available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Human factors in information security: The insider threat – Who can you trust these days?

Carl Colwill

BT Security, UK

Keywords:
Insider threat
Human factors
Security risk management
Outsourcing

ABSTRACT

This paper examines some of the key issues relating to insider threats to information security and the nature of loyalty and betrayal in the context of organisational, cultural factors and changing economic and social factors. It is recognised that insiders pose security risks due to their legitimate access to facilities and information, knowledge of the organisation and the location of valuable assets. Insiders will know how to achieve the greatest impact whilst leaving little evidence. However, organisations may not have employed effective risk management regimes to deal with the speed and scale of change, for example the rise of outsourcing. Outsourcing can lead to the fragmentation of protection barriers and controls and increase the number of people treated as full time employees. Regional and cultural differences will manifest themselves in differing security threat and risk profiles. At the same time, the recession is causing significant individual (and organisational) uncertainty and may prompt an increase in abnormal behaviour in long-term employees and managers – those traditionally most trusted – including members of the security community. In this environment, how can organisations know who to trust and how to maintain this trust?

The paper describes a practitioner's view of the issue and the approaches used by BT to assess and address insider threats and risks. Proactive measures need to be taken to mitigate against insider attacks rather than reactive measures after the event. A key priority is to include a focus on insiders within security risk assessments and compliance regimes. The application of technology alone will not provide solutions. Security controls need to be workable in a variety of environments and designed, implemented and maintained with people's behaviour in mind. Solutions need to be agile and build and maintain trust and secure relationships over time. This requires a focus on human factors, education and awareness and greater attention on the security 'aftercare' of employees and third parties.

1. Introduction

The insider threat is always present and manifests itself in many ways. This paper highlights that insider risks should be examined in the context of changing technical, social, business and cultural factors. Experience shows that an over-reliance on technology without consideration of other factors can have disastrous results for managing the insider threat

1.1. *Insiders can cause great harm*

The lethal consequences of armed insiders turning against their colleagues was demonstrated in November 2009 to UK forces in Afghanistan (BBC, 2009a,b) and US forces at Fort Hood, USA (BBC, 2009a,b). Such deadly attacks on people are not the focus of this paper but rather malicious threats to information assets – though many of the human factors

E-mail address: carl.colwill@bt.com

1363-4127/$ – see front matter © 2010 Laura Pritchard. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2010.04.004

discussed apply across all scenarios, especially the need to look for 'warning signs'. It is important to remember that non-malicious threats, for example, the accidental loss or release of information, can also have a major, negative impact.

A malicious insider has the potential to cause more damage to the organisation and has many advantages over an outside attacker: they have legitimate and often privileged access to facilities and information, have knowledge of the organisation and its processes and know the location of critical or valuable assets. Insiders will know how, when and where to attack and how to cover their tracks. Outsiders need to target and gather many sources of intelligence before they can take action, while the insider can target information directly and will not have to overcome most of the barriers facing the external attacker. It is usually far more cost-effective and quicker for an external threat source to place, or subvert, an insider to exploit vulnerabilities to steal information rather than launch an attack through multiple layers of protection. Insiders have time and are given capability and opportunity. The situation is further complicated by the increase in outsourcing which can lead to the extension and potential dilution or fragmentation of protection controls and an increase in the number of third parties given the same privileges and access rights as insiders. This is providing new opportunities for threat actors to identify information and vulnerabilities in geographic areas where individuals may be more susceptible to targeting and successful attack.

1.2. *Security is improving but technology alone is not enough*

Many forms of technology are available to protect information but this is usually applied to identify and restrict outsider access with off-the-shelf products such as firewalls and intrusion detection systems. The latest UK Government Department for Business Enterprise and Regulatory Reform (BERR, 2008) information security breaches survey notes improvements in overall organisational security controls, mainly focused on outsiders:

- 55% have a documented security policy;
- 40% provide ongoing security awareness training to staff;
- 14% use strong, multifactor authentication;
- 11% have implemented BS7799/ISO27001;
- 99% back up their critical systems and data;
- 98% have software that scans for spyware;
- 97% filter incoming email for spam;
- 97% protect their website with a firewall;
- 95% scan incoming email for viruses;
- 94% encrypt their wireless network transmissions.

Outside attacks tend to be easier to detect and defend against, but the tools used to protect against outsiders are seldom scalable or cost-effective to apply to every employee who must be given access to information and assets so that they can do their job. An over-reliance on traditional, perimeter-based security controls focusing on external attacks should be re-appraised. This model provides an effective layer of security against outsiders, but contains inherent weaknesses, especially in outsource environments, for increasing numbers of third party insiders. In these circumstances, we may not know which insider is actually using security credentials to authenticate via the firewall (as the control of user account management may also have been migrated to the third party) and once through defences the monitoring of subsequent activity may be limited or non-existent.

Far less investment is made in controls to protect against insider threats. Research indicates that 70% of fraud is perpetrated by insiders rather than by external criminals but that 90% of security controls and monitoring are focused on external threats (McCue, 2008). Even where technical controls for insiders are available, they must not be considered in isolation (Jones and Colwill, 2008). Greater investment in organisational human factors is required to balance against the funding in technology: with the appropriate motivation and time, human beings will find their way around most technical controls.

1.3. *A practitioner's perspective on managing the insider threat*

This paper will not evaluate technical security controls but focus on human factors to show that protecting the organisation from the malicious insider can only be achieved if a holistic approach is taken. The paper emphasises why it is essential that organisations apply a risk-driven approach that explicitly incorporates insider threats. In practical terms, this means applying appropriate focus and tools and investing in a balance of technical controls and procedures that take into account human factors. This paper highlights the key factors relating to insider risks that are prominent in BT's information security risk assessments. Insiders will always be part of your organisation and the key is to achieve a balance between the privileges needed for someone to perform their job and the application of appropriate levels control and audit. Loyalty, trust and security awareness are inherently intangible topics but effort should be made to make them more comprehensible and discernible. This requires an active focus on behaviour in the workplace.

2. The insider threat is real and here to stay

There is much debate on the insider threat but, compared to outsider attacks, there is far less factual data on which to base analysis and conclusions. In the USA, the National Infrastructure Advisory Council (NIAC, 2008) highlights that awareness and mitigation of insider threats varies greatly among companies and sectors and is often dealt with poorly. The BERR (2008) concludes that in the UK many organisations are still not doing enough to protect themselves and their customers' information (including some areas significant for the insider threat):

- 52% do not carry out any formal security risk assessment;
- 67% do nothing to prevent confidential data leaving on USB sticks, etc.;
- 78% of companies had computers with unencrypted hard discs stolen;

- 84% of companies do not scan outgoing email for confidential data.

Most physical and electronic attacks can be assisted or conducted by an insider but some attacks can only be committed by insiders, such as the unauthorised release of proprietary information or the sabotage of assets that only employees can access.

2.1. *Accidental and malicious insider threats*

Insiders can compromise information confidentiality, integrity and availability and both *accidental* and *malicious* risks must be considered. Insiders are prone to accidental information security failures, as shown by the infamous case of the UK Government's Revenue and Customs Department (HMRC) losing personal details of 25 million people in a single incident Thomson (2007) and subsequent UK public sector disclosures. RSA/IDC research (Grant, 2009) shows that accidental security incidents by insiders happen more often and could have greater potential for harm than malicious insider attacks: 52% of insider incidents were accidental (including 6244 incidents of unintentional data loss).

Sometimes even apparently innocuous insider activity can cause serious accidental damage, for example, inappropriate internet access which not only wastes the organisation's time and resources but:

- Puts the organisation's network and systems at risk of virus infections and malware;
- Could lead to potential lawsuits across a wide range of areas, for example, criminal action, copyright infringement and claims of sexual harassment, racism, bullying or defamation;
- Could lead to significant impact on an organisation's reputation and future revenue.

This is echoed by The Economist Intelligence Unit (EIU, 2009) which finds an increase in the number of organisations damaged by sensitive information appearing on blogs and social networking sites.

From a malicious perspective, Wilding (2007) notes that no terrorist group or external electronic attack has ever come close to causing the commercial collapse of any major company. By contrast, the disasters of Barings, BCCI, Worldcom, Enron, Societe Generale and, more recently Satyam (Blakey, 2009), Stanford and Madoff (FT, 2009a,b), have all been the result of failure in internal controls and abuse and illegal activity by a small number of employees with legitimate authority: *trusted insiders*, usually in senior positions.

2.2. *Growing insider threats, risks and impacts*

The problem is significant, risks are real and compromises and impacts are occurring. The RSA/IDC findings (Grant, 2009) show that:

- Most chief security officers (CSOs) were more worried about outsider threats rather than insider risks;
- 82% of respondents responsible for security decisions were unclear on the source of their company's insider risk;
- In the past year, contractors and temporary employees posed the greatest source of insider threat and outsourcing companies lost nearly $800k because of insider breaches;
- 5830 malware/spyware attacks originated from the inside;
- 5794 incidents were from abuse of privilege and access control rights;
- 19% of the attacks were believed deliberate.

Critical national infrastructure (CNI) implications must also be considered, particularly where a CNI organisation's information is in the hands of third party foreign nationals. The NIAC (2008) highlights that insider risks extend far wider than just one organisation as impacts can cascade across sectors and into the state's CNI. NIAC (2008) also concludes that economic espionage from nation-state threat sources poses a real threat to both company and national competitive viability.

On a smaller scale, the threat of insiders exploiting their positions to steal customer information has become a regular media event, particularly in outsource environments. It has been reported (Raywood, 2008) that the placing of moles by criminal gangs, especially in financial institutions, is becoming common. This is likely to be facilitated by poor background checks (or a lack of even basic recruitment vetting). Effective checks and vetting can be time-consuming and expensive. In effect, many organisations hire strangers and give them access to sensitive information. These moles are then able to operate unchallenged over a period of time. The Information Security Forum (Muncaster, 2009) and other research (Castle, 2009) conclude that many criminal gangs are not only launching external attacks but that they are now applying more targeted attacks to infiltrate organisations via insiders – in order to seek specific information or exploit the access that the job might provide.

2.3. *Action is required*

Insider threats and risks require assessment, prioritisation and, most of all, action rather than reaction. Cole (2008) crystallises the issue: "The insider threat is like a tumor. If you realise there is a problem and address it, you will have short-term suffering but a good chance of recovery. If you ignore it, it will keep getting worse and while you might have short-term enjoyment, it will most likely kill you."

Even taking into account the recognition that insiders present growing security risks, the response of organisations varies considerably. Cole (2008) believes that there are three key reasons why the insider threat is being ignored:

- Organisations do not know it is happening;
- Organisations fear bad publicity;
- It is easy to be in denial.

The author suggests that another underlying reason is that organisations now appreciate that the threat is real but don't know what to do with it. Hacking and insertion of malware from external sources tend to be public affairs with known signatures and wide-spread reporting and discussion.

However, there are often few measures in place to identify insider attacks, let alone monitor them over time. Organisations should therefore make efforts to reach out to others who may have a better understanding of the threats. NIAC (2008) found that partnership and information sharing on insider threats and attacks are key components to the success of protection. Success in information sharing is dependent upon building strong public–private partnership and establishing trusted relationships among the key players in each sector and with the government. This is sometimes not even attempted as it is perceived as too difficult and that significant barriers exist. The fear of public and market reaction to insider risks and attacks is a key barrier to sharing information. Insider attacks are often viewed as 'one-offs' and kept private and consequently the true scale of such attacks and their impacts is difficult to measure. BT's experience shows that developing information sharing relations via a trusted 'broker' has many beneficial results to create new security standards and raise overall levels of protection: in the UK the Government's Centre for Protection of National Infrastructure (CPNI) can act as broker within sectors and across sectors that comprise the CNI.

2.4. *How do we start to address the insider threat?*

Denying that the insider threat exists is no longer acceptable, but even when the threat is acknowledged, knowing where to take the first bite of the elephant can be difficult. A study by the Ponemon Institute (2007) found that 60% of senior information security professionals believe their businesses are unable to effectively assess or quantify insider risks even though they realise the dire risks posed by this inability. Little seems to have changed.

Ineffective focus on threats will lead to wasted investment and a false sense of security. Appropriate focus can only be achieved by ensuring a risk management approach to insider dangers. There should be no doubt that threat actors and threat sources will exploit insiders and the onus is the organisation to ensure that the risks associated with insider attack are qualified and quantified and that cost-effective mitigations are identified. This will require asking questions and assessing scenarios that are frequently avoided (for example, recognising that those most trusted can cause the greatest impact). Equally, security assessments must take into account explicitly human behaviour in the context of changing technical, social, business and cultural factors.

3. Technical and social factors affecting the insider threat

Technology is changing social attitudes by making data and mobile communications increasingly available and easy to use. This capability to exploit new opportunities is having a major impact on social interactions and social structures both at home and work.

3.1. *Technology is impacting on social interactions*

In recent years there has been a rapid merging of the systems and applications used at work and home. Applications previously used only at home now appear on business systems. As a result, employees are challenging the technology status quo in their organisation. The EIU (2009) believes that more workers are demanding "technology democracy", that is, a greater freedom to use the IT applications and devices of their choice in order to communicate and conduct their work more effectively. This so called *Generation* Y (also known as the "millennials") is populating the workforce in increasing numbers and soon they will occupy middle management posts. Increasingly reliant on technologies such as personal networking sites and instant messaging, this generation will challenge the established modes of IT (and security) management in organisations. Some believe that we have already reached the time when more businesses will allow their employees to use the devices they want at work as technology development becomes increasingly consumer driven (Flinders, 2010).

3.2. *Security is not keeping up with technological and social changes in the workplace*

The threat from employees being lax with or ignorant about security is likely to be exacerbated as people merge their working and home lives. The National Computing Centre (Mohamed, 2009) states that individuals find it difficult to have a true boundary between work and home life and that they spend time sharing personal and business information on social networking sites with "a trusting innocence". This leaves themselves and the organisation open to range of issues from pornography and music downloads to a variety of malware attacks. Thomson (2009) argues that organisations have buried their heads in the sand over the use of social networks and mobile technology in the workplace and need to start dealing with the risks. Pressure is growing on companies to give staff greater freedom but technology democracy must be supported by clear rules and regulations to prevent a descent into chaos. Few organisations appear to be providing this guidance and risks and rewards must be balanced (Miller, 2010).

On a basic technological level, portable data devices facilitate information compromises from the inside: research (Kavanagh, 2006) showed that 89% of employees connected a personal portable device to their company network at least once a week and that more than half of UK businesses had no controls to manage the use of removable media devices. People have been tricked into using an apparently abandoned USB memory stick loaded with a "friendly" Trojan and, similarly, people in the security-conscious financial services industry in the City of London loaded free CDs onto systems despite clear warnings printed on the CDs to check company guidelines before loading.

Security policy, controls, guidelines and training are lagging behind changes. Most executives in the EIU (2009) survey claim that their firms have drafted IT policies to govern employees' use of devices, applications and websites, but few have begun to instil these guidelines in the minds of employees: only 21% of surveyed firms provide training on the use of personal communications devices and only 17% do this for social networking applications. More worryingly, only 20% have plans to increase awareness in the future.

4. Business and economic factors affecting the insider threat

The business world has changed. All organisations, particularly commercial businesses, are faced with creating new strategies to survive in dynamic national and international markets. The current global recession is causing much pain as traditional business models become defunct, costs increase, revenues decline and sources of investment dry up.

4.1. *Outsourcing can increase insider risks*

In today's increasingly competitive environment, most organisations have had to transform and outsourcing is a common means to achieve this. The number of third party personnel given long term access to organisations' critical systems and information is growing rapidly. A single outsourcing transaction can change the status of many hundreds of 'outsiders' to 'insiders' and may blur the distinction between a company's employees and third party personnel: they may be granted logical and physical access levels on par with an organisation's full time employees. Sometimes components of security infrastructures are also outsourced. Whether the sourcing is onshore or offshore there is a growing number of third parties and contractors (usually foreign nationals) who are given long term access to critical systems and information. Dynamics in workforce markets are increasing the rate of employee turnover, which in turn, increases the exposure of companies to intellectual property loss and the likelihood that high-value or high-impact knowledge could be transferred to a competitor or other outside sources.

A further issue is that offshoring information may be creating an aggregation of data from a large number of organisations – that do not knowingly share information – into a relatively small number of regions and centres. This presents opportunities for malicious insiders who now have access to sets of information that have not previously been brought together and for which none of the individual contributing offshoring parties have responsibility or an understanding of the implications. This will not have escaped the eyes and ears of criminals, foreign intelligence services and terrorists.

4.2. *The global recession is affecting insider behaviour*

The pressures of the current economic problems are creating many drivers that will affect employee motivation. CEOs and managers have to reduce costs, increase sales and revenue and improve debt ratios, balance sheets and income statements. As a result, most organisations are now subject to 'headcount challenges', possibly on a scale not seen in a generation; similarly many are facing pay freezes or cuts. This will impact on the long-term employees and those where most trust and loyalty is expected; senior managers and security teams are not exempt.

Research shows that the global economic recession is changing behaviour and this has direct implications for insider attacks at all levels of the organisation. McAfee (2008) believes that the recession is creating a fertile ground for cybercriminals to dupe unsuspecting insiders into divulging sensitive information about themselves and their organisations. Surveys also show that there is a direct correlation between falling national prosperity and increasing crime rates, so as more people feel the bite, the more inclined they are to become involved in illegal activity (Mohamed, 2009). Under these circumstances, levels of loyalty and trust will be tested. A survey carried out by Cyber-Ark (2009) shows that:

- 35% of IT workers admit to accessing corporate information without authorisation;
- 74% of respondents stated that they could circumvent security controls to prevent access to internal information.

HR records and redundancy lists are now likely to be key targets for insiders. The surveys (Mohamed, 2009; Cyber-Ark, 2009) also reveal that as the economic climate worsened, there was a sharp increase in the number of respondents who said that, if fired or made redundant, they would take proprietary data and information critical to maintaining competitive advantage and corporate security. There was also an increase in those who would take financial reports or merger and acquisition plans, CEO passwords and research and development plans.

5. Cultural factors affecting the insider threat

At least two cultural perspectives must be considered when examining the insider threat: organisational culture; and national/regional culture. Both of these can impact on behaviour and the effectiveness of levels of information protection.

5.1. *Organisational culture*

Of all the data losses reported by the UK Government since the incident at HRMC, only 5% is believed to be due to technology issues whilst 95% is due to cultural factors or the behaviour of people (Royds, 2009). Most organisations are undergoing some form of transformation and traditional cultures are being dismantled and rebuilt – including perceptions and behaviours towards security. However, if not addressed explicitly, cultural change can cause fear, uncertainty and doubt in employees which can impact on attitudes towards security. Change must be managed. Within BT, transformation programmes now utilise the *Congruence Model* (Oliver Wyman, 2008) which looks at the 'fit' of changes to both formal and informal cultures as well as the infrastructure and processes of the organisation; this model is also being used by security teams as an analysis tool.

5.2. *Regional culture*

Regional and national attitudes and propensities towards crime differ significantly as does the means of protecting against them. The lack of long-term experience of (and more importantly a thorough understanding of the reasons behind) critical security controls such as physical and logical access logging and analysis, can lead to a lip service approach. It is often difficult for Westerners to understand some of the cultural, religious and societal pressures, for example, the caste system and hierarchical implications in India: orders are expected to be obeyed and the rules required at work will always be less important than behaviour ingrained over countless generations. Outsourcing highlights the language differences that can cause problems of misunderstanding and misinterpretation at all levels. Most Westerners responsible for writing contracts and security requirements will have little or no experience of the country in which they will be applied. Even where there is no disagreement over the explicit meaning of the wording, the implicit perceptions and expectations behind them may differ – driven by the history of security approaches within any given company and country. BT provides opportunities for those writing third party security policies to get involved in offshore reviews and audits to help educate them on potential implementation issues.

Acceptable norms for doing business also differ according to region. Practices that are considered illegal in the Western world, for instance the giving of substantial gifts (namely bribes), may be a common and accepted practice in some regions where the wheels of business need to be "oiled".

It is under these different regional circumstances that the influence of external sources on insiders may be easier to apply, either directly by coercion or indirectly via sophisticated social engineering methods.

6. Why and when do insiders "go bad"?

The linkage between *potential* threat and *actual* malicious action must be explored. Insider attacks are made with varying degrees of motivation, opportunity and capability. *Motivation* will come from internal, personal drivers, whereas *opportunity* and *capability* will be given to insiders overtly by your organisation to perform their role, or may be attained covertly once they are on the inside.

6.1. *Trust and loyalty*

Employee trust and loyalty are oft-quoted Holy Grails. It can be argued that organisations with a large percentage of long-term personnel have seen more buy-in to security, not for security's sake, per se, but by strengthening reliance on the organisation and the desire to see it survive to protect the employees' own futures. This situation was supported by clear, long-term career structures and reward schemes. The resultant organisational culture facilitated the development of personal relationships with other members of staff and management and helped enhance levels of underlying personal trust, loyalty and mutual dependency. The situation has changed significantly and it is now more normal for staff to move between organisations and regions on a regular basis to improve their financial position and advance their career. This may result in less affinity, a 'loosening' of loyalty and a difficulty in stabilising organisational culture. Note that homeworking tends to reduce contact with other members of the organisation and may inhibit the development of relationships and bonds that usually help to forge loyalty to the team and the organisation. Effort should therefore be made to ensure periodic team interactions and bonding events and face-to-face meetings.

Changes to the nature of employment have affected the control that the organisation has on its infrastructure, culture and the relationships and levels of trust that can be developed with the people that work within its boundaries. Outsourcing strategies may create additional problems: staff may fear that their roles are next in line for offshoring and may feel alienated and disaffected. For the third party employee, loyalty is difficult to achieve in a call-centre with deskilled jobs, short contracts and 40% churn of staff. These people will have lower levels of company and country affinity and loyalty but, as effective insiders, may be given privileged access to information within your organisation. We are now faced with varying perspectives of loyalty, for example, loyalty to customer (who will seem an intangible entity far removed – geographically and culturally – from any considerations of reward), loyalty to organisation (the outsource supplier who actually pays the employee's wages), loyalty to country or culture, loyalty to profession or straight-forward loyalty to pay cheque.

6.2. *Factors leading to attack*

Much focus has been made on linking 'disgruntled' employees with insider attacks. This provides only a stereotype and an oversimplification could lead to a focus on the wrong people, for example, union officials and employees with genuine grievances. NIAC (2008) finds that there is no direct correlation between disgruntled workers and insider threats and that the majority of disgruntled employees never come close to betraying their employer. True analysis of motivation and betrayal requires complex psychological analysis and will vary from individual to individual. Shaw et al. (1999) identify six personal characteristics believed to have direct implications for malicious insider risks:

- False sense of entitlement – lack of acknowledgement or status resulting in a desire for revenge;
- Personal and social frustrations – anger, alienation, dislike of authority and an inclination for revenge;
- Computer dependency – aggressive loners, poor team players, desire to explore networks, break security codes, hack and challenge security professionals;
- Ethical flexibility – lacking moral inhibitions that would normally prevent malicious behaviour;
- Reduced loyalty – identifying more with their profession or computer specialty than with their employer;
- Lack of empathy – disregard or inability to appreciate the impact of behaviour on others.

NIAC (2008) concludes that people who commit malicious insider actions have a causal experience or mechanism that affects motivation and leads to betrayal. These experiences can be classified into three main sources:

- Growing, exacerbated or unaddressed discontent with their place or value in the organisation;
- Recruitment by hostile outside entities or groups;
- Infiltration of a malicious threat actor to a trusted position.

Militant religious fundamentalism, particularly Islamic, may be leading to a growth of potential terrorist sympathisers. These people may see no moral or ethical problems in providing their religious mentors with information for attacks against 'Western' culture because their motivation comes from a desire to make a high-profile statement rather than cause direct harm to the organisation in which they work. The process of radicalisation is dynamic and it can occur after employees have gained the trust of their employers, such as passing background checks. To the above must be added the uncertainty and unrest caused by the current global recession, on a scale few workers will have experienced before. This may act as a catalyst for bringing to the surface many of the characteristics listed above – via internal fears or by exploitation from external sources.

6.3. *How do we detect shifts towards malicious action?*

Identifying the warning signs for malicious insider behaviour is a major challenge for most organisations, as is taking appropriate action to resolve problems; this requires time, effort, investment and, most of all, commitment. A common finding of most post-incident investigations is that warnings signs of changes in people's attitudes, behaviours and actions had been seen by others but that nothing had been done about it. People may have noticed indications that something was wrong but failed to report the activity because they did not understand its significance, felt that it was not their job to take any action or they did not know how to report it to. This tendency for inaction must be addressed. Any display of potential betrayal characteristics, as listed earlier in this paper, should be reported.

Monitoring staff activity can lead to a clash of security controls and human factors. Some employees will be unhappy if they believe they are under constant scrutiny whereas others may find this a comfort. Perceptions and expectations will vary from office to office, department to department and across organisations. Employers do have the right to monitor employee activity and should not shy away from this fact, even though the subject of employer 'snooping rights' is very topical (Marsden, 2009). There is no correct model other than ensuring an effective balance. Anonymity will usually play a role in determining malicious insider actions as most individuals have inhibitors to being caught if they break the rules (typically they can lose their job or may face prison). Everyone should comprehend that their actions are under a magnifying glass. Equally controversial is the provision of a formal 'whistle-blowing' facility for staff to report other insiders perceived to be breaking the rules or acting suspiciously, with potential rewards for helping to reduce risk and impact.

The CPNI (2009) highlights the need for all staff to recognise attempts at manipulating other staff or for planning sabotage. Manipulation may using a range of influencing techniques and social engineering to create situations whereby someone will willingly provide access to information, systems, sites or people to someone unauthorised to receive it. These techniques aim to exploit basic human tendencies such as returning a favour or helping a colleague in need. Attackers may try to gain information piecemeal over a period of time or through seemingly innocent conversations. Determined attackers will be well-prepared and be able to demonstrate affinity and rapport with other staff. They might send emails with attachments containing malicious code, pretend to have lost computer passwords or be acting on a manager's urgent request. Sabotage and denial of service attacks on information are very noticeable and are usually committed by a former employee seeking revenge because of a personal grudge caused by an experience such as dismissal. Such attacks are typically planned well in advance – and may therefore provide warning signs. Sabotage does not have to be committed onsite but can be triggered remotely or via 'logic bombs'. Methods of defending against manipulation and sabotage risks include (CPNI 2009):

- Providing specific training in detecting manipulative attempts to all customer facing staff;
- Warning all staff to be alert to anyone asking for sensitive or restricted information;
- Being alert to all unknown enquirers who try to extract information in a rush, with intimidation, stressing authority or refusing to give contact details;
- Encouraging managers to be alert to individuals who are excessively negative about the organisation or their work;
- Establishing a formal grievance procedure for staff to vent their feelings;
- Setting up an easy and confidential system for staff to report any abnormal behaviour from their colleagues;
- Backing up information and keeping a secure copy in another location;
- When employment is terminated – for whatever reason – ensuring that all access to systems, sites and information is ceased.

The search for warning signs of adverse insider behaviour shifting from potential concern to actual attack needs to be kept on the agenda. This should involve a combination of procedural measures and thorough people management and performance management – for all of those under a manager's remit, including third parties. This should lead to a closer relationship between security requirements and 'business as usual' line management. This includes active rather than reactive approaches by both the manager and individual to report changing circumstances. The main objective should be to 'connect the dots', that is, not just collect disparate pieces of data on anomalous behaviour but to collate and analyse the data to determine patterns and courses of remedial action.

Once action to address unacceptable behaviour is deemed necessary, this action should be swift and proportionate; much behaviour stems from ignorance and often all that is required is a discussion on the situation to gauge perceptions and expectations and to reinforce positive secure behaviour. Where a pattern of concerns is emerging, more stringent action should be considered, including the speedy removal of access to critical information and, potentially, security clearances, or straight-forward suspension from duty whilst investigations take place.

Organisations can no longer just concentrate on tracking stereotypes of disgruntled employees but open their eyes to the greater impacts and information compromises that can be caused by 'trusted' insiders. The ultimate question is "who polices the policemen?", especially senior management and security team activity. This can only be dealt with through proper audit and governance frameworks under the scrutiny of external and internal stakeholders and independent bodies. Within BT this is achieved under the remit of the internal audit division who report to non-executive board members; equally, many of BT's processes involving sensitive data are open to examination by the UK Government and other major customers.

7. The importance of non-technical mitigations for the insider threat

There is little argument that minimum technical controls against insider attacks should include:

- Encryption;
- Access control;
- Minimum privilege;
- Monitoring, auditing and reporting.

However, even though technical controls have improved, organisations should realise that their people can be their greatest vulnerability. A balance with non-technical, human factors is required and a holistic perspective should be maintained (Jones and Colwill, 2008). This requires a focus on human factors, perceptions and expectations and not a simple 'tick in the box' exercise.

7.1. Enforce baseline security policies and procedures

Effective implementation of security policy is essential: even though most companies have policies, only a minority appear to enforce them (Kavanagh, 2006). Organisations need to establish clear and consistent rules for what is expected of their insiders. One approach is to enforce policies strictly and prohibit any personal use of company assets in the workplace. This would involve locking down networks to all but essential business applications and strictly controlling access to non work-related websites to ensure legal compliance, avoid time wasting and prevent the risk of malware infections. Attention should also be paid to effective employee classification to define granularity in access rights for all types of insiders, including third party personnel. BT applies strict control and auditing to all forms of connection and access to corporate logical and physical assets.

7.2. Extend traditional policy and guidance

All employees should be made aware of acceptable and unacceptable behaviour in the workplace. The use of guidelines, if not formal policy, is a means to achieve this. 'Grey areas' must be addressed to establish clear accountability for actions and setting expectations and boundaries for employee conduct. Acceptable personal use of email, the internet and social networking sites are key targets today. If employees have no rules or guidelines they will form their own views of what is and is not permissible and this can make it difficult for the employer to achieve a united approach, to maintain security and to take disciplinary action when necessary. Clear parameters are needed highlighting situations where individual may come close to malicious action, together with the consequences of misuse.

7.3. Conduct ongoing personnel checks

Effective employee background checks and vetting are essential. All organisations should screen new employees to validate their past employment and other background details to verify they are who they say they are and that they have done what they say they've done – before they start working for you! It is also important that it is applied to all levels of staff, especially management and people assigned to roles that have been given powerful privileges. More stringent vetting must be applied to those with access to sensitive information (for example, commercial or Government data). Employee vetting can be an effective means of ensuring a basic level of trust at a point in time only, however, because people's circumstances, attitudes, behaviours and motivations will change over time. The importance of vetting 'aftercare' cannot be underestimated. Staff must be monitored over time for changes in their role, personal circumstances and behaviour, especially for security people with higher levels of clearance. Responsibilities for this aftercare must be understood and met by both the individual and their manager. In the UK, the CPNI (2008), provides comprehensive vetting guidelines. BT has built these guidelines into its procedures. Wherever practicable, requirements should be extended to third party insiders.

7.4. Implement focused risk assessments

In simple risk modelling terms, human threat can be decomposed into the factors of *motivation*, *opportunity* and *capability*. These factors should be included in insider threat assessments and BT uses tools based on HMG's *IS1 Method* (2008) to achieve this. Specific analyses are conducted on the number and type of people required to collude effectively to subvert or compromise key assets, functions or processes, not just to effect an attack but for the capability of increasing access privileges or altering logs. The influence of external threat sources that can influence on insiders such nation-state, terrorist or organised crime should be included. This decomposition will also help identify mitigation controls: a mixture of technical and procedural measures exist that can be used for *opportunity* and *capability* but addressing *motivation* is often more difficult, with awareness and deterrent measures featuring strongly. The implications of the rapid expansion of outsourced insiders should also be considered.

8. Education is critical – security training and awareness

Protecting an organisation's information is the responsibility of all staff. Education, training and awareness are perhaps the greatest non-technical measures available and a common theme for human factors and security. Security topics and requirements need to be integrated into normal business behaviour, through clear policy and staff education. Many insider problems stem from ignorance rather than malicious motivation but this is equally dangerous because accidental failures can have large impacts and interconnection can increase the potential scale of impact. Within BT, security education is mandatory and audited alongside legal and regulatory requirements.

8.1. *Behavioural change is necessary*

A focus on changing and measuring actual behaviour in the workforce as part of organisational development is required. Basic training and briefings can be used but a greater focus on integrating security awareness and understanding into organisational culture is required. Insiders must change their behaviour in order to protect assets and information; this requires not just increased the awareness of staff but their buy-in to the security cultural values of the organisation.

Sasse et al. (2007) highlight that awareness and education can prepare the ground but changing behaviour involves *breaking* old habits and establishing new ones via targeted training. To be truly effective, this needs to be more than regurgitating security policies but a *process* of building understanding, empathy and ownership, and developing knowledge of situations that cause security risks and the behaviours and reactions required. This emphasises the importance of organisational behaviour and 'citizenship' – involving the informal aspects of work roles and relationships that can be managed via personal 'psychological contracts' negotiated with employees, rather than depending on a command and control approach. Acceptable use policies and guidelines can be used to facilitate such contracts.

Culture change should also cater for regional and diversity issues that affect the workforce, whether they are direct employees or as part of the extended outsourced workforce. This may require the development of local measures and processes.

8.2. *Ensure real understanding of the reasons for security controls*

Security education and awareness programmes should aim to enhance levels of trust between employer and employee by developing an understanding of the reasons for the security policies and controls that have been applied – and the fact that they are in everybody's long-term interest. Education on the real security threats and vulnerabilities that exist is needed, for example, social engineering methods or the use of untrusted sources, devices and other unsafe computing practices. These will have deterrent effects and staff will be more aware of the issues and are more likely to recognise and report any suspicious activity.

Unacceptable, non-malicious behaviour should also be targeted, for example, those who attempt to cut security corners to meet business deadlines. Increased staff awareness should also reduce the likelihood of accidental breaches and increase the probability of malicious activity being detected and reported. Effort should be made to ensure that no insiders can plead ignorance to the rules. Some cultures may defer to managers' actions even when these actions are known to break the rules and this behaviour must be changed. Messages need to be applied to every level of the organisation, together with potential sanctions for abuse. Ongoing awareness programmes are essential in environments with large turnovers of staff, though measuring the success of such programmes can be difficult.

A key success factor is demonstrating that the security controls deployed (including employee monitoring and associated sanctions policy) are proportionate to the potential risks involved and not heavy handed or ineffective. Good security behaviour should be reinforced and rewarded. Some organisations emphasise that monitoring can actually benefit staff where employees are reassured that the company they work for is safeguarded against confidential leaks and hence possible damage to its reputation or financial loss – this can protect jobs. Monitoring can also protect employees against false accusations (Kavanagh, 2006).

8.3. *Educate those outside your organisation*

Third parties are now always present somewhere in your organisation and may require education on par with your full time employees. Effective education will remain difficult in outsourced environments where providers are growing rapidly and hiring thousands of new employees in a month; this requires significant training in the supplier's standards, let alone the supplier's customers. This has a cost and from BT's experience it has proved beneficial to provide the third party supplier with training material, for example, computer-based training (CBT) and onsite training personnel. In certain regions, additional consideration should be given to the way in which organisational ethics are promoted and the way in which staff are trained and rewarded.

9. Conclusions

This paper has examined many human factors and themes that can be used for assessing and managing the insider threat. The following insider topics addressed by BT to achieve this are pertinent to most organisations:

- Do not deny that there is a threat as this will result in failures;
- Raise insider risks and impacts to board level;
- Perform appropriate risk assessments taking into account insider motivation, opportunity and capability;
- Accept that those in trusted positions may cause you the greatest harm;
- Expect accidental information breaches to be more likely than malicious attacks;
- Do not wait to take action until you've been attacked or leak information;
- Encrypt all sensitive information and communications;
- Apply your policies consistently (including acceptable use);
- Apply and maintain minimum privilege ALWAYS;
- Monitor behaviour and identify opportunities to reinforce positive security attitudes to enhance commitment and ownership (people want to know "what's in it for me?");

- Monitor and audit the success of your policies and controls;
- Perform thorough background checks and ensure effective aftercare;
- Address cultural issues at a variety of levels;
- Realise that the recession is causing unpredictable changes in attitudes and behaviours;
- Share insider risks and attack information outside your organisation, using a trusted 'broker', where necessary;
- Explicitly review the risk of aggregation of information via outsourcing;
- Apply strict exit controls on staff that are likely to leave;
- Accept the maxim "education, education, education"!
- Balance investment between outsider and insider threats.

In conclusion, it should be accepted that the insider threat to information security cannot be eliminated but that it can be assessed and managed. Accidental information compromises should not be allowed to happen. The human factors discussed in this paper provide practical levers to gain a better understanding of the real risks facing organisations in today's global commercial environment. Organisational transformation, especially when involving outsourcing, shifts responsibilities and creates a complex mixture of 'hostile' environments and an increase in insiders with lower levels of trust and loyalty. No organisation exists in a vacuum and most employees do not just exist for work. The changing organisational, cultural, technological, social and economic environment will continue to place demands on organisations to re-evaluate the way in which they access and protect information assets. In times of increasing interconnection it is essential that insiders are given access only to the information that they need for the period that they need it, that their use of this information is monitored and that any abnormal behaviour is investigated and acted upon.

Who can we trust? – This will be dependent on the success of a combination of procedures (such as vetting) and people management (to understand your staff and notice changes in their behaviours and characteristics). We have to trust insiders but trust and loyalty can be transient and must no longer be assumed but supported by the appropriate demonstration and evidence of behaviour and understanding. Trust created via personal relationship remains crucial but must be complemented with periodic checks, reviews and management.

Technology can provide a means for controlling access to information and help the monitoring and detection of malicious activity, but it is the working environment and human factors that will provide the real foundations for success. Changes must be supported by ongoing education and awareness and a means of measuring success. In terms of mitigation controls, technology should not be considered in isolation: if people do not co-operate with, and comprehend the reason for security controls, they may find cause and means to subvert or circumvent the technical restraints imposed on them, particularly if they impact on reward (Sasse et al., 2007). Security controls must therefore be agile and workable in a variety of environments and, preferably, be developed with end user participation.

Insider risks need to be moved up in importance and discussed in boardrooms prior to attacks, not after a significant information compromise. Proactive measures need to be to taken to stop insider attacks from occurring, not reactive measures to clean up the mess. Risk management and compliance and governance frameworks should be augmented to create a means of recognising, capturing, assessing and testing human factor implications. Taking into account negative public perceptions and concerns about data loss and financial imprudence, all organisations should be able to provide evidence to their customers and stakeholders that appropriate risk processes (including a focus on insider threats) have been applied and that security compliance is being maintained.

Ultimately, human factors and insider behaviour are far less tangible to comprehend than racks of IT components and the security benefits may be longer-term rather than short-term. This must be weighed against commercial realities and priorities: rebalancing spend to face insider issues may require substantial justification in organisations during a time of recession but this is a challenge that must be accepted.

REFERENCES

BBC. Five British soldiers shot dead, 4/11/09, http://news.bbc.co.uk/1/hi/8341659.stm; 2009a.

BBC. Deadly shootings at US army base, 6/11/09, http://news.bbc.co.uk/1/hi/8345713.stm; 2009b.

BERR. Department for business Enterprise and regulatory Reform (BERR) information security breaches survey 2008, http://66.102.9.132/search?q=cache:LK4aPYKu4gcJ:www.berr.gov.uk/files/file45714.pdf+berr+2008+breaches&;cd=2&hl=en&ct=clnk&gl=uk; 2008.

Blakey R. PwC auditors 'ignored' Satyam fraud for fees, The Times, 24/4/09, http://business.timesonline.co.uk/tol/business/industry_sectors/technology/article6154910.ece; 2009.

Castle I. Beware the enemy within, secure computing Magazine, 5/1/09, http://www.scmagazineuk.com/Beware-the-enemy-within/article/123505/; 2009.

Cole E. Addressing the insider threat with NetIQ security and Administration Solutions Dr. Eric Cole and NetIQ, https://www.netiq.com/f/mynetiq/login.asp?title=Addressing+the+Insider+Threat+with+NetIQ+Operational+Change+Control+Solutions&pagepath=%2Fsolutions%2Focc%2Fdefault%2Easp&formid=3048&redirect=%2Ff%2Fform%2Fwhitepaperrequest%2Easp%3Forigin%3Dwebsite%5Fcms%26ctsource%3Dwebsite%5Fcms%26id%3D3048&ForcingHTTPS=1; January 2008.

CPNI. Centre for the protection of national infrastructure (CPNI) ongoing personnel security: a good practice Guide, http://www.cpni.gov.uk/; October 2008.

CPNI. Insider attacks, http://www.cpni.gov.uk/MethodsOfAttack/insider.aspx; 2009.

Cyber-Ark. Snooping about, CIR Magazine; August 2009.

EIU. Economist intelligence Unit: Power to the people? Managing technology democracy in the workplace, http://graphics.eiu.com/marketing/pdf/Technology%20Democracy.pdf; June 2009.

Flinders K. Employees will choose their own computers in 2010, Computer Weekly, 18/1/10, http://www.computerweekly.com/Articles/2010/01/19/239999/Employees-will-choose-their-own-computers-in-2010.htm; 2010.

FT. Madoff Scandal, 12/12/09, http://www.ft.com/indepth/madoff-scandal; 2009a.

FT. Stanford Scandal, 18/12/09, http://www.ft.com/indepth/stanford-scandal; 2009b.

Grant I. Insiders cause most IT security breaches, Computer Weekly, 26/8/09, http://www.computerweekly.com/Articles/

2009/08/26/237455/insiders-cause-most-it-security-breaches-study-reveals.htm; 2009.

NIAC. HMG IA standard No. 1, technical risk assessment part 1 (Issue 3.2); October 2008.

Jones A, Colwill C. Dealing with the malicious insider. In: 9th Australian information and Warfare security Conference; December 2008.

Kavanagh J. Security special report: the internal threat, Computer Weekly, 25/4/06, http://www.computerweekly.com/Articles/2006/04/25/215621/security-special-report-the-internal-threat.htm; 2006.

Marsden R. Should my employer be allowed to snoop on me online, The Independent, 18/11/09, http://www.independent.co.uk/life-style/gadgets-and-tech/features/rhodri-marsden-should-my-employer-be-allowed-to-snoop-on-me-online-1822277.html; 2009.

McAfee. Virtual Criminology report, http://resources.mcafee.com/content/NAMcAfeeCriminologyReport; December 2008.

McCue A. Beware the insider security threat, CIO Jury, 17/4/08, http://www.silicon.com/management/cio-insights/2008/04/17/beware-the-insider-security-threat-39188671/; 2008.

Miller N. Balancing risk and reward in staff web usage policies, Computer Weekly, 19/1/10, http://www.computerweekly.com/it-management/risk-management/; 2010.

Mohamed A. CW security trends for 2009, computer Weekly, 20/1/09, http://www.computerweekly.com/Articles/2009/01/20/234316/security-trends-for-2009.htm; 2009.

Muncaster P. Security experts warn of insider threat timebomb, Enterprise Security Technology, 24/6/09, http://www.v3.co.uk/v3/news/2244699/experts-renew-insider-threat; 2009.

National Infrastructure Advisory Council (NIAC). Final report and Recommendations: the insider threat to national infrastructures, 8/4/08, http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf; 2008.

Oliver Wyman. Congruence model: a roadmap for understanding organisational performance, http://www.oliverwyman.com/fr/pdf_files/Congruence_Model_INS.pdf; 2008.

Ponemon Institute. Addressing the insider threat, community Banker, 1/8/07; 2007.

Raywood D. Companies being hit by moles who are employed by gangs to steal data. Secure Computing Magazine; 2008. 2/10/08.

Royds J. Virtual battlefield. CIR Magazine; August 2009.

Sasse MA, Ashenden D, Lawrence D, Coles-Kemp L, Fléchais I, Kearney P. Human vulnerabilities in security systems, human factors working group, Cyber security KTN human factors White paper; 2007.

Shaw E, Post J, Ruby K. Inside the mind of the insider, security management; 1999.

Thomson. HMRC data loss leaves 25 million exposed, ITN News, 22/11/07; 2007.

Thomson R. Bosses have their heads in the sand over new technology, Computer Weekly, 29/9/09, http://www.computerweekly.com/Articles/2009/09/29/237920/bosses-have-their-heads-in-the-sand-over-new-technology.htm; 2009.

Wilding E. Insiders are the biggest enemy. Strategic Risk Magazine; September 2007.

Carl is a Principal Consultant in BT Security's Consultancy and Information Assurance Services team and specialises in security risk management and information assurance with a current focus on critical national infrastructure and global sourcing activities. Carl leads security studies and compliance reviews for BT and his consultancy role is certified under the UK CESG Listed Advisor Scheme (CLAS). Carl is also responsible for implementing best practice security risk modelling tools and techniques and is the lead of the risk management discipline in BT's security professional community.

Carl joined BT in 1980 after gaining a BSc(Hons) in Computer Science from the University of Warwick. Initially employed in applications and systems programming, he supported the implementation of new field-based systems to assist telephone engineers. Carl subsequently served as a senior systems performance engineer and was responsible for developing and applying techniques to facilitate the monitoring, analysing, modelling and tuning of systems and networks. Since 1990, he has been involved with IT security and risk analysis and has been responsible for managing programmes and projects across BT Group and its ventures. Carl was a founder member of BT's Information Assurance team established in 1997 to assess emerging threats and risks with a national infrastructure perspective.

Carl gained an MBA in 1992; other professional qualifications include Chartered Engineer, Chartered IT Professional, Fellow of the British Computer Society, Member of the Institute of Information Security Professionals, Member of the Institute for Risk Management, Member of the Association for Project Management, IRCA ISO27001 Principal Auditor.