REVIEW OF TECHNOLOGIES TO TACKLE INSIDER THREATS

Author: Rizwan Mahmood **Published: March 2017**

1 SYNOPSIS

Insider incidents account for billions of dollars annually in "actual" and "potential" lost revenue, according to CERT© (Carnegie Melon University), a well-recognized source for insider threat data. This analysis is consistent with other independent research bodies like FBI, Forrester and Lloyds Risk Register which show authorized staff (insiders) to be the leading cause of data breaches, with some studies claiming it to be over 70% of the risk faced by companies today.

However selecting the appropriate technology which deals with the various uses cases and challenges associated with insider threat has become a complicated issue. The main reason for this is that insider threat has become a BUZZ word and every vendor tries to pitch their technology as a possible solution even though they might only be handling a few use cases.

The paper lists down the PROs and CONs of each type of technology in light of the **most difficult and important use cases** associated with insider threats.

2 WHAT IS INSIDER THREAT

The National Insider Threat Task Force (NITTF)[i], a task force setup by President Barrack Obama to tackle this issue, defines an insider and the insider threat as follows:

*"An **insider** is any person with authorized access to an organization's resources to include personnel, facilities, information, equipment, networks, or systems."*

*"The **insider threat** is the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practices."*

Several high profile leaks such as Edward Snowden, WikiLeaks, HSBC[ii], NBN (Australia)[iii], New Zealand Police[iv] etc give the impression that this threat is only limited to large organizations and governments when in fact the insider threat risk is consistent across any size organization. For smaller organizations there are many reported cases of insider threat activities in the form of sales staff taking the client list, copying architectural drawings, taking financial information, taking copyrighted source code of a specific project on which the user has been working on etc. For smaller organizations the impact of this risk is much higher as it threatens the very survival of the entire organization.

3 KEY INSIDER THREAT USE CASES AND THE RELATIVE EFFECTIVENESS OF TECHNOLOGIES

	KEY INSIDER THREAT USE CASES	KEY TECHNOLOGIES				
		Firewalls /Next Gen Firewalls	DLP	SIEM	UBA/ UEBA / EM	PCS
1	**USE CASE 1** →Involves authorized users accessing information for which they have legitimate access.	No	No	Partial [4]	YES	Yes
2	**USE CASE 2** →Involves normal working behaviour which cannot be regarded as malicious.	No	No	No	No	Yes
3	**USE CASE 3** →Involves malicious behavior of an authorized user different from his normal working patterns. Like copying 100s of files.	Partial [1]	Partial [1]	Partial [4]	YES	Yes
4	**USE CASE 4** →New forms of communication media (cloud storage, smart phones, and social media) and new working styles (working from home, BYOD etc) makes it a challenge to control corporate information.	Partial [2]	No	No	YES	Yes
5	**USE CASE 5** →Highly sensitive information at risk like acquisition documents, retrenchment plans etc are produced on an ad-hoc basis and are mostly not shared with IT Security as believed to be above their pay grade. As such the security of this information relies on the TRUST of the senior management dealing with it.	No	No	No	No	Yes
6	**USE CASE 6** →Leakage of information to internal users. Example leakage of a bonus sheet internally.	No	Partial [3]	No	No	Yes
7	**USE CASE 7**→Leakage of information from company's trusted partners external to the organization	No	No	No	No	Yes
8	**USE CASE 8**→Finding a balance between privacy and monitoring. This involves monitoring of Senior management and C level which control majority of the sensitive information but are reluctant to be monitored by IT staff who are considered their juniors.	No	No	Partial [4]	No	Yes

Partial 1. Reports are based on TOP 10 or thresholds without any user behaviour analytics.

Partial 2. Some new forms of firewalls have the ability to analyze content from various new forms of communication media however their coverage is limited to only when the user is using corporate network.

Partial 3. DLP can stop internal leakage as long as the internal user is not authorized to have access to the information. However in the event the information is wrongly classified DLP will not be able to prevent it.

Partial 4. SIEM systems are limited to only corporate systems like ERPs, Databases etc. They don't have any logs of the events where a user uses non-corporate applications like Dropbox, Gmail or transfers information using offline means e.g. USB, SD cards or by syncing files to a phone.

3.1 FIREWALLS/CLOUD FIREWALLS AND SERVER SIDE FILTERING SOFTWARE

Many organizations have tried to use traditional security tools like firewalls, blockers, filters but have consistently failed. If we are to understand why these technologies fail we have to understand the philosophy on which these technologies are built.

They are built to block external known threats such as hackers, spam etc. The adversary for them has always been anyone **not authorized** (external) to the organization. We can think of them as walls of a fortress around our city. Unfortunately in case of the insider threat it is the authorized users who are the adversary and the attack vector is reversed.

Applying the same methodology to internal authorized users by blocking access to some of the websites fails to prevent the insider threat. This method not only hinders productivity and is easily circumvented (user accessing information from outside the corporate network), but are also highly inefficient as there is no limit to the number of ways an authorized user interacts with the internet or with information.

The limited success of these tools can be seen in banks which are primarily closed and highly restricted businesses and tend to block access to majority of the internet. Some have now started to do more detailed analysis of the traffic and can be used to address **USE CASE 3** but the evidence produced is not clear or sufficient to take any conclusive action and is after the fact/leak. In general, not a technology which is built to handle the insider threat and doesn't address the challenges listed.

3.2 DLPS (DATA LEAK PREVENTION/PROTECTION SOFTWARE)

DLPs are built on the blocking philosophy. They block movement of information based on information classification or hard restrictions such as complete blocking of a specific communication mechanism like USB port. The BLOCK or ALLOW basis on which these products are built are not in sync with the new forms of communication media (smart phones, cloud environments etc) and working styles (BYOD, working from home). They struggle to block most of the new forms of communication mechanisms and hence fail to address all the key challenges mentioned above.

In cases where the new communication media or working styles are not being used they have faced serious implementation issues. As they are operated and controlled by IT security teams, in the case information is wrongly classified they end up over blocking and require overriding from IT Security which becomes a major hindrance. On the other hand in case the information is not classified they don't pick it up at all. Further measures like blocking USB ports stop people from legitimately transferring files.

Lack of easy classification mechanisms have resulted in a never ending battle between IT security and end-users who are required to provide the correct classification and in the end too many gaps exist within the network. For this reason over the years DLPs have developed a bad reputation as a **disastrously long project**.

The blocking capability of DLPs have found success in financial institutions specially banks which are highly regulated and are ok to take in the overheads of over blocking specially in terms of PCI DSS compliance. The over blocking have resulted in DLP software to move to passive monitoring and producing alerts primarily in line with **USE CASE 3** however these reports are of limited effectiveness as lack the user behaviour analytics capabilities. These reports are primarily top 10 or threshold based reports.

Overall DLPs in most other cases, concerning the insider threat, where information to be monitored is not standard, is created on an ad-hoc basis and is ever evolving they fail drastically as they have to rely on the end-user to classify the information in the first place for them to protect it.

3.3 SIEM (SECURITY INFORMAITON AND EVENT MANAGEMENT) SYSTEMS

SIEM systems record the interaction of an authorized and unauthorized user with the internal applications of a company but have absolutely no information of what happens to this information once it leaves the internal system. For example they will not have a record if information is copied to a USB or sent out via Gmail, free cloud services etc. As such it can be argued that they have limited capability in terms of **USE CASE 1**. This limited visibility allows them to comply with the privacy **USE CASE 8** but with some obvious drawbacks on security.

In the case of insider threats SIEM vendors are now incorporating user behaviour analytics and are using it to pick malicious activity with company's internal applications i.e. **USE CASE 3**. Further SIEM logs are also an important source of information in an insider threat investigation to find out from where the information originated. However, considering the limited visibility provided by SIEM systems they can't address the more complicated challenges related to insider threats.

3.4 UBA/UEBA/EMPLOYEE MONITORING SYSTEM

More recently, because of the failure of the DLP and SIEM software to address the insider threat, we have seen the rise of user behaviour analytics systems. Gartner started to mention this category in 2014 and later added the letter "e" depicting entity in 2015 making it into UEBA. They have many similarities to another category of systems highlighted by Gartner as Employee Monitoring systems.

These systems are built on human behaviour principals of **TRUST BUT VERIFY**. They start from the concept that, as it is too cumbersome to block, it is better to trust the users and allow them to use different forms of new communication media but verify by having visibility of all transactions. The monitored information is than analyzed using various behaviour analytics and machine learning techniques to pick up various anomalous user behaviour. Examples include copying of large number of files, user accessing the system at odd hours of the day, a user copying higher number of files using non-traditional transfer mechanisms such as Dropbox etc.

These systems are excellent in picking up malicious activities by authorized insiders i.e. **USE CASE 1 and USE CASE 3**. Further as they are built on monitoring philosophy they don't block users from doing their work and are future proof against new forms of communication i.e. **USE CASE 4**.

Although UEBA systems are starting to prove their worth in tackling some forms of insider threat however implementation of these systems is proving to be challenging. Privacy (USE CASE 8) is a major issue for these systems and are usually likened to **BIG BROTHER** systems. For this reason senior staff are usually not monitored and hence the key information is not protected. Further as the information is monitored by IT staff they fail to detect in time leaks due to normal working behaviour (USE CASE 2).

3.5 PEOPLE CENTRIC SECURITY BASED SYSTEMS

The concept of People Centric Security was first introduced by Gartner in 2012 by Tom Schultz[v]. PCS systems provide a drastically new way of solving the insider threat. These systems are built on the user

behaviour principals of **EDUCATE**, **EMPOWER**, **TRUST AND VERIFY** philosophy. Using this philosophy they are able to address some of the most use cases related to insider threats.

The corner stone of this principal states that as all issues arising from insider threats are related to internal users as such the solution to the problem should also start from them. End users should be given the **responsibility** of securing the information themselves but with relevant **education** and **accountability**. Following are key characteristics of PCS systems and how they mitigate various challenges posed by insider threats.

User behaviour monitoring but with user empowerment →PCS system are built on visibility rather than blocking and are based on the principal of Trust. They incorporate UEBA/employee monitoring capabilities however; rather than just relying on IT security they extend the trust and the verification process to the department heads and in some cases to even each user of the company. This empowerment enables department heads, who understand the value of the information, to decide if that event is a transgression and if so the user is educated instantly. This process enables these systems to handle **USE CASES 1, 3 and 4**.

Data centric classification and protection by information owners → PCS systems provide data centric classification and protection via rights management mechanisms. These are not just limited to central IT security but are also extended to each information owner who can classify/protect the information via encryption as it is created and also get reports on its usage. This ensures ad-hoc produced information gets classified and protected ie. **USE CASE 5** as it is being produced. Further, a decentralized reporting structure allows PCS systems to handle multiple different privacy and monitoring scenarios. For example, monitoring of C level can be done only by Head of Risk hence ensuring a balance between privacy and security i.e. **USE CASE 5 and 8**.

Additionally, as information gets monitored by people who understand the sensitivity of that information, PCS ensures that non-malicious usage of this information is picked up whether it is the copying of a single sensitive file or emailing a sensitive file to an internal unauthorized user i.e. **USE CASE 2 and 6**.

The data protection module of PCS systems ensure data remains protected in the new working scenarios (work from home, BYOD) and when being accessed by partners i.e. **USE CASE 7**.

Data centric monitoring ensures privacy and better security → the data centric ability of PCS systems ensures that they only monitor company related information, this allows for better end-user privacy. Further the decentralized reporting ensures end-users are fully aware of what is being monitored. This helps to automatically establish a culture of education, trust and security awareness i.e. **USE CASE 8**.

4 ABOUT THE AUTHOR

Rizwan Mahmood is the Director (Projects) for e-Safe Systems - a UK based security company specializing in preventing security threats arising from human behaviour. Rizwan has 16 years of experience in the R&D of information security and artificial Intelligence based systems. He holds a Masters in Information Technology Management from Staffordshire University, UK and is a certified Project Management Professional PMP®. Rizwan's area of expertise include managing security threats arising from user behaviour, operationalising information security, image processing and resource optimisation algorithms. He has been involved in design and development of a wide variety of security systems (comprising both physical and digital security) used by many organizations including law enforcement and defence forces.

Rizwan has been involved with e-Safe Systems and its products from inception and has setup and managed the global research and development facility for e-Safe Systems in Malaysia before moving to Australia. In his current role at e-Safe Systems (Australia), he is responsible to establish the strategic direction for e-Safe System's security products in light of the new security challenges and market needs.

5 REFERENCES

[i] https://www.ncsc.gov/nittf/docs/National_Insider_Threat_Policy.pdf

[ii] https://en.wikipedia.org/wiki/Swiss_Leaks

[iii] http://www.news.com.au/technology/online/nbn/melbourne-raids-follow-a-long-list-of-nbn-leaks-and-political-gamesmanship/news-story/2bf53f2619ec2307342960792a9e7d5a

[iv] http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11511711

[v] Tom Scholtz, GARTNER (2012). Maverick* Research: Kill Off Security Controls to Reduce Risk