INTERNAL THREATS

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself and not your enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."
-Sun Tzu: The Art of War

Define "Internal Threats"
Damage done to an organization by a trusted person who has/had access to a trusted area of the organizations infrastructure.

Examining the Definition

- *Damage*: This can be any damage/loss to the organization; the following areas give possible classifications:
  - Financial
  - Credibility
  - Reputation
  - Intellectual property
  - Trust,
  - Image
  - Property
  - Data
- *Trusted Person*: This includes permanent staff, family members, contractors, and corporate visitors. Basically anyone to whom the organization gives access.
- *Infrastructure*: An organization has (both in the physical and the logical sense) areas of its infrastructure where outsiders are generally not allowed. Therefore allowing anyone else any access to these areas shows some level of trust being placed in these individuals.

Internal attackers are a risk, and normal risk management procedures say that the severity of a certain risk is made up of a company's exposure to a certain type of attack. This can be expressed

(Vulnerability (as a %) x Threat (expressed as annual % of occurrence) = Risk)

Threats
Any internal threat aims to do, or will end up doing, certain common things to an organizations infrastructure/ assets:

- *Delete/Remove*
- *Change/Alter*
- *Copy/Duplicate*
- *A combination of the above, such as taking a copy and then deleting the original.*

Or lets look at that a different way. Any organizations digital assets must be guaranteed in three areas:

- *Confidentiality*: There will always be data in the company that must be kept private. This can be because it is of a sensitive nature or because it gives a competitive edge in business. For whatever reason, measures must be put in place to ensure that the data remains confidential
- *Integrity*: While some data must be kept private, it is also just as important that the data is still correct. What use is a trade secret formula if someone has managed to change the amounts used? So the measures must also ensure that the data is trustworthy.
- *Availability*:You data could be private and you may trust it fully, but is it useless if you cannot access it. This may happen because of theft, a disaster, and deletion, basically anything that makes the data unavailable for use. So finally, measures must also ensure that the data is timeously available.

Thus any threat to these three key properties of the organizations data is what must be protected against. These

threats are embodied in:

- *Disgruntled staff*
- *Coerced/Pressurised Staff*
- *Planted Staff*
- *Unintentional damage*
- *Unintentional access*

Exposure
The best way to gauge exposure to a certain threat is to look at the absence of those measures that are used to safeguard against that threat, the measures, which are taken against insider threats, can be broadly broken down into:

- *Policies*
- *Logical*
- *Physical*

Lets look at each section to see where the lack of cover in each creates exposure: -

Policies

- Does the organization have policies for:
  - Network usage
  - Pre-hire checks
  - Enforced leave
  - Non-disclosure agreements
  - Company resources usage
  - Disciplinary processes
- Are the policies:
  - Known
  - Reviewed
  - Consistent
  - Enforced
  - Explained
  - Understandable
  - Legal
  - Reasonable

Policies are important because in all organizations there is a point at which staff must be trusted and logical or physical countermeasures cannot be used. This is where policies and their enforcement come into play. A lapse in any of the above points means that you are seriously hampering the usage of the policy and therefore have less legal recourse in using them.

Logical

- Can the systems create proper audit trails?
- Are users singularly accountable? i.e.; no shared accounts
- Is “least privilege” principle applied?
- Are access right controls centrally approved/controlled?
- Are roles regarding access right assignment adhered to?
- Is there a company-wide enforcement of roles and rights?
- Are hosts (server and client) setup as per best business practises?
- Is the network securely designed?
- Are there proper, standard and adequate access controls?
- Is there a regular review of access rights?

Logical controls exist to not just prevent unauthorised access to your information assets, but also to create accountability for the actions authorised people undertake on the information assets they have access to. Without proper audit trails or logical measures then the organization can never really say who did what to what. This once again severely limits not only the detection of insider threat but the recovery and prosecution thereof.

Physical

- Are personal devices prohibited?
- Are personal data-shuttle capable devices prohibited?
- Are business data-shuttle capable devices registered, monitored and audited?
- Are the entrance/exit points of the organization manned?
- Are those manning the entrance/exit points capable of identifying and checking all possible data-capable devices or forms?
- Are staff complaints and problems resolved?
- Does the organization know its staff?
- Are logs of allowed devices and/or data kept?
- Are spot checks of done, even of allowed devices?
- Are people entrusted with data responsible for the data?

One of the main advantages a malicious insider has is that in order to do work, the organization has already granted some level of access. This means that logical controls may not be able to stop a person getting their hands on data. This is where physical controls come into play, the organizations need to be able to monitor what data is leaving/entering their infrastructure on a physical level. This way even if a person does misuse their access, it will not help them. A failure here means, quite literally, that your data can walk out the door.

Threats
Lets also take a closer look at the embodiment of the threats as we mentioned them earlier:

- *Disgruntled Staff*: These are staff members who feel they have been wronged in some way by the organization. They now want to do something to "get their own back". These people are generally very easy to spot, just watch people who react badly after not getting the raise/promotion/leave they wanted, those that have just been disciplined, etc. While they are easy to spot, they are also the most unpredictable, as when a person's emotions are high they very often do things they may later regret, but that still doesn't bring back your database. This type of threat generally aims at the deleting/destruction of an organization's resources and are not really too worried about other people knowing who it was.
- *Coerced/Pressurised Staff*: Here things get a bit worse, with your upset staff you at least had some warning, as you generally know and can visibly see who is upset. In this case, nothing has happened at work to influence the staff member, but something outside of work has now placed pressure on this staff member to do something damaging to the organization. These pressures could range from blackmail, debt, bribery, threats, urgent need for money, etc. The other problem is that these people may not want to be noticed and the damage they do may not be readily apparent (as is the case with making a copy of sensitive data).
- *Planted Staff*: With this classification of threat, we are upping the game substantially. Planted staff are generally involved with industrial espionage, which is a lot more common than a person may think. The problem here is that the person planting the staff member will make sure that their agent has all the qualities you want. Also this person will be very careful to not draw attention to what they are and what they are doing. Making it difficult to find and catch them.
- *Unintentional Damage*: This is what happens when your staff have no malicious or harmful goals in mind, but because of weak or missing controls, they have the ability to perform certain actions that they should not be able to. When they make a mistake therefore, they may end up doing a lot more damage than if the controls had been in place. Think of a person deleting a file by mistake, but they end up removing it from the server. This type of problem can also occur by people changing jobs. The job market is a lot more fluid now then it ever has been, especially for 'knowledge workers'. Now when these staff leave, they will probably go work in a similar job and this generally means that they will be working for the competition, therefore any knowledge the person had will now go with them to the new job. There is nothing you can do about this, except make sure your staff do not have excess access and that you do not purposely drive these

people away.
- *Unintentional Access*: This is where the organization has expanded its internal network into something that is externally accessible. That sounds strange but think of this, when an organization installs wireless onto their trusted network, the border of that network now ends where the radio waves end, and therefore anyone able to use those radio waves is now an insider. Or when people are allowed access from homes or hotels, suddenly now all of those places and the communication medium between the areas is now also the trusted network. An organization that does not properly structure their network can end up with large headaches.

Why Worry?
The simple answer here is: Do you trust every member of staff 100%, 100% of the time? No one in a modern medium-to-large organization will say yes, there are just too many variables and possibilities. Am I being harsh? Ask yourself this: Why do you trust your staff? What have they done to earn that trust? You would not trust a person walking past the organization's building on the street, so why when you hire that person do you now suddenly trust them? Upon what does the organization base that trust? Now add into the mix that even trustworthy people can do something wrong when they are under stress or are being pressurised, and suddenly the problem is a lot larger. Then we need to add in the damage that someone could unintentionally cause due to a lack of controls, and suddenly the need to worry is apparent.

So What?
Even if there is a chance of damage, why should I worry about it? Look at it this way, firewalls, intrusion-detection systems, encryption and other technical measures have made it very difficult (or it should anyway) for an attacker to gain access to your trusted network. This therefore limits the number of people who could commit these attacks. But your trusted network is generally setup ..well.. more trustingly. This is because it makes it easier for your staff to work on it and accomplish their jobs. Therefore, if an attacker had access directly to your trusted network, bypassing most logical defences, then the knowledge and skill required to commit an attack is drastically reduced. This is an important point to remember, insider threats are easy and extremely damaging. Plus, most staff are given some level of network resource access in order to do their job, making any potential attackers job easier. An insider will also be able to become familiar with the processes and procedures and their weak points, with what data is valuable and where it is stored, and other contextual information which make committing an attack easier. These are just some of the reasons why organizations need to worry.

What Can I Do?
The first thing to realise here is a simple fact: Prevention is ideal but detection is a must. Full insider threat prevention is impossible, it will happen, but the organization must be able to assess the damage, mitigate it, and recover quickly and efficiently. Next you must know what is being attacked. Does the organizations know which are its critical resources? And why? Once you know this you can begin to work out an acceptable level of loss, remembering that the lower that level is set, the more resources and measures have to be put in place. Once you know what is critical you can then look at the next most important fact; access. Who has access? Why do they have access? What access do they have? How did they get the access? Remember that access to the organizations resources is what makes insider attacks such a threat, so understanding those questions can begin to point you in directions to start making changes.

Once you know all of the above you can start reasonably putting measures in place, but as a starting point here are some general prevention mechanisms to put in place:

- *Education / Awareness*: Any organizations weakest point is its staff. All your staff are on the trusted network and have varying levels of access, therefore if they can be manipulated into helping an attacker (social engineering) then you are facing a large problem. But if you can educate your staff, raise their awareness, then you have an entire organization of people who will be able to help you find and deal with all threats – including insider threats.
- *Defense in Depth*: This is a general concept that simply means that an organization must not place all its security needs on one system or setup, because that would mean that once an attacker –internal or external- is past that system, then they have free rein. The better idea is to have multiple levels of security

within the organization, so that any attacker would need to bypass multiple levels of security to get what they want.

- *Backups/Archiving*: It has already been said that there will be loss, and that the recovery and detection of an insider attack must be quick and effective. For this to occur any organization will need a comprehensive backup plan for its critical resources, as well as an archive of its logs and audit trails to ensure that no information is lost which may help resolve the incident.
- *Least Privilege*: This is a very important principle. Anyone should only have the access needed to do their job, anything else should not be allowed. Bear in mind, that this does not mean taking away resources, which may hinder them in fulfilling their job, but just the access to excess resources. Access is very important in any insider threat model and attack, if you properly and carefully monitor that, you will go a long way to dealing with the threat. Note, this does not only apply to logical resources (access to files, documents, etc) but also to physical resources. For example, how many people in the company actually need access to their USB ports for business purposes? Or need to bring in personal data-shuttle-capable devices?

Final Words

The idea of insider threat is one that companies do not like to face, because it is difficult and very often requires a change in mindset and how things work. But ignoring it will not make it go away, it will just make it the chances of it happening greater and the damage it causes when it does a lot more. Better to take some short-term pain for a longer-term benefit. I also do not advocate seeing the insider threat as the answer to why everything goes wrong, but it should at least be a consideration. So start looking into this stuff and as always, have fun and learn.