Edith Cowan University
Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2008

Dealing with the Malicious Insider

Andy Jones
Edith Cowan University

Carl Colwill
Security Risk and Compliance, BT Design

DOI: 10.4225/75/57b562dab876e
Originally published in the Proceedings of the 6th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 1st to 3rd December 2006.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/52

Dealing with the Malicious Insider

Dr. Andy Jones[1,2]
Carl Colwill [3]

[1] Centre for Information & Security Systems Research, BT
[2] SECAU – Security Research Centre, Edith Cowan University
andrew.28.jones@bt.com
Phone: +44 1473 646133
Fax: +44 1473 644385

[3] Security Risk and Compliance, BT Design
carl.colwill@bt.com
Phone: +44 29 2072 3169
Fax: +44 29 2072 2168

Abstract

This paper looks at a number of issues relating to the malicious insider and the nature of motivation, loyalty and the type of attacks that occur. The paper also examines the changing environmental, social, cultural and business issues that have resulted in an increased exposure to the insider threat. The paper then discusses a range of measures that can be taken to reduce both the likelihood of an attack and the impact that such an attack may have. These measures should be driven by focused and effective risk management processes.

Keywords: Insider, attack, holistic, countermeasures, risk management

INTRODUCTION

This paper will look at some of the steps that can be taken to deter and to catch the malicious insider and to reduce the threat they pose to organisations at a time when network boundaries are softening and becoming more flexible.

The paper will examine the changing technical, social and business environments, examine the nature of the insider threat and will put forward a number of technical and non-technical measures that can be used to reduce the likelihood of an attack and the impact that such an attack would have. This paper will demonstrate that protecting the organisation from the malicious insider can only be achieved successfully if a holistic approach is taken to securing assets and infrastructure. As this may entail substantial cost, the paper will also discuss why it is essential that the appropriate focus is applied to risk assessments, the implementation and maintenance of security controls and the provision of compliance evidence.

A focus is taken on malicious threats to information assets, but it is important to remember that non-malicious threats (for example, the accidental loss or release of information) can also have a major impact as has been demonstrated by recent cases in the UK (Thompson 2007, BBC News 2008).

In many organisations, the majority of security effort is invested in protecting the assets, whether they are physical or intangible, from those outside the organisation such as thieves, individuals involved in economic espionage and hackers. In reality, a malicious insider has the potential to cause at least as much, if not more, damage to the organisation and has many advantages over an attacker from outside the organisation. These

advantages include having legitimate and often privileged access to facilities and information systems, having knowledge of the organisation and its processes and procedures and the location of the assets of value. They are also likely to know how to achieve the greatest impact or carry out the attack while leaving little or no evidence. While the person outside the organisation will need to gather intelligence before they can take action, the malicious insider already has access to the information needed and will not have to overcome many of the barriers that face the external attacker. It is also worthy of note that it is usually far more cost-effective for an external threat source to place, or subvert, an insider to exploit vulnerabilities rather than launch an attack through layers of protection.

The situation is further complicated by the continuing increase in outsourcing. All outsourcing decisions can lead to the extension and potential dilution or fragmentation of organisational protection barriers and controls and an increase in the number of people that have the access rights assigned to insiders. This can provide new opportunities for threat actors to identify information assets and vulnerabilities in geographic areas that may be more susceptible to targeting attacks as lines of defences are stretched.

THE CHANGING TECHNICAL ENVIRONMENT

Historically, we have protected our infrastructure and networks by placing the majority of the defences at the system boundary. This approach was totally in keeping with the historical precedent of the fortress concept, where the people inside the walls were ‘friendly’ and those outside the walls were ‘the enemy’. In the early days of computing, where the architectures available were largely of mainframe systems where the access terminals were inherently dumb and the systems were managed and controlled by a skilled staff, this was considered to be reasonably effective. In this environment there was tight control on what was, in reality, the very limited processing power and data storage resources of the system and access to these could be heavily regulated.

As a range of technologies developed, faster and more powerful processors, increased storage capacity and much greater communications bandwidths became available. This allowed a transition into a much more distributed environment where the processing power within the networks was increasingly decentralised and ever greater volumes of data were stored locally on the end user device. As a result, the management of the systems also became increasingly decentralised and greater responsibility and trust was invested in the end user. As technologies developed and the ways in which they were used were adapted to make use of the new capability, new procedures and tools were also introduced in attempts to provide protection for the equipment and information in this environment. Examples of this include approaches such as whole disk and file encryption, built in fingerprint readers and virtual private networks (VPNs).

Historically, technological research and development was mainly funded and led by governments for use by the military. As a result of this, the way in which new technologies were brought into use tended to be well considered, with systems being designed to meet the specific purpose that they were required for and heavily tested before being released. This has now changed significantly and business and the commercial sector are the main drivers for technological development, with the result that there is a far stronger imperative to bring the products to market in the shortest possible time and for the new systems to be as widely useable as possible. One of the effects of cheaper and faster processors and larger storage devices has been that the requirement for the software running on the systems to be well coded and as efficient as possible no longer exists. This has contributed to new products being brought to market with less rigorous testing and has resulted in software of all types being used that contain significant flaws and functionality that was not required to carry out the function of the application and that was not required or expected by the end user. In a rapidly changing environment, this has meant that ensuring that the measures that have been implemented to protect assets are working effectively is increasingly difficult.

The environment that has evolved as a result of these enabling technological developments and the demands of the users is of devolved and distributed systems that can be accessed from almost any location using a wide range of devices and services. While many organisations have clung to the barrier type architectures that are well understood and tested and which they have experience with, such as firewalls, Intruder Detection Systems (IDSs) and demilitarised zones (DMZs), the reality is that since the days of the mainframe, these have been of decreasing value and effectiveness. Some organisations have embraced the new environment and have adapted

their protective and defensive measures to more effectively meet the developing needs, but they are in an ongoing ‘arms race’ with the people who seek to attack their systems and must constantly re-evaluate the risks involved in adopting the available technologies. This now brings with it significant cost, scalability and compatibility issues: the cost of maintaining a large, layered defence infrastructure could be on par with that of running the systems essential to the core purpose of the organisation.

THE CHANGING SOCIAL AND CULTURAL FACTORS

At the same time that technologies have continued to develop, there have been significant changes in the social and cultural issues that affect the way in which technology is used. In the early days, computers and networks were precious resources that were an exclusive domain and were available to only a few trusted individuals. As they became more widely available and integrated into business processes, so the circle of people that had access to the computer systems expanded. The increasing speed of the computer processors and greater storage capacities, the reduction in the size of the devices and the increase in communications bandwidths have continued to provide the opportunity to exploit the technologies for ever more diverse purposes.

With the increasing integration of technology into all aspects of our lives, the level of familiarity and user competence has developed so that a far greater number of people now have a good understanding of how the technology works and how it can be employed. The cost of the devices has dropped which has made them increasingly affordable for leisure use, particularly as the western world has become more affluent. The systems used at home are now the same or similar to those used at work and the user interfaces for both types of systems are becoming more intuitive. Technology has provided the capability to exploit opportunities to communicate and enjoy greater mobility. We are becoming increasingly interconnected in every aspect of our lives – between individuals, organisations and countries - and interconnection can bring with it a host of unexpected functionality, vulnerabilities and opportunities for experimentation and exploitation. Younger generations are considered to be greater risk takers (Greenfield, 2007) and, combined with greater computer literacy, exhibit a willingness to explore the functionality and push capabilities (and rules) to the limit – both outside and inside work.

Mobility is also having a major impact on social interactions and social structures both at home and work. One example of this is the concept of remote working, where a person works in one part of the country while living in another, which has become increasingly achievable and acceptable. This has seen a growth in the ‘home worker’. In the past, staff worked in office or factory environments but as technology has enabled the change, so increasingly has it become acceptable and desirable for people to work either at home or be based from home. The business benefit of home working is that the cost of staff accommodation can be significantly reduced, there is access to a wider pool of potential employees and there is a perceived improvement in staff morale. Mobility and in particular overseas travel for business and pleasure, whist maintaining connectivity with home and work, has also become both achievable and popular, although events such as rising fuel costs and concern about carbon footprints may change this.

THE CHANGING BUSINESS ENVIRONMENT

The business environment of the past was of predominantly single focus businesses that concentrated on their core area of expertise and knowledge, but undertook all of the associated disciplines such as human resource management, payroll and logistical support to achieve this. This has changed significantly as the result of organisations diversifying and de-risking in order to survive and prosper. It is now much more the norm that commercial organisations are operating in a number of markets and market sectors and as a result of globalisation, there are increased levels of competition. Partially as a result of this there has been a significant increase in the rate at which takeovers, mergers, de-mergers and partnerships are taking place.

In order to survive in this increasingly competitive environment and meet the growing demands of the customers, organisations have also had to become adaptive. One of the ways in which organisations have changed to meet this is to reduce activity cycle times. However, doing this without an effective agile and flexible environment could result in greater tolerance of errors, an increased level of risk and creates a more volatile

environment. Decreased timescales may also increase the willingness of employees to cut corners in order to expedite the delivery of products and services or to sign contracts.

Increased speed and capability in computer processors and communications links have enabled businesses to implement fundamental structural changes in the ongoing drive to reduce the costs of operation and maintain profitability. These changes have included the rationalisation of organisations with the removal of multiple layers of management, the return to core competencies and the resultant outsourcing, partnering arrangements and the use of sub-contractors. Global communications provide opportunities to outsource and offshore functions that were previously carried out strictly within the organisation in the home country to new locations virtually anywhere around the world. This can involve moving organisational activities to regions where the taxation structure is more beneficial, where the costs of the infrastructure or manpower are lower and where overseas companies offer services at a competitive price or can provide scarce skills. Sourcing may not only result in data or functions being physically offshored but may also provide offshore access to a host of onshore data and activities.

Outsourcing has become ubiquitous for both public and private sectors. The number of third party personnel who are given long term access to company critical systems and information is growing rapidly. This was highlighted by Colwill (2008) who notes that 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. This rapid expansion of the class of *outsourced insiders* could pose a distinct threat that should be considered in security risk assessments. The term "third party" can covers a diverse collection of outsiders who become insiders and who may be granted logical and physical access levels on par with a company's full time employees, for example, outsource vendors, suppliers, contractors, support and maintenance personnel, together with guards and cleaners. These people work within the extended boundaries of companies, often with privileged access rights and varying levels of operational control and opportunity for attack, but typically with lower levels of company and country affinity, loyalty and trust.

A further issue is that offshoring information and processes to the new global sourcing regions and companies 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 centres. This has created threats from malicious insiders who now have access to sets of information that had not previously been brought together and for which none of the individual contributing offshoring parties have responsibility or an understanding of the implications. This could have major repercussions for intellectual property rights and the impacts of such aggregation should be considered in security risk analyses.

WHAT IS THE THREAT?

Insider security threats come in many shapes and forms and it is usually necessary to perform threat and risk assessments that take into account the three key properties of information security ('confidentiality', 'integrity' and 'availability)' and the potential impacts that could arise from the compromise of these properties. In the USA, the National Infrastructure Advisory Council (NIAC, 2008) has stated that the insider threat must be considered real and serious: impacts can be far wider than just one organisation and may cause consequences that cascade across sectors and into nation state critical national infrastructures. The NIAC also found that economic espionage poses a significant threat to competitive viability and that awareness and mitigation of insider threats varies greatly among companies and sectors and is often dealt with poorly. The true scale of insider attacks and their impacts is however difficult to measure, as most organisations, especially large private companies, may be reluctant to publicise incidents or share information on attacks and losses due to the adverse commercial impact it may have.

The threat of insiders exploiting their positions to conduct confidentiality attacks is often highlighted in the media, particularly cases involving the theft of customer information in outsourcing environments (Annesley 2006, Biswas 2005, BBC 2006). These threats and crimes, whether individual or organised, are usually for direct financial gain, for example, selling customer personal or financial and credit card information. It has been reported (Raywood, 2008) that the placing of moles by criminal gangs, especially in financial institutions, is becoming common. These insiders have then been able to operate unchallenged over a period of time aided by

the fact that in many cases, the companies had made the mistake of storing all sensitive and confidential data (financial and intellectual property) in one place which makes it very easy to target.

Attacks on the integrity of information and systems tend to relate to financial fraud or 'cooking the books' which remain prime motivators for insider attacks. Wilding (2006) 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 and Societe Generale, have all been the result of failure in internal controls and abuse by a small number of employees with legitimate authority: *trusted insiders*, usually in senior positions. However, new, insidious integrity threats may be driven by longer-term objectives, for example, planting a wide variety of 'malware' (malicious software) to effect confidentiality or availability attacks at some time in the future or to poison critical data over a period of time (for example compromising access monitoring logs or back up data sources to frustrate recovery from availability attacks). This malware can come in many forms such as 'time bombs' (code activated at certain times/events) and 'backdoors' (to allow unauthorised remote access and/or control) to sophisticated means of monitoring user activity, stealing information and capturing logon credentials.

Attacks on the availability of information or systems usually involving the disruption of critical services, tend to be readily detectable and the potential sources of attack identifiable. As such, these are relatively rare from an insider perspective unless the attacker has no fear of being caught: anonymity and accountability usually play a major role in determining malicious insider actions as most individuals have inhibitors to being caught; they can lose their job or may face prison.

The linkage between potential threat and actual malicious action must be considered within risk assessments. Attacks by people within your organisational boundaries 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. Once again, technology is an enabler, for example the use of small USB devices (such as memory sticks and wireless dongles) for confidentiality and integrity attacks. There are few realistic controls that can be applied to motivation (other than, perhaps, awareness and deterrent measures) but a mixture of technical and procedural mitigation measures exist that can be used for opportunity and capability.

It is not only current employees or outsourced insiders that pose a threat. Former insiders may now lack access, but they might have retained knowledge of information, security measures and vulnerabilities that can be exploited personally or sold on to outsiders.

Loyalty and Betrayal

In the past, staff used to work for the same organisations for long periods of time. This was partly a result of the structure of the businesses and was also influenced by the lack of mobility of the employees. People were largely reluctant to relocate and as a result, they worked for the organisations that were operating in the area that they lived. One result of this was that staff developed a loyalty to the organisation, partly because of their reliance on it for employment and the desire to see it succeed in order to maintain the norm. They also, for the most part, had a clear career structures and paths for financial and status advancement. Another result of their long term involvement with the organisation was the development of personal relationships with other members of staff and management and this also tended to enhance levels of trust, loyalty and mutual dependency.

This 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. In addition, with the increases in the communication bandwidths available and the improved processing speeds and storage capacities of personal computers, home-working is being increasingly adopted by a significant number of organisations. One possible unfortunate effect of this, while as yet unproven, is that with the reduced contact with other members of the organisation, the home worker may not develop the relationships and bonds that help to forge loyalty to the team and the organisation. The recent adoption of outsourcing strategies also creates a range of new potential problems that include the loyalty of the staff that remain (who may feel alienated and disaffected if they believe that it is only a matter of time before their job is offshored) and that of the staff of the selected offshore partner (where there may be issues of language and understanding, differing cultural values and the laws in the different jurisdictions).

All of these changes have affected the control that the organisation has on its infrastructure and the relationships and levels of trust that can be developed with the people that work within its boundaries. We are now faced with varying perspectives of loyalty that need to be considered, especially in an offshored environment, for example, loyalty to customer, loyalty to company, loyalty to country or culture, loyalty to profession or straight-forward loyalty to pay cheque.

Much focus has been made on linking 'disgruntled' employees with insider attacks. This approach usually provides a useful stereotype (and realistic target for risk assessment) but an oversimplification could lead to a focus on the wrong people (for example, union officials and employees with genuine grievances). NIAC (2008) finds that, despite the appearance of contrary evidence, 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. However, Shaw et al (1999) identify six basic personal characteristics believed to have direct implications for malicious risks:

sense of entitlement (lack of acknowledgement or status resulting in a desire for revenge);

history of personal and social frustrations (anger, alienation, dislike of authority and an inclination for revenge);

computer dependency (computer-addicted individuals who are more likely to be aggressive loners, poor team players and dominated by an interest in exploring networks, breaking security codes, hacking into computer systems and challenging and beating security professionals);

ethical flexibility (a lack the moral inhibitions that would normally prevent others from committing malicious acts);

reduced loyalty (high-tech individuals who identify more with their profession or computer specialty than with their employer;

lack of empathy (a disregard or general inability to appreciate the impact of actions on others).

This is echoed by NIAC (2008) conclusions that people who commit malicious insider actions usually 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;

Further consideration of these categories indicates that the first can be seen as stemming internally from the individual, possibly stimulated by external sources, whilst the other two have direct drivers from external sources. External forces are therefore critical factors to include in risk assessments, with the influence of nation-state, terrorist or organised crime sources featuring strongly. It may be very difficult, however, to develop appropriate scenarios for assessment, for example, economic espionage is not just state-sponsored and the loss of intellectual property through employee turnover is common and represents a significant risk. Dynamics in workforce markets are raising the rates of employee turnover, which in turn, increases the exposure of companies to intellectual property loss and the likelihood that high-value or impact knowledge could be transferred to a competitor or other outside sources. Militant religious fundamentalism, particularly Islamic, may be leading to a growth of potential sympathisers who see no moral or ethical problems in providing their 'brothers' with information as their motivation comes from a desire to make a high-profile statement to the State or western culture rather than cause any direct harm to the company in which they work. The process of radicalisation is often dynamic and it can occur after employees have gained the trust of their employers. In general, external sources may apply pressure either directly by coercion or blunt state direction or indirectly via sophisticated social engineering methods.

TECHNICAL MEASURES TO REDUCE THE LIKELIHOOD AND IMPACT OF AN INSIDER ATTACK

The range of technical measures that can be adopted to mitigate insider attacks is relatively well known, but is sometimes ignored or not well used as a result of the cost or complexity. These measures may also sometimes be deployed on a piecemeal basis without any consideration to creating a 'big picture' of protection. While it is possible to employ a number of technical measures that will constrain the activity of people and prevent them from accessing certain information, the reality is that the group of people within the organisation that have the highest level of access are also most often those that are subject to the lowest level of control and monitoring. These are the management, system administration and security staffs: "who polices the policemen?" When technical measures are used to constrain insider activity within a network, it is essential that the systems that are used to achieve this are regularly monitored so that any potential malicious behaviour can be detected at the earliest opportunity. The key to achieving an effectively controlled environment is not to rely on one set of controls but to utilise a complementary and holistic set of controls.

The most obvious non computer based solution is physical security measures, such as the walls and fences around establishments and the locks on doors and bars on windows, together with internal perimeters. When these are combined with CCTV monitoring and guard patrols they provide the first layer of protection for an organisation. As with any other measure that is taken to protect the assets of an organisation, the level of investment that is required must be commensurate with the value of the assets that are to be protected. If an organisation is perceived to have a 'good' level of security measures in place, then the malicious insider may be deterred, as they will believe that there is the strong likelihood of their actions being detected and suffering the consequences.

Additional systems that can be used include access control measures for computer systems that ensure that the person who is using a device is actually the person that they claim to be. In the past this has primarily been achieved through the use of a user identification and password. It has long been understood that this is a weak system as it relies on the individual to remember a string of up to 12 or more alphanumeric characters. The conventional wisdom is that if the password is to provide any protection to the system at all, then it must be complex and contain non-alphabetical and preferably non-printable characters. The problem is that people have difficulty in remembering them and as a result will either choose a weak password that can easily be cracked or will write the strong password down. An article (Dan 2007) identified the 10 most common passwords as:

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. (b)link182
10. (your first name)

It will not take anyone with malicious intent long to try all of these and also any of the other more personalised common choices such as the name of their partner or pet or words related to their interests. While this type of attack is not constrained to the insider, they will have the advantage of access to the users' terminal and environment and will probably have a better knowledge of the individual and their relationships and likes and dislikes. In addition, the insider may be able to take advantage of techniques such as 'shoulder surfing' or the straightforward exploitation of a personal relationship developed over time in order to gain access to userIDs and passwords. While the option of writing down the password is actually a sensible choice if the process is formalised and the written copy of the password is stored in a secure location, this is most often not the case and it is stored in a convenient place for the user, close to the terminal that it will be used on (under the keyboard and in the top draw of the desk are the two most common locations).

Traditional perimeter-based security models (with IT security usually dependent on firewalls and IDS) should be appraised for effectiveness and *true* control of people granted legitimate remote access to assets on the inside your defences. This model provides an effective layer of security against outsiders, though it can be argued that it contains inherent weakness for the new class of third party insiders, where we may not actually know who is using the security credentials to authenticate via the firewall (as the control of user account management may also have been migrated to third party remit) and once through defences the monitoring of subsequent activity may be limited or non-existent.

The developments that have taken place in technology have opened up the possibility of alternate and stronger methods of verifying the identity of the user. These include the use of tokens that can generate a one time character string and smart cards. However, these can also be easily shared and devices that can use biometrics to identify the individual offer less opportunity for abuse. We have moved from authentication having to be something that you know (a password) to being able to use something that you own (a token) or something that you are (a biometric identifier). While arguably stronger than the password, the other means of verifying the identity of the user still have their weaknesses and the true value lies in combining more than one method, for example a password and a biometric. When used in combination, they can provide a much higher level of confidence that the individual operating a device is the person that they claim to be. However, strong controls and audit processes must be established to reduce the likelihood of the abuse of logon credentials: there are often long lead times associated with the allocation of IDs and tokens and shortened business cycle times can be a driver for short-circuiting processes and policies to meet objectives (and thereby achieve financial rewards). Technical controls should be provided on an 'end-to-end' basis, that is, to cover the *full* lifecycle of a given role performing its duty in providing service (log-on to log-off); this includes the growth of outsourced insiders.

BT's experience has been that additional technical measures can also be considered to cater for the growing number of third party insiders:

- forbid direct access to corporate networks and systems and deploy network authentication within your offices;
- deploy standard, technical logical access solutions for all third parties (regardless of location, even if in your buildings), utilising a combination of strong authentication techniques;
- check for and prohibit the sharing of logon credentials;
- apply role-based segregation (physical and logical);
- ensure that third parties are given role-based minimum privileges (no elevated privileges such as root or admin where not required) and apply frequent review and monitoring of privileged accounts;
- restrict onward network connectivity to applications;
- apply strict control to workstation and server builds to restrict the use of USB devices and access to services, email and Internet.
- consider providing and controlling the infrastructure and devices that will be used by third parties;
- integrate logical and physical security mitigations and controls;
- deploy vendor-specific gateways to enforce different levels of control.

Knowing who is using a system does not provide much protection if you do not have in place an effective system to monitor the activity that is taking place. Computer systems are capable of producing audit logs for almost anything that you might like to monitor, but these logs are pointless if they are not combined to provide a coherent view of potential activity, for example room to room, database to database. It is also necessary to refine logging to a subset of events appropriate to business requirements and to avoid filling up rooms of storage devices. Crucially, someone has to be assigned responsibility for the effective and timely analysis of the logs and reaction to incidents – both actual and suspected. Having separate audit logs for each workstation, server, firewall and the Intruder Detection System (IDS) will not, on their own, give an easily useable system to monitor what is happening on the network. It is only when they are combined that the management has a realistic chance of understanding what is happening.

When the sensors and barriers that are deployed are placed in the network, we have historically placed them on the boundary of the system to keep out the external attacker and detect intrusions into the systems. This was done in the belief that the main threat to the systems and the information came from outside the organisation. The internal staff was always considered to be trustworthy. The statistics that have been generated for a number of years by organisations such as the Computer Emergency Response Team[1] have shown this to be a relatively naive assumption, and reports that 34% of attacks came from people within the organisation, 37% came from outsiders and 29% came from unknown sources. These figures would indicate that as much effort should be invested in protecting the assets inside the organisation and monitoring the staff as is invested in protecting the boundary. This can be achieved, in part, with access control measures, by the segmentation of the internal network and the use of internal firewalls and sensors to enforce and monitor this. The management of what applications are allowed on each element of the network and which resources are allowed to be accessed by which members of staff can also be used as an effective control measure.

Effective protective monitoring and the identification of anomalous behaviour is critical, especially with regard to access to critical assets. Such monitoring must include more than just analysing failed access attempts but include the activity of authorised, successful access. There is an emerging market in products to help analyse patterns of access and information use based on expected, acceptable behaviours. Some of these product can be combined with identity management systems to provide protection from the time of users attempting to log on. Alarms can be generated and access prohibited before any harm can be done rather than the anomaly being identified at a later time. A mixture of real-time and periodic historical analysis is desirable with a focus on critical roles, activities and data to provide priorities for reaction. To be effective, the staff that manage the systems must be given the tools and time required to monitor the output of the sensors and there must also be a system in place to monitor the people who are monitoring the systems.

Protective monitoring regimes need to link physical and logical audit trails, plus the egress of data out of the organisation (not just via electronic transmission). Insider-based security failures should be investigated and visible action taken. In an outsourced environment, this may put the onus on the third party supplier but their understanding of the issues and capability and experience in conducting effective investigations may be limited compared to your own organisation and intervention may be required.

The reality is that for many organisations monitoring is often ineffective and, even when (or if in some cases) the logging is turned on, specific information from the sensors that would give an indication of malicious activity is often not captured or reviewed. While this would be acceptable if based on an assessment of the relative costs and risks, the situation normally arises as a result of ignorance of the objectives of protective monitoring or a simple failure to act. A key problem for effective, holistic protective monitoring is that there is no ‘one size fits all’ and efficiency can sometimes only be achieved after a process of evolution dependent on contingent circumstances. Greater granularity in segregation and hierarchy of controls provides better protection and reaction capability but also creates greater complexity in management and ultimately the cost of implementation and maintenance, together with the amount of log data that must be analysed.

NON-TECHNICAL MEASURES TO REDUCE THE LIKELIHOOD AN IMPACT OF AN INSIDER ATTACK

In addition to the technical measures that can be taken to prevent the successful execution of an attack or to mitigate the impact of it, there are a range of non-technical measures that can be taken to reduce the likelihood of an insider attack or detect miscreants. Some of these are procedural and can be managed and tested and others will be aimed at affecting the environment and the culture of the staff.

The types of procedural measures that can be taken may include steps such as dual key controls, where no one individual can gain access to key functions or sensitive information to cause damage. While this type of measure cannot totally prevent malicious insider activity, it forces either collusion between two or more staff or for the individual to take steps to find a way round the control measure. Either of these increases the likelihood of detection and thus reduces the probability of an attack. It is recommended that specific analyses is 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 theft but for the capability of increasing access privileges or altering logs. It may also be necessary to apply restrictions on the number of people and the period of time they have access to information and operational functionality.

Other procedural steps may include better screening of new employees to validate their past employment and other background details and the monitoring of staff for changes in their personal circumstances. Employee vetting can be an effective means of ensuring a basic level of trust; but this cannot be used as a one-off measure as people's circumstances, attitudes, behaviours and motivations will change over time. 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 can be applied to those with access to high-impact assets.

The design of an office and associated work-flow processes can also have a deterrent effect. If staff can always be overlooked and the actions that they are taking can be seen by their managers and peers, then another deterrent is created. Establishing clear accountability for actions and setting expectations and boundaries for employee conduct can also have significant potential mitigation effect, especially when employers believe an individual is near to taking malicious action.

When staff are trained on the dangers of a range of malicious attacks that may be initiated by insiders or people outside the organisation and the indicators that are likely to be present in the period leading up to and during a malicious attack, there are dual benefits. The first is the deterrent effect that raising the subject to the consciousness of the members of staff will have and the second is that other staff will be more aware of the issues and are more likely to recognise and report any suspicious activity. The use of training and briefings can be used to increase the awareness of staff in the security cultural values of the organisation. Security education and awareness programmes may also play a factor in enhancing levels of trust between employer and employee by helping to develop an understanding of the reasons for the security policies and controls that have been applied. Education on the real threats that exist – from both outsiders and other insiders – is needed, with an emphasis on the social engineering methods that can be employed to gain information or access and other malicious attacks such as 'Phishing' (usually emails masquerading as legitimate requests from financial or other well-known institutions for individuals to reply with personal or business information that can be used for future attacks), 'Trojans' (executable code, often masquerading as benevolent files within emails, that can download malware), or straight forward viruses that can be spread by circulating emails.

Unacceptable, non-malicious behaviour should also be targeted, for example, third party and company people who attempt to cut security corners with "good intentions" to meet business deadlines. This can include the types of activity that are considered to be acceptable and indicators of activity and behaviours that are not. Increased staff awareness should also reduce the likelihood of accidental breaches and increase the probability of malicious activity being detected and reported. On many occasions, after an incident involving a member of staff, it has been discovered that other members of staff had noticed indicators that something was wrong. For the most part, they failed to report the activity because they either did not understand its significance, they felt that it was not their job to take any action or they did not know how or who to report it to. Some cultures may defer to managers' actions even when these actions are known to break the rules. Messages need to be applied to every level of the organisation, involving a full understanding of the nature of the privileges their people are being granted and the 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.

Effective security cultures may have an impact on the likelihood of insiders to shift from loyalty to betrayal. While there will always be the financial incentive (bribery) and blackmail, the likelihood of staff accepting a bribe or not reporting a blackmail attempt can be reduced. In order to create this type of environment, some of the measures that can be adopted can include:

- giving consideration during the selection of staff for their ability to fit into the team and the organisation;
- providing facilities to create a pleasant but appropriate working environment;
- ensuring that there is an adequate and fair reward system and a clear process for progression through the organisation;
- creating a caring environment in which staff believe that they can approach and receive support from the management and human resources teams when they have problems;
- demonstrating that the employee monitoring system (and associated sanctions policy) is proportionate to the potential risks involved and neither heavy handed nor ineffective.

Another aspect that can be addressed is that of ensuring that the organisation has a good understanding of any regional cultural issues that affect the workforce, whether they are direct employees or as part of the extended outsourced or offshored workforce. Organisations that have offshored functions to the Indian sub-continent have developed an increasing understanding of the effect of different cultures and the values that they hold and

the impact that these can have on the delivery of the required services. Many of the organisations have made significant investments in understanding the effects and developing local measures and processes to ensure that they do not have an adverse impact.

In a business world increasingly dominated by outsourcing and third parties, standard outsourcing contractual security frameworks are necessary to cover physical, IT and personnel security and the inclusion of international standards (such as ISO27001) is recommended to facilitate understanding. The following requirements are normally mandated for third parties who have insider-based roles and privileges:

- physical, IT and personnel vetting security polices and procedures;
- security training and awareness programmes;
- security and compliance audits;
- penalties for security breaches.

The above are all required for strong, baseline requirements but may need to be enhanced, depending on the outcome of risk assessments. More stringent controls and a focus on insider threats can be applied where personal, financial and critical infrastructure data implications exist. Specific mitigations will be necessary for validating source code created via the contract and imported products used by vendors.

Specific attention should also be applied to employee classification (Colwill, 2008). Access rights of insiders, including third party personnel, to physical locations, networks, systems and information must be designed carefully and allocated, authorised, monitored and maintained appropriately. Third party personnel should not be treated in the same way as company full time employees even when they are working within the same physical boundaries. Investment should be directed at employing effective workforce categorisations to cater for all people who have access to assets. The categorisation process should ensure that the nature of employment remains obvious:

- mandate risk assessments for all third parties having access to company locations and assets;
- apply standard definitions and attributes to identify non-company personnel;
- create a controlled, 'single truth' source for entering categorisations into Human Resource (HR) databases;
- allocate responsibility for assigning people to categories to company managers, for example, those controlling the outsource project;
- ensure that categories are always visible in HR-related systems (directories, address books, etc.) and that job titles, employer affinity, employment addresses and email IDs are displayed in a consistent way for the duration of the contract;
- provide an automated means of dealing with personnel changing projects or moving off projects - agility is needed to cater for the churn of people and to update information at short notice;
- map people categories onto role-based security profiles (including logical and physical access tokens) – risk assessments are necessary to take into account potential aggregation of roles and access within a small number of people.
- link procedural audit regime with other technical and monitoring regimes to ensure consistency and currency.

Assurances and evidence should be sought that all third parties are able to manage a dynamic workforce where people move in and out of, and around, outsourced projects together with requirements to maintain audit trails of user account management (including userID, password and security token authorisation, allocation and management). This evidence should be available 'on demand'.

Insider risks and associated mitigations are now at a level that requires inclusion in corporate governance, compliance and audit regimes. Taking into account the growing shift in 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 mitigation has been applied and that security compliance is being maintained, especially minimum privilege and protective monitoring.

Organisational Risk Appetite

The organisation's security risk appetite also has a bearing on approaches to insider threats and mitigation options and this may vary across divisions within one organisation. For example, global sourcing is driven by

senior management or corporate objectives and security requirements must be balanced against commercial and organisational benefits. In many cases this could result in the acceptance of more risk than in the past and, though this may seem to frustrate the objectives of security teams, it can be used as an opportunity to help target a small subset of corporate "crown jewels", namely a focus on areas (such as high-value and high-impact functions, services and data) where senior management agrees that more investment in protection is needed. In today's competitive market, insider risk mitigation programs should also include measures to protect intellectual property and the risk represented by employee turnover and, to some degree, the knowledge that ex-employees retain and reuse.

CONCLUSION

It should be accepted that the insider threat cannot be eliminated but that it can be assessed and managed. The insider threats and risk factors discussed in this paper should be assessed to gain a better understanding of the real risks facing organisations in today's global commercial environment; the use of simple stereotypes or assumptions is insufficient and could result in security investment in the wrong areas. Changing business practices, especially outsourcing, shifts responsibilities and creates a complex mixture of 'hostile' environments and the need for trusted insiders. The detection and apprehension of malicious insiders is not simply a technical or procedural issue as the cause is fundamentally a people issue. Knowledge and understanding of the true impact of insider attacks is limited. NIAC (2008) found that partnership and information sharing on insider threats and attacks are key components to the success of critical infrastructure protection. Success in information sharing is dependent upon building an ever-stronger public-private partnership and establishing trusted relationships among the key players in each sector and with the government.

Technology can provide the means for reducing the level of access that an individual can achieve and the monitoring and detection of malicious activity, but it will be the working environment and the security that is provided by the physical, procedural and personnel measures that will provide the foundations of a system that will reduce the likelihood of a malicious attack occurring and increase the likelihood of any attack being detected. In terms of mitigation options and controls, technology is administered at a system and process level and 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). Outsourcing projects must accept that additional controls are necessary and these have also been negotiated into contracts with third parties. Security awareness and education programmes should be used to create a proper understanding of threats and repercussions of the failure of controls.

The changes in the ways that we structure organisations, the continuing developments in technologies, the changing nature of insiders and the requirement for an ever more flexible and mobile working environment will continue to place demands on organisations to re-evaluate the way in which they protect their information assets. With the probable continued trend towards greater organisational agility, home working, mobility, outsourcing and offshoring, mergers and de-mergers, considerable effort will have to be invested to ensure that staff have access to the information that they need, at the time that they need it, to carry out their function effectively. In doing this, it will be essential to ensure that they only have access to the information that they need for the period that they need it, that they do not have access to other information and that their use of the information is monitored and any abnormal behaviour is investigated and acted upon. This requires the implementation of an ongoing risk management framework encompassing insider threat analysis and compliance and audit regimes. This has a significant cost and focus must be taken to identify and protect an organisation's "crown jewels", identify appropriate security tools and processes and maintain customer and stakeholder confidence while optimising security investment.

Finally, the implications of the current, global 'credit crunch' are still emerging but it is reported (Grant, 2008) that the uncertainty caused, the plummeting of stock prices, forced mergers and acquisitions and the threat of recession could prompt an increase in abnormal behaviour in staff. This may require an immediate reassessment of insider threats.

REFERENCES

Annesley, C. (2006) *UK firms must wake up to security*, Computer Weekly (24/10/06)

BBC Reporter (2006) *Man held for call centre 'scam',* BBC (12/10/06),

http://news.bbc.co.uk/1/hi/world/south_asia/6044402.stm

BBC Reporter (2007) *UK's families put on fraud alert*, BBC (20/11/07), http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

BBC News, (2008), *Extent of data losses is revealed*, 19 August 2008

Biswas, S (2005) *How secure are India's call centres?*, BBC (24/6/05),

http://news.bbc.co.uk/1/hi/world/south_asia/4619859.stm

Colwill, C. (2008) *Outsourcing and the Insider Threat: an Increasing Security Risk*, International Conference on Information Warfare, April 2008

Dan, (2008) *Top 10 Most Common Passwords*, Intechnology.com (accessed 24 Oct 2008)

Grant, I., (2008) *Credit crunch increases internal security risks*, Computer Weekly (18/9/08)

Greenfield, S. (2007) *Risky Thinking: Brain, Biology & Behaviour*, IRM Risk Forum, 2007

National Infrastructure Advisory Council (NIAC) (2008), *Final Report and Recommendations: The Insider Threat to national Infrastructures*

Raywood, D., (2008) *Companies being hit by moles who are employed by gangs to steal data*, SC Magazine (2/10/08)

Sasse, M.A, Ashenden, D., Lawrence, D., Coles-Kemp, L, Fléchais, I., Kearney, P. (2007) *Human Vulnerabilities in Security Systems*, Human Factors Working Group, Cyber Security KTN Human Factors White Paper

Shaw, E., Post, J., and Ruby, K., (2007) Inside the Mind of the Insider, Security Management (1999)

Thomson, (2007), HMRC data loss leaves 25 million exposed, ITNews, 22 November 2007 (accessed 01 Oct 08)

Wilding, E. (2007) Insiders are the biggest enemy, Strategic Risk Magazine (09/07)

Andy Jones and Carl Colwill ©2009. The author/s assign Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.