Insider Threats within the Financial and Movie Sectors:

A Comparative Study

Samantha J. Daniels

Insiders are members of a trusted community. Insider attacks occurred when these members use their knowledge of an organisation to perpetrate harm or gain information. Studies have been conducted involving specific organisations. This paper looks at how these studies can be compared to develop a general understanding of insider activities and present general recommendations to assist any organisation in countering the illicit insider activities. Initially an overview is made of two papers looking at insider activity; firstly at the banking and finance industry and secondly at the movie production and distribution industry. Following this a comparison is done of the different findings from each paper, next a comparison of the recommendations. Conclusions are draw of what general recommendations can be made to assist organisations counter insider attacks.

1. Introduction

Insiders are considered members of a trusted community who have access to systems. An insider is defined by [4] as someone "in a unique position with the privileges entrusted to them and the knowledge about their computational environment, and this already translates directly to a certain amount of capability." This then allows an insider to attack a system by "maliciously leverage their system privileges and familiarity and proximity to their computational environment to compromise valuable information or inflict damage." In 2004, a survey carried out by the United States Secret Service and the CERT® Coordination Centre, [3], found that out of 500 surveyed attacks, 29% were committed by insiders. Hackers (outsiders) were found to be the greatest form of attacks at 40%, while the next greatest threat, 31%, came from former employees or contractors. According to [2] insiders who threaten an organisation are "individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm." This implies that any individual who has previously worked for any organisation will be considered an insider for that organisation.

Measuring the effects of insider activity is often a lot harder than outsider activities. Insiders are more inconspicuous and attempt to try to cover their tracks more carefully than outsiders. [4] believes this is since outsiders using the Internet have a certain amount anonymity while an insider belongs to their organisation and the organisation has all the necessary details about the insider to track them and prosecute them. [2] believes insider incidents are also under-reported which makes analysing the circumstances and effects difficult. Insider attacks are not reported due to several reasons. Out of the 500 organisations surveyed in [3] 58% believed that the damage they incurred would not warrant criminal charges, 36% believed they lacked the evidence for prosecution, 27% did not want to sustain negative publicity and 11% did not want to give their competitors the edge against them due to the attack.

Insider attacks can have disastrous affects on companies since the attackers often know the location of the areas of attacks as well as being able to access the information through

legitimate commands making them difficult to track. In [2] 91% of the organisations in the study suffered a financial loss and 30% suffered a loss of over US$500,000. The greatest loss was US$691 million. Not only financial losses are experienced. In [3] 25% of organisations reported a critical disruption to their organisation and 15% suffered damage to their reputations.

Several papers have been conducted looking at insider threats in different industries. A study conducting by the United State Secret Service and CERT® Coordination Centre conducted a study looking at insider attacks in the banking and finance sector of the USA. Another study looked at insider attacks in the movie production and distribution industries. Both of these studies provided recommendations to counter insider activities. This paper will consider the recommendations of both areas to see if there are any general recommendations that can be applied to other organisations. Before looking at these there is first an overview of the banking and finance paper and an overview of the movie industry paper. Following this is a comparison of the findings and a comparison of the recommendations.

2. Illicit Cyber Activity in the Banking and Finance Sector

In August 2004, the United States Secret Service and the CERT® Coordination Centre conducted an extensive study on insider activity within the banking and finance sector, [2]. The US Secret Service is an organisation set up for the protection of political figures in the United States of America, political buildings, such as the White House, as well as planning, designing and implementing events of national security. It is also involved in criminal investigations which threaten the security of the USA, including areas such as fraud, identity theft and computer-based attacks against national organisation in the USA. CERT® Coordination Centre is part of the Software Engineering Institute of Carnegie Mellon University in Pittsburgh, Pennsylvania. This institute is sponsored by the US Department of Defence to research and develop solution to security issues on the Internet.

The study [2] consisted of a case study of insider incidents, a review of insider activity and a survey of recent insider activity. This paper looks at the case study in detail.

The case study looked at 23 incidents from 1996 until 2002. These incidents occurred throughout the period, Table 1, and in a variety of sectors, such as credit unions, banks, investment firms and credit bureaus.

Year	Number of Incidents
1996	4
1997	4
1998	2
1999	1
2000	2
2001	7
2002	3

Table 1. Insider Incidents by Year of Initial Damage [2]

2.1. Results

Seven major results were observed during this case study analysis, each of which included implications and recommendations to other companies. The seven findings from [2] are:

1. Most incidents required little technical sophistication.
2. Perpetrators planned their actions.
3. Financial gain motivated perpetrators.
4. Perpetrators did not share a common profile.
5. Incidents were detected by various methods and people.
6. Victim organisations suffered financial loss.
7. Perpetrators committed acts while on the job.

2.2. Recommendations

For each area, Cappelli et al., [2], elaborated the findings they used to reach their conclusions and the recommendations for each finding are derived from the analysis of these findings. These recommendations were:

1. **Most incidents required little technical sophistication**
    - Secure and monitor the networks.
    - Address the lack of appropriate technical and non-technical practises, policies and procedures.
    - Review the interactions between business processes and technologies used.
    - Segregate duties of employees to limit access to information.
    - Enforce proactive password protection such as mandatory password and change policies.
    - Deactivate employees' access and accounts when contract is terminated.
2. **Perpetrators planned their actions**
    - Allow and encourage employees to report suspicious behaviour to a central person or location.
    - Increase employees' awareness of an organisation's security procedures and actions against any illicit behaviour.
3. **Financial gain motivated most perpetrators**
    - Deactivate employees' access and accounts when contract is terminated to avoid behaviour motivated by revenge.
4. **Perpetrators did not share a common profile**
    - Make management aware that any common ideas of an insider may be inaccurate.
    - Do background checks on potential employees, including a basic criminal record check, to help identify persons with histories of fraud, theft or other criminal behaviour.
5. **Incidents were detected by various methods and people**
    - Create an environment were all employees have a responsibility for the security of the system and are aware that preventing or limiting illicit behaviour benefits the employees as well as the organisation.

- Train managers and staff on business and security policies to enhance awareness of suspect or illicit behaviour.
- Provide a formal process through which an employee can report suspected behaviour.
- Use automated checks on information systems to detect any inappropriate behaviour.
- Use anomaly detection tools to detect when a user does something unexpected from his normal profile, although these can be expensive and have little effectiveness.
- Use auditing and monitoring by reviewing audit logs and observing employees after any suspicious activity within a system.
- Use random or unknown auditing procedures to avoid insiders that may work around such times.

6. **Victim organisations suffered financial loss**
    - No recommendations provided.
7. **Perpetrators committed acts while on the job**
    - Educate the organisation on how to prevent or report suspicious behaviour.
    - Do not allow remote access to critical or sensitive data – access should be limited to onsite.
    - Frequently audit and log any transactions made remotely.

No recommendations were provided to assist organisations reducing the insiders motivated by financial gain or reducing the financial loss suffered by organisations.

This paper therefore largely looked at the different circumstances and methods surrounding the observed cases of insider activity and provided the above recommendations for counting such activity.

3. Security Vulnerabilities in the Movie Production and Distribution Process

Byers et al. in 2003 in their paper, "Analysis of Security Vulnerabilities in the Movie Production and Distribution Process", [1], looked at the affect piracy has on the organisations involved in producing and distributing movies. The Motion Picture Association of America (MPAA) estimates that the United States movie industry suffers a loss of around $3 billion annually due to piracy [5].

Byers et al. [1] looked at both insider and outsider affects on the movie industry. Areas that are susceptible to insider attacks are during the editing process, screenings, giving copies to award judges, cinema viewing and prior to the release of the DVD or VHS. During editing, insiders can produce a copy of the movie that may differ slightly from the final version if the editing is incomplete. The movie may also have identification marks or frame-counters superimposed over the movie, as seen in Figure 1. Screeners may include promotion teams or critics and the movie frames may occasionally contain text similar to Figure 2 or Figure 3. Award judges' copies would likely include text similar to Figure 4. Insiders who copy a movie during the cinema viewing are the cinema staff who have access to the projection room and can film the movie from the same angel as it is projected as well as getting good sound quality. Prior to the DVD or VHS release insiders are staff members who are working in retail and have access to the product and are able to make their own copies at home.

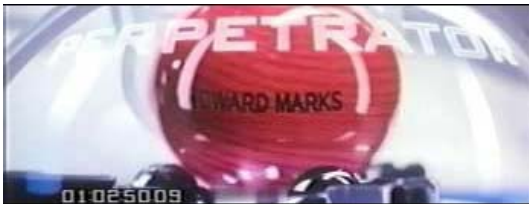

Figure 1. Production frame - contains a counter on the bottom left and two blurred watermarks at bottom centre (after [1])

Figure 2. Screener copy (after[1])

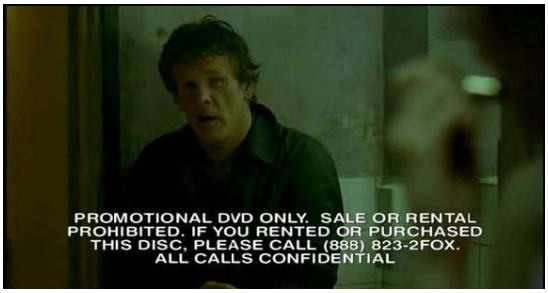

Figure 3. Promotional Copy (after [1])

Figure 4. Award Consideration Copy (after [1])

Outsiders can make their own copies by taking a camcorder into the cinema, copying a hired or purchased DVD or VHS, or recording from television.

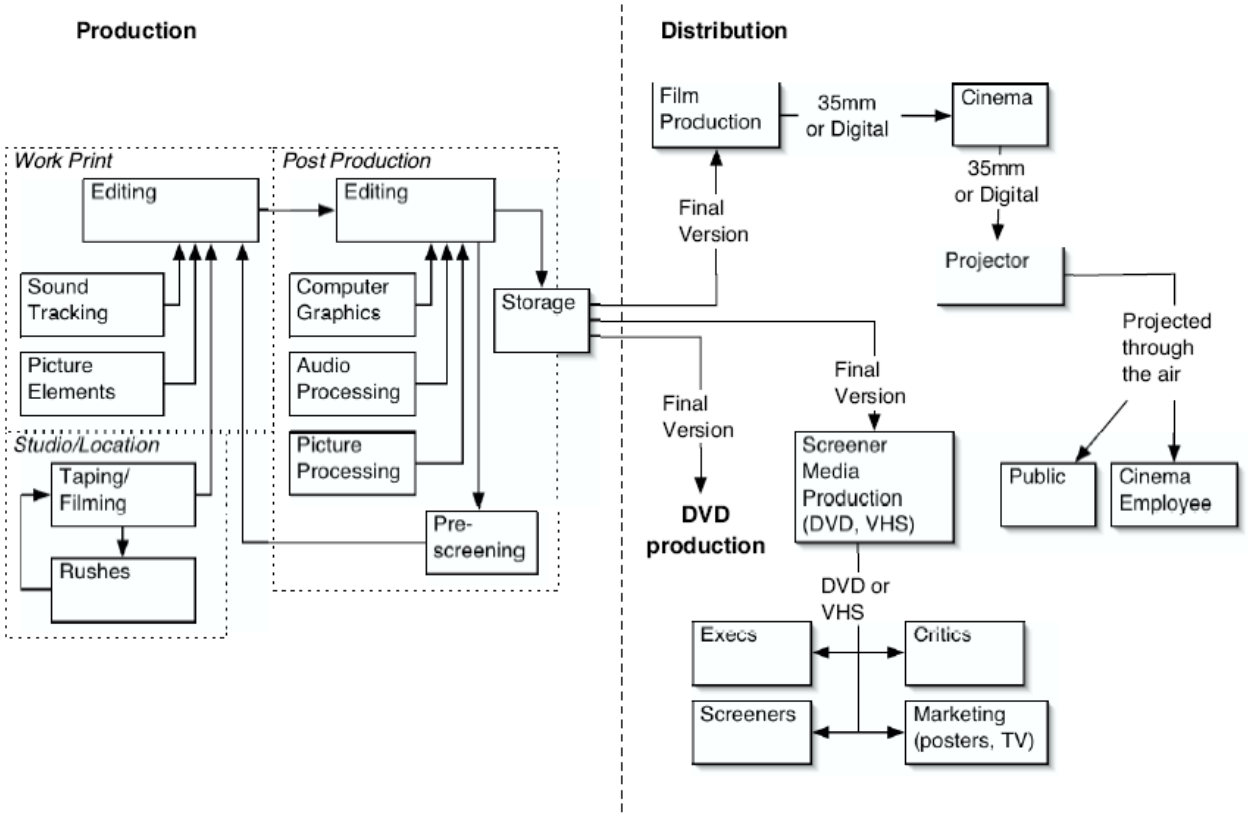

Figure 5. Movie production and distribution process (after [1])

Throughout the movie production and distribution process, Figure 5, are areas that are susceptible to insider attacks. Each area in Figure 5 is vulnerable to attacks. Insiders exist in all the areas until the distribution phase reaches the public at which point it becomes open to outsider attacks as well.

Although outsiders appear to be a greater threat since they have access to the complete movie at the best quality (DVD) and have no employment contracts binding them, a few points found in [1] counter this view. The highest demand for pirated movies is for fresh and good quality movies. A fresh movie refers to how soon before the release at the cinemas the movie becomes available. Outsiders, not including camcorders at the cinema that are likely to get poor audio and visual quality, are expected to get near perfect quality. But, since they will only be able to access the movies after the cinema release and the retail release, there is no freshness. It is assumed that no outside can produce a pirated

movie of high freshness and quality and therefore any fresh, good quality movie is understood to come from an insider.

3.1. Results

The paper [1] looked at 312 movies which were released in the United States. Out of these, 285 were successfully found, downloaded and viewed from a single content verification site on the Internet. These 285 movies were analysed for the date they appeared on the site and compared to the cinema release date and the DVD release date. Copies were assumed to have been insiders if:

- the movie appeared before the cinema release date.
- the movie contained obvious editing room equipment, such as Figure 6.
- the movie contained industry related watermarks, such as Figure 1, Figure 2, Figure 3 and Figure 4.
- the movie was DVD quality before the DVD release date.

Figure 6. Insider copied movie - note the boom microphone in top centre (after [1])

Out of the 285 movies, 77% met the above criteria and were assumed to be insider copies. Only 7 movies appeared before the cinema release and 5% appeared after the DVD release.

3.2. Recommendations

[1] made several observations of the current prevention of insider activity and suggested recommendation to further improve the situation. Their recommendations fall into three categories – short-term, medium-term and long-term mitigation. Short-term mitigations are actions which are simple and can be implements immediately to prevent leaks. Medium-term modifies existing technologies and develops technical solutions to the insider problems. Long-term mitigations are advanced content management technologies. The term short, medium and long are not related to the affect of the recommendation but rather when the recommendation can be implemented. Changing a procedure can be done almost instantaneously while modifying a technology takes a bit longer and changing the whole technology system will take the longest.

1. **Short-term mitigation**
    - Treat movie content as sensitive data and establish a chain of custody to track the movie at all times and remain aware of who has it at any time.
    - Ensure an appointed recipient of the movie is present at any screening to avoid screeners copying the movie.
    - Specify the environment in which the movie is viewed allowing the movie producers to control the situation and viewers.
    - Reconsider the policy of allowing executives to check out a movie for personal viewing before the release.
    - Ensure any computer system which stores any part of the movie content has a set of security policies.
    - Provide more monitoring and more stringent control over DVD production facilities and distributors.
2. **Medium-term mitigation**
    - Provide an encrypted playback device for critics or award judges to use to prevent them copying the content.
3. **Long-term mitigation**
    - Implementing a Digital Rights Management (DRM) system which encompasses all the companies used during the production and distribution, is flexible over many different procedures and is simple to use.

- Ensure any identified insider who illicitly copies a movie is subject to termination of their contact as well as legal actions and even criminal charges.

All employees who are insiders within the movie production and distribution process should be considering equally without receiving preferential treatment. Since the movie industry is estimated to lose around $3 billion per annum in the United State alone, spending extra time and money in preventing insider threats should be at the forefront of investors' minds.

4. Comparing the Findings

The findings of Cappelli et al.'s paper, [2], (Section 2.1) specifically looks at the banking and financial sectors of the United States of America. The findings are in relation to the 23 case studies looked at. But, can the findings be generalised to other areas of insider activity? Being able to generalise the findings in [2] would provide investigators and security analysts a better idea of the vulnerabilities of systems and the likely causes of illicit cyber activities. Following is a comparison of the findings in [2] and [1] set out according to the list of findings of [2].

4.1. Applying the Findings

Finding 1: Most incidents required little technical sophistication

In [1], 77% of downloaded movies were determined to be insider jobs. Only 7 movies out of 285 were available for download before the cinema release date but 163 were available before the DVD release. Since it was not specified how many of the 77% contained industry related watermarks, such as Figure 1, Figure 2, Figure 3 and Figure 4 one cannot specify how technically advanced these insider attacks would have been. For an insider to be able to remove any industrial watermarks they would require a degree of technical sophistication which would not be available to the average insider. In the banking and finance sector, [2], it was found that 87% of insiders used simple, legitimate commands to carry out their attacks. In the movie industry, removing the watermarks would

probably not be a legitimate command the insider would use in everyday work. If the movie is stored on a computer it would not require much technical sophistication to burn the information to a CD to take home. For an insider in the distribution industry, leaking a copy of a movie would be far simpler. For an employee in a DVD manufactures they would only need to make an extra copy to take home. Once at home, an insider could use relatively simple computer commands or programs to rip the DVD and upload it to an Internet site. Similarly for an employee in the retail industry of selling or renting movies, they would just need to be able to "borrow" a DVD over night to copy in the same way as a DVD manufacturer. If there is no security procedure preventing employees in either the manufacturing or distributing industries from removing items from the organisation it may be difficult to monitor for 1 DVD that goes missing for one evening or for the removal of a copy of a CD being made onsite.

Finding 2: Perpetrators planned their actions

Without any information being provided in [1] regarding the background to these attacks it is relatively difficult to presume whether the finding from [2] is consistent across industries. [1] states that in some cases copies may have been made by families or friends of an insider with a copy (for example, a judge for the Oscars is provided with a copy of the movie for judging). This would at least suggest that even if the insider did not plan to make a copy of the movie, they at least shared the sensitive information (the movie) with an outsider. In [1] family and friends of an insider who have access to the movie become insiders. In the banking and finance sector, [2], 13% of insiders shared their plans with friends and 9% shared their plans with family. Insiders also shared their plans with co-workers (22%) and 61% shared their plans with more than one person from different areas of their lives.

There is no study of individual insiders who copy the movies as to whether they frequently do this sort of activity. If they were "serial attackers" of the movie industry one could assume that their actions were planned – they knew when they would be able to access secure information and what they would be able to do with it. With the lack of more detailed results one cannot assume whether the majority of insiders planned their attacks in advance or whether it was due to situational circumstances – for example, the

employee finding themselves alone in a room with DVDs and a clear means of getting that information home without any colleagues noticing.

Finding 3: Financial gain motivated most perpetrators

It is possible that some insiders would have a deal running with friends and family that they would secure them a copy of a fresh movie in exchange for money. But, all 285 movies analysed in [1] were found on a content verification site where the authors were able to download and view the movies. They did not specify whether there was a charge for these downloads but with peer-to-peer systems such as KaZaa and eDonkey it appears that movie pirates are more concerned with being the first to provide a fresh movie or believing that citizens should be able to see a movie without paying for it. There does not seem much evidence for financial gain in movie piracy as analysed in [1] while in [2] 81% of insiders were motivated by financial gain.

Finding 4: Perpetrators did not share a common profile

Again, this was not an area that was looked into by [1]. But, from the range of areas that insiders can attack the movie production and distribution process, this seems a likely conclusion. Since the movies that are getting out there and available for downloading include watermarks that indicate a critics review movie, a promotions review movie, an award judge's consideration movie and a editing room movie this incorporates a wide range of people. One would assume that the award judges would be people unlikely to leak movies to the Internet, although there are such examples. One could assume that this is due to family members or friends rather than the actual judge copying the movie, but this is an assumption with no evidential support. Since a wide range of people in different areas have all leaked copies of movies to the Internet it is an assumption that there is no common profile of people who are likely to pirate movies. No analysis has been done on the age, gender, nationality or any other area to come to an accurate conclusion.

Finding 5: Incidents were detected by various methods and people

Movie piracy can be done subtly without the victim organisations even being aware of it. Insiders can copy movies onto their own devices while at work and take away the evidence when they leave at the end of the day. Detecting piracy within an organisation is

extremely difficult. Byers et al., [1], found the movies in their data set through Internet searches. Once a movie is found it can be difficult to tell where it came from and even if it was an insider in the production process or an insider in the distribution process. If the watermarks are still on the movie then that narrows the search down a bit, but unlike the banking and finance sector where damage (theft of funds, alteration of information etc.) is more obvious, it is difficult to pin point the actual area of attack. It is therefore difficult to first detect the incidents let alone investigate who makes the discoveries.

If a system within the production organisation contains the movie system logs it may then be able to be used to detect that a copy has been done and this could even be used to find who did the copying. As in the banking and finance sections, [2], system logs were used in 74% of the incidents discovered to find who the insider was that committed the act.

Some cases may be brought to the attention of the organisations involved by users of the Internet who come across pirated movies that have not yet been released at the cinemas. In [2] 35% of all incidents were detected by customers. Generally this occurred when customers found a problem with their only personal accounts so the general Internet users for incidents in [1] are unlikely to have the same motivation to report incidents to the appropriate organisations.

Finding 6: Victim organisation suffered financial loss

This is a result already discussed previously. Reports from MPAA state that it is estimated that $3 billion in the United States is lost annually due to piracy [5]. Production companies, investors, actors, cinemas, retail organisations and other companies involved in the production and distribution of movies lose out due to the piracy of movies.

Finding 7: Perpetrators committed acts while on the job

The paper [1] does not discuss where most of the incidents took place but it is likely that this statement is not always true for the movie industry. While insiders in the production stage of a movie most probably have to commit part of the act while on the job, such as copying the movie from the computer systems onto their own personal devices, the remaining part of the offence, such as burning the movie onto DVD to give to friends and family, or uploading to the Internet, is probably an activity that takes place at home, or at least outside of the work environment. This is due to the nature of the insider activity

which is providing pirated movies to individuals who do not have to pay for the cinema movie or wait and pay for the renting or purchasing the DVD or VHS.

Due to the fact that the analysis of insider activities within the movie industry, [1], was not carried out in the same means as the insider activities in the banking and finance sectors, [2], clear conclusions cannot be made. But, by looking at the general workflow of the movie industry and some of the details provided by the study, [1], the above assumptions can be made. These conclusions do not state that all 7 of the findings cannot match the movie industry in some situations but it does imply that the findings made in [2] were largely due to the sector that was studied rather than being an overview look at general insider activity.

5. Comparing the Recommendations

Both papers, [1] and [2], provide some recommendations to counter the insiders attacks faced in the different sectors. Comparing these recommendations for similarities and consistency in the different areas would provide other industries with a broader understanding of ways in which they might be able to counter insider attacks.

[1] divided their recommendations into three sections; short-term, medium-term and long-term mitigation (Section3.2). [2], on the other hand, provided specific recommendations (Section 2.2) for the individual findings within the paper (Section 2.1). The method that [1] used to present their recommendations has been applied to those in to [2], Table 2. Looking at both these results and the results from [1] (Section 3.2) indicates that there are a lot more available recommendations for short-term mitigation than medium-term and long-term. Short-term mitigations, as mentioned previously, are actions that are simple and can be implemented immediately. These points also make short-term mitigations effective in countering the insider threats quickly and effectively before too much damage can occur. Medium-term and long-term mitigations appear to be more expensive solutions to the insider threat and will take longer to implement. This is not saying that these solutions are not effective, but for organisations looking at

immediately countering insider activities, short-term mitigations are simple procedures that can instantly be put in place to assist the organisation.

Short-Term Mitigations	Secure and monitor the network.
	Segregate duties of employees to limit access to information.
	Deactivate employee's access and accounts after contract termination.
	Allow and encourage employees to report suspicious behaviours.
	Increase employees' awareness of an organisation's security procedures and actions against illicit behaviour.
	Make management aware that any common ideas of insiders may be inaccurate.
	Do background checks, including basic criminal record checks, on potential employees.
	Create an environment in which all employees are responsible for the security of the system and are aware of the benefit to themselves as well as the organisation.
	Review any existing audit logs and observe employees after any suspicious activities.
	Randomise any existing auditing procedures.
	Do not allow remote access to sensitive data.
	Frequently audit and log any remote access if auditing exists.
Medium-Term Mitigations	Address lack of appropriate practises, policies and procedures.
	Review the interaction between business processes and technologies used.
	Enforce proactive password protection and policies.
	Train managers and staff on security policies.
Long-Term Mitigations	Use automated checks on information systems.
	Use anomaly detection tools to detect unexpected behaviour.
	Set up auditing logs if they do not already exist.

Table 2. Recommendations for the Banking and Finance sector in terms of Short-Term, Medium-Term and Long-Term Mitigation

The recommendations made by [1] can be compared to those made by [2] for any consistencies. Any consistencies between the two different areas can be assumed to be

general solutions against insider attacks that would related to many different areas of organisations.

Table 3 displays which recommendations from each paper, [1] and [2], are similar. From here general recommendations are established which can then be applied to organisations suffering from insider attacks. In some cases two recommendations are similar to only one from another paper, which is indicated by combined cells.

Movie Recommendations	**Finance Recommendations**	**General Recommendations**
Treat movie content as sensitive data and establish a chain of custody to track the movie at all times	Review the interactions between business processes and technologies used	An organisation should be aware of the movement of any sensitive data, either electronically or physically, and should be aware of who has the data at any time.
Ensure an appointed recipient of the movie is present at any screening	Address the lack of appropriate technical and non-technical practises, policies and procedures	The finance recommendation can be applied to all organisations in general
Reconsider the policy of allowing executives to heck out a movie for personal viewing		
Ensure any computer systems which stores any part of the movie content has a set of security policies	Secure the networks	Any organisation with sensitive data on a network should ensure that the network is secure and only accessible to those with the correct permissions
	Enforce proactive password protection and change policies	To avoid inappropriate access of sensitive data the data should be protected by strong passwords that are changed on a regular basis.

Ensure any identified insider who illicitly copies a movie is subject to termination or their contract as well as legal action and criminal charges	Increase employees awareness of an organisation's security procedures and actions against any illicit behaviour	Every organisation should ensure that their employees are aware of what is considered illicit behaviour and what the consequences are for such behaviour. This would help avoid accidental access to sensitive data.

Table 3. Comparison of recommendations and general recommendations.

Any recommendations from the findings of the two papers that are not specified in Table 3 are found to be specific to the individual sectors and cannot be generalized to other industries.

6. Limitations

Both the study of the finance and banking sector, [2] and the study of the movie industry, [1] used different methodologies. Each study looked at different areas of concerns and created their recommendations according to those areas. This makes comparing the studies difficult. Although an attempt has been made to provide some consistency in the result by comparing the findings in [2] to the analysis of [1] and arranging the recommendations of [2] into the same format as [1] there is still a large discrepancy between the papers. This prevents a clear analysis of the results to provide an overall general approach to insider activities in all areas.

It is possible that there may not exist general recommendations for all industries. Perhaps each industry that is susceptible to insider attacks requires analysis of the potential areas of an insider attack before the problems can be fixed. Chinchani et al. in 2005, [4], developed a model to represent the weaknesses in a system. Their model enables the organisation and system administrators to discover the likely targets, methods and strategies of attacks in order to develop appropriate security mechanisms.

Unfortunately, even though the papers provide recommendations to counter the insider problem they do not actually suggest actual procedures in which to counter the problem. This is most likely due to the fact that different organisations would have different ways of carrying out a recommendation.

7. Conclusion

From looking at two studies, [1] and [2], done on insider attacks within two very different sectors a few recommendations and findings can be generalized to other sectors not included in the studies. Many recommendations from each paper were inapplicable to other sectors due to the dissimilarity between the two industries. This implies that each separate industry needs to looks at their own area's weaknesses in order to develop an appropriate model to counter insider activities. Instead of just looking at who could possibly be a dishonest insider, since [2] stated that there is no common profile, organisations should look at the areas that are vulnerable to attacks and take measures to prevent exposure to such infiltration. Each industry would need to develop specific procedures that are suited to the organisation in order to counter attacks. Although this study provided some general recommendations, to fully protect a system an organisation would need to develop their own model of vulnerabilities as described in [4].

---

[1] S. Byers, L. Cranor, D. Korman, P. McDaniel and E. Cronin, "Analysis of security vulnerabilities in the movie production and distribution process", *Proceedings 2003 ACM Workshop on Digital Rights Management*, ACM Press, 1-12, 2003.
[2] D. Cappelli, M. Keeney, E. Kowalski, A. Moore, M. Randazzo, "Insider threat study: Illicit cyber activity in the banking and finance sector", *United States Secret Service Report*, CERT Coordination Centre, Software Engineering Institute, Carnegie Mellon University, 2004.
[3] CERT & United State Secret Service, "2004 E-Crime watch survey: Summary of findings", 2004. Available at `http://www.cert.org/archive/pdf/2004eCrimeWatchSummary.pdf`, September 2005.
[4] R. Chinchani, A. Iyer, H. Q. Ngo and S. Upadhyaya, "Towards a theory of insider threat assessment", *Proceedings of the 2005 International Conference on Dependable Systems and Networks*, IEEE, 2005.
[5] Motion Picture Association of America, Anti-Piracy, 2003. Available at `http://www.mpaa.org/anti-piracy/`, October 2005.