IP and Sarbanes-Oxley Compliance

• Sarbanes-Oxley requirements apply to asset control and monitoring systems
• IP assets are critical to many current business models
• Systematic means for protecting and monitoring IP assets are needed as part of overall Sarbanes-Oxley compliance systems
• Executives and IP specialists must focus on IP management systems to avoid loss of IP assets and reporting errors
IP and Sarbanes-Oxley Compliance -- Topics

• Types of intellectual property (IP) to protect and monitor
• Sarbanes-Oxley requirements applicable to IP management and valuation
• Components of IP asset control systems
  – Risk assessments
  – Essential system components
  – Weak system indicators

Types of Intellectual Property – General Definition

• Intellectual property includes intellectual ideas and works that have replicable value
  – Intellectual property rights (IPR) exist independently of the products that depend on them
  – Business value is frequently associated with IPR
    • IP as business product (e.g. movies)
    • IP as basis for product (e.g. Coca-Cola formula)
    • IP as basis for service (e.g. Google patents)
    • IP as basis for making product (e.g. manufacturing know how)
### Types of Intellectual Property – Patents

- Typically cover new and useful processes, machines, articles of manufacture, compositions of matter, or any new and useful improvements of these items.
- Require application to United States Patent and Trademark Office (USPTO)
  - Drafting of applications is highly specialized
  - Scope of resulting protection depends on both drafting scope and advocacy with examiners
- Examination may be lengthy and costly

### Types of Intellectual Property – Patent Enforcement

- Patent valid for 20 years from date of application
- Allows patent holder to prevent others from making, using, selling, or importing the patented invention and from aiding parties in these tasks
- Patent infringement damages can include treble damages for willful infringement
- Patent rights are transferable through assignments (transferring all rights) or licenses (transferring specific rights to do something otherwise prohibited)
Types of Intellectual Property – Copyrights

- Apply to “original works of authorship” including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished
- Gained upon fixation of work in a tangible form from which it can be retrieved
- Recording of copyright with Copyright Office is not needed, but may aid enforcement
- Copyrights protect new expression but not ideas or reuse of old expression

Types of Intellectual Property – Copyright Enforcement

- Copyright holders can prevent others from copying a protected work
- Copyright holders can also prevent parties from using the protected work in other valuable ways such as in public performances or in creating derivative works
- Fair use of protected works is allowed
  - Usages with minimal impact on commercial value of the protected work
  - Usages (e.g. news reporting) in the public interest
### Types of Intellectual Property – Trademarks

- A trademark is a word, name, symbol, or device that is used in trade with goods to indicate the source of the goods and to distinguish them from the goods of others.
- Service marks are similar to trademarks but indicate the source of services.
- Trade dress refers to the shape of product packaging (e.g. the distinctive shape of a Coca-Cola bottle) and can be protected like trademarks.

### Types of Intellectual Property – Trademark Enforcement

- A trademark must be registered and used in order to gain nationwide enforcement.
- Local rights may be obtained through sustained use.
- Trademark rights can be used to prevent others from using a confusingly similar mark to sell the same type of goods.
- Trademark rights will not to prevent others from making or selling the same goods under a clearly different mark.
Types of Intellectual Property – Trade Secrets

- A trade secret is any formula, pattern, device or compilation of information which is used in secret in a person’s business, and which gives the person an advantage over competitors who do not know or use it

- Trade secrets are often lost due to:
  - Failures to maintain reasonable physical secrecy
  - Failures to restrict employee disclosures
  - Independent rediscovery by others
  - Disclosures upon product introduction

Types of Intellectual Property – Trade Secret Enforcement

- Trade secret enforcement depends on state law

- Persons who have access to trade secrets in their work can be prevented from disclosing the trade secrets or using them for other businesses

- Persons who acquire trade secrets through wrongful means – for example, by trespass or knowingly causing others to breach their obligations to keep trade secrets confidential – can also be precluded from using or disclosing the trade secrets
Sarbanes-Oxley Requirements Related to IP

- Public companies must disclose internal control systems for monitoring and valuing assets (Sarbanes-Oxley Act § 404)
  - Asset control systems extend to intellectual property (IP) assets where material
  - Asset acquisition and maintenance arrangements for IP assets are difficult due to intangible character
  - Asset valuations for IP assets are complex and highly context-specific
  - Reporting methods for IP controls are unclear

Sarbanes-Oxley Requirements Related to IP (Cont.)

- Public companies must accurately disclose financial condition and business prospects (Sarbanes-Oxley Act § 906)
  - Valuation problems may carry over into financial reporting errors
  - Positive statements about IP potential may overstate business prospects or understate known problems in perfecting or enforcing IP rights
  - Omissions about IP flaws or IP threats from competitors may undercut accuracy of business disclosures
Sarbanes-Oxley Requirements Related to IP (Cont.)

- Corporate officers must certify accuracy of corporate disclosures (Sarbanes-Oxley Act §§ 302, 906)
  - Requirements extend to accuracy of both control system and financial condition disclosures
  - Parties required to certify include CEO and CFO
  - Penalties for knowing miscertification include criminal sentences and substantial civil fines
  - Threatened liability focuses strong attention by corporate officers on integrity and results of corporate asset control systems such as IP control systems

IP Asset Control Systems – General Criteria

- Reasonable diligence
- Risk assessment as basis of design, implementation, evaluation and redesign
- Essential components
  - Standard setting
  - Training
  - Monitoring
  - Discipline and responses to system failures
- Typical indicators of weak systems
IP Asset Control Systems – Diligence

• An effective program will be reasonably designed, implemented, and enforced so that it generally will be effective in securing IP assets and reporting on them accurately

• Essential tasks
  – Development and inventory of IP assets
  – Valuation
  – Accurate reporting

IP Asset Control Systems – Diligence

• Development and inventory of IP assets
  – IP control begins with knowledge of IP worth protecting and IP already protected by another
  – Fluid nature of IP produces inventory problems
  – Need to prefect IP interests to retain them adds to inventory problems
  – Actions that may lose control of IP at unexpected points create inventory issues
  – Possible IP infringement requires separate inventory and business risk assessments
IP Asset Control Systems – Diligence

• IP Valuation
  – Methods
    • Replacement value
    • Earnings value
    • Market value
  – Difficulties in IP Valuation
    • Business-specific value
    • Possibility of greater value to other businesses is hard to measure
    • Lack of general markets
    • Uncertainty of replacement value under changing technology and knowledge

IP Asset Control Systems – Diligence

• IP reporting
  – Reporting of IP assets and value is complex due to non-standard character of IP interests
  – Scope of value may depend on varying business conditions, IP rights scope, and IP usages
  – Size of income from IP usage may depend on uncontrolled activities of IP licensees
  – Materiality and value of IP may turn on underlying IP rights enforceability problems
  – Disclosure of IP rights problems may conflict with confidentiality concerns in IP rights enforcement
IP Asset Control Systems – Risk Assessment

• An effective IP asset control system should include ongoing efforts to periodically assess the risks of IP asset and business losses in the course of an organization’s activities
  – Risk assessments should evaluate both the nature and business seriousness of risks to IP assets
  – Risks should be reevaluated periodically to take into account changing products, markets and IP surroundings
  – Risk evaluation and associated program adjustment should establish an ongoing cycle

IP Asset Control Systems – Essential Components

• IP control standards and procedures
  – Actions to be followed by corporate employees and agents to manage IP assets and threats from IP of others
  – Defined in conduct codes and further rules, practices and procedures of organization
  – Should address IP identification, business impact assessment, valuation, and reporting
IP Asset Control Systems – Essential Components

• IP control standards and procedures (cont.)
  – Standards should be reasonably capable of reducing the likelihood of:
    • IP asset non-recognition
    • Failures to perfect rights and protect IP assets
    • IP infringement in the organization’s activities
    • Failures to accurately describe IP assets and risks in public documents
  – Standards typically address practices most likely to lead to IP asset losses or infringement

• High-level managerial responsibility
  – Members of senior management should be knowledgeable about the content and operation of their company’s IP asset control system and exercise reasonable oversight with respect to the program
  – At least one senior executive should have primary management responsibility for the performance and success of the program
    • Oversee day to day control
    • Report periodically to other senior managers
    • Report directly to corporate board where special IP problems threaten significant company interests
IP Asset Control Systems – Essential Components

• High-level managerial responsibility (cont.)
  – Costs of IP asset perfection and control suggest that asset program oversight for a particular corporate unit or activity should not be performed solely by the managers who are responsible for the profitability of that unit or activity
  – Short-term costs of IP development and protection typically lead to mostly long-term benefits, which may also cause cost-driven facility or operations managers to short change IP protection in the short run

IP Asset Control Systems – Essential Components

• Due care in the selection and retention of parties with key IP responsibilities
  – Persons who have substantial authority within an organization – that is, substantial discretion over the use or application of significant corporate resources – should have proven track records of concern and respect for IP
  – Responsible delegation of authority to these sorts of parties will help to avoid incidents of knowing infringement of IP interests, which can lead to treble damages
  – Conduct of substantial authority personnel with respect to IP is also critical to set proper management tone as an example for subordinates and other corporate personnel
IP Asset Control Systems – Essential Components

• Due care in the selection and retention of parties with key IP responsibilities (cont.)
  – Parties will generally be assumed to have sufficient knowledge and values to properly handle IP issues unless contrary conduct is found
  – Actions failing to protect known IP interests or accepting known infringement of other parties' IP interests should produce a corporate response in removing the party from responsible positions and preventing advancement to more responsibility

IP Asset Control Systems – Essential Components

• Steps to communicate IP asset standards and procedures to all employees and other agents
  – Information on IP asset protection and infringement avoidance practices should be communicated periodically and in a practical manner to employees and agents who are likely to originate or use IP
  – Communication of standards and procedures involves both publications and training
    • IP control standards will have the greatest force if they are transmitted to employees by top corporate executives
    • A company should conduct training programs and undertake other steps to disseminate information appropriate to the recipients' respective roles and responsibilities in the company and their involvement in IP creation, protection, and use
IP Asset Control Systems – Essential Components

• Steps to communicate IP asset standards and procedures (cont.)
  – Means for disseminating include:
    • Distributing codes of conduct
    • Informal discussions of IP asset standards or issues between managers and their subordinates
    • Briefings at new employee orientations
    • Memoranda and speeches by senior managers
    • Group meetings and briefings
    • Articles in company periodicals
    • Posted notices

IP Asset Control Systems – Essential Components

• Monitoring and auditing systems
  – Monitoring targets
    • Sources of new IP and means of protection
    • Missed opportunities to gain protection for IP
    • Loss of IP interests
    • Misappropriation of IP of others
    • IP Valuation Errors
    • IP Reporting Errors

  – Features of successful monitoring
    • Monitoring should be reasonably designed to detect IP asset control problems in these areas
    • Monitoring systems should include means whereby a company’s employees and agents may report or seek guidance regarding potential or actual IP asset system problems without fear of retaliation
    • Monitoring systems should also include means for periodically evaluating the effectiveness of the company’s IP asset control systems, including both the degree to which planned control system activities were carried out and the IP protection and use results obtained through those practices
IP Asset Control Systems – Essential Components

- Monitoring and auditing systems (cont.)
  - Regular information gathering leading to reports to management
    - Possible IP infringement problems can be assessed from the content and results of informal complaints, administrative proceedings, and civil suits
    - Patterns of infringement problems can often identify ongoing IP usage deficiencies, such as management policies or practices that are promoting misuse of IP or IP control system monitoring activities that are giving too little attention to IP misuse in a particular corporate department or facility
    - Additional studies can focus on whether planned IP protection procedures are being followed and whether those procedures have been sufficient to achieve their intended effects
  - IP control system audits
    - IP control system audits involve systematic, documented, periodic and objective reviews of facility operations and practices related to meeting IP control objectives
    - Legal audits are studies completed apart from the pressures of existing litigation that search for “legal soft spots” – that is, patterns of activity which either create risks of later legal trouble or which do not take full advantage of some untapped legal potential
    - IP audits can produce evaluations of a corporation’s status under applicable IP laws at the time of an audit, recommendations for corrective actions, and assessments of developing legal risks meriting future attention

- Consistent enforcement of IP asset control standards through disciplinary mechanisms
  - Meaningful IP asset control systems should include disciplinary responses to violations of IP control standards or misuse of other parties’ IP
  - A corporation should promote and consistently enforce its IP asset control standards throughout the company to ensure attention to the standards by employees in times of performance stress
  - Types of discipline: discipline for violating IP control program standards and discipline for failing to take reasonable steps to detect or prevent IP misuse
IP Asset Control Systems – Essential Components

• Consistent enforcement of IP standards (cont.)
  – Exceptions to discipline for “top producers” sends message to other employees that IP standards can be overlooked when compliance is inconvenient
  – Companies should resist the urge, in the face of a loss of a significant IP asset or IP misuse leading to corporate liability, to “put the incident behind them” and return to normal activity without assessing responsibility and imposing discipline
  – Incident follow ups should include discipline for parties who engaged in insufficient monitoring and reporting of IP control system flaws or problems

IP Asset Control Systems – Essential Components

• Active organizational responses to IP control system failures and reforms to prevent further problems
  – Steps in a proper response
    • Study the scope and causes of the failure
    • Determine whether the company’s IP monitoring processes should have detected the offense at an earlier stage
    • Assess the need for alternative operating practices and IP control system monitoring procedures that would lessen the likelihood of a similar problem
IP Asset Control Systems – Essential Components

- Active organizational responses (cont.)
  - Other useful reviews
    - Assessments of the sufficiency of company IP monitoring practices to ensure that similar failures will not go undetected in the future
    - Follow up reviews to ensure that implemented reforms remain in effect once intense scrutiny related to a liability crisis or other incident has died down
    - Evaluation of the sufficiency of implemented reforms to achieve their intended effects in IP asset control and infringement prevention
  - Consequences of weak responses
    - Loss of IP interests
    - Failed opportunities to prevent repeat problems
    - Possible IP misvaluations or reporting errors

IP Asset Control Systems – Indicators of Weakness

- Features suggesting a control system is deficient
  - Lack of adherence to industry standards
  - Failure of system to comply with applicable government regulations
  - Recurrence of IP losses or infringement
  - Involvement of top executives or IP control system officials in IP losses or infringement
  - Failures of parties with knowledge of material IP losses or infringement to report these problems to company managers or to make corresponding public disclosures
### Conclusions

- IP asset control systems are critical in many business enterprises
  - IP assets have significant value in many modern businesses
  - IP infringement can lead to massive liability and large-scale business disruptions
  - Loss of IP assets can threaten corporate survival
  - Accurate valuations and descriptions of IP assets are required for compliance with Sarbanes-Oxley requirements

### Conclusions (cont.)

- Advantages of applying compliance management techniques to IP control systems
  - Prevention of IP asset loss
  - Avoidance of IP infringement liability
  - Minimized business losses due to unexpected unavailability of IP
  - Decreased D&O liability under Sarbanes-Oxley
  - Reduced shareholder claims for D&O liability based on IP misuse
  - Diminished punitive damages risks