Assessing insider threats to information security using technical, behavioural and organisational measures

Kuheli Roy Sarkar
Information Security Officer, The Salvation Army, UK Territorial Headquarters, UK

Abstract

The UK government took a bruising in the headlines (Sep 2008) after a Home Office contractor lost a USB stick containing unencrypted data on all 84,000 prisoners in England and Wales. As a result, the Home Office terminated the £1.5 million contract with the management consultancy firm. The world woke up to the largest attempted bank fraud ever when the UK’s National Hi-Tech Crime Unit foiled the world’s largest potential bank robbery in March 2005. With the help of the security supervisor, thieves masquerading as cleaning staff installed hardware keystroke loggers on computers within the London branch of a Japanese bank, to steal £220m. It is indeed sobering to imagine that any organisation could fall victim to such events and the damage an insider can do. The consulting firm lost the contract worth £1.5 million due to a small mistake by an employee. The London branch of the Japanese Bank would have lost £220 million had not the crime been foiled.

Insider threat is a reality. Insiders commit fraud or steal sensitive information when motivated by money or revenge. Well-meaning employees can compromise the security of an organisation with their overzealousness in getting their job done. Every organisation has a varied mix of employees, consultants, management, partners and complex infrastructure and that makes handling insider threats a daunting challenge. With insider attacks, organisations face potential damage through loss of revenue, loss of reputation, loss of intellectual property or even loss of human life.

The insider threat problem is more elusive and perplexing than any other threat. Assessing the insider threat is the first step to determine the likelihood of any insider attack. Technical solutions do not suffice since insider threats are fundamentally a people issue. Therefore, a three-pronged approach - technological, behavioural and organisational assessment is essential in facilitating the prediction of insider threats and pre-empt any insider attack thus improving the organization’s security, survivability, and resiliency in light of insider threats.

1. Introduction

In today’s globally connected business world, nearly all transactions take place electronically, resulting in an ever-growing volume of personal and sensitive data. Organisations now recognise the value of sensitive data; regarding it as the assets and lifeblood of their business operations. With changing technology and de-perimeterisation, sections of the assets are accessible by mobile users, business partners and contractors thus increasing the possibility of external threats and attacks. Implementing perimeter defences can protect an organisation from the outside but it cannot address the dangers from within. Although overshadowed by outsider threats, insiders can pose a significant risk to information security if motivated. Let us look into the relevance of some ‘statements’ concerning insiders:

E-mail address: kuheli@hotmail.com.
1363-4127/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
1.1. **Statement 1: “The insider threat is real”**

Insider threats conjure up images of disgruntled employees planning to take revenge or malicious employees looking for financial gains. Just as this is true, insiders ‘plague’ every organisation with good intentions trying to do their job but unknowingly put their employers at risk. These insider ‘threats’ can be accidental or due to ignorance.

A survey conducted by The Computer Security Institute indicated about 44% of all organisations suffered abuse of computer systems in 2008 which dropped to 30% in 2009; 42% reported loss of laptops both in 2008 as well as 2009; and 17% reported theft of customer data (CSI, 2008). The 2009 survey (CSI, 2009) also indicate 25% of the respondents felt that 60% of the financial losses were due to insiders; that unauthorised access or privileged access by insiders is 15%; and insider abuse of the internet access and e-mails are the fourth most prevalent incident. Both the surveys indicate that insider threats are real and nearly rising to the level of an external threat. The Fig. 1 below gives examples of the insider threats.

1.2. **Statement 2: “Who is more dangerous- an insider or an outsider?”**

Is a hacker i.e. an outsider, more dangerous than a disgruntled employee, i.e. an inside with access to the ‘jewels’ of an organisation? While the outsider has to conduct a lot of research on the organisation he wishes to attack, the insider on the other hand has the knowledge of the systems, access privileges, opportunity and the temptation. Table 1 represents the capability of an insider to cause significant damage that can rival or even exceed the damage caused by outsider agents.

1.3. **Statement 3: “Never underestimate the power of the terminated system administrator”**

According to Verizon (2009), IT administrators and end-users continue to be behind most breaches. That the IT administrators are responsible is not surprising as higher privileges do provide a lucrative opportunity and temptation for abuse of the systems. Of the insider cases studied by Verizon, in 2008 it was found that two-thirds were the result of deliberate action and the remaining were unintentional. The year 2009 saw an increase in data breach by insiders by 26% (Data Breach, 2010). If an IT administrator who has been terminated or laid off or who got wind of the possibility of being laid off, he or she may be tempted to retaliate. The higher the privilege, the more is the risk and consequentially the impact.

1.4. **Statement 4: “Organisations are not aware of insider attacks”**

According to a study published by PricewaterhouseCoopers (Safeguarding the new currency of business, 2008), about 42% do not know the source of incidents – whether the attack was most likely to have originated from employees (either current or former), customers, partners or suppliers, hackers or others. Organisations are unaware that in many cases, insiders may be stealing or destroying information until an incident occurs.

1.5. **Statement 5: “Insider attacks – easy to do, hard to detect”**

A study conducted by CERT and US Secret Service shows that most insider attacks are easy to execute and do not really need technical skills. Again, insiders have valid authorisation; they know the vulnerabilities of the organisation, any attack by these insiders can be very difficult and challenging to detect as compared to the footprinting activities of an external hacker. Malicious insiders can meticulously erase their activities from the logs to avoid detection; and they can use new IT tools like steganography or wireless technology to steal data. All these make it difficult to detect insider attacks.

1.6. **Statement 6: “The hacker on the inside is dangerous”**

While there have been intensive studies concerning hackers and their methods of attacks, it is quite helpful to look at the methods used by the insiders too. Since insider attacks are not just centred on technical vulnerabilities, it is quite challenging to generalise a method as attacks can take many forms.
Richard Stiennon, an independent security consultant described a model of an insider attack as shown in the Fig. 2 below:

These ‘statements’ establish that insider threats are real and difficult to defend against when motivated. They know when, where and how to strike by the nature of their position and their intimate knowledge of the business or organisation. With new technologies, threats are becoming faster, more frequent and even dangerous, demanding that organisations stay well ahead in technological expertise to keep protected. It is important for businesses and organisations to employ technologies to help identify and address insider threats. In order for businesses to be better equipped to handle insider threats, there is a need for a better means to predicting and detecting the threats. Since insider threats are a human issue, employing just traditional computer security defences will not be sufficient. It has to combine the behavioural and organisational measures to provide the means of predicting a possible insider threat and provide meaningful controls to protect a business or organisation.

2. The threat from within

Today, Information Security is a major concern for governments and organisations alike. There is enough evidence to show that hostile forces are in operation on the internet and most organisations using the infrastructure are vulnerable to attacks. Companies offering solutions for viruses, malware or services to counter hackers etc., reinforce the importance of the external attacks. However, it is essential not to overlook the potential problems much closer to home. Just as there is evidence of external attacks, there is also evidence to indicate that insiders have been responsible for significant and expensive security incidents. This creates a worrying situation, since insiders are legitimate users with a high probability of success.

2.1. Psychology of the insider

The greatest security threat comes from the person with authorised access. People design, develop, and use as well as misuse information systems. It is, therefore, necessary to understand the psychology of people involved in both malicious and non-malicious insider activity.

In “Inside the Mind of the Insider,” an article about the psychosocial characteristics of malicious insiders, authors Eric Shaw, Jerrold Post, and Keven Ruby identified six personal characteristics with direct implications for risk (Sean Steele and Wargo):

2.1.1. Sense of entitlement

Insiders develop a sense of ownership for systems/applications that they develop from scratch. In most cases, employers totally rely on their expertise and consequently the insider develops the feeling of entitlement. Reactions may be triggered if the entitlement is challenged or the management fails to recognise the ‘contributions’.

2.1.2. History of personal and social frustrations

Insiders are often loners with poor social skills; they possess general antagonism towards management and a tendency to flout ‘rules’ of the organisation. They are generally poor team players, have primary interests like exploring networks, or breaking into secure systems, cracking code, challenging and outfoxing security professionals.

2.1.3. Ethical flexibility

Insiders committing internal breaches do not think that the violations are unethical. They do not possess the moral inhibitions that are mostly defined by their culture, background and character.

2.1.4. Reduced loyalty

The growing culture of open and interconnected world combined with transfer of jobs overseas, downsizing, outsourcing, economic downturn, restructuring to adapt to the pressures of global economic competition, rapid technological change, and increased hiring of part-time workers to avoid paying benefits are shaping the employees’ sense of job.

### Table 1 – Type of insider and their level of harm

<table>
<thead>
<tr>
<th>Level of harm</th>
<th>Type of insider</th>
<th>Motivation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serious</td>
<td>Disgruntled employee</td>
<td>Self-satisfaction and revenge</td>
<td>Delete backups</td>
</tr>
<tr>
<td>More serious</td>
<td>Insider recruited from within the target company</td>
<td>Espionage for money</td>
<td>Steal proprietary/intellectual property</td>
</tr>
<tr>
<td>Most serious and most damaging</td>
<td>Individual recruited by a competitor, trained to excerpt sensitive data</td>
<td>Financial gain</td>
<td>Steal intellectual property or Extract data and send it to the recruiter</td>
</tr>
</tbody>
</table>

### Fig. 2 – Anatomy of an inside attack (http://www.zdnet.com/blog/threatchaos/new-anatomy-of-a-hack/330). Stage I: Identifying which systems have the data and who has access to the systems. Stage II: Steal the credentials of the privileged user through key logging devices. Stage III: Move the funds to his personal account. Stage IV: Make an ‘escape’ – erase logs if any.
security and loyalty to employer. Economic changes like working from home can affect loyalty and devalue the long-term employer–employee relationship.

2.1.5. Lack of empathy
Different people react differently under extreme personal stress. Some insiders often react from a range of being absent from work to self-serving decisions, theft of sensitive data, sabotage of critical systems, or even espionage. One important psychology of an insider is the total disregard for the impact of his/her action on the organisation.

Psychology plays an important role in understanding the danger of insider behaviour and identifying the behavioural precursors enable organisations to gear themselves in combating the threats posed by insiders.

2.2. Categorizing insiders

Every employee of a business or organisation has specific access levels based on their job profile. Any other third party like clients, contractors etc., are all provided specific levels of access. Insiders are categorised here based on the classification made by authors Dr. Eric Cole and Sandra Ring in their book “Insider Threat: Protecting the Enterprise from Sabotage, Spying, and Theft” (Cole and Ring) i.e., pure insider, insider associate, insider affiliate, and outside affiliate. The diagram (Fig. 3) below describes the grouping of threat agents:

2.2.1. Pure insider
A pure insider is an employee with necessary privileges like keys, access cards, and network logs available to him in order to perform his job function. System administrators have the highest level of access to systems and networks. Accounts of terminated employees or employees who left the organisation are not often de-activated. Pure insiders may be a well-meaning employee, but can also be disgruntled or malicious.

2.2.2. Insider associate
Insider associate are often contractors and third party personnel, for example: guards, cleaners, or suppliers with limited authorised access like access to a facility or restricted access to networks. Third party personnel like cleaners have unlimited access to facilities generally after office hours; they have access to employees’ desks, bins etc. They may find sensitive information/documents on the desks like usernames and passwords left in bits of paper under keyboards, stuck on monitors, or may plant key logging devices to retrieve sensitive information.

2.2.3. Insider affiliate
An insider affiliate is often a spouse, friend or client of an employee with no direct access privilege but can use the credentials of the employee to gain access. It can be as simple as a client coming in and while in the building wanders around the facility; or more malicious such as an impostor pretending to be an employee. It can be a spouse borrowing the office laptop to access the internet; or the spouse is provided with access details like the username and password or access card to collect papers from the office.

2.2.4. Outside affiliate
Outside affiliates are outsiders who are not trusted. They may gain access to the organisation’s network through open access like a wireless access that is unprotected, or plant a ‘mole’, or socially engineer the credentials of authorised employees.

2.3. Classification of insider misuse

Insider misuse can be classified based on the level of access, by system consequences, by reason for misuse, by access privileges or by the level of impact. The following discusses classifications based on reason of misuse and on system consequences.

2.3.1. Reasons for misuse
Motivation is the main factor that drives insiders to commit misuse. G.B. Magklaras and S.M. Furnell (2001) identified insider misuse as either intentional and accidental. Besides these two reasons, ignorance is another reason for misuse, since many breaches occur due to lack of knowledge on policies or training. Fig. 4 shows reasons for misuse:

2.3.1.1. Accidental misuse. Many well-meaning employees may circumvent company security policy in order to meet business needs that could lead to an accidental security breach. The irony of ‘accidental threat’ is that employees, who are working to do their job, do the damage. For example, some users may accidentally click ‘Reply All’ instead of ‘Reply’ when sending confidential documents by email. Others may accidently expose sensitive company information using emails, Web sites, blogs, or social networks, like Facebook, LinkedIn etc. Data from such sites when compiled may provide a wealth of information, providing attack vectors for phishing or social engineering attacks against the insider’s organisation.

---

Fig. 3 – Categorising insiders.

Fig. 4 – Classification by reason of misuse (Magklaras and Furnell, 2001).
2.3.1.2. Intentional misuse. Insiders with self-interest can use organisational facilities during working hours to promote their own business or surf the internet to shop online, download music and software or surf unauthorised sites. Insiders with malicious intentions often use the corporate internet connections and laptops outside office hours and in their own time. With an economic slowdown, many employees may be tempted to sell sensitive corporate information for financial gain or employees disgruntled by pay-cuts or layoffs may try to extract revenge by intentionally exposing sensitive corporate information or sabotaging the critical infrastructure. Terminated employees may cause a security breach when their accounts are not disabled on termination or when they work on the day of their termination with full access rights and privileges, giving them the opportunity to create backdoors.

2.3.1.3. Misuse by ignorance. Employees cannot be expected to intuitively protect data without the awareness necessary to effectively safeguard information. Employees may load large volumes of unencrypted data on laptops or mobile devices and take them out of the corporate facilities exposing the data to be lost or stolen because of their ignorance that data needs to be encrypted. It is also a common scene where personnel leave laptops and storage media unsecured, in clear view, in their cars, on coffee shop tables, in airports and other public places, where they are stolen, often due to ignorance or the lack of a security culture. Most employees when changing jobs normally, ‘clear’ their desk of all ‘personal’ belongings. This may include copies of software, or of contracts, or databases and reports created by them, without realising that the employer is legally the owner since they were created in the course of employment. When employees join another organisation, and use that software, they are unwittingly using proprietary software, thus jeopardising the new organisation into possible legal action.

2.3.2. By system consequence

According to G.B. Magklaras and S.M. Furnell (2001) insider misuse can be classified by modifications done to the operating systems, the network data and hardware. The misuse on the basis of system consequences i.e. operating system components, network data, application and hardware, is given in the Fig. 5 below:

2.3.2.1. O/S based. Insiders can misuse operating systems by modifying the configurations files that may render the system unstable or vulnerable to attacks. Installing unlicensed software may lead to the introduction of malware like Trojans or rootkits. Default operation system may be modified accidently or intentionally and in both the cases, it is insider misuse.

2.3.2.2. Network based. Insiders may footprint other workstations in the network by ‘pining’ or ‘nmapping’ either through idle curiosity or with malicious intent. Other misuse may be trying to access prohibited material, online shopping, or downloading inappropriate materials.

2.3.2.3. Hardware based. Any modification i.e., removal or addition of hardware components can leave the computer vulnerable to insider misuse. For example, installing a modem or hardware key logging device is modification against the baseline defined by the organisation. Any such modification either accidentally or intentionally, is a misuse.

2.3.2.4. Application based. Data collection at application level can help identify insiders who may pose a threat either due to ignorance or with malicious intent. For example, an insider may input inappropriate data to an application like an ‘SQL injection’ on a web application or an insider may try to query a database containing sensitive data.

2.4. Reasons why most insider threats are ignored

Based on the findings of the survey by CERT - 2007 E-Crime Watch Survey (2007), it is noted that about 40% of the organisations who bore the brunt of e-crimes did not report for legal action, and according to the 2010 survey (CERT, 2010) 72% of the insider incidents are handled internally. They found that the damage level was not significant enough to warrant prosecution; about (34%) say there was lack of evidence and about (28%) could not identify the individuals responsible. Other factors like the fear of negative publicity contribute to the reasons why insider threats are ignored.

2.4.1. Fear of negative publicity

The impact of negative publicity can be quite damaging like loss of customer confidence with many immediately going to rival companies, loss of partner confidence, and cost of having to revive reputation, or recovery, or legal costs and the cost of cleaning up after the act.

2.4.2. Difficulty in identifying culprits

Even when there is a security breach, most often companies struggle to identify the real culprit since insider criminals are legitimate users. Often co-workers refrain from reporting any suspicious activity as most feel it is not their job to take any action or they do not know how and where to report.

2.4.3. Ignorance of the attacks

Due to the nature of insider attacks, most organisations are not aware that a security breach has taken place. Moreover, the organisation’s security systems may not trap or trace the attacks taking place e.g. piecemeal attacks also known as the ‘salami attack’.

2.4.4. Insider threats are overlooked

Organisations actively working on insider threats tend to overlook the threats posed by the insider activity, mainly
because the damage level is not high. For small damages, employees are normally given a warning. Organisations face a maze when proceeding through a court and most often regard that as the last option.

2.5. The consequences of insider attacks

Security breaches associated with insider activity can cause damage such as losing working hours, loss of company’s intellectual property, loss of customer data, business disruption, harm to individuals or reputational damage. Table 2 illustrates some examples of the consequences of malicious insider activity.

Besides some of the consequences mentioned in the table above, damage to reputation, theft of intellectual property, or insider sabotage can have devastating effects on a business or organization.

2.5.1. Loss of reputation
Most companies try to avoid public announcements on insider abuse as the publications might have a negative effect on brand integrity or the reputation of the whole industry. Any insider attack when made public has a direct impact like resulting in loss of customer confidence, loss of customers to competitors, and huge financial loss of restoring normal service or cleaning up after the act.

2.5.2. Theft of intellectual property
Theft of intellectual property includes those cases where an insider’s main goal is to steal confidential or proprietary information mostly for business advantage, for financial gain, or for offerings of a new job with a competitor. Insiders with a perceived importance of his contributions develop a sense of entitlement thus triggering the insider to ‘own’ the proprietary information.

2.5.3. Insider sabotage
Employees with a personal grudge against the organisation or a co-worker, often carry out most of the sabotage. For sabotage, a certain amount of sophistication is often involved such as a remote access capability, logic bombs, backdoors or username-password combinations of users and administrators. Stressful events like organisational restructuring or withdrawal of privileges, contribute to the possibility of insider sabotage. Technical employees possibly are the most dangerous because of their intimate knowledge of an organization’s vulnerabilities; and have used that technical ability to sabotage their employer’s system or network in revenge for some negative work-related event.

2.5.4. Insider espionage
Espionage is about spying or planting spies in order to gather sensitive information about competitors or rival governments. With technology, espionage has become easier and faster. Good examples of e-espionage tools are GhostNet and Snooping dragon. Changes made in an organisation like restructuring or when personal crisis like financial problems occur can threaten their self-image at some point in their lives and trigger individuals to commit espionage. Some insiders often have patriotic disposition towards their own country and steal for the benefit of their governments.

2.6. Drawbacks of current approaches

Traditional security solutions focus mainly on securing the perimeter of a business or organisation, but these solutions are not suited for defending attacks that generate from within the perimeter.

2.6.1. Focus on securing the perimeter
Some organisations spend millions building strong perimeter defences to protect their critical infrastructure and data from hackers and outside attackers. These defences however, do not address the violations committed by insiders. A study conducted by Verizon (2009 Data Breach Investigations Report) indicate that internal breaches continue to be much more damaging than other sources of attack. In addition, the 2010 Data Breach Investigation Report indicate that there is more insider breaches this year than ever before. Yet, companies focus mostly on preventing external attacks.

2.6.2. Ignorance of behavioural characteristics
A heavy reliance on technology is insufficient in handling insider threats. In fact, psychological and behavioural characteristics of insiders can provide precursors to predicting a possible attack. However, current approaches do not emphasis the psychological characteristics of an insider, vital in detecting and controlling incidents.

2.6.3. Lack of consistent policies
Although many organisations have policies and procedures in place, they are either incorrectly implemented or employees

<table>
<thead>
<tr>
<th>Table 2 – 1: Examples of the consequences of insider activity.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insider activity examples</td>
</tr>
<tr>
<td>Changing passwords of administrator accounts.</td>
</tr>
<tr>
<td>Changing passwords by masquerading.</td>
</tr>
<tr>
<td>Shutting down networks routers</td>
</tr>
<tr>
<td>Unauthorised modification/deletion of customer data.</td>
</tr>
<tr>
<td>Planting logic bombs in application systems.</td>
</tr>
<tr>
<td>Deleting proprietary software, backups, designs etc.</td>
</tr>
<tr>
<td>Introduction of virus, trojan through unlicensed software or</td>
</tr>
<tr>
<td>illegal websites.</td>
</tr>
</tbody>
</table>
circumvent them in order to meet their business demands. Some polices are often complicated and hard to follow. In addition, the culture of the organisation shapes employee behaviour and that may override the security policies and processes.

Handling insider threat is a complex issue and challenging. Since it is a human problem, it cannot be solved by technological means only. Psychological and organisational factors are essential in addressing insider threats.

2.7. Future trends of insider threats

There is much discussion regarding insider threats and most security professionals consider them as time bombs. They believe that insider threats are more widespread than predicted, since many organisations do not disclose any breach. Besides insiders, also use non-technical means to compromise sensitive data.

2.7.1. Framing

The psychology of most perpetrators is to commit a crime and then destroy the evidence or blame a co-worker. Any insider with a grudge against a co-worker/supervisor may compromise their user accounts, act maliciously and build legitimate evidence to indict the co-worker. The trend is chilling since innocent co-workers may become victims, and if prosecuted it would be devastating.

2.7.2. Planting

Some planting techniques include recruiting a ‘sleeper’ into the target organisation then activates as and when required. Installing technical logic bombs or inserting malicious code like a trapdoor or planting key logging devices to trap key strokes are some examples of planting threats. The case of Sumitomo Bank Heist, the largest attempted bank robbery in history reported in, (http://www.theregister.co.uk/2005/04/13/sumitomo_bank/) demonstrates how easy and effective it is to plant devices capture sensitive information and cause financial loss.

2.7.3. Social engineering

Social engineering techniques, which is gaining access through manipulation of a person or persons who can permit or facilitate access to a system or data, are fast becoming one of the top methods used by insiders. Social engineering exploits human nature. A social engineer can then implement information gathering techniques like ‘dumpster diving’, ‘desktop snooping’, ‘shoulder surfing’ or ‘CD/USB dropping’.

2.7.4. Moles

‘Moles’ are individuals who enter an organization with the explicit intent to commit espionage, fraud or embezzlement. They are recruited, trained or planted by an outside organisation such as a competitor or may be recruited after they are already inside the organisation. The mole ‘tunnels’ his way into the organisation, sometimes into a position of authority, gains access to critical systems and passes sensitive details to the external organisation. The case of FBI traitor Robert Phillip Hanssen who sold secrets to Russia, (http://www.fbi.gov/pressrel/pressrele01/hanssen.htm) is a good example.

2.7.5. Outsourcing

Many organisations outsource specialist IT jobs to third parties with expertise in specialised sectors. However, with sensitive or personal data in the hands of the third party (insider associate), there is a high risk of data misuse. Security threats associated with outsourcing include sensitive or confidential information not being properly protected and unauthorized parties gaining access to private files.

2.7.6. Social networking

Web 2.0 technologies, such as Facebook, MySpace, LinkedIn or Twitter, are a major security concern for businesses. Employees may unintentionally release sensitive information. They may plant clues like where they work, who their colleagues are and the projects they are working on, without realising that it could be useful for sophisticated social engineering attacks. Employees using social networks and internet for illicit activities reflect badly on the company. Either way a company could ultimately be at unintended risk.

2.8. Current statistics

The statistics below provide an insight to the trends of insider activities, their growth and their impact.

2.8.1. CERT Findings

According to CERT’s 2007 E-Crime Watch Survey (2007), it indicates that insiders (34%) are fairly close to outsiders (37%) in causing most damage. Participants indicated that they were not giving much attention to the insider threats. According to this, there has been a drop in background checks (from 73% to 57%), account/password management policies (from 91% to 84%), employee monitoring (from 59% to 42%) and employee security awareness training (from 68% to 38%) as compared to the statistics for the year 2006. The CERT’s 2010 E-crime Survey (2010) indicates while outsiders are the main culprits of cyber crime, insiders cause the most costly and damaging attacks.

2.8.1.1. Insider E-crime ranking. Survey results of 2010 show that most insiders unintentionally exposed private or sensitive information.

1. Unauthorised access to organisation information, systems and networks (23%),
2. Theft of intellectual property (16%),
3. Theft of other information including financial and customer records (15%)
4. Unintentional exposure of sensitive information (29%).

2.8.1.2. Ranking of the mechanisms used in committing insider threats. Survey results of 2010 showing the top four significant misuse:

1. Using laptops (44%).
2. Copying information to mobile devices like USB drives or iPods (42%).
3. Downloading information to home computer (38%).
4. Stealing information by sending it out via email (34%).
2.8.2. Other findings

2.8.2.1. 2009 CSI computer crime and security survey (CSI, 2009). Key findings from the survey shows 43.2 percent of respondents stated that at least some of their losses were attributable to malicious insiders; but clearly non-malicious insiders are the greater problem. Twenty-five percent of respondents felt that over 60 percent of their financial losses were due to non-malicious actions by insiders.

2.8.2.2. 2010 information security breaches survey (Data Breach, 2010). The survey shows a significant increase in the insider threat by 26 percent. Of the cases involving internal threat agents in 2009, investigators determined 90 percent were the result of deliberate and malicious activity.

2.8.2.3. The 2008 insider threat survey (Insider Threat Survey, 2008) http://www.rsa.com/document.asp?doc_id=9699. The survey findings indicate that mobile employees have the responsibility of protecting the information that is carried outside of the organization. Of the respondents polled, it has been found that:

1. One in 10 has lost a laptop, smartphone and/or USB flash drive with corporate information on it.
2. 79% frequently or sometimes leave their workplace carrying a mobile device containing sensitive information related to their jobs, such as a laptop, smartphone and/or USB flash drive.

The surveys clearly indicate that insider threats are becoming more of an issue and more widespread than accounted for. One reason is the use of non-technical means like social engineering by insiders to gain unauthorised access and compromise company’s sensitive data. As organisations are fortifying their perimeter, criminals are using more sinister means to gain access to the organisation’s proprietary information by ‘planting’ insider threats. The insider ‘time-bomb’ is compounded by many factors like:

- Many organisations do not report insider misuse, so the scale of the problem is hard to estimate.
- Employees are merging their working lives with their private lives.
- Organisations are introducing a mobile work force, so the perimeter is becoming more porous, employees are carrying sensitive data on laptops, mobiles and USBs which when lost or stolen compromises the data.

With the credit crunch, it is likely that there will be an increased risk of insider activity particularly in regard to bribery and fraud.

3. Misuse within the perimeter

Insider threats are certainly not new. They have always been around. The advent of Internet and sophistication of technologies have provided a new dimension for the insider threats to thrive more than before. A screen shot (Fig. 6) from Computer Economics, 2009 gives a statistics about the types of insider misuse and how organisations view the threats:

Insider activities mostly revolve around stealing, destroying or modifying data. These activities can be classified as misuse under Information systems, external websites and internal networks:

3.1. Searching information systems

The insider threat has always been around and many do not realise that their actions are termed as misuse. At the information system level, insider misuse may be fishing in various sources for information or making copies of documents etc. The types of misuse as shown below are quite common.

3.1.1. Seeking information
Many employees often keep themselves abreast of opportunities through shoulder surfing, social engineering, and browsing accessible files and directories for information. Employees may unintentionally publish sensitive information through emails or maliciously sell them to a competitor for a price.

3.1.2. Copying sensitive documents
A common action of an insider is knowingly or otherwise, to make copies of sensitive documents. Even well-meaning employees make copies for themselves as a backup while some may make copies for a competitor.

3.1.3. Emailing classified/sensitive documents
One of the simplest ways to copy sensitive documents is to self-email them as attachments to a personal email account. Insiders often use this method with intentions ranging from
an innocent activity like making backup copies to a malicious activity like selling to a rival organisation.

3.1.4. Hiding directories and files
Another method is to create copied files in systems areas with names similar to existing system files. These files raise no suspicion due to the naming convention. Another form used by insiders is to create hidden directories and make copies of files in the hidden directory. Renaming files with specific file extensions works well. Popular searches are generally for executables (.exe) or document files (.doc) but not files with other extensions, so insiders may hide their copies using less relevant file extensions.

Making copies of sensitive documents within less sensitive documents is another good way to smuggle out sensitive information. The technique known as ‘Steganography’ is used where information can be hidden by embedding information on to a seemingly innocent file. It is mostly used with graphics, sound, text, HTML and PDF files.

3.1.5. Removable media
Removable media such as USBs have become a very common means for insiders to sneak data out of organisations. Since they come in various forms i.e., as watches, pens, mobiles, pendants etc, their existence becomes quite ‘invisible’ to the human eye, thus enabling malicious insiders to slip data out. Data breaches can also occur when well-meaning employees make data dumps on USBs for their own convenience for putting in more hours of work at home and then later misplacing them.

3.1.6. Rogue accounts
Many organisations do not strictly adhere to the policy of closing user accounts of employees who are terminated or have resigned. Such accounts become ‘rogue’ accounts and can be used for malicious activities like circumventing manual or automated controls. Sometimes system administrators create certain shared accounts for testing and training. As there is often no accountability to these accounts insiders may exploit them in various ways.

3.1.7. Key loggers
Key logging devices can become a security nightmare. Insiders use such devices to record computer user’s keystrokes like retrieving the username/password of colleagues, and gaining access to systems and other applications for which they do not have legitimate access.

3.1.8. Encrypting documents
If an organisation does not have sanctioned encryption software, then no employee is expected to be using encryption. Insiders may use encryption programs not authorised by the organisation and may be using it to encrypt specific sections of his directory or communications.

3.1.9. Uploading files/directories
While the use of USBs may be quite handy, they can be a hindrance. Few organisations are implementing the policy of disabling USB ports. Insiders find ways to circumvent this portability by uploading sensitive documents on disk space available on the web.

3.2. Accessing websites
The Internet comes with its share of vices. Everyday new websites are created and not all of them are genuine. Employees surf for both personal and professional needs. While using technologies such as Instant Messaging and Peer-to-Peer file sharing, insiders may introduce threats to the systems in the form of viruses and worms.

3.2.1. Downloading and installing free software
Employees can unwittingly download software (trial packs) from websites, or attachments from emails unaware that these may contain malicious code such as Adware, Spyware, Trojan, viruses, rootkits or key-loggers. This malicious freeware may, for example, turn their computers into zombies that join armies of similarly infected PCs in botnets to launch denial-of-service attacks on Web sites, or other attacks.

3.2.2. Using instant messaging
The use of Instant Messaging is another insider threat. Instant Messaging is widely used and is convenient for users, however, employees may inadvertently introduce variants of email worms. Insiders using compromised instant messaging accounts may be lured into revealing sensitive organisation information.

3.2.3. Using social networking sites
With the increase in popularity and use of social networks, insiders may unconsciously post sensitive information about themselves or their colleagues, or discuss professional issues about projects they are working on. Social networking malware is thriving, so, insiders may inadvertently be exposing the organisation to potential harm.

3.3. Networks
Many organisations today restrict access to the Internet and firewalls are configured to allow only specific traffic in and out. Employees find it very restricting not to be able to access all sites from inside a trusted network. The ability for any insider to be able to tunnel out sensitive documents is really the insiders dream come true.

3.3.1. Installing modems
Unless made clear in Security Policies, well-meaning employees may install a modem in order to be able to work from home rendering the network insecure. This has also been seen as a malicious practice for insider crime.

3.3.2. Creating/installing unauthorised wireless access
Malicious insiders may install rogue wireless access points to enable packet sniffing or make company resources available to an outsider To avoid being caught, employees will go to great lengths to cover their tracks, such as configuring an access point to use a hidden SSID.

3.3.3. Use of laptops/PDA/mobile devices
Any device like a laptop, a PDA or a mobile that accesses a corporate network or store data is a potential risk to intellectual property or sensitive customer data. These portable
devices are a great source of data leakage. This is highlighted by the statistics (Fig. 7) provided by a study (June 2008) of 106 major U.S. airports and 800 business travellers published by the Ponemon Institute and Dell Computer, including the fact that about 12,000 laptops are lost in airports each week (Airport Insecurity).

These statistics provide an indication of the amount of data that is lost by loss of laptops with company data on them. It is also a common scene at cafes where employees leave their laptops open to a roving public eye. Data on mobile devices is often not backed up or encrypted thus creating additional risk, let alone the loss of the equipment.

4. Insider threat assessment

Insider threat assessment enables organisations to identify the extent to which an insider can be a potential threat and the likelihood of the realisation of the threat. Insider threat assessment should be an integral component of risk assessment. While traditional risk assessments focus mostly on technical vulnerabilities, insider threat assessments need two more dimensions - the people and organisation factors, to enable early detection of employees’ improper access to sensitive/valuable data. The output of the assessment will provide a guideline to identify the controls to address the threat.

4.1. Need for insider threat assessment

Organisations need to perform insider threat assessments in order to identify the insider threats that a system is facing and the threat agents that are able to manifest them. There should be a limit to employees’ access to sensitive data to limit negative financial impacts and regularity penalties.

According to George Fyfffea (2008), personal records are highly valued and some, harvested from databases, are worth an astounding £4–8 per record in the open market. It is only when an organisation knows the value of its assets, (for example a database of credit card details made available in the black market) that it will understand the importance of securing it, as well as identifying the threats that may pose harm to the asset. Therefore, performing an insider threat assessment will enable organisations to identify the threat agent that may contribute to a compromise of the asset.

According to CERT (2007), the results of who caused the most damage, insiders or outsiders, in terms of cost or operations, it was fairly close with insiders at 34%, outsiders at 37%, unknown at 29%. This indicates that the threats from insiders nearly equal the number of threats posed by outsiders. Hence, it highlights the need for an organisation to be proactive in dealing with insider threats.

Insider threats are easy to do but hard to detect, since an insider is an authorised user that makes it difficult to predict malicious activities. They are not perceived correctly because it is difficult to ‘measure’ as compared to an outsider attack. The lack of tools and techniques adds to the difficulty. Insider attacks may not be as frequent as the outsider attacks but their chances of success and impact are very high. Although we talk about insiders and their capability to cause a security breach, it is also important not to underestimate the power of a terminated insider whose account is still active and who has been a system administrator. In order to identify and control such threats, insider threat assessments are vital.

New laws and mandates have made it imperative for organisations to conduct vulnerability and risk assessments and to ensure that the protection they implement is cost effective. Organisations are now expected to be information security conscious and should implement necessary controls based on the results of the internal vulnerability and risk assessments. These assessments enable organisations to uncover known weaknesses and vulnerabilities in its technical and organisational infrastructure, prioritise the impact of the vulnerabilities, and implement safeguards to mitigate the identified weaknesses. The principle reason for mitigating risk in any organisation is to protect its mission and its assets. Importantly, insider threat assessments should be an integral part of risk assessments. Insider threat assessments need technical and management involvement, as they are an organisational, behavioural and technical issue.

The insider threat problem is complex; even if an organisation has excellent physical security and proper access control systems, professional criminals and extremists may infiltrate by making use of methods to circumvent the security, like recruiting and implanting a ‘sleeper’ into the organisation and ‘activate’ them as and when needed or by targeting employees and exploiting their weaknesses. These weaknesses can be exploited with offers of cash for sensitive information, physical threats, intimidation, offers of drugs and sexual favours. Again, such threats can be identified and controlled through an insider threat assessment.

Hence, insider threat assessment will provide the framework for establishing a systematic guideline. The framework produces a report where each insider threat is identified, analysed individually with their likelihood of occurrence and the consequence if they occur. The threat is prioritised in order of severity, so they can be used to prepare the security strategy.

4.2. Stages of insider threat assessment

Before going straight into the stages of insider threat assessment, it is vital to define the terminologies in use throughout the document. The meaning of some terminologies has been modified to include the characteristics of insiders and the threats they pose.
An insider threat assessment is a statement of threats posed by ‘trusted’ insiders of an organisation that are related to vulnerabilities, assets, and insider threat agents. It is a statement of the believed capabilities, motivation and opportunity that those threat agents possess and also the statement of possible impact.

A Vulnerability is a measure of the exploitability of a weakness that encompasses the business processes, communication systems, and information technology supporting the mission of the organisation.

An Insider threat is the potential for a particular insider threat source with the Motivation, Capability, and Opportunity to successfully exploit a particular vulnerability or compromise a system.

The motivation of an insider is the extent to which the insider is prepared to execute a threat. The motivational factors of insiders that drive them to consider misusing an organisation’s assets are:

- The desire to address issues that may be related to employment or personal relationships, finance, revenge etc.
- Peer pressure.
- Religious or political issues for example, by espionage agents or financial gain.

The capability of an insider is the extent to which an insider threat agent is able to execute a threat. The capabilities to launch an attack depends on the following:

- The access and the ability to correctly use tools and techniques necessary to implement an attack.
- The access to training, manuals to support the correct use of various tools and techniques.
- The level of access to resources and the ability to acquire more over time.

The opportunity of an insider is the perfect condition when the insider threat agent can execute an attack.

In order for a threat agent to bring its capability to bear against a target he must have the correct conditions to do so, and in order for his capabilities to be effective and have an impact on the target, the target must be vulnerable to attack. Impact is used to denote the consequences of an insider threat causing a level of harm to an organisation’s asset.

Threat impact level could be the following:

- Low: unauthorized use of asset without actual loss, no other effect in enterprise
- Medium: business disruption, moderate changes in way of conducting business
- High: out of business unless countermeasures are deployed immediately

The impact level is based on the type of organisation, for example, impact level would be ‘high’ if the organisation offers an online service.

An insider threat assessment will help identify the threats that a system is facing, and the agents that are able to manifest them. It is important to incorporate the process of identifying and analyzing threat agents. Gathering Intrusion Detection System data and analyzing it is a challenge on its own, but identifying threat agents, and analyzing their attributes is challenging due to its inherent nature. Typical questions that must be answered are: Is the agent motivated enough to pursue his/her target? Does the agent have the technical capability and the knowledge required to exploit vulnerability or break a system?

The next factor is determining the level of threat that an insider makes to an information system. The diagram (Fig. 8) presents all the stages that insider threat assessment must follow i.e., calculating the motivation, opportunity, capability, the probability of the threat agents carrying out a successful attack, and the impact that a successful attack would have on the business.

4.3. Organisation characterisation

In order to assess the risk of insider threats to information security, the first step is to define the scope, which is normally done when risk assessment is performed. Identification and characterisation of resources and information, is established when defining the risk. System related information that includes hardware, software, networks, databases etc and insider behaviour information are essential in assessing insider threat.

4.3.1. Gather system information

A good understanding of existing systems in an organisation can pave a way to identifying the risks. As insider threat assessment is an integral part of risk assessment, information on systems i.e. ‘assets’ conducted for risk assessment can provide the input needed for insider threat assessments. Gary Stoneburner, Alice Goguen, and Alexis Feringa provides a comprehensive list of system and systems components from where information can be gathered. The following has been adopted from the comprehensive list to gather necessary input for insider threat assessment:

- Hardware & software.
- Internal and external Interfaces.
- Data and information.
- Employees supporting and using the systems.
- Application systems.
- System and data criticality.
- System and data sensitivity. (The level of protection required to maintain system and data integrity, confidentiality, and availability.)

**Fig. 8 – Insider threat assessment cycle.**
Further details required, are inputs of the operational environment and its related data that is provided by the following list:

- The functional requirements of the system
- Users (technical support, application) and their privileges.
- Organisation security policies with respect to all systems including compliance to standards, industry practices and the law
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection system.
- Flow of information pertaining to existing systems (e.g., system interfaces, system input and output flowchart)
- Technical controls used for existing systems (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)
- Management controls (e.g., rules of behaviour, security planning)
- Operational controls (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment (e.g., facility security, data centre policies)
- Environmental security implemented (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

Inputs from systems that are in the design or development phase is acquired from design or requirements document. System design documents and the system security plan would provide useful information about the security of a system that is in development.

For an operational system, data is collected about the system in its production environment, including data on system configuration, connectivity, documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the IT system.

4.3.3. Techniques of information gathering
Gathering information from within the defined scope can be done through the following stages:

4.3.3.1. Interviews. Collection of useful information can be facilitated through interviewing technical and non-technical personnel and management. On-site visits can help in assessing personnel to observe and gather vital clues about the environmental and operational security of the organisation’s systems.

4.3.3.2. Questionnaire. In order to gather relevant information, questionnaires should be sent out to all technical and non-technical personnel involved in the design, implementation and support of the organisation infrastructure both system and operational. Real-time interviewing of users can also provide data for the questionnaires.

4.3.3.3. Document review. System documents (user guides, manuals, design, requirement analysis), policy documents (directives), and security related documents (previous audit investigations, requests of annual, medical or personal leave, attendance records, annual review results, legal and disciplinary issues, complaints made by and/or against the employee, employment history, references etc.

- Insider Associate - Contractors, suppliers and their access to the organisation and its infrastructure: Data can include references from clients they work with, type and location of supplier/contractor, information related to auditing, accreditation, adherence to standards, security culture, liability issues and compliance with laws and regulations.

- Insider Affiliate - Clients and their access to the organisation and its infrastructure: Client data includes data from client history and financial status.

Additional details of the insider behaviour should be also gathered from the following sources:

- Access privileges, access patterns from historical data (for base lining) (i.e., users with similar job functions are likely to have similar access patterns to applications and similar levels of demand for information)
- Real time usage pattern and user behaviour data.
- Real time user behaviour based on location, logging hours etc.
- Social behaviour.

Threats may sometimes arise from ‘model’ employees too. Employees refusing to take vacation can possibly be indicative. Often insiders committing fraud or stealing data or manipulating data needs to be in control over those systems to maintain the deceit and avoid being caught. Employees arriving early and leaving late have access to files, computers and the office in general and may indicate financial or personal relationship problems which may lead to insider compromise. Working from home, working strange hours or remotely could mean that the employee do not wish his activities be noticed by his co-workers or his supervisors.

4.3.2. Gather behavioural information
In order to assess insider threats, it is not sufficient to just identify assets, their sensitivity and their vulnerability; the major challenge is to continuously assess the behaviour of each employee, as every employee can be a potential threat like well-meaning employees who are over-zealous, naïve users with their ignorance or malicious users with their intentions. Gathering information on each employee from human resources on a regular basis will provide the necessary indicators. Details should be gathered on the following:

- Pure Insiders - Current and former employees (full time as well as part time): Data includes national origin, visa status, educational qualifications, outputs of background
report, previous incident report, system test results, system security plan, security policies), HR documents (employee history, annual reviews, exit interviews) can be a good source of information related to security controls.

4.3.3.4. Monitoring tools. Various technical methods (system logs, application logs, security logs, event logs etc) can be used to collect system and user behaviour information.

Human resources provide information related to the behaviour of employees, contractors and suppliers. Insider threat agents are the employees of a business or organisation; hence, human resources can provide relevant information of the insiders. Annual reviews and exit interviews can provide further information.

4.4. Insider threat and threat agents

The term ‘Insider threat’ as described earlier, is an individual with legitimate rights and authorisation and has the capability, motivation and opportunity to violate security and cause harm to a business or an organisation. In order to understand what an ‘insider threat’ is, it is necessary to identify the elements that constitute the threat. The insider threat can cause harm intentionally, accidentally or due to ignorance. Each type of insider threats consists of threat agents and they can denote an individual or group that can manifest a threat. Such agents have the following features, as based on “Threat-agent relationship by Andy Jones & Debi Ashenden” and is as shown in the diagram (Fig. 9) below.

For an insider threat agent to pose a threat to an organisation, it must have the capability, motivation, access to resource, opportunity, catalyst, inhibitors and amplifiers.

4.4.1. Insider threat capability

The elements that make up the capability of an insider threat have been based on components of capability by Andy Jones & Debi Ashenden as shown in the diagram (Fig. 10) below:

The effectiveness of any insider attack is directly proportional to the capability of an insider threat agent. The higher the capability the greater is the threat. That means there is a good chance the agent can attack and sustain the attack as well as destroy any replacements. Every agent needs capability like resources, knowledge, technology etc, in order to carry out any attack.

4.4.2. Insider threat motivation

Motivation of an insider threat agent can range from idle curiosity to malicious intentions. The diagram (Fig. 11) provides the elements of motivations of an insider threat agent.

Every employee in an organisation may be a potential threat agent if they possess the motivation to take advantage of their capabilities and the opportunities they have while working for the organisation. The malicious insider’s motivation may come from personal gain, revenge, competitive advantage, ideology or could be a combination of them.

4.4.3. Insider threat opportunity

In order for the insider with the capability and motivation, to execute an attack on the organisation the agent would need the opportunity to do so. Fig. 12 shows the elements that make up opportunity for insider threat:

For example, having compromised a user account or finding an unattended workstation logged on with the valid user, the insider makes of copy of a sensitive document, when the user is not around.

4.4.4. Insider threat agent identification

One of the important stages of insider threat assessment is the identification of the threat agents. Since the attributes of the threat agents are dynamic, the identification process should always be an ongoing process. For example, an innocuous employee may turn out to be malicious on a certain trigger. Data on the users’ activity like the event or system logs, browsing history or network logs enable identification of unusual behaviour and identify these users as possible threat agents. The next phase would be to classify these threat agents according to their nature and the scope of the assessment. The moment the threat agent is identified and classified, a record of the insider is made and archived for continuous monitoring. This is because the identified insiders may be enumerating an attack. The classification may exist in

---

**Fig. 9** – Factors contributing to the creation of an insider threat.

**Fig. 10** – The components of capability (Jones and Ashenden).
many forms e.g. active, inactive, dormant, and dead. Within the boundaries of the law following fundamental privacy and data protection principles, the employer should monitor the identified threat agents throughout their lifetime.

Identifying insider threat agents using technical means may not always be effective. Since such threats are human elements primarily, it also requires the involvement of human resources. So, both technical as well as psychological means should be used in order to identify insider threats.

4.4.4.1. Technical measures. A range of technical measures can be adopted to identify insider threat agents. Examples of technical precursors are downloading and using hacker tools, unauthorised access to co-worker’s systems, system access after termination or inappropriate access of internet at work. Logging and analysing insiders’ activities can give a wealth of information to predict possible misuse of organisation’s resources.

Besides logging, there is a need to have a strong audit process in order to review the logs. Logs provide a wealth of information about the perpetrator, its activities as well as the victim. Logging can be used during exit interviews to ensure data is not taken to a competitor. While at the exit interview, a print of the last few emails, network activity or websites visited may provide clues of any misuse.

A combination of Intrusion Detection Systems i.e. network-based intrusion detection systems (NIDS) and host-based intrusion detection systems can be used to detect insider attacks. Collecting and analysing the data collected can yield multiple indicators to a possible insider abuse and misuse. These indicators can be monitored to predict a possible attack, although there is a high chance that an insider can turn off or disable the IDS, so IDS should not be the only mode of detection. E. Eugene Schultz (2002) in his paper ‘A framework for understanding and predicting insider attacks’ mentioned the conclusive indicators of an insider attack and the following is based on them.

4.4.4.1.1. Deliberate markers. Sometimes insiders may leave ‘markers’ and that can provide indicators of a possible attack. For example, a disgruntled insider may deliberately misconfigure a modem, or software. This may be due to ignorance, or intentional. However, a major focus should be finding and tracking such small ‘markers’ before any significant attack.

4.4.4.1.2. Meaningful errors. Any insider intentionally trying to carry out an attack on the system is likely to leave some indicators like mistakes. For example, someone who wishes to make access to sensitive documents might try to read the file and receive the error message ‘Access denied’ or ‘You do not have authority to view this file’, or someone who tries to move a sensitive file from one directory to another might make mistakes in the command line. There is always a chance that the insider may erase the relevant log files and the command history but forget to erase the error log files. Therefore, it will be possible to deduce who they are and what the perpetrator has been trying to do by investigating the error logs. The Table A.2 in Appendix I is adopted from NIST to give an idea of possible indicators that can be flagged as malicious.

4.4.4.1.3. Preparatory behaviour. The insider’s behaviour may be indicators as part of the preparatory phase of an attack. The insider may, for instance, enumerate to gain as much information about the potential target system. To do so, the insider may use typical commands like ping, nmap, nslookup, finger, whois, rwho, or use techniques like key logging devices or social engineering. In doing so, an attacker can expose their intentions.

Each of the indicators gathered from deliberate markers should be flagged for further monitoring and a new entry or increasing the account of the event should be made into the database for archival purposes. According to Terrence Walker (2008), event characteristics should be stored for behaviour base-lining. Table A.3 in the Appendix I provides the possible list of event characteristics needed for behaviour base-lining. It is essential to obtain baseline information prior to any intervention. Therefore, data collected from event characteristics stored over a long period will help create the behaviour baseline for insider threats. Lack of such baselines may lead to erroneous conclusions.

According to the authors Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis in (Stolfo et al.) a ‘Honey-token’ is another means to catch insider misuse. AS ‘Honey-token’ is a specific piece of data disguised to look like a sensitive and confidential piece of data. This piece of data is used to ‘trap’ the insider for misuse. It is a piece of data that should never be accessed. Any interaction with a honey token
will most likely be unauthorized or malicious activity. It can be placed, for example, in a database containing bogus credit card details. All security systems like the IDS, IPS content and email filtering can be configured to ‘look’ for the ‘honey token’. If the ‘honey token’ is found traversing through the network, there is a good chance that an insider is trying to copy the data. This technology is quite new and there are issues of ethical, legal and personnel to consider.

Technical measures can constrain the activity of every insider and prevent them from accessing certain information; however the reality is that the users with the highest level of access are the ones who are least monitored and are subject to the lowest level of oversight. Based on the level of access, user activity should be monitored, so that any changes can be detected at the earliest opportunity.

4.4.4.2. Behavioural measures. The psychological behaviour and socio-economic aspects are linked to insider attack in many cases. The behaviour may be indicative of the predisposition towards an act of sabotage. According to CERT investigation on insider threat agents shows that the perpetrators had previous behavioural history. Most organisations have employees who may be dissatisfied with bonuses or restructuring, while some may grumble and accept it. But there are some who continue to hold grudge. It is important to monitor those set of employees who continue the bear a grudge and those who exhibit, for example, hostile behaviour towards co-workers or other staff. Quite often organisations tend to overlook behavioural precursors, with the hope that with time the employee may accept the changes and settle down. However, this allows the insider to prepare groundwork for attack. For example, a privileged user may create a backdoor for future use, or create a logic bomb. Precursor observations of behavioural or sudden changes in socio-economic circumstances should be a trigger for organisations to monitor individual activities in order to either detect or prevent a possible attack. According to Verizon (2009), the abuse of system access and privileges are common. Most insider attacks generally start with abusing the system, and then violating security policies. According to E. Eugene Schultz (2002), verbal behaviour and personality traits present pointers to detecting the likelihood of an attack. Organisations concerned about insider threats should develop specific attack methods that are indicators of observable behaviour i.e., verbal and personality.

4.4.4.2.1. Verbal behaviour. Expressions of dissatisfaction, or aggression, are quite often indicative of an insider attack. Perpetrators can be quite vocal about their dissatisfaction or may go all quiet while planning an attack. An example would be email messages to co-workers, friends or even social networking sites about his dislike/hatred towards an employee or manager. It is during this period that recording and analysing any requests for elevated privileges or network activities, or access to files or computers may yield the necessary pointers.

4.4.4.2.2. Personality traits. Basic characteristics can be used in predicting insider attacks. Some insiders may have reduced inhibitions, may be ethically ‘flexible’ or generally a loner with poor social skills. Cultural backgrounds, religious beliefs or political views may influence the characteristics of an individual.

It is important for organisations to consider a different facet of the insider while analyzing behavioural aspects. The psychological outlook of an insider can be shaped by his place of origin, cultural or educational background. Organisations that have outsourced operations to a different country need to understand that the behaviour of contractors (Insider Associate) would be aligned to the culture, value and serviceability of the country of origin.

4.4.4.3. Organisational measures. Organisations find it very challenging to balance trusting their employees. They provide them with the access necessary to perform their job function in meeting the organisation’s mission, yet need to protect its assets from being misused by the same employees. The combination of employees’ access, knowledge of the organisation’s business, technical weaknesses and drawbacks in business processes can be quite dangerous since given the opportunity, and motivation the insider can exploit the organisation. Therefore, it is mandatory that organisations deploy measures to identify insider threats and pre-empt them before-the-act. The following inputs can provide pointers in predicting insider threats:

- Violations of clearly documented policies and controls.
- Reports about suspicious behaviours from security conscious employees (This is normally seen when organisations introduce a security culture and awareness training).
- Negative work place issues may nurture the likelihood of insider threats.
- Reports from Human Resource reviews of current and previous employees (identifying changes in personal circumstances), new employee screening to establish past employments and other background details.
- Violations of physical security measures.

The collection, integration and analysis of technical, behavioural and organisational data can provide the indicators to predict possible insider misuse. The combined data will provide a coherent view of insider risks within the organisation and management can get a realistic picture on the activities from the analysis, which in turn can guide the organisation into taking adequate steps to protect and manage the insider problem.

4.5. Insider threat evaluation

Insider threat evaluation is based on a number of factors in assessing the capability, opportunity and motivation of an insider threat agent. Fig. 13 Bishop et al. show the evaluation of an insider threat agent and the factors involved.

4.5.1. Quantifying insider threat attributes

Some of the common attacks that have occurred previously or listed in open source database on insider threats and attacks provide the starting point in identifying insider threat agents or possible attacks or the attacks itself. However, all insider threat agents are very specific to the type and culture of an
organisation. Known attacks are generic; all organisations should base the findings on the attributes of their employees, their capability, their motivation and culture. In order to evaluate the insider threat it is necessary to quantify the attributes i.e. motivation, capability and opportunity, of the threat agents. The calculation of the insider threat agents is based on the methods defined by Dr. Stilianos Vidalis and Dr. Andrew Jones. Other factors influencing the insider threat agent to execute an attack are the changes taking place in the organisation, their technical expertise, and the finances or general morale of the employee.

4.5.1.1. Insider threat agent capability calculation. The capability of an insider threat agent depends upon the complexity value of the organisation’s asset value, access rights, vulnerabilities and weaknesses as well as the sophistication of both the agent and the target. It may be sufficient for an insider to use own access privileges to achieve an objective but may require higher level access for a desired effect. In order to quantify the capability of an insider threat agent, data from the following sources are relevant:

- Tables containing metrics for each insider threat agent category,
- List of organisations’ assets, their value, and sensitivity and vulnerabilities,
- Identified insider threat agent access privileges,
- Insider threat agent data (like education, employment history, skills and knowledge) from internal and external to the organisation sources.

4.5.1.2. Insider threat agent opportunity calculation. Every insider threat agent motivated enough may seek opportunities to exploit the vulnerabilities of the assets or execute an attack. Opportunity can be effective if the insider has access to the assets and has knowledge of new technologies to exploit safeguards and bypass system security. The insider agent can exploit vulnerabilities not discovered or inadequate policies and procedures or the lax of the organisation in employing a safeguard or even exploit the ‘trust’ laid on him by the organisation. Quantifying opportunity will require data from the following sources:

- List of the insider threat agents identified for monitoring,
- Current knowledge, perception and opinion on the insider threat agents,
- Reports on the examination of the technical, business and physical environment in which the organisation is operating,
- List of the identified vulnerabilities of the assets and for implementing safeguards.

4.5.1.3. Insider threat agent motivation calculation. Motivation factors are diverse and the insider threat agent may operate singly or in a group. Some of the primary groupings of insider threat agent motivators could be political, personal gain, revenge, ego, religion, even terrorism. In order to evaluating the motivation of an insider, data from the following sources will be helpful:

- List of the insider threat agents (individuals and groups) selected for monitoring,
- Insider threat agent data (like education, employment history, skills and knowledge) from internal (Human Resources) and external to the organisation sources,
- Tables containing metrics for each insider threat agent category,
- List of organisations’ assets, their value, and sensitivity and vulnerabilities.

For the insider threat agent to be able to misuse an organisation’s assets, the factors that make it possible are motivation, capability & opportunity.

Evaluating the insider threat through capability, motivation and opportunity is challenging. Insiders can remove traces of their behaviour by attempting to hide malicious activities by operating within acceptable behaviour. It is quite demanding to identify such insiders by specific boundary solutions.

4.6. Predicting the likelihood of insider attack

The main objective of the insider threat assessment should be detective, corrective or preventive. Logging activities of network and systems is vital for detection, which plays a critical role in risk control.
The insider threat problem is very complex. It involves physical security, information technology, management, data "owners", software engineering, and human resources. Organizations need a guideline to merge the wealth of available information into a single actionable framework.

To predict the likelihood of insider attack, it is helpful to imagine that the raw data traverses through a multi-layered analysis process as shown in the Fig. 14. Raw data made available from various sources like firewalls, intrusion detection systems can give indications of malpractice. For example, taking the statistics of internet traffic may imply that an insider has been downloading or uploading large volumes of data not seen normally, or data from the human resources implies that an insider has been working at odd hours. The observation derived when the data processed against the organisation’s baseline may indicate ‘high amount of downloading/uploading’ or ‘working abnormal hours’.

These observations may give indications of insider misuse or a probability of a misuse. Such indications may be from direct observation. The insider threat may be predicted by matching the behaviour against the database of insider activity from internal and external sources. However, a major challenge is identifying malicious behaviour from normal activity.

Predicting the likelihood of insider misuse enables an organisation to prioritise and allocate resources to address the threat. Insider threat assessment can take place before or after any system that goes live. If any threat is envisaged then it is necessary to get the threat data to calculate the likelihood of each threat agent. Perspective and knowledge of management and staff is essential in predicting insider threats.

4.7. Analysing the impact

A business review and setting priority to identified threats should be the next stage on completion of the assessment phase. At this stage, strategic decision makers of each department like IT, legal/compliance, operations, human resources and senior management teams should meet to review the findings of the assessment

1) to identify, and prioritise critical areas of concern and 2) to determine the impact that may result following a successful insider attack.

Impact can best be defined in terms of impact on confidentiality, availability and integrity of an organisation’s asset. A scoring mechanism may be used to make it meaningful, reusable and easily communicable like assigning values (e.g., a criticality range of 0 to 9) as shown with examples in Table A.4 Appendix I below or assigning impact levels (e.g. Low, Medium, High) as shown in Table 3 and adopted from Stine et al. For example, trade secrets, human resources and financial data have high confidentiality level, trade secrets and financial data have high integrity level whereas human resources have low availability level.

Taking another example, a bank might label a threat of employees writing down passwords of emails accounts as ‘Medium’ with a financial exposure of £1m per year, or customers stealing personal information about other customers as ‘High’ with a financial exposure of £100m per year.

Some impacts can be measured quantitatively in terms of financial loss like the cost of replacing a system, or the person-hours required to rectify a problem created by an attack. However, others like loss of reputation, loss of public confidence cannot be measured quantitatively but can be described as high, medium, and low impacts.

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Loss of confidentiality leads to a limited effect on the organization.</td>
<td>Loss of integrity leads to a limited effect on the organization.</td>
</tr>
<tr>
<td>Medium</td>
<td>Loss of confidentiality leads to a serious effect on the organization.</td>
<td>Loss of integrity leads to a serious effect on the organization.</td>
</tr>
<tr>
<td>High</td>
<td>Loss of confidentiality leads to a severe effect on the organization.</td>
<td>Loss of integrity leads to a severe effect on the organization.</td>
</tr>
</tbody>
</table>
Other risk management methodologies like business impact analysis (BIA), quantitative and qualitative risk analysis may provide further inputs to determine the priorities. On completion of the prioritisation process, the findings should be documented, circulated among senior management of the business and reviewed on a regular basis.

4.8. Control recommendations to reduce insider threats

Control recommendations are countermeasures that will help reduce the probability of insider misuse. Insider threats are the threats posed by humans. Technology can drastically reduce the insider threat problem but only if it is concurrent with non-technical measures. Businesses and organisations need to implement specific types of controls based on their objectives and goals. The following discusses the common control principles that can be applied to any organisation.

4.8.1. Technical recommendations

Ranges of technical measures that can be recommended to help reduce the likelihood of insider misuse are relatively well known but due to cost implications, many are ignored. Simple recommendations are:

- Strong password policies (not easily breakable); keeping the lifetime of them short, and not writing them down.
- Two (or Three) factor authentication - a stronger method of verifying access like using a combination of ‘something you know’ (passwords), ‘something you have’ (a token) and ‘something you are’ (biometrics).
- Role-based access control can be implemented to provide a framework that can bring the principle of ‘Least Privilege’ and ‘Separation of Duties’ to realisation,
- Audit logs from various sources such as software and hardware applications, servers, firewalls, Intrusion Detection Systems, Intrusion Prevention Systems etc., need to be combined to provide a coherent view of activity inside the network.
- Encryption policies like encrypting sensitive data that is either at rest (databases) or in motion (emails, instant messages, and portable devices).
- Sensors to detect any intrusion should be resource based instead of boundary based.
- Staff should have tools and time to monitor the output of the sensors Use of portable device policies, like using USBs to store and transfer data.
- Policies regarding the use of unsecured networks like logging in from cafes, airports.
- Policies related to use of internet, free webmail, or emails.
- Strict policies of deactivating accounts of users, who have been terminated, laid-off or have resigned.

Although the above recommendations are not an exhaustively list, it is a starting point that may help to reduce both malicious and accidental insider threats.

4.8.2. Non-technical recommendations

Non-technical recommendations need merging with the technical to prevent the opportunity for any insider executing an attack on resources and assets of an organisation or a business. Some recommendations are procedural while others should be aimed at the effecting the working environment and security culture.

- Physical security measures (e.g. swipe access cards) and CCTV monitoring (with facial recognition and object tracking) to provide a first layer of protection.
- Dual key control for access to key functions and sensitive information.
- Strong Human Resource policies on checking references, past employments details of prospective new employees; employment contracts to include ‘Acceptable Use Policy’ of IT resources; regular appraisals and exit interviews to be conducted that will help identify any feeling of disgruntlement; and the means for staff to confidentially report any suspicious activity.
- Security awareness programs to be conducted on a regular basis for all staff (increased awareness will reduce accidental breaches); Information Security personnel to be provided with regular training on new technological developments.
- All policies should be easy to comprehend, consistent, enforced, clear and regularly updated.

Since insider crime is fundamentally a people issue, technological controls alone will be insufficient to control the insider misuse. Use of technology may reduce the level of access, provide monitoring to identify the threats, but it has to be concurrent with organisational and behavioural controls. The use of technological, organisational and behavioural controls will lay the foundation for developing a security culture, thus reducing the likelihood of an insider attack.

4.9. Documenting results of assessments

After identification of the insider threats agents, the vulnerabilities of systems, asset sensitivity levels, and estimated impact of attacks the findings should be documented in an official report or briefing. This management report provides a guideline for the senior management, to make decisions on security policies and procedures.

4.10. Summary

Insider Threat assessment aims to discover the likely tactics and strategy of an insider threat agent, so it is appropriate to employ adequate counter measures. It enables organisations to get a clear picture, gain a better understanding of the threats posed by insiders and an enhanced capacity to assess and manage the allied risks. The assessment can provide a comprehensive tool for senior management as it combines technical, organizational, psychological, business security, and process issues into a single, actionable framework.

The process of insider threat assessment is analytical and addresses many issues, as shown below:

- Provides behaviour patterns revealing a path to action,
- Provides a clear distinction between expressed threats and posed threats,
Senior management can gain substantially from an Insider Threat assessment report. It provides a strategy to control, reduce or eliminate potential insider threats by using a framework to improve the security attitude of the organisation thus providing them with a justification of the return on security investment.

5. Conclusion

Insider threat is a unique problem; it can never be eliminated. Although it has a generic pattern, every incident has special characteristics. No single clue is sufficient in predicting a potential threat. Moreover, insider threats are unique to organisations i.e. threats posed by an insider at a software development house is not the same as that posed by an insider of a bank. The uniqueness of insider threat makes it difficult for organisations to seek standard solutions. In order to address the threats posed by insiders, every organisation needs to have its own architecture that prioritises assets and resources, gleans information from logs and human resources, gathers information from analysing email habits, and instant messaging use, in order to produce a threat rating associated with each user. The architecture should encompass the entire organisation.

Laying the foundation to address insider threats can be a tricky business. It is indeed a challenge for organisations given the complexity of infrastructure, the diverse mix of employees, contractors, suppliers and consultants. Much has been mentioned about employee monitoring for a good reason. However, this could be counter-productive as honest employees may feel they are not trusted to do things right. This is likely to create an environment of scepticism and distrust thus invariably lowering the morale of employees, and disillusioning them regarding the misuse systems. It is merely a misconception that monitoring is done for malicious insiders. It may be a handful in an organisation who may be malicious, with the vast majority being truly honest and loyal, yet it is worth noting that trusted employees can commit mistakes like opening attachments containing malware, overlooking software updating, or emailing sensitive documents without encryption. Therefore, it is vital that employees are made aware of the level of monitoring and the policies of the organisation. It creates an open working environment of trust and user productivity with adequate levels of security for employees to safely share information while accepting different cultures and business practices.

Sometimes it is the lack of support from the senior management that indirectly is responsible for security breaches. The basic reason for this is the gap in the perception of insider threats by management. Most organisations feel that it is the responsibility of the technical staff to do the right things to thwart insider threats but these are not just technical but organisational issues.

For technical, behavioural and organisational measures to be effective, it is important that security staff have time, and the tools to monitor, assess and analyse the output of monitoring systems. In addition, the staff monitoring the system should not themselves be above monitoring so there must be a system in place to monitor them.

Organisations perceive security as expensive and that is a deterrent. They clearly fail to see the ‘Return on investment’ of good security measures and systems leaving themselves vulnerable to attacks. Some organisations fail to realise that investing in effective security protections pales in comparison to the cost of a security breach. The cost of a security breach can be prohibitive; it can involve the cost of recovery of systems affected, the cost of recovery of reputational loss, and the costs of litigation. However, organisations with limited security budgets should implement best practice to provide a cost effective solution. Implementing the following basic baseline can be a useful starting point.

5.1. Strict HR policies

HR should have a strict guideline for effective screening of new employees as well as routinely checking on employed personnel. This is more so for employees in sensitive positions, contractors, suppliers, consultants, and partners. Anyone dealing with the organisation should sign and agree to adhere to the security policies. Exit policies and interviews should be conducted for every employee leaving the organisation.

5.2. Mandatory awareness training

Every organisation should have a comprehensive security awareness program. All employees must go through a periodic training with smaller briefings if necessary. Training should include awareness of the use of social engineering techniques to retrieve sensitive information.

5.3. Technical controls

Access to systems should be based on the security principles of factor authentication, least privilege (providing access just enough to do the assigned job), separation of duties (for employees dealing with sensitive transactions), and fail-safe defaults (default being the lack of access). There should be a convention regarding password length, the format and their lifetime. Default administrative accounts must not be used...
since it makes accountability difficult. Databases containing sensitive data should be encrypted and backups regularly tested.

5.4. Hardware controls

Mobile staff with laptops containing sensitive data should have two factor authentication to logon and use encryption for sensitive documents. Organisations must implement restrictive use of USB storage devices.

5.5. Network access controls

All firewalls and IDS must be configured according to security best practices. The organisation must have policies regarding P2P file sharing, downloads, the volume of outbound and inbound file transfers, use of instant messaging, and restricting information sent on email.

5.6. Auditing and monitoring as detecting controls

It is necessary to configure logs and audit trails for every system. Each of them must be protected by access control to ensure integrity.

The key issue in this paper is that insider threat assessment requires identifying, assessing and evaluating the insider threats 'before-the-act'. This can enable businesses and organisations to be proactive by creating a matrix of users who have access to assets, and prioritise them according to their value and sensitivity.

One of the greatest risks is users with access to the resources of greatest value. Security personnel should prioritise resources to protect valued assets and monitor the users likely to pose the greatest risk. By admitting that insider threats exists, is the first step to controlling it. It cannot be controlled by technological means only, organisational measures and human resources need to be involved concurrently to control insider risk.

Appendix I.

<table>
<thead>
<tr>
<th>Misuse</th>
<th>Monitoring level</th>
<th>Attribute(s) to monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illegal content</td>
<td>Network</td>
<td>Packet content</td>
</tr>
<tr>
<td>Excessive/anomalous usage</td>
<td>Network</td>
<td>Bandwidth usage</td>
</tr>
<tr>
<td>Resource exhaustion</td>
<td>Network</td>
<td>Bandwidth usage</td>
</tr>
<tr>
<td>Playing network games</td>
<td>Network</td>
<td>Bandwidth usage</td>
</tr>
<tr>
<td>Illegal software distribution</td>
<td>Network</td>
<td>Bandwidth usage</td>
</tr>
<tr>
<td>Access to isolated subnets and machines</td>
<td>Network</td>
<td>IP address</td>
</tr>
<tr>
<td>Access from unauthorised machines</td>
<td>Network</td>
<td>IP address</td>
</tr>
<tr>
<td>Access to prohibited content</td>
<td>Network</td>
<td>URL</td>
</tr>
<tr>
<td>Use of web-based email</td>
<td>Network</td>
<td>URL</td>
</tr>
<tr>
<td>Recreational surfing</td>
<td>Network</td>
<td>URL</td>
</tr>
<tr>
<td>Instant messenger</td>
<td>Network</td>
<td>Service usage</td>
</tr>
<tr>
<td>Unauthorised network services</td>
<td>Network</td>
<td>Service usage</td>
</tr>
<tr>
<td>File sharing network,</td>
<td>OS</td>
<td>Service/bandwidth usage, file attributes</td>
</tr>
<tr>
<td>Web hosting</td>
<td>Network</td>
<td>Service/bandwidth usage</td>
</tr>
<tr>
<td>Resource exhaustion</td>
<td>OS</td>
<td>CPU, memory, disk usage</td>
</tr>
<tr>
<td>Storage of image and multimedia files</td>
<td>OS</td>
<td>File extensions</td>
</tr>
<tr>
<td>Anomalous command usage</td>
<td>OS</td>
<td>Command usage</td>
</tr>
<tr>
<td>Anomalous application usage</td>
<td>OS</td>
<td>Application usage</td>
</tr>
<tr>
<td>Information disclosure</td>
<td>OS</td>
<td>File (read)</td>
</tr>
<tr>
<td>Breach of privacy</td>
<td>OS</td>
<td>File (read)</td>
</tr>
<tr>
<td>Data theft</td>
<td>OS</td>
<td>File (read, copy)</td>
</tr>
<tr>
<td>Alteration of data files</td>
<td>OS</td>
<td>File (write)</td>
</tr>
<tr>
<td>Alteration of system files</td>
<td>OS</td>
<td>File (write)</td>
</tr>
<tr>
<td>Hardware installation</td>
<td>OS</td>
<td>File (create, write) configuration files</td>
</tr>
<tr>
<td>Software installation</td>
<td>OS</td>
<td>File (execute) unauthorised program</td>
</tr>
<tr>
<td>Illegal program execution</td>
<td>OS</td>
<td>File (execute) unauthorised program</td>
</tr>
<tr>
<td>Sabotage</td>
<td>OS</td>
<td>File (write, delete)</td>
</tr>
<tr>
<td>Privileged program exploits</td>
<td>OS</td>
<td>System calls, (file, memory) access, I/O usage</td>
</tr>
<tr>
<td>Data hiding</td>
<td>OS</td>
<td>Input files to programs</td>
</tr>
<tr>
<td>Encryption</td>
<td>OS</td>
<td>Input files to programs</td>
</tr>
<tr>
<td>Program exploitation</td>
<td>Application</td>
<td>User (input, interaction)</td>
</tr>
<tr>
<td>Alteration of input</td>
<td>Application</td>
<td>Function usage</td>
</tr>
<tr>
<td>Function usage</td>
<td>Application</td>
<td>Queries, API calls, Windows messages</td>
</tr>
<tr>
<td>Anomalous database Access</td>
<td>Application</td>
<td>User queries</td>
</tr>
<tr>
<td>Inconsistent data (fraud)</td>
<td>Data</td>
<td>Batch numbers, date, time, strings, numbers</td>
</tr>
<tr>
<td>Duplicate entries (fraud)</td>
<td>Data</td>
<td>Batch number, uniquely identifiable entities, etc.</td>
</tr>
<tr>
<td>Maximum value</td>
<td>Data</td>
<td>Number of employees, bonuses, extra time work, etc.</td>
</tr>
<tr>
<td>Minimum value</td>
<td>Data</td>
<td>Hourly pay rate, work hours, etc.</td>
</tr>
</tbody>
</table>
Researchers at the InfoSec 2009 Europe conference stopped passengers at a London train station and asked what it would take to get them to give up their company’s sensitive data. While 63 percent said they couldn’t be bribed, 37 percent said they would sell out for incentives ranging from a hearty meal to $1.5 million.

Table A.2: Possible indicators that flag an event as possibly malicious.

Indicators that flag the event as possibly malicious

- Anonymous user accounts.
- Unsuccessful logon attempts to applications, systems etc.
- File names with unusual characters.
- Large volume of uploads or downloads.
- Copying a database containing sensitive data (e.g. credit card details).
- Viewing sensitive data, including payroll records and medical information, without authorization.
- Slow access to hosts on the Internet.
- Unexplained modifications to file lengths and/or dates, especially in system executable files.
- Unexplained attempts to write to system files or changes in system files.
- Unexplained modification or deletion of data.
- Denial/disruption of service or inability of one or more users to login to an account.
- Unexplained system crashes or Poor system performance.
- Operation of a program or sniffer device to capture network traffic.
- Use of attack scanners, remote requests for information about systems and/or users.
- Large number of bounced emails.
- High email traffic with large attachments or suspicious contents.
- Reports of social engineering attempts.
- Unusual time of usage & usage patterns.
- An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user.

Table A.3: Event characteristics needed for behaviour base-lining (Walker, 2008).

Event characteristics needed for behaviour base-lining

- Enterprise management system events.
- Operating system events.
- Entire data stream for critical assets and services.
- Commercial Of-The-Shelf Application transaction logs.
- Event logs.
- Detected vulnerabilities.
- Forensic evidence.
- IDS/IPS signature triggers.
- Gateway inspection and filtering logs.
- Anti-Malware logs.
- Bespoke application logs.
- Communication and Information Systems policy violations.
- Access control logs.
Table A.4: Impact level and type with examples.

<table>
<thead>
<tr>
<th>Impact level</th>
<th>Impact type</th>
<th>Examples</th>
</tr>
</thead>
</table>
| 0            | Trivial, temporary and commonplace | – Using emails and browsing Internet exceeding the Company’s policy of “reasonable personal use”.
|              |            | – Using fax and telephone for personal use. |
| 1            | Potentially serious for personal financial gain | – Expense fraud |
|              |            | – Modifying data in accounting systems (e.g. purchase orders) |
|              |            | – Selling company assets (e.g. computing equipment) |
| 2            | Serious short-term impacts, motivated by revenge | – Planting “logic bombs” |
|              |            | – Deletion or alteration of customer data |
| 3            | Serious long-term impacts, motivated by revenge or personal gain | – Copying and selling customer database to a competitor. |
|              |            | – Revealing confidential information such as financial results, acquisition information to third parties. |
|              |            | – Copying large volumes of Credit card data |
| 4            | Catastrophic impacts | – Arson |
|              |            | – Permanent, irretrievable, destruction of critical data assets |

**References**


Sean Steele, CISSP and Chris Wargo, CISSP. An introduction to Insider Threat Management. Interlock Technologies Arlington, VA, USA.


Dr. Eric Cole, Sandra Ring, Insider Threat -Protecting the Enterprise from Sabotage, Spying, and Theft, Syngress Publishing.


Insider Attack and Cyber Security - Beyond the Hacker, Salvatore J. Stolfo, Steven M. Bellovin, Shlomo Hershkop, Angelos D. Keromytis, Columbia University, USA and Sara Sinclair, Sean W. Smith, Dartmouth College, USA, Springer


Dr. Stilianos Vidalis, Dr. Andrew Jones, Analyzing Threat Agents & Their Attributes, School of Computing, University of Glamorgan, UK., [http://www.comp.glam.ac.uk](http://www.comp.glam.ac.uk)