SETEC INVESTIGATIONS

White Paper

Investigating Intellectual Property Theft

Corporate Headquarters
8391 Beverly Blvd. #167, Los Angeles, CA 90048
Tel 323.939.5598 Toll-Free 800.748.5440 Fax 323.939.5481
www.SetecInvestigations.com

With 70 percent of the world's intellectual property within the United States, US-based companies continue to dedicate extensive resources to research and development, achieving substantial value and benefit from their intellectual property. Given the high degree of emphasis companies place on their intellectual property, a dangerous trend has emerged, illustrated by recent studies conducted by the American Society of Industrial Security (ASIS) and the FBI that demonstrate that over one-third of surveyed Fortune 2000 and middle-market companies have no formal program for safeguarding intellectual property and spend less than 5% of their budgets on security.

As the regularity and intensity of intellectual property theft continues to escalate, with losses now calculated by ASIS at over $150 billion per year compared to a loss of $45 billion in 1999, the protection of intellectual property and information assets has become a critical business issue. Although managerial and legal steps can and should be taken to safeguard such sensitive information, today's technologically advanced world in which information is shared globally in a matter of seconds has changed the nature of how companies create, identify, maintain, and thus must safeguard and protect, intellectual property.

At the core of this paradigm shift is the realization that relying on previously accepted best practices can no longer thoroughly protect intellectual property. The introduction of information systems and computer technology into business environments, especially as intellectual property is now commonly stored in the form of data and transmitted invisibly through the Internet, has changed the fundamental requirements that underlie any attempt to secure intellectual property and prevent against its theft. Similarly, when the theft of intellectual property does occur, responding to, investigating, and prosecuting such illicit activities has the added dimension of encapsulating electronic information that, by its very nature, is volatile and difficult to thoroughly capture.

To most effectively and efficiently prevent against and respond to intellectual property theft, companies must leverage a robust array of information security controls, including properly preserving electronic evidence. Companies often become enmeshed in litigation relating to intellectual property theft only to find that the electronic evidence they thought they could rely upon has not been recovered or that the integrity of the evidence has not been preserved.

With the continued increase in the value of intellectual property, which now regularly surpasses the value of physical corporate assets, proactive steps to prevent the unauthorized disclosure of intellectual property and reactive steps to respond to intellectual property theft become critical. Although preventing against and responding to intellectual property theft is not limited to information security mechanisms alone, with legal considerations playing a vital role, the focus of this paper is to provide a practical, realistic, and cost effective roadmap to safeguard intellectual property and respond accordingly should a theft occur.

Know Your Enemy

Although companies struggle to prevent hackers from stealing intellectual property by fortifying their enterprise networks from external entities, the real threat continues to arise from employees, former employees, and other direct members of a company's workforce. With more than 75% of

intellectual property theft being perpetrated by inside employees or contractors, as continuously modeled by ASIS and FBI studies, the most devastating thefts of intellectual property come from individuals who are deemed trusted insiders.

In light of this reality, the weakest link of a company's information security program to safeguard intellectual property is the human element. Anyone who has physical or electronic access to information assets, including contract workers, temporary workers, visitors, interns, and support and maintenance workers, has the opportunity to access unlocked computer workstations, computer servers, paper files, and any passwords or other sensitive data left unprotected. It is vital to not overlook the importance of protecting against the threat from within, as even if a company has extremely robust IT security controls in place, all it takes is one careless, uninformed, or disgruntled person with access to engage in the theft of intellectual property.

The evaluation of the threat from within isolates four main criteria for which insiders are directly responsible for the theft of intellectual property:

1. Insiders are ignorant and are not aware, or do not comprehend, the extent and gravity of the security practices, policies, and controls the company has in place
2. Insiders are careless, having not taken into consideration how their actions, in opposition to well defined security practices, policies, and controls, would negatively impact the company's ability to safeguard its intellectual property
3. Insiders disregard security, aware that their actions enhance the risk of intellectual property theft, however, choose to act in a manner that abandons security practices, policies, and controls
4. Insiders are malicious, acting for financial gain or simply personal gratification, intentionally seeking to corrupt, destroy, or steal intellectual property from the company

With the relevance of the insider threat as a force capable and often responsible for the theft of intellectual property, the following high-level and summary guidelines can be employed to directly minimize this risk and further facilitate the protection of a company's intellectual property:

1. Ensure that access privileges, such as passwords, are disabled immediately following the resignation or termination of an employee
2. Restrict employees from sharing a single authorized account used to gain access to network resources
3. Inform all employees that their usage of network resources and interaction with information assets will be monitored and audited
4. Track the inventory of portable computing devices, such as laptops and PDAs, to ensure no systems that may contain intellectual property go missing or remain in the possession of ex-employees
5. Implement console locking mechanisms on computer workstations so that systems left unattended will automatically log off and become password protected

6. Assign access privileges to employees based on their specific job functions and need to access intellectual property so that employees who do not require access to sensitive information assets do not have it
7. Instill a corporate culture in which safeguarding intellectual property is a high priority and each employee understands his/her responsibility to adhering to security practices, policies, and controls

As a company's inside workforce generally possesses a strong understanding of what is the most critical intellectual property for the business, where it is located, and how it is protected, every company must avoid operating with a false sense of security and establish and maintain a strong operating guide to prevent against and respond to the theft of intellectual property.

Protecting Intellectual Property Through Defense in Depth

Critical to the protection of intellectual property is the adoption of the concept of defense in depth, in which multiple layers of safeguards and security controls are integrated and managed. With the utilization of multiple safeguards, the impact of a failure of one specific mechanism will be lessened.

The importance of defense in depth is reinforced, as all information systems responsible for the creation, storage, and transmission of intellectual property possess a certain degree of intrinsic risk. In light of this, a security program to protect intellectual property must strive to reduce risk to an acceptable level while maintaining the confidentiality, integrity, and availability of the intellectual property itself and the systems governing it.

The following distinct and practical actionable items constitute the core elements of a company's effort to prevent against the theft of intellectual property:

Establish Strong Password Controls

As fixed passwords form the first and sometimes last line of defense against those individuals seeking to steal intellectual property, their strength is vital to safeguard information assets. Remaining the primary method for authenticating an asserted identity, passwords must be sufficiently strong and protected to ensure the integrity of information assets and maintain control over who may or may not access sensitive intellectual property.

Intellectual property thieves, recognizing the proclivities of password dynamics, often attempt to gain access to intellectual property by leveraging and exploiting weak, old, or deficient passwords. Successfully compromising a password gives an intellectual property thief a tremendous amount of freedom, as such a thief can conceal his/her true identity by masquerading as an authorized user and directly gain access to information assets.

As a high-level guideline, the following constitutes the summary elements of strong passwords:

- Passwords must be at least eight characters long
- Passwords must contain at least one letter and at least one digit

- Passwords must not be based on the user's name or login ID
- Passwords must not be based on a dictionary word, in any language
- Passwords may not contain more than two paired letters (e.g. abbcdde is valid, but abbbcdd is not)
- Passwords must expire in regular, pre-established intervals and require the creation of a new password

Deploy Two-Factor Authentication Mechanism

As there are clear limitations to the usefulness and effectiveness of traditional fixed passwords, the use of a two-factor authentication mechanism is a viable security solution for companies to implement in the protection of intellectual property. Two-factor authentication mechanisms provide greater overall security than static password and single sign-on access schemes by providing a two-factor form of authentication before resources can be accessed. When utilizing a two-factor authentication mechanism to gain access to the network, users must possess both a user ID and the mechanism itself, as the mechanism uses a password that is not static or pairs different forms of credentials, removing passwords altogether and creating an additional level of protection for intellectual property.

Two-factor authentication mechanisms are available as both a software client or as a small piece of hardware such as a keyfob or a USB device. A commonly used two-factor authentication method is a hardware token that creates a new one-time authentication code generated approximately every sixty seconds that is synchronized with the security server and is used to positively identify and/or authenticate the user by forcing the user to enter both the one-time authentication code and the user ID. If the code is validated, the user is granted access and authorization is allowed. An additional benefit of many two-factor authentication mechanisms is that they provide an audit trail as the authentication server tracks user activity.

Implement Physical Access Controls & Barriers to Disclosure

Fixed passwords and two-factor authentication tokens, which safeguard electronically based intellectual property from disclosure or compromise, are not sufficient to ensure intellectual property manifested in a physical form is thoroughly protected. As such, physical barriers, such as restricted areas, designated authorized access, and access control mechanisms must be implemented to limit access to intellectual property to those users who have a definitive need to access such information.

All intellectual property must be clearly marked as such, with written information and computer files being labeled as either "confidential" or "proprietary". In addition, when such confidential information is not physically in use, it must remain protected from unauthorized disclosure. This should include, but not be limited to, the utilization of anti-theft devices and sufficiently strong storage mechanisms to isolate and segregate intellectual property from readily available and non-sensitive information.

Integrate an Intrusion Detection Infrastructure

A company must utilize an Intrusion Detection System designed to inspect network- and host-based activity and identify suspicious patterns that may indicate an authorized or unauthorized user is attempting to engage in intellectual property theft. As a company cannot guarantee with 100% accuracy that its systems are secure enough to safeguard intellectual property and prevent against its theft, a critical function of an Intrusion Detection System is to provide the company with a degree of certainty that the majority of attack and abuse attempts, regardless if they are successful or not, will be detected and the perpetrator identified.

Deploy Computer-Based Surveillance Devices

In contrast to Intrusion Detection Systems that provide an alarm mechanism to indicate wrongdoing, companies also possess the legal protection and technical means to deploy computer-based surveillance devices to monitor, record, detect, and log authorized, unauthorized, and specifically designated suspicious activities undertaken by their workforce. Often employed to capture any malfeasance or misconduct perpetrated by employees utilizing network resources, computer-based surveillance devices can be strategically positioned as an invisible and undetectable mechanism that will capture all user activity on the specified computer systems as a means to verify and validate the occurrence of abuse. If a computer-based surveillance device does record the theft of intellectual property, its log files will serve as clear electronic evidence, which may be efficiently reviewed and utilized by legal counsel and law enforcement.

Employ Anti-Deletion Mechanisms

In addition to the constant threat that a company's intellectual property will be stolen, a company must also be concerned that an employee will attempt to permanently delete intellectual property from computer systems. Due to the intrinsic limitations of information technology, it is possible for a company's intellectual property to be deleted in such a way that it would not be normally backed up. Although not meant to replace the need for a company to regularly backup and archive data, anti-deletion mechanisms can be employed to provide a company with the ability to instantly recover deleted data, such as electronic files, email messages, and log files. As a valuable tool to safeguard intellectual property, anti-deletion mechanisms can operate in such a manner that, although employees believe that items are being deleted, they will actually be preserved, preventing the permanent loss of intellectual property and providing a record of intellectual property theft.

Perform Regular Data Backups

Data backups are an integral component of business operations as electronic information, including intellectual property, can easily be rendered useless or lost as a result of technical failure, inadvertent deletion, manipulation, or through a security incident. The creation, categorization, and storage of data backups ensures that information may be quickly and efficiently recovered in the event that parts of the operative data are lost or if an investigation into the theft of intellectual property must commence.

The presence of data backups facilitates the recovery of electronic information from the point-in-time the backup was performed. Backups are principally intended for disaster recovery purposes and are not intended to serve as short-term data storage or to frequently recover deleted items, which is the intended functionality of anti-deletion mechanisms. Surrounding the theft or destruction of intellectual property, data backups are a vital component to minimize a single point of failure that could result in the permanent loss of sensitive information assets.

Establish Security Policies & Procedures Governing Intellectual Property

A strong information security risk management framework, comprised of security policies and procedures governing intellectual property, is paramount to preventing against and responding to the theft of intellectual property. A company's management must actively strike a balance between business and security goals to establish a supporting organizational infrastructure to maintain and continuously foster a high level of protection for its intellectual property, while mitigating the risks and threats it faces. This is predominantly advanced through the utilization of a variety of documents, including organizational responsibility statements, policies, standards, operational procedures, and enforcement mechanisms.

As high-level statements that are specifically drafted and communicated to certain groups of people inside, and in some cases outside, the company, security policies and procedures detail management instructions by indicating a predetermined course of action to sustain intellectual property safeguards and, in the event that a problem arises, provide employees with guidance.

Institute Employee Training Program

Security policies and procedures designed to protect a company's intellectual property do not actively contribute value if they are not understood and adhered to by employees. As many employees may inadvertently take or disclose intellectual property due to a lack of understanding of how or why intellectual property must be safeguarded, accidental disclosure or the disregarding of security controls may occur if employees are not properly trained. With common practice dictating that a company's policies and procedures regarding the safeguarding of intellectual property is included in the employee handbook, additional training will reinforce and foster security awareness in which employees' possess a perceived responsibility to prevent against the theft of intellectual property.

Perform Employee & Vendor Background Screening

While new hire and continuous employee training efforts are critical to preventing against the theft of intellectual property and fostering security awareness, companies should take steps to minimize the likelihood that an individual or vendor they employ will be predisposed to perpetrating intellectual property theft. Pre-employment screening efforts can isolate and highlight negative activities or unethical behavior, such as a criminal record, resume fraud, previous terminations, or other indiscretions, in a candidate's past. Thorough background screening efforts should entail the scrutiny of online databases and communication with courthouses and the appropriate municipal offices to retrieve and evaluate public documents.

This necessary due diligence is a valid manner in which companies can minimize the risk they introduce into their workforce in an effort to protect their intellectual property.

Conduct an Intellectual Property Assessment

The defined actionable items contained within this paper constitute summary considerations and a baseline from which every company's efforts to prevent against the theft of intellectual property should be comprised. As every company is unique, containing its own set of business requirements and security needs, the key to developing a tailored and in depth security program to prevent against and respond to the theft of intellectual property is the identification and evaluation of the company's intellectual property and the manner in which it is best protected. The manner in which intellectual property should be safeguarded, to facilitate the highest degree of security readiness, is the synthesis of the risks, threats, and vulnerabilities impacting the intellectual property based upon how it is created, store, and transmitted.

An Intellectual Property Assessment will help to define appropriate security measures by evaluating a company's intellectual property and identifying what needs to be protected, determining why it is at risk, isolating threats and vulnerabilities, and developing both technology- and practice-based solutions. By performing such an Intellectual Property Assessment, a company will gain the strategic and tactical insight to ensure the preservation and integrity of its intellectual property.

When an Intellectual Property Assessment is conducted in coordination with a company's legal counsel, the assessment is not limited to information or physical security, but rather becomes an additional tool to determine the most appropriate legal form of protection for the intellectual property.

Reacting to Intellectual Property Theft

Although proactive security is the most mature and effective manner to safeguard a company's intellectual property, minimizing the likelihood that it will be stolen, the reality of risk management dictates that it is impossible to achieve a level of security that can, with 100% certainty, neutralize all forces seeking to successfully engage in the theft of intellectual property. As such, and in response to the theft of intellectual property through computer-based means, companies have the obligation to undertake well-orchestrated and thoughtful reactive measures to respond to the theft of intellectual property in a manner that will ensure electronic evidence is preserved and to establish a sustainable posture for internal or legal action.

At the core of a company's response to the theft of intellectual property is the initiation of computer forensics to identify, gather, analyze, and preserve electronic evidence. The computer forensic process is complex and relies upon experienced and certified professionals, dedicated forensic investigative tools, and a thorough understanding of technology and legal systems, identifying pertinent electronic evidence on computer systems is essential to responding to the theft of intellectual property.

The discovery, collection, investigation, and production of electronic information for investigating and handling computer-related crimes or misuse surrounding the theft of intellectual property is a well-defined process grounded in government and law enforcement guidelines. The following ten high-level steps are meant to provide clarity with respect to the collection of electronic evidence when investigating the theft of intellectual property:

Step 1: Send a letter of notification to all involved parties
A notification letter that is sent to all involved parties informing them that electronic evidence will be sought will help to ensure that electronic information and, specifically, intellectual property, is preserved. In addition, a protective order may be sought at the time the notification letter is sent that compels all parties to safeguard electronic evidence that may be relevant for subsequent litigations.

Step 2: Include specifications regarding electronic evidence in the written discovery request
Definitions of the electronic evidence requested, instructions, and specific questions must be included in the discovery request, in addition to the form of production requested, whether electronically or in hard copy form. In addition, a request for computer forensic experts to physically examine and analyze the computer hard drive(s) in question should be admitted and interrogatories should be sent in an attempt to gain an overview understanding of the target computer system(s).

Step 3: IT staff should be deposed via Rule 30(b)(6)
Throughout the course of the IT staff depositions, if asked, employees will be required to provide information regarding the manner in which electronic information is stored, the types of hardware and software utilized, and how the company backs up electronic information.

Step 4: Gather backup tapes
Backup tapes contain electronic information that may help a company recover from a disaster and should be collected as soon as possible. The company should have been creating backup tapes on a regular basis, thus they should contain electronic information that is no longer readily available on a computer system's hard drive.

Step 5: Gather removable media, such as CD-ROMs and zip drives
Such as is the case with backup tapes, removable media often contains information that is not available on a computer system's hard drive, therefore, they should be collected as soon as possible. In addition, such removable media may contain ad hoc backups of files and email messages that may be pertinent to subsequent litigations.

Step 6: Question all available employees about their specific computer usage
All employees can be questioned as to how they specifically store data on their computer systems and other network resources. In addition, employees should be questioned with regards to their home computer systems in the event that they have removed electronic evidence from their work systems and transferred them to their home systems.

Step 7: Create a forensic duplication of the computer hard drive(s) in question
In preparation for computer forensic analysis, an initial forensic duplication of relevant media

devices should be performed, achieved through bit-by-bit copying using a designated computer forensic investigative platform, which will preserve the presence of electronic evidence, maintaining its forensic integrity and court admissibility, while supporting the ability to conduct subsequent forensic analysis activities. As it is critical during the forensic duplication process to prevent against writing to, manipulating, or altering data on suspect hard drives, a hardware-based write protect device should be employed to ensure the original media and data are not altered.

Step 8: Mathematically authenticate forensically duplicated data
Upon completion of the forensic duplication, a mathematical verification process should be initiated in which a MD5 sum is employed for authentication purposes, confirming a true bit stream backup was created and demonstrating that a forensically duplicated hard drive or other media device is precisely identical to the original.

Step 9: Ensure the proper chain of custody is followed
A proper chain of custody ensures that the data presented is "as originally acquired" and has not been altered prior to admission into evidence. An electronic chain of custody link should be maintained between all electronic data and its original physical media throughout the production process.

Step 10: Initiate computer forensic analysis
Thorough computer forensic analysis performed by a skilled and certified forensic examiner, possessing a sound analytical foundation that carefully balances critical investigative requirements with vital legal and evidentiary needs, results in the reconstruction of the activities of a computer user, recovery of deleted files, and exploration of sensitive data, while providing insight into an investigation. Leveraging the capabilities of a computer forensic investigation to investigate malfeasance, collect electronic evidence in support of misconduct, and certify forensically the nature of and those responsible for the abuse, electronic evidence can be identified, isolated, analyzed, and framed so that it may be efficiently reviewed and utilized by an organization and its legal counsel.

Conclusion

All companies possess intellectual property that must be safeguarded from abuse, disclosure, theft, and destruction. However, too many companies are operating with a false sense of security surrounding their ability to prevent against the theft of intellectual property, contributing to the dramatic rise in occurrence and escalation in intensity of intellectual property theft. Proactively working to prevent intellectual property theft is a manageable undertaking and is the only way to attain a true level of trustworthiness within a corporate environment. As no company can possibly be totally proactive by predicting and neutralizing every possible risk and threat to intellectual property, defensive tactics and reactive techniques are vital to efficiently respond to the theft of intellectual property theft. All predictions demonstrate that intellectual property will continue to increase in value over the next decade and, as such, intellectual property theft will remain a growing problem that companies must consider, address, and react to.

About Setec Investigations

Setec Investigations is a subsidiary of Setec Security, a leading independent provider of vendor neutral information security solutions, incorporating a cross-disciplinary team comprised of computer forensic investigators, attorneys, law enforcement specialists, and seasoned business professionals offering unparalleled expertise in computer forensics and enterprise investigations. Setec Investigations combines today's most advanced computer forensics and litigation support expertise to provide intelligent, effective, and forensically sound computer investigative and litigation support solutions that carefully balance critical investigative requirements with vital legal and evidentiary needs.