the weakest link – employees
- Attention to Security Culture – Security culture is about encouraging and developing an organisation (including staff and board members) to adhere and follow standard policies and practices towards security (Weinberg *et al*, 2014)

Therefore, it is important for individuals in organisations to follow such guidance in order to manage risks, given that good cyber security depends on human behaviour and technical methods. In order to help and provide direction to small business and large organisation, The UK Centre for the Protection of the National Infrastructure (CPNI) has

issued definitive guidance to board members and risk managers in key sectors of the economy (HoMER, 2012).

**A Brief Summary of Existing Guidance**

CPNI underscores the importance of businesses managing risk arising from human behaviour. For monitoring and safeguarding an organisation, CPNI's Holistic Management of Employee Risk (HoMER) approach provides guidelines for safeguarding organisation from malicious, negligent etc. behaviour (HoMER, 2012). The guidelines encourage:

- A Holistic Approach
- A Risk-based Approach
- Security culture
- Single accountability
- Transparency and Legality

HoMER guidance helps accountable persons to perform their tasks. It defines the responsibility of board members/top level management, a single point of contact for handling people risk and an Implementation team to help in assess, protect and help recover after an incident. Similarly, the Software Engineering Institute (SEI), is working with organisations to safeguard them from Insider Threat through technical measures providing layered strategy consisting of procedures, controls and policies. Sensible advice from both CPNI and SEI sets out the need for organisations to implement policies, effective line management and protective monitoring in order to identity signs of growing Insider Threat threats. Some of the indicators of an increase of an Insider Threat include: changed behaviour in the workplace, altered document copying activities and attempts to access non-role relevant information and systems, travel to unusual countries, a gradual decline in performance, recognisable substance abuse, etc. (Tehnical report SEI, 2012).

These indicators are clearly shaped by national security concerns (e.g. copying classified material, such as Edward Snowden's leaking of classified documents to the media). No doubt corporate examples would be similar. In a survey conducted by Oxford Economics for CPNI, 21% of industry respondents reported theft of classified or sensitive information (Oxford Economics, 2014). However, because of the national security heritage of CPNI's approach - most of these signals are pretty gross and depend on colleagues, line mangers and others detecting or observing them whilst they working their normal roles. This is a substantial requirement, but will help organisation create a

first line of defence from Insider Threat. Whilst in the past, when printing or copying large amounts of documents would have been obvious and something arousing suspicion, in most workplaces these days this is nothing remotely **unusual.**

Equally, the norms of courtesy and non-interference that predominate (normally helpfully) in the modern workplace mitigate against necessarily having any knowledge of a colleague's work and its scope, nor any curiosity about changes or easy ways to make any disquiet known to others. Given the ease of scanning, photographing, emailing, saving to portable or cloud media and the generally chaotic nature of corporate data systems – the challenges of happening to notice atypical behaviour by anything other than chance or through some massive and obvious breach is small. Similarly, whilst in the past a holiday in Eastern Europe or Cuba would rightly have aroused suspicion about an employee in a weapons design facility, these days an adversary is as likely to be a commercial rival as much as an agent of a rival nation.

Espionage is an act of stealing large volumes of sensitive data, remotely or otherwise, or of any information that its owner might want to protect. In two separate incidents in 2011, one ex-employee of Motorola was stopped at a US airport when trying to flee with more than 1000 confidential documents valued at more than $600 million (MI5). In another published case, Renault sacked three top executives for sharing confidential information with a third party, an area where Renault and Nissan invested $5.5 Billion in technology for battery powered cars (Marsh and Reed, 2011).

In addition, where fraud is absolutely within the ability of an Insider Threat to pursue – much as Leeson knew information systems and processes so well he could conceal his criminal activities – procurement professionals can place corrupt contracts, favour contacts and purchase counterfeit items, all very well-hidden and apparently fully and legally documented. Procurement fraud is a thoughtful deception planned to make financial gain or loss in the 'procure to pay' cycle (National fraud authority, 2011). According to KPMG's *Fraud Barometer*, supply chain fraud worth £61 million contributed to fraud cases totalling half a billion pounds in the first half of 2013 alone (KPMG, 2013). Such sums are created by acts large and small, for example, in 2012, £117,812 was stolen by an NHS procurement professional who created a fictitious care home supplier - linking it with a legitimate customer but making payments to their personal bank account (Albert, 2012).

At the much smaller, but important, level of business – start-ups in technology, life sciences and associated industries face existential threat should their Intellectual Property (IP) be stolen. Even for established companies, if they have invested significant funds and resources into the development of IP – this can be destroyed by the transfer

of that to a rival or actions that undermine trust and confidence in that IP. The 2014 Information Security Breaches Survey shows that 4% of surveyed small businesses and 16% of large organisation admitted to suffering IP theft in the last year: many more are too embarrassed to admit this – or will have ceased trading.

The famous trade secret case of Coca Cola (where three employees tried to sell Coke's recipe to Pepsi for $1.5 million) (Associated Press, 2006); loss of a defence contractor's key sales staff; food product contamination; automotive supply-chain fraud (e.g. counterfeit parts); theft of client list of an investment fund; leaking of details of patents about to be filed – for all of these real-world eventualities, and more, this paper suggests that much weaker signals than those mentioned by CPNI and others need to be sought by and in companies and public sector organisations (let alone by their regulators, insurers and investors). This is an even bigger challenge, but is necessary. Although it may not be easy, the costs and challenges of doing it are much more palatable than attempting to survive after an Insider Threat has wreaked havoc. What must be balanced, however, is caution against paranoia or the encouragement of a surveillance culture.

## Concepts for detecting and engaging Insider Threat:

The preceding section has presented (in summary form) some of the ideas that CPNI and commercial consultancies have put forward to help organisations detect Insider Threats. We have drawn attention to some substantive shortcomings and the focus of this section is to introduce two concepts which, when translated into and implemented within industry or public sector contexts, will help detect and avert the worst excesses of Insider Threat.

### 1. Capacity for Corporate Early Warning from Weak Signals and Sentinel Events

Whilst the intent of CPNI and others' guidance to get early warning of an Insider collecting sensitive information and booking strange holidays is excellent, clearly these are insufficient flags for corporate concern in the current era. Whilst the monitoring of network behaviour (e.g. attempting to access databases or systems which are entirely unrelated to current role) is easy to do, we do not dwell on this as our expectation is that effective Systems Administrators and relevant automated monitoring should detect such activity. Similarly, hacking and the exploiting of unchanged default passwords are the purview of conventional technical security, just as personnel security procedures should weed-out activists, ex-employees of a competitor and criminals - whilst physical security should prevent people from 'tailgating' into offices, plants and laboratories.

Our concern is with promoting the growth of awareness of companies and organisations in weak signals that they could and should be sensing. *Weak signals* – usefully defined as disconnected or random pieces of information that may appear to be background noise at first sight- that, through analysis can be shown to be a part of a meaningful and important pattern (Schormaker and George, 2009). However, as the term suggests, weak signals are nothing like as gross (or obvious) as the holiday on the Black Sea or bundles of paper product specification details being taken home.

Line managers, human resource partners, network and systems administrators, associated technical systems, co-workers, cleaners, maintenance staff and others need to become distributed sensors for an organisation's Early Warning (EW) capability. Whilst this may at first sound somewhat overblown, it is the consequences of security breaches that could put the jobs of all of those individuals' whose job roles are mentioned above at risk. The notion here is akin to that of the organisation as an organism which is sensitive to its internal environment: literally *sensing* unusual change. The changes flagged may be of no consequence, or may require further investigation in order to be certain that they are (or are not) of consequence. The context of the organisation/company will determine what counts as meaningful-unusual behaviour for its security (or cyber-security) culture, and no doubt a socio-technical approach is needed in order to collect, collate and analyse data on behavioural changes.

A good deal of this information may already be held or may be accessible. There may not be easy ways of currently accessing or aggregating it, but achieving this should be the role of the modern and intelligence security / continuity / resilience / audit / governance functions in companies and public bodies. This adds a knowledge or intelligence management dimension to the heart of the risk discovery, management, mitigation and avoidance process (HoMER, 2012).

The organisation also needs to look beyond its internal environment. Increasing evidence is accruing, for example, that the social media activity of staff can be useful indicators of some changes (Augustine *et al*, 2014). Sometimes these changes will not be significant from a security point of view but may create problem at a later stage. For example, indicate issues of workplace dissatisfaction, stress, relationship problems where the modern organisation should reach out and offer care and support. Not least, this helps prevent people – for example, drifting into positions where they may be vulnerable to, say, blackmail due to substance abuse or unwise Internet activity (e.g. sharing intimate images). Indeed, indicative research suggests that social media postings that are not coherent with work place behaviours and values have been discovered, albeit after events, with 16% of large organisations and 5% of small businesses detecting that a security breach had occurred *through* social networking sites (Ferrante, 2010).

*Sentinel Events* (SE) whilst the above challenges may seem tough enough for most organisations to cope with, our research has identified a further, related concept to add resilience and awareness to corporate cyber / personnel risk assessment: that of the sentinel event. These are occurrences that indicate the need for immediate response and evaluation (Radtke, 2003). They may be weak signals that are indirectly related to - or may be indexes for - something that really does affect corporate security and that could provide useful Early Warning. Equally, the information may not be meaningful, or may relate to something else that is helpful for the organisation to have advance sight of.

The authors first encountered the notion of the sentinel event in the case of a serendipitous linkage established between collapsing numbers of wild waterfowl in New York and a major spike in the number of cases of human Influenza a few weeks later. Typically, one would not be looking for early warning of a new wave of human Influenza anywhere other than in doctors' surgeries, health-support telephone lines, hospital admissions and, maybe, sentiment expressed on social media. However, the advance notice available there will be very limited. There isn't much time to institute public health communications to remind people to wash their hands, develop a new vaccine or even encourage uptake of the existing one. However, if one could see an early warning in another place entirely all of these things may be possible. Lives may be saved, hospital admissions reduced, sick-days reduced but this is only possible if sensors (of whatever form(s)) are available which are actively scanning for information which may help generate a meaningfully rich information assessment.

Whilst many security-related developments are blighted by the curse of hindsight – where correlations could not have actually been made at the time because information was not available and there was no plausible or rational link between cause and effect – we believe that sentinel events in organisations may well be a useful way of encouraging security managers and others of unleashing useful data already held or findable. Especially in an era of 'big data'' there may well be massive amounts of data currently held where existing smart people could develop ways of looking for patterns across data and databases (Sentinel event policy, 2015).

Just as, again in the era of the Cold War, the US and USSR tried to find sentinel events to indicate that something else was occurring (classically, an increase in the number of pizzas ordered-in to planning and other functions in Washington DC, representing the fact that people were staying late to work on some strategy) organisations need to mine their technical and human intelligence to detect unusual activities that merit further investigation and either the introduction of risk mitigation measures or, if the issues uncovered are not directly of security relevance, apply other interventions, e.g. welfare.

Organisation can begin to increase their safeguarding by adopting a few important policies:

*Sentinel Events (SE) database*: Organisations should maintain a SE database. This will help the organisations in safeguarding 'big data' and trends/pattern from earlier events can trigger an alert. Simply put, a better understanding of what constitutes baseline data of events (normal and sentinel alike) can help security and other functions draw together an insightful and actionable view of events, near misses, unusual correlations and so on (Sentinel Events, 2013). Much of this information in the era of big data may already exist in HR systems, personal development review documents, CCTV footage, audio recordings of voicemail and dialled calls, social media activities and other available or accessible data sources.

Naturally, there will be a balance to be struck between having access to potential sources of early warning and legitimate concerns about surveillance. However, when (as noted above) IP can be removed from buildings with easily concealed USB sticks and cyber threats brought in on them, there is a pressing imperative for companies and public authorities to protect their information, livelihood or reputation from destruction or degradation which could occur in mere moments.

*Grow a Bespoke Security Culture from an Existing Healthy Workplace* - Whilst some information will be available or could be made available to assess changes in risk exposure, still further valuable insight is very likely to be 'locked' in the people who work in the organisation closest to the *threat* (individuals whose behaviour may be changing) or the *vulnerability* (the item(s) of value exposed to peril). Organisations need to create a risk and security culture that incorporates - from induction to training, governance/ risk assessment and crisis (incident response) processes and talent (people) – a total appreciation of the risk profile being encountered. Whilst through background investigation of employees is a necessary first step towards securing an organisation, it is far from sufficient in itself. Periodic and unconventional checks and effective monitoring is key (Veiga and Martins, 2014).

This calls for progressive companies and institutions to devote energy (not necessarily vast sums of money) to the promotion of a safety culture. Defined by the UK Health and Safety Executive (HSE) as the "psychological characteristics of employees (i.e. 'how people feel'), corresponding to the values, attitudes, and perceptions of employees with regard to safety within an organisation" (HSE, 2005: iv), we extend this definition. For us, the term safety culture can be used to describe the mesh of practices, policies, values and behaviours which enable an organisation to leverage the trust and loyalty of its employees, contractors, customers, observers, partners and even competitors.

In order to have trust, loyalty, openness to sharing ideas and thoughts about potential risks or how to avoid them, companies must already have the kinds of ethics in place where transparency and feedback (no matter how unwelcome) is sought and embraced. The simple reason for this is that just because a matter is about security does not mean that normal ways of behaving are suspended or disregarded. If shop-floor staff are only too used to having any bright ideas rejected, then it is very unlikely that their working culture will inspire them to share ideas about reducing risk or reporting on strange occurrences (by colleagues, contractors, Information technology systems, etc.).

If a company is competitive, sustainable and has a very high level of trust, loyalty and commitment in place – all that may be required is a 'priming' of staff on the types of information or concerns that may be of interest. Naturally, this process may be novel and require some creative thought, we set out some ideas to assist below.

**2. Risk Communication: Entrenching a Security Culture through Nudge**

Changing how individuals behave is hardly ever a trivial matter. When a workforce is being asked to do something completely new – such as consider security and look for potential breaches of it in a novel way – the domain of risk communication has much to offer in terms of pragmatic advice. Risk Communication is an 'interactive process of exchange of information and opinion among individuals, groups and institutions concerning a risk or potential risk' (Behavioural Insight team, 2014) - needs to be a dialogue whereby the host organisation shares its thoughts, fears and concerns and to which employees respond with information (or nil returns!) aligning with those matters or that supplement them (sentinel events).

Risk communication has been seized upon by regulators in health, safety and other areas as a more effective means of securing compliance than traditional training courses and penalties. Policy-makers sensing an opportunity to both achieve real impact and save money have commissioned research into proactive approaches which seek to secure compliance through 'nudge' activities (Mindspace, 2010).

Nudge is an approach to understanding and changing people's behaviour by analysis, improving, designing and offering choice for people, so their decisions are more likely to produce helpful outcomes for those people and society (Vallgårda, 2012). According to research conducted on Reducing Mobile Phone theft and improving security by Behavioural Insight team (2014), better educated customers help reduce the risk of mobile theft. By working with manufacturers, Police and network operators can nudge mobile owners into behavioural changes that reduce the risk of experiencing the theft of a mobile phone.

In order to achieve effective nudges in terms of influencing workplace (or workplace-relevant) behaviour, the employer must have the ability to meaningfully and effectively communicate and engage those employees. In seeking to nudge workers into becoming aware of or curious about potential security challenges, weak signals and sentinel events – the careful development of relationships with employees will be needed. Bespoke ways of educating and relating to workers at all levels in a company will be needed. As noted earlier, this will not occur with specific and limited reference to security matters but will have to be a particular example of an open, frank and blame-free communications exchange that is already in place, proven to work fairly and trusted to be confidential.

## Conclusion

This paper has demonstrated emerging prospects for improved security and resilience in private and public sector organisations arising from a refreshed approach to looking for early warning, sentinel events, safety culture and drawing on the emerging discipline of 'nudge' behavioural change. We have provided hints at the ways in which Management Boards and functional leaders (e.g. heads of security) must work together, building on established best practice in employee engagement in order to gain foresight on risks which are knowable but currently not sought after.

## References


1. Agar, P. (2014) The decline and fall of British investment banking http://www.ft.com/cms/s/0/72350e66-d6be-11e3-b251-00144feabdc0.html#axzz3EhzqZ03k, accessed 29th September 2014.
2. Albert, A. (2012) Procurement fraud costs UK more than £5 million

   http://www.supplymanagement.com/news/2012/procurement-fraud-costs-uk-more-than-ps5-million, accessed 16th October 2014.
3. Associated Press (2006) Coca-Cola trade secrets theft case set for trial http://www.nbcnews.com/id/15209024/ns/business-us_business/t/coca-cola-trade-secrets-theft-case-set-trial/#.VDMl6fldWSp , accessed 03rd October 2014.
4. BBC (2013) Ministry fined after Cardiff prisoner details emailed to families http://www.bbc.co.uk/news/uk-wales-south-east-wales-24615978, accessed 30th September 2014.

5. Bird, M. (2014) The World's Second-Largest Retailer Is Imploding http://www.businessinsider.com/tesco-accounts-investigation-2014-9, accessed 29th September 2014.

6. Chinchani, R., Iyer, A., Ngo, H. Q., Upadhyaya, S. (2005). Towards a theory of insider threat assessment. *International Conference on Dependable Systems and Networks*, 108-117.

7. Common Sense Guide to Mitigating Insider Threats 4th edition 2012. http://www.sei.cmu.edu/reports/12tr012.pdf, accessed on 12th November, 2014.

8. Ferrante, P. (2010). Risk & Crisis Communication. *Professional Safety.* **55** (6): 38-45.

9. Fraud increases 38% but real cost is human misery. (2013)

   http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/Fraud-increases-38-to-over-%C2%A305bn-but-real-cost-is-human-misery-according-to-latest-KPMG-Fraud-barometer.aspx, accessed 16th October 2014.

10. Greitzer, F. L., Kangas, L. J., Noonan, C. F., Brown, C. R., Ferryman, T. (2013). Psychosocial Modeling of Insider Threat Risk Based on Behavioral and Word Use Analysis. E - Service Journal **9** (1): 106-138,141.

11. Health and Safety Executive (HSE) (2005). A Review of Safety Culture and Safety Climate Literature for the Development of the Safety Culture Inspection Toolkit (prepared by Human Engineering for the HSE), HMSO: Norwich: iv.

12. Information Security Breaches Survey Technical Report. (2014) http://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf, accessed 30th September 2014.

13. Jefferies, T. (2014) Tesco in turmoil: Shares fall another 4% taking supermarket giant to HALF the value it was a year ago as sales fall 4.5 http://www.thisismoney.co.uk/money/news/article-2765522/Tesco-chairman-Sir-Richard-Broadbent-pressure.html, accessed 29th September 2014.

14. Magklaras, G B; Furnell, S M; Brooke, P J. (2006) Towards an insider threat prediction specification language. *Information Management & Computer Security* **14** (4), 361-381.

15. Marsh, P., Reed, J. (2011) http://www.ft.com/cms/s/0/ba6c82c0-2e44-11e0-8733-00144feabdc0.html?siteedition=uk#axzz3GFmjsWwk, accessed 16th October 2014.

16. MI5 https://www.mi5.gov.uk/home/about-us/what-we-do/the-threats/espionage.html, accessed 16th October 2014.

17. MINDSPACE Influencing behaviour through public policy. (2010) http://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf, accessed on 10th February, 2015.

18. National Fraud Authority. (2011)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118460/procurement-fraud-public-sector.pdf, accessed 16th October 2014.

19. Oxford Economics Cyber-attacks: Effects on UK Companies. (2014) http://www.oxfordeconomics.com/publication/open/250836, accessed 30th September 2014.

20. Pang, A; Nasrath, B B A H; Aaron C Y C. (2014) Negotiating crisis in the social media environment: Evolution of crises online, gaining credibility offline. *Corporate Communications* **19** (1) : 96-118.

21. Radtke, K. (2003). Take the fear out of sentinel events. *Nursing Management* **34** (6): 24.

22. Schoemaker, P. J. H.; Day, George S. (2009)

http://www.supplymanagement.com/news/2012/procurement-fraud-costs-uk-more-than-ps5-million, accessed 16th October 2014.

23. Sentinel event policy. (2014)

http://www.jointcommissioninternational.org/assets/3/7/17-Sentinel-Event-Policy.pdf, accessed on 18th November, 2014.

24. Smolaks, M. (2014) ICO Fines The Ministry Of Justice £180,000 For Prison Data Breaches http://www.techweekeurope.co.uk/news/ico-fines-ministry-justice-180000-prison-data-breaches-151456, accessed 30th September 2014.

25. Sentinel Events (SE). (2012)

http://www.jointcommission.org/assets/1/6/CAMH_2012_Update2_24_SE.pdf, accessed on 15th October, 2014.

26. Tate, J., Londoño, E (2013) Judge finds Manning not guilty of aiding the enemy, guilty of espionage http://www.washingtonpost.com/world/national-security/judge-to-announce-verdict-in-bradley-manning-case-today/2013/07/29/e894a75c-f897-11e2-afc1-c850c6ee5af8_story.html, accessed 29th September 2014.

27. The Behavioural Insights Team. Reducing Mobile Phone Theft and Improving security (2014) http://www.behaviouralinsights.co.uk/sites/default/files/HO_Mobile_theft_paper_050914_FINAL.PDF, accessed 06th October 2014.

28. Vallgårda, S. (2012) Nudge—A new and better way to improve health? *Health Policy*, **104**(2): 200-203.

29. Veiga, A. da, Martin, N. (2015) Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security.*

30. Warkentin, M., Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems, suppl. Special Issue. *Behavioral and Policy Issues in Information* **18** (2): 101-105.

31. Weinberg, A., Kaplan, J.; Bailey, T. (2014).

http://www.ft.com/cms/s/0/1c4115e8-885a-11e3-85a2-00144feab7de.html?siteedition=uk#axzz3GFmjsWwk, accessed 15th October 2014.