Protecting the Motion Picture Industry from Intellectual Property Theft

Terry M. Gudaitis, PhD
Stasi P. Poulos
Johnny C. Johnson

For more information, contact Mindstar at 703-404-1100

Protecting the Motion Picture Industry from Intellectual Property Theft

Terry Gudaitis, PhD
Stasi Poulos
Johnny Johnson

Most likely, while you are reading this paper, your employees, contractors, and people not even associated with your organization are stealing your intellectual property - your scripts, your films, your promotional items, and your trade secrets. They are stealing from multiple points of vulnerability - during the pre-production phase, during the production process, during the editing and distribution phases, as well as from within your marketing, public relations, and advertising endeavors. According to the Motion Picture Association of America (2003 - http://www.mpaa.org/anti-piracy) it is estimated that an excess of $3 billion is lost annually due to unauthorized copying, redistribution, and pirating of movies. This estimate deals only with the physical media. It is projected that the losses due to Internet and electronic re-distribution of movies may reach upwards of $4 billion in 2003 and 2004, according to "The Impact of Piracy on the Film Industry" by Deloitte and Touche (June 2003). The losses are only going to get worse and the calculation of these losses will become more complicated.

Other Costs of Intellectual Property Theft may be Difficult to Estimate or are Overlooked

- Investigation costs associated with incident response.
- Legal costs resulting from an investigation, filing a civil lawsuit, or attempting to recover the stolen information.
- Negative publicity resulting in lost sales due to a diminished reputation.
- Research and development costs or other investment costs associated with developing, legally obtaining, or legally purchasing the proprietary information.
- Extortion costs.
- Cost of recovering or reproducing the information.
- Cost of improving security to prevent future incidents.
- Loss of consumer confidence.

A number of studies, articles, and news reports have highlighted the issue of security within the motion picture industry. The focus of these reports consistently remains on finding the technological silver bullet to solve the problem. The primary service in the information security industry is to offer technological solutions and preventions. Although the current services offer a wide array of technical solutions to prevent damaging incidents (i.e., watermarking, digital signatures, firewalls, locks, biometrics, network penetration testing, metal detectors, night-vision goggles used in theaters and screening rooms to find illegal camcorders), financially damaging incidents are still being committed by humans.

If all of these technologies were working, security incidents in the motion picture industry would have ceased years ago. Instead, the perpetration of intellectual property theft is increasing. Why is this occurring? Why is the industry that demonstrates some of the most cutting edge technology (i.e., special effects software) and some of the most creative minds having such difficulty controlling its intellectual property? Because *people* are still behind the theft, and the current technical solutions operate in isolation of the people operating within the industry.

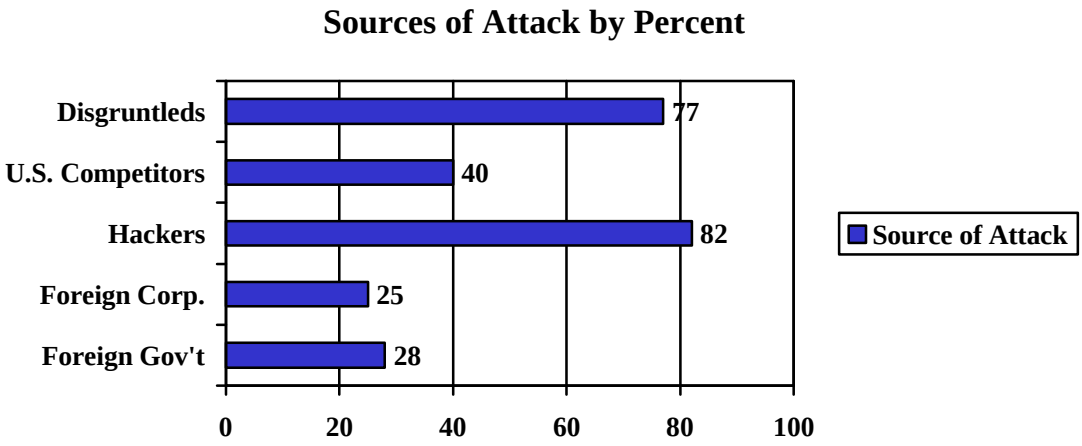
In order to understand the people behind the crimes, techniques from the fields of criminology, behavioral science, and psychology must play an equal and complimentary role with computer science and information technology to more successfully secure the integrity of data and information. Understanding the behavior of the person who will commit corporate espionage or steal intellectual property is key to developing more robust security solutions.

Understanding The State of Security Now

In order to combat intellectual property theft in the motion picture industry several foundational elements must be understood and defined: 1) who is stealing; 2) where are the points of vulnerability; and, 3) what are the new technologies that can proliferate theft.

Who is Stealing - Insider or Outsider?

The debate over where the biggest threat originates has been going on for several years. Some surveys and security experts suggest that the biggest threat comes from the inside; others swear the exact opposite. The insider versus outsider debate also differs along the dimension of access type -- physical access compromise or network/system access penetration. The long-standing debate might possibly endure for years because an attack, compromise, or theft, may not be as black and white as insider versus outsider. According to the 2003 CSI/FBI Security Survey, insiders, defined as disgruntled employees top the chart of perpetrators.



Source: 2003 CSI/FBI Survey

Even the most recent published study by ATT Labs, and one geared specifically to the motion picture industry, *Analysis of Security Vulnerabilities in the Movie Production and Distribution Process* (September, 2003 http://lorrie.cranor.org/pubs/drm03.html), defines the problem as insider versus outsider. It is not that simple. The human behavior associated with intellectual property theft is far more complicated than a straightforward inside versus outside perspective. It is perhaps more accurate to define these cases in four categories: Insider, Outsider, Inside-Out, and Outside-In.

The purely *insider* cases and purely *outsider* cases are fairly clear-cut. Basically, an insider can be defined as anyone employed by, contracted to, affiliated with, or provided organizational authorization to gain physical or network access to the organization (as an employee would). An outsider would be anyone who is not employed by, contracted to, affiliated with, or provided organizational authorization to gain physical or network access to the organization. *Inside-Out* and *Outside-In* are the combination platters and can add to both the investigative complexities as well as the political and bureaucratic complexities within an organization.

Inside-Out can be defined as the primary perpetrator being an insider who either feeds information to a secondary perpetrator(s) on the outside or who actually commits the penetration, compromise, or theft from the outside. To complicate an investigation, an insider can also make it appear to be "inside-out" or an "outside" by committing the penetration, compromise, or theft from a remote or outside location, or spoofing such a location.

Outside-In can be defined as the primary perpetrator being an outsider who uses an insider (either willingly or unknowingly) to provide information which would lead to the penetration, compromise, or theft of information by the outsider. To complicate an investigation, the outside-in attacker could make the compromise appear to be coming from the inside.

An "Outside-In" Job Causes Financial Loss

Universal Pictures' *The Hulk* began circulating on the Internet two weeks before its June 20, 2003 theatrical release. A stolen copy contained incomplete special effects, but the movie in its entirety was in the wild. The studio discovered that the source for the illegal copy of the film was due to an "outside-in" relationship between an employee at a print advertising firm that was promoting the movie and a "friend" external to that firm.

The opposing statistics provided in surveys and studies are probably due to this combination of inside-out and outside-in. In cases where the perpetrator is not identified at all - or cases where the perpetrator is identified but the investigation ends prematurely once a trophy arrest or termination occurs - the case may be inadvertently misclassified as a simple "insider" or "outsider" event.

As criminals, film thieves, and hackers become more sophisticated, so will their techniques. It is fair to assume that infiltration into targeted organizations will be accomplished through one of these four ways. While committing a crime completely from the outside provides distance and sometimes anonymity, the easier road is to attain inside knowledge and information. Although the gathering of inside information can be conducted through remote means, surveillance, reconnaissance, and publicly acquired information, the insider typically holds the most knowledge. Thus, regardless of the debate, protecting and securing proprietary information, trade secrets, and critical network/system information is critical to every organization.

"Security managers and CIO's are well aware of the threat posed by insiders, but often find it easier technically and politically to take action against external threats instead."

Victor S. Wheatman
Managing Vice President, Gartner Inc.
May 29, 2003

The most significant obstacle, however, is the "insider" issue - whether that is the pure insider, the inside-out, or the outside-in. When access, authority, authentication, and trust are part of the equation, the vulnerability increases substantially. According to a study conducted by AT&T Labs (September 2003) 77% of all popular movies being illegally traded over the Internet initially came from people who worked inside the movie industry. Even though profits are lost and intellectual property is stolen on the copying of DVD's by pure outsiders at the end of the distribution process, the money lost from the inception of a project through all of the process before it even makes it to a DVD is far more significant. While it makes sense to continue generating new and better watermarking, copy protection, and other mechanisms to stop or track illegal DVD

copies, the real security needs start at stage of the creation of a script. Real security needs to include the insider. While focusing on the insider is frequently a provocative proposition, some industry accepted practices and unwritten rules must be overturned - or at least seriously questioned.

Survey Results: 500 U.S. Workers and Managers who Handle Sensitive Data

- **66% said their co-workers, not hackers, pose the greatest risk to consumer privacy; only 10% said hackers are the greatest threat.**
- **62% reported incidents at work that put customer data at risk for identity theft.**
- **46% said it would be "easy," "very easy" or "extremely easy" for workers to remove sensitive data from the corporate database.**
- **32% said they're unaware of internal company policies to protect customer data.**
- **28% said their company does not have a written security policy or they didn't know if it has one.**

Source: Harris Interactive Inc., (May 2003)

Specifically, some of the insider threat stems from standard operating procedures that have been implemented in the industry for decades:

- Someone becomes a "trusted" insider after they have been in the industry for years. They have been unofficially blessed as "ok" and trusted to move about locations, editing suites, and other sensitive areas without question.
- Most individuals involved in the pre-production, production, and post-production phases of a project operate as "contractors" for that project but are treated as employees. In most other industries and within the US Government, contractors are restricted, have specific accesses, and do not function as fully "cleared" or screened employees.
- The software and data management tools utilized by pre-production, production, and post-production specialists are generally not integrated. Data does not flow consistently and easily from one production phase to another. Thus, in order to move information from one point to another within the entire production, paper is being used, someone has to re-enter data, copies of documents are being made - all with no logging, no record, and ultimately no security. Controlling data flow is critical to controlling the security of who gets access, what they are allowed to access once in the system, and how long they have access.
- Security policies may exist, but they are not enforced. Consequences for inappropriate or criminal behavior rarely exist for the insider.
- As a quote earlier in this document states, it is easier politically to address the outsider issue. It is also easier to employ hardware solutions to keep the outsiders out. Justification for firewalls, intrusion detection systems, security guards,

cameras, badge authenticators, cipher locks is something everyone can agree on - keep those who do not belong out. Psychologically, this is the easier route. It is not easy, politically, legally, or emotionally to turn the cameras to the inside.

- There are no basic minimum standards for the security of a set, a production office, an editing lab, or a special effects studio. In most other industries where there is either a lab environment (i.e., pharmaceutical testing, forensics/evidence processing, food processing, hi-tech development) there is a security criteria for operations. In other industries when there is movement of sensitive data between parties (i.e., bank records, money transfers, medical records) there are minimum security requirements for operations.

Employees and Contractors - The Biggest Risk

Current and former employees and on-site contractors with authorized access to facilities and networks continue to pose the most significant risk to intellectual property such as research data, customer files and financial information.

Source: American Society for Industrial Security (July 2003)

Each studio and each production office has its own sets of rules, policies, and unwritten rules which may, in turn, be creating and exacerbating the environment for an unscrupulous insider to operate successfully. While some physical security devices do assist in monitoring and deterring some illicit behavior, once someone is on the inside, a layered security approach must be utilized. The layers must include technology, but also must include a behavioral understanding of the environment. Some of the most significant security enhancements may come from low-tech solutions, once the environment and organizational culture are understood.

Points of Vulnerability

There are numerous security gaps throughout the production process where information can be compromised. By its very nature, the development of a motion picture is an extremely collaborative process crossing multiple boundaries between organizations and technologies. But this collaboration, in part, creates the vulnerabilities. So we have a paradox; how do you secure the intellectual property without infringing on the artists' ability to work freely?

The solution will likely be found by first acknowledging that no individual vendor can provide a single solution that will completely stop the loss of material. Instead, a partnership of technology based companies, information security consultants, and physical security specialists, must work together to create the most effective solution for

a given situation. It's only through human intelligence, balanced with appropriate technical measures that the motion picture industry will achieve the optimal solution to protecting its intellectual property.

At the core of motion picture development is the story. Initially, this might be stored in generic word processing documents and eventually take shape in one of the commonly used Script Processors. More specialized than a generic word processor, a Script Processor frees the writer of tedious script formatting requirements and allows creation of scripts that conform to industry formatting standards. Furthermore, they track production-related elements that are important to the writer and other personnel later in the production stream. There are at least 5 companies with professional-grade script processors.

After the script reaches an acceptable level of completion, the next step is for a producer (a studio, a production company, or an individual) to consider what is required to actually convert the written script into a visual work. This introduces the tasks associated with pre-production called Budgeting and Scheduling. Budgeting, as the name implies, is simply picking apart the script and determining the costs associated with creating each scene. Scheduling also involves the script, and results in lists of required elements, dates required, and an optimal order to photograph the scenes based on budgetary constraints. Since these two tasks depend on each other, they are typically done and re-done together. At least 4 companies market software that support budgeting tasks, scheduling tasks, or both.

Once the pre-production tasks are completed, budgets and schedules approved, and the decision is made to proceed with production, a 'production office' is built to house a small core team that manages the production. While the production office handles the administrative aspects of the production, the crew and production team handles the creative and technical details of building sets, arranging lighting, photographing scenes, and delivering footage to an editor. During production, film or videotape passes through several hands enroute to lab processing facilities, telecine facilities, and ultimately back to the editor. In addition, production data is gathered by several key personnel on the set and reported back to the production office. The data includes work times, scenes that were photographed or omitted, script changes, and crucial logging information that is necessary for an editor to make sense of the hours of footage that will appear on his or her desk. Traditionally, many of the administrative tasks on the set are strictly paper-driven. One company markets software that automates most of the administrative tasks on the set, while a handful of others attempt to address some smaller, more specific areas.

The post-production phase begins when the editor assembles the 'raw footage' into a story that, in theory, reflects the story in the script. This work is typically done in an edit facility, sometimes housing more than one production at a time. The administrative data gathered on the set must be hand-transferred into the editing system, a laborious process; but crucial to the editor's job. At least 3 companies market software that collect and transport some or all of this data from the set to an editor.

Throughout all these tasks, a common thread becomes visible; that numerous tools are used to manage the data that feeds a production. Of all the software products available, only one addresses every phase of production, creating a 'pipeline' of data through which all information must flow. Without tools that create a tight pipeline, network security measures that provide safe transmission of data, and adequate physical security measures, there can be no hope of preventing loss of information from this stream. An integrated, multi-disciplinary approach is the only way to lock down and secure the millions of dollars that are spent from the early scripting phases through editing and distribution.

There Are No Stereotypes - 70-Year-Old Insider Caught Pirating

Columbia Pictures Industries and Warner Bros. filed lawsuits against Carmine Caridi, a 20-year Academy member who has appeared in "The Godfather: Part II" and "NYPD Blue."

Caridi, 70, has told investigators he sent VHS copies of about 60 movies he received each year to his Illinois friend, 51-year-old Russell Sprague, who used a software program to convert the VHS tape into DVD format and then sent the original tapes back to Caridi, authorities said.

Investigators said a search of Caridi's Hollywood apartment turned up 36 original Academy screener tapes, including "The Last Samurai," "In America," "Shattered Glass" and "Mona Lisa Smile".

Source: Associated Press, January 29, 2004

New Technologies

New technologies are the tools and means of committing more creative and sophisticated thefts with ease and stealth. Policies and detection technologies will never keep up. The entertainment industry, as every other industry, will become victimized by advancing technology and new "toys." While most new gadgets on the market are used by people to facilitate their job, to make data transfer easier and faster, some of these technologies are just too dangerous to trust to your insiders. Some of the items on the market which may warrant evaluation include:

- USB Port Keyrings - greater than one Gig
- Wireless networks
- Wireless network scanners
- Network and Internet Sharing capabilities
- DVD/CD Burners, Copiers
- Miniature Cameras (i.e., watches, pens, PDA's)

Using any one of these devices - or devices in combination - anyone can walk out of a facility with gigabytes of data. Pre-production offices, post-production facilities, special

effects labs, and early-release distribution destinations are just a few of the points of vulnerability. Industry leaders and management must realize that even though these new technologies facilitate productivity, the same devices can be turned against you and used to steal information.

Understanding The State of Security in the Future

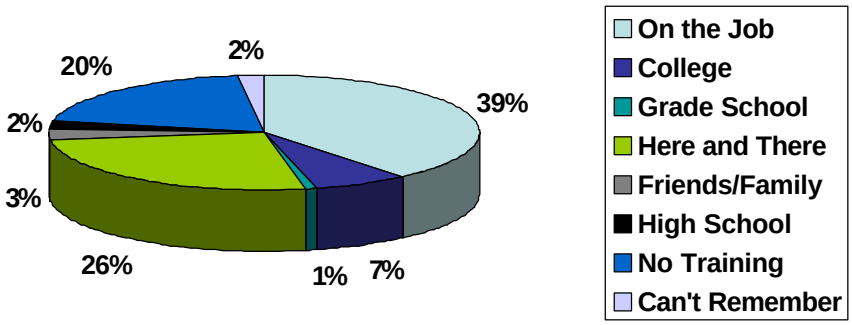
The financial losses to the motion picture industry are only going to increase in the future. Due to the new technologies discussed above and the globalization of business, intellectual property theft will be on the rise. Another factor that will add to this increase is once again the human factor. As young, new production assistants, grips, script supervisors, graphic artists, computer animators, and editors enter the workforce, their cyber-ethics (or lack-thereof) will also enter the workforce. Surveys and research indicate that children (elementary, high school, and college) are not well educated in cyber-ethics.

> "....when the technology does grow robust enough for movie trading, consumers will almost certainly do it. In a recent survey of 12- to 20-year-olds published by Forrester Research, 20 percent said they had already downloaded a feature film."
>
> Josh Bernoff
> Principal Analyst
> Forrester Research

An alarming study from Brainbench/ITAA, indicates that children do not learn what is appropriate from school or from their family. Only 39% are being trained on computer policies and acceptable behavior on the job. The question posed in the survey asked, "Where do People Learn their Cyber Ethics?" The results of survey include:

- 39% - On the Job
- 26% - “Here and There”
- 20% - No formal Education or Training
- 1% - Grade School
- 2% - High School
- 7% - College
- 3% - Friends/Family

The majority of the workforce is then relying on whatever ethical behavior they have deemed and defined as appropriate. The impact to the motion picture industry will be a greater number of digital thefts in the future when these children join the workforce.



Security Solutions

In order to combat the ever-growing capacity for intellectual property theft, the solutions must come from a combination of policy makers working with production management, physical security, and network/computer security.

- The policy makers and decision makers within the entertainment industry at the studio and MPAA level must draw a broader line around the issue of intellectual property theft and include the insider threat. The top level of management must push solutions down and enforce them.

- The directors, producers, and production managers must assess the environments in which they operate and evaluate the vulnerabilities. They must assess solutions which will both help them do their jobs as well as maintain the highest level of security and protection of the intellectual property. New solutions and recommendations must be pushed up to the policy makers.

There are ten recommendations for both the MPAA and production management:

1) Change the Culture - begin changing the organizational and industry culture with regard to "trusted" insiders. As stated earlier, most other industries do not treat contractors the same as employees. While there are bonafide employees within a studio structure, most people working on a film are really contractors.

2) Change the Behavior - In order to change behavior, or in this case deter the stealing of intellectual property, two major behavioral changes from within must take place. There must be monitoring of insider behavior - and that includes *everyone*. While it might not be comfortable or politically correct to suspect and assume one or more of your insiders will steal, it is the reality. And, there must be consequences for security violations.

3) Implement technology solutions that fit with the security needed. While devices like the 1 Gig keyring are fun and really convenient - and may increase productivity to a certain level - they are very dangerous in the workplace. It is too easy to plug into the USB port, drag and drop a few files, grab and go. Allowing the use of such devices also does not allow for a possession stream. It is extremely important that an audit trail exist regarding who has touched what data and when.

4) Create Criteria for minimal security - and real consequences for non-compliance. There does not appear to be a common or baseline security criteria for the motion picture industry. Within each stage of the process a minimum baseline of security must be measured and certified. Tools and facilities that do not adhere to this baseline level of security should not be used. While this may initially create an extra step in the process of shooting a film and may be perceived to crimp the "creative process" - the more damaging crimp will be in the money lost when intellectual property is stolen. Not only should each stage in the process have basic standards, but those standards should be enforced at the union level, the studio level and at the MPAA.

5) Assume Your Organization and Production will be a Target - and targeted from the inside. Your "trusted" people will steal, they will be social engineered, they will be stolen from, and they will inadvertently assist an outsider in attaining trade secrets and intellectual property.

6) Really Understand Organizational Vulnerabilities (network, physical, reputation, political, social). Identifying and understanding organizational vulnerabilities can be difficult when the processes involved with the product are splintered. Within the film making process there are multiple "hand-offs" of information to other departments to other specialties.

7) Put Security Where it is Really needed First- What is the Most Sensitive information?
According to ATT Labs Report September 2003, "the copying of commercial DVDs accounted for a relatively insignificant amount of the illegal films, the study found, as only 5% of the movies first appeared online after their corresponding DVDs were released. On average, the movies first appeared on the Internet 100 days after their theatrical release and 83 days before their DVD release." While the back-end of the distribution process is important, more of your theft is occurring prior to release. Thus, the processes and people involved in the pre-production, production, and post-production stages should be where the heart of security starts.

8) Education Programs and Training Programs must be inside as well as outside the industry.
As part of its campaign to thwart online music and movie piracy, Hollywood is now reaching into classrooms with a program that denounces file-sharing and offers prizes for students and teachers who spread the word about Internet theft.

Educate the Children - They are Next Year's Employee

"What's the Diff?: A Guide to Digital Citizenship" was launched this month with a lesson plan that aims to keep kids away from Internet services that let users trade digital songs and film clips: "If you haven't paid for it, you've stolen it."

The Motion Picture Association of America also paid $100,000 to deliver its anti-piracy message to 900,000 students nationwide in grades five through nine over the next two years, according to Junior Achievement Inc., which is implementing the program using volunteer teachers from the business sector. On October 31, 2003 public service announcements were released to approximately 5,000 theaters nationwide. While these are great steps to start educating the children...education must be even more forceful and prolific on the inside. Unions should be educating their members, production studios should be educating their employees, producers, directors, assistants - everyone should be receiving training from the industry.

9) Know Where to Seek Assistance
There are many companies, services and products - and some that are very new to market - that may be of assistance to a specific production or to a studio. Be diligent and comprehensive about the solutions evaluated and chosen. Don't always rely on what was done last year, two years ago - or the traditional vendor that has been there for 20 years. The issues and problems that face the entertainment industry today did not exist 10 or 20 years ago.

10) Accept that there is no "security" silver bullet and there will never be one. Security is a non-stop, vigilant process.